UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

ESTRATEGIA PARA MITIGAR FRAUDES DE ANGLER-PHISHING BASADOS EN INGENIERÍA SOCIAL EN PLATAFORMAS DE REDES SOCIALES

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

ÁREA: Seguridad de la información

LÍNEA DE INVESTIGACIÓN: Tecnologías de la Información y Sistemas de control

AUTOR: Ariel Hernán Jinde Sisa

TUTOR: Ing. Félix Oscar Fernández Peña, PhD.

Ambato – Ecuador

febrero - 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: ESTRATEGIA PARA MITIGAR FRAUDES DE ANGLER-PHISHING BASADOS EN INGENIERÍA SOCIAL EN PLATAFORMAS DE REDES SOCIALES, desarrollado bajo la modalidad Proyecto de Investigación por el señor Ariel Hernán Jinde Sisa, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2024

Firmado electrónicamente por:
FELIX OSCAR
FERNANDEZ PENA

Ing. Fernández Peña Félix Oscar, PhD

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: ESTRATEGIA PARA MITIGAR FRAUDES DE ANGLER-PHISHING BASADOS EN INGENIERÍA SOCIAL EN PLATAFORMAS DE REDES SOCIALES es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2024

Ariel Hernán Jinde Sisa

C.C. 1805343033

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero 2024

Firmado electrónicamente por:
ARIEL HERNAN JINDE SISA

Ariel Hernán Jinde Sisa

C.C. 1805343033

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Ariel Hernán Jinde Sisa, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado ESTRATEGIA PARA MITIGAR FRAUDES DE ANGLER-PHISHING BASADOS EN INGENIERÍA SOCIAL EN PLATAFORMAS DE REDES SOCIALES nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, febrero 2024

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
OSCAR FERNANDO IBARRA TORRES

Ing. Mg. Oscar Fernando Ibarra Torres

PROFESOR CALIFICADOR

Firmado electrónicamente por:
EDISON HOMERO ALVAREZ MAYORGA

Ing. Mg. Edison Homero Álvarez Mayorga

PROFESOR CALIFICADOR

DEDICATORIA

El presente trabajo de titulación se lo Dedico a mis padres Emma y Hernán, cuyo amor, apoyo y sacrificio han sido la luz que ha guiado cada paso de mi camino académico. Su dedicación y ejemplo han sido mi mayor inspiración y motivación. Este logro es el resultado de su inquebrantable fe en mí y de su eterno respaldo. Gracias por ser mi roca y mi guía.

A mi amada Myriam, tu amor, comprensión y aliento han sido mi refugio en los momentos de duda y dificultad. Esta tesis lleva impreso el eco de tus palabras de aliento y el brillo de tu confianza en mí.

A mis queridos hermanos Randy, Erick y a toda mi familia, su apoyo incondicional, sus risas contagiosas y su constante estímulo han sido mi mayor fortaleza.

A todos aquellos que han creído en mí y han sido parte de este viaje, este logro es también suyo.

Gracias por inspirarme a ser mi mejor versión.

Ariel Hernán Jinde Sisa

AGRADECIMIENTO

Agradezco primeramente a Dios, por su guía y bendiciones en este viaje académico.

A mi tutor Ing. Feliz Fernández por su orientación experta y sus valiosos consejos que han sido fundamentales para dar forma a este trabajo.

Agradezco profundamente a mis padres y familia por su amor incondicional, su constante aliento y su comprensión durante los momentos de dedicación intensa a este proyecto.

Finalmente, mi más sincero agradecimiento a mí amada novia, Myriam, por su amor incondicional, su paciencia infinita y su constante aliento. Tu presencia en mi vida ha sido invaluable, y tu apoyo durante los momentos de desafío ha sido fundamental para alcanzar este logro.

Ariel Hernán Jinde Sisa

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

La presente investigación titulada “Estrategia para mitigar fraudes de Angler-Phishing basados en ingeniería social en plataformas de redes sociales”. Para lo cual se trabajó en base al objetivo general el cual es definir una estrategia para prevenir y reducir la incidencia de fraudes de Angler-Phishing basados en Ingeniería Social. El trabajo conto con una metodología de enfoque mixto al recopilar y analizar datos provenientes de usuarios de redes sociales. A través de la exploración de las experiencias de individuos que interactúan en estas plataformas, particularmente aquellos susceptibles a la ingeniería social y al angler-phishing, se identificaron soluciones viables para atenuar los riesgos de fraude. Además, se trabajó con una población infinita, dado que resulta impracticable contabilizar el número exacto de usuarios activos en las redes sociales en la actualidad. Como resultado relevante se encontró que al aplicar una estrategia integral basada en la metodología OSSTMM para una efectiva integración de instrumentos de Tecnologías de la Información (TI), con el propósito de prevenir y reducir la incidencia de ataques resultando en una estrategia centrada en fomentar la colaboración entre diversas soluciones tecnológicas, tales como autentificación de dos pasos, sistemas de detección de intrusiones y filtros de correo electrónico, además se destaca que esta concordancia entre instrumentos fortalece la capacidad defensiva la cual sigue una aproximación estratégica que abarca distintas capas de seguridad.

Palabras clave: Angler-Phishing, redes sociales, ingeniería social y cybersecurity

ABSTRACT

This research titled “Strategy to mitigate Angler-Phishing fraud based on social engineering on social media platforms.” For which we worked based on the general objective which is to define a strategy to prevent and reduce the incidence of Angler-Phishing frauds based on Social Engineering. The work has a mixed approach methodology when collecting and analyzing data from social network users. By exploring the experiences of individuals who interact on these platforms, particularly those susceptible to social engineering and phishing, viable solutions are identified to mitigate fraud risks. Furthermore, we worked with an infinite population, given that it is impracticable to count the exact number of active users on social networks today. As a relevant result, it was found that by applying a comprehensive strategy based on the OSSTMM methodology for an effective integration of Information Technology (IT) instruments, with the purpose of preventing and reducing the incidence of attacks, resulting in a strategy focused on promoting collaboration between various technological solutions, such as two-step authentication, intrusion detection systems and email filters, it is also highlighted that this agreement between instruments strengthens the defensive capacity which follows a strategic approach that encompasses different security layers.

Keywords: Angler-Phishing, social networks, social engineering, and cybersecurity

CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema de investigación

ESTRATEGIAS PARA MITIGAR FRAUDES DE ANGLER-PHISHING BASADOS EN INGENIERÍA SOCIAL EN PLATAFORMAS DE REDES SOCIALES.

1.1.1 Planteamiento del problema

El planeta experimenta una revolución tecnológica constante, centrada en el manejo de datos, con las Tecnologías de la Información y la Comunicación como su base fundamental. La adopción de estas tecnologías impulsa el progreso social, generando transformaciones notables en diversos ámbitos, como la industria, el empleo, las áreas rurales, la movilidad, la salud, las finanzas, la conservación del medio ambiente, el entretenimiento y las relaciones humanas. Estos cambios se ven robustecidos por la influyente fuerza catalizadora de la tecnología[1].

La creación de Internet representó un hito transformador al introducir un sistema de comunicación sin precedentes. Sin embargo, fueron las Redes Sociales las que impulsaron la expansión más vertiginosa en el ámbito de las tecnologías de la información y la comunicación, dando lugar a una proliferación de puntos y plataformas de acceso a Internet que se multiplicaron. Este fenómeno amplió de manera significativa las oportunidades de comunicación multimodal, permitiendo el intercambio de información en diversos formatos en cualquier momento[2].

Las Redes Sociales constituyen plataformas digitales que congregan comunidades de individuos compartiendo intereses, actividades o relaciones afines, ya sea amistad, parentesco o ámbito laboral. Estas redes facilitan el contacto entre personas, operando como un medio para la comunicación fluida y el intercambio de información[3].

La Ingeniería Social emplea tácticas de manipulación para inducir a las personas a compartir información confidencial, descargar software no autorizado, acceder a sitios web no seguros, realizar transferencias de dinero a manos de delincuentes, o cometer

otros errores que puedan comprometer tanto sus activos como su seguridad personal o empresarial[4].

El avance de las nuevas tecnologías, las diversas formas de comunicación a través de las redes sociales y el impacto de la pandemia han contribuido al notable crecimiento de la presencia digital en Ecuador. Sin embargo, este aumento también ha propiciado un incremento en la actividad de cibercriminales. El fraude financiero, el reclutamiento para esquemas piramidales, la suplantación de identidad, entre otros delitos cibernéticos, se han incrementado de manera considerable. Esto se agrava debido a la falta de conocimiento que tienen las personas en el país acerca de la Ingeniería Social. Esta combinación de factores ha llevado a un aumento exorbitante en el porcentaje de ciberdelitos[5].

Según un informe de la empresa de seguridad Kaspersky, emitido en agosto de 2021, los ataques cibernéticos en Latinoamérica experimentaron un aumento del 24% en los primeros meses del año pasado. En este contexto, Ecuador se posiciona como uno de los países más vulnerables a las actividades de ciberdelincuentes, ocupando el segundo lugar después de Brasil, con un 13,3% de usuarios afectados. Este dato resalta la importancia de fortalecer las medidas de ciberseguridad y concienciar a la población sobre las amenazas digitales en la región[6].

1.2 Antecedentes Investigativos

Recopilando datos de los repositorios de universidades, IEEE explore y bibliotecas virtuales se han obtenido diversos trabajos cuya información será de apoyo para el desarrollo del presente proyecto. Esta fuente de conocimiento proveniente de los trabajos académicos contribuirá significativamente a enriquecer y fundamentar el contenido del proyecto en curso. La comprensión de los antecedentes investigativos es esencial para situar cualquier estudio en un contexto relevante y significativo con el objetivo de contextualizar la importancia y la pertinencia del presente estudio.

El propósito de la revisión de literatura es exponer las estrategias destinadas a mitigar fraudes de angler-phishing basados en ingeniería social en plataformas de redes sociales.

W. Syafitri, Z. Shukur, UA Mokhtar, R. Sulaiman y MA Ibrahim [7] llevaron a cabo una revisión sistemática de la literatura sobre la prevención de ataques de ingeniería social, identificando tres áreas clave de investigación: campañas de concienciación sobre seguridad, vulnerabilidad de los usuarios a la ingeniería social y protocolos de uso compartido para proteger la información en redes sociales. Destacaron la importancia de un modelo de vulnerabilidad del usuario, el cual puede incorporar recomendaciones de ingeniería social en redes sociales y evaluaciones de riesgos de respuesta del usuario. Además, mencionaron la utilidad de un protocolo co-útil que facilite el intercambio de información entre usuarios y reduzca la desconfianza al incluir la reputación del usuario.

J. Alzas [8] realizó un estudio de fraudes basados en la técnica de Ingeniería Social en lo que resalta que los ciberdelincuentes utilizan diversas técnicas de ingeniería social para engañar a sus víctimas y lograr sus objetivos malintencionados, aprovechando la amplia disponibilidad de información en Internet y herramientas poderosas. Estableciendo como esencial que las personas estén conscientes de esos métodos y aprendan a protegerse mediante la educación y la concienciación. Concluyendo que la ingeniería social se ha vuelto más fácil con el tiempo, y es crucial que las empresas y los usuarios tomen medidas preventivas para protegerse contra estos ataques cada vez más sofisticados.

L. Machaca [9] realizó un estudio donde destaca la importancia de la educación y el uso del doble factor de autenticación para reducir el número de víctimas de ataques de phishing. Propone estrategias como programas de concientización de seguridad, análisis de riesgos, inversión en tecnología, pruebas de pentesting, capacitación del personal, actualización sobre nuevos métodos de phishing, división entre equipos de tecnología e implementación de servicios de ciberseguridad externos.

L. Rosero[10] empleó una metodología analítica descriptiva de enfoque cuantitativo, junto con la técnica de mapeo sistemático para su desarrollo. Este proyecto concluyó que la mejor medida de prevención contra ataques de phishing es mantenerse

constantemente capacitado. Esta estrategia no solo contribuye a reducir el impacto económico y financiero de los ataques, sino que también fortalece la resiliencia ante posibles amenazas de seguridad.

F. Albán; M. Urvina y R. Andrade [11] aplicaron la metodología CRISP-DM, un modelo de proceso independiente para la minería de datos que consta de seis fases. En sus conclusiones, destacaron que el método utilizado de manera consistente por los atacantes es el abuso de vulnerabilidades conocidas públicamente. Esto se debe a que resulta más rentable en comparación con descubrir vulnerabilidades que aún no han sido identificadas. Además, la comprensión de esta tendencia puede ser crucial para fortalecer las medidas de seguridad, priorizando la protección contra vulnerabilidades conocidas en la prevención de ataques.

I. Collins y J. Mahoma [12] en su investigación sobre ataques de phishing ha demostrado la importancia de proteger la información personal de los usuarios cotidianos frente a ciberdelincuentes. La metodología incluyó una revisión de literatura, una encuesta en línea y entrevistas a expertos. Se destaca la necesidad de formular preguntas detalladas en la encuesta para obtener información precisa. Aunque la actualización de las preguntas prolongó el proceso de recopilación de datos, la investigación resultó reveladora y valiosa para comprender la ciberseguridad.

D. Arévalo y D. Valarezo [13] optaron por la metodología ágil Scrum para llevar a cabo las actividades de su proyecto de manera más organizada. Como conclusión, identificaron que factores como la susceptibilidad, la percepción del riesgo, el estrés, el miedo, e incluso los datos demográficos, desempeñan un papel crucial en la vulnerabilidad de un usuario frente a ciberataques, como es el caso del phishing. Estos hallazgos resaltan la importancia de considerar aspectos psicológicos y de percepción de riesgos al diseñar estrategias de seguridad cibernética.

1.3 Fundamentación teórica

Ciberseguridad

La ciberseguridad se define como la práctica destinada a defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques

maliciosos. También se conoce como seguridad de Tecnología de la Información o seguridad de la información electrónica. Por otro lado, la seguridad de red consiste en la práctica de salvaguardar una red informática de intrusiones, ya sean perpetradas por atacantes dirigidos o por programa maligno oportunista. Este enfoque se centra en implementar medidas preventivas y correctivas para garantizar la integridad, confidencialidad y disponibilidad de la información que fluye a través de la red [14].

La seguridad de las aplicaciones se centra en preservar la integridad y funcionalidad del software y dispositivos, evitando amenazas que podrían comprometer su correcto funcionamiento. Una aplicación comprometida podría exponer datos sensibles que debería proteger. Es crucial que la seguridad se considere desde las fases iniciales de diseño, mucho antes de la implementación de un programa o dispositivo. Además, la seguridad de la información se ocupa de proteger tanto la integridad como la privacidad de los datos, tanto durante su almacenamiento como en su tránsito. Esta disciplina se esfuerza por garantizar que los datos estén resguardados contra accesos no autorizados y que se mantengan íntegros y confidenciales, formando un componente esencial en la estrategia general de ciberseguridad de una organización o sistema [15].

La seguridad operativa abarca los procesos y decisiones destinados a gestionar y resguardar los recursos de datos. Esto incluye los permisos que los usuarios poseen para acceder a una red, así como los procedimientos que especifican cómo y dónde se pueden almacenar o compartir los datos [16].

En cambio, la recuperación ante desastres y la continuidad del negocio definen la manera en que una organización responde a un incidente de ciberseguridad o cualquier otro evento que interrumpa sus operaciones o cause la pérdida de datos. Las políticas de recuperación ante desastres establecen cómo la organización restaura sus operaciones e información para recuperar su capacidad operativa previa al evento. La continuidad del negocio es el plan que la organización implementa para operar sin ciertos recursos en caso de interrupciones, asegurando que pueda mantener sus funciones críticas y minimizar el impacto en sus operaciones [17].

La capacitación del usuario final se enfoca en el factor de ciberseguridad más impredecible: las personas. Si no se siguen las buenas prácticas de seguridad, cualquier

individuo puede introducir accidentalmente un virus en un sistema que, de otra manera, sería seguro. Instruir a los usuarios sobre la eliminación de archivos adjuntos de correos electrónicos sospechosos, la precaución al conectar unidades USB no identificadas y otras lecciones fundamentales es esencial para la seguridad de cualquier organización. Este enfoque educativo contribuye significativamente a la prevención de amenazas y fortalece la conciencia de los usuarios en cuanto a la importancia de su papel en la protección de la ciberseguridad de la organización [18].

Seguridad de la Información

La seguridad de Tecnologías de la Información (TI) constituye un conjunto de estrategias en ciberseguridad diseñadas para prevenir el acceso no autorizado a los activos organizativos, tales como computadoras, redes y datos. Su función principal es preservar la integridad y confidencialidad de la información sensible, al mismo tiempo que impide el acceso de hackers sofisticados y otros actores malintencionados. En esencia, la seguridad de TI trabaja para asegurar que los recursos digitales de una organización estén protegidos contra amenazas y ataques cibernéticos [19].

Tipos de seguridad de TI

Seguridad de la Red

La Seguridad de la Red se implementa para prevenir el acceso no autorizado o malicioso a una red, garantizando que la facilidad de uso, confiabilidad e integridad no se vean comprometidas. Su objetivo principal es impedir que hackers accedan a datos dentro de la red y evita que afecte negativamente la capacidad de los usuarios para utilizarla [20].

Con el aumento de la cantidad de terminales y la migración de servicios a la nube pública, la Seguridad de la Red se ha vuelto cada vez más compleja. Este escenario requiere enfoques y medidas más sofisticados para garantizar una protección efectiva contra las amenazas emergentes en un entorno digital en constante evolución [19].

Seguridad de Internet

La Seguridad de Internet se refiere a la protección de la información que se envía y recibe a través de navegadores, y está estrechamente relacionada con la seguridad de

red en aplicaciones basadas en la web. Su objetivo principal es monitorear el tráfico entrante de Internet para detectar programa maligno y tráfico no deseado. Esta protección se implementa a través de medidas como firewalls, soluciones antimalware y antispyware. Estos componentes trabajan en conjunto para salvaguardar la integridad y confidencialidad de los datos que circulan a través de las conexiones en línea, mitigando posibles amenazas y riesgos asociados con el uso de la red [21].

Seguridad de Terminales

La Seguridad de EndPoints proporciona protección a nivel del dispositivo, abarcando dispositivos como teléfonos móviles, tabletas, laptops y computadoras de escritorio. Su función principal es prevenir que estos dispositivos accedan a redes maliciosas que podrían representar una amenaza para la organización. La protección contra programa maligno y el uso de software avanzado para la administración de dispositivos son ejemplos de medidas implementadas en la seguridad de EndPoints. Esta capa de seguridad se centra en salvaguardar la integridad y funcionalidad de los dispositivos utilizados por los usuarios, contribuyendo así a la protección global de la infraestructura tecnológica de la organización [19].

Seguridad en la Nube

La transición de aplicaciones, datos e identidades hacia la Nube implica que los usuarios se conectan directamente a Internet, quedando fuera del alcance de los productos de seguridad tradicionales. La Seguridad de la Nube se encarga de proteger el uso de aplicaciones de software como servicio (SaaS, Software as a Service) y la nube pública. Para lograr esto, se pueden emplear herramientas como un agente de seguridad de acceso a la nube (CASB, Cloud Access Securtity Broker), una gateway de Internet segura (SIG, Secure Internet Gateway) y una gestión unificada de amenazas (UTM, Unified Threat Management) basada en la nube. Estas soluciones contribuyen a garantizar la seguridad en el entorno de la nube, proporcionando una capa adicional de protección para los usuarios y los datos que interactúan con servicios en la nube [22].

Seguridad de las Aplicaciones

Con la Seguridad de Aplicaciones, las aplicaciones son codificadas de manera específica durante su creación con el objetivo de ser lo más seguras posible,

garantizando que no sean vulnerables a ataques. Esta capa adicional de seguridad implica una evaluación del código de la aplicación para identificar posibles vulnerabilidades y asegurar que el software esté robustamente protegido contra amenazas. Al incorporar medidas de seguridad desde la fase de desarrollo, se busca prevenir y mitigar riesgos de seguridad antes de que las aplicaciones se implementen, fortaleciendo así la integridad y la resistencia de las aplicaciones frente a posibles ataques [23].

Políticas de seguridad

Las políticas informáticas tienen como objetivo principal establecer directrices y normas que contribuyan a la protección de la confidencialidad, privacidad y disponibilidad de los datos, así como de los sistemas y equipos informáticos de una empresa. Estas políticas están diseñadas para proporcionar un marco estructurado que guíe el comportamiento y las acciones de los usuarios en el entorno digital de la organización. Al enfocarse en la seguridad y el uso apropiado de los recursos tecnológicos, las políticas informáticas ayudan a prevenir amenazas, garantizar la integridad de la información y mantener la continuidad de las operaciones de la empresa [24]

Tipos de políticas de seguridad informática

Cuando se analizan las reglas de seguridad informática en las empresas, generalmente se pueden identificar dos tipos de protocolos:

1. Políticas de buenas prácticas informáticas

Son aquellas que se refieren a las directrices destinadas a establecer claramente las acciones necesarias para garantizar la seguridad informática. En otras palabras, son las medidas que todos los empleados deben llevar a cabo en pro de la seguridad de la información. Esto puede incluir acciones como ingresar la contraseña al iniciar sesión en la computadora, acceder a la red informática virtual de la empresa, mantener limpios los dispositivos informáticos, o cualquier otra acción proactiva de mantenimiento que los empleados deban seguir para asegurar un óptimo funcionamiento tanto del hardware como del software [25].

2. Políticas de riesgos informáticos

La Política de Riesgos Informáticos se centra en identificar y prevenir acciones que deben evitarse a toda costa. Un ejemplo de esto es la prohibición de compartir contraseñas de la empresa con terceros ajenos a la organización. También se destaca la restricción de descargar programas desde sitios web no oficiales y sin previo análisis de seguridad. Otro punto crítico es la advertencia contra hacer clic en enlaces sospechosos que puedan llegar a través de las redes sociales. En resumen, estas políticas abordan prácticas riesgosas que podrían comprometer la privacidad, confidencialidad e integridad de los datos, enfocándose en la prevención de amenazas potenciales [24].

Ciberdelincuencia

En la actualidad, el mundo se encuentra más interconectado digitalmente que nunca. Esta transformación en línea, sin embargo, ha abierto oportunidades para que los delincuentes aprovechen los puntos débiles de las redes, infraestructuras y sistemas informáticos. Este tipo de ataques tiene repercusiones económicas y sociales significativas a nivel global, afectando tanto a gobiernos como a empresas y particulares. La magnitud de estas amenazas destaca la necesidad urgente de fortalecer las medidas de ciberseguridad a fin de salvaguardar la integridad y la seguridad de nuestras redes y sistemas en este entorno digital cada vez más interdependiente [26].

El Phishing, el Ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas. Además, constantemente surgen nuevos tipos de ciberdelitos. Los ciberdelincuentes muestran una creciente agilidad y una organización más eficiente, evidenciada por la rapidez con la que explotan las nuevas tecnologías y su capacidad para adaptar y coordinar ataques de manera innovadora entre ellos. Este dinámico panorama destaca la necesidad constante de evolucionar y fortalecer las estrategias de ciberseguridad para hacer frente a una variedad de amenazas en constante evolución [26].

Ingeniería Social

La Ingeniería Social es una técnica empleada por ciberdelincuentes con el objetivo de ganarse la confianza del usuario, manipulándolo y engañándolo para que realice acciones perjudiciales. Estas acciones pueden incluir desde la ejecución de programas maliciosos hasta la facilitación de claves privadas o la realización de compras en sitios web fraudulentos. Este enfoque se centra en aprovechar la confianza y la interacción humana, más que en explotar vulnerabilidades técnicas, convirtiéndolo en un método de ataque sofisticado que requiere una sólida conciencia y educación en ciberseguridad por parte de los usuarios [27].

La Ingeniería Social es una estrategia que manipula a las personas para que compartan información confidencial, descarguen software no autorizado, visiten sitios web fraudulentos, envíen dinero a delincuentes, o cometan otros errores que ponen en riesgo la seguridad de sus activos, ya sea a nivel personal o empresarial. Esta técnica se aprovecha de la psicología humana y de la confianza para lograr que las personas realicen acciones perjudiciales sin ser plenamente conscientes de las consecuencias, siendo una amenaza significativa en el panorama de la ciberseguridad. La conciencia y educación en este tema son esenciales para mitigar los riesgos asociados con la Ingeniería Social [4].

Tipos de ataques de Ingeniería Social

Baiting

El Baiting atrae a las víctimas para que, de manera consciente o inconsciente, divulguen información confidencial o descarguen código malicioso, tentándolas con ofertas atractivas o incluso objetos valiosos. La estafa nigeriana es posiblemente el ejemplo más reconocido de esta técnica de Ingeniería Social. Ejemplos contemporáneos incluyen la descarga de software, música o juegos gratuitos que, lamentablemente, pueden estar infectados con programa maligno. Sin embargo, algunas formas de Baiting pueden carecer de sofisticación, aprovechándose de la curiosidad o la confianza de las personas de manera menos ingeniosa pero igualmente perjudicial. La prevención y la conciencia son fundamentales para mitigar los riesgos asociados con esta táctica [4] [15].

Tailgating

En el Tailgating, también conocido como "piggybacking", una persona no autorizada sigue de cerca a otra persona autorizada hacia un área que alberga información confidencial o activos valiosos. El Tailgating puede ser de naturaleza física, como cuando alguien sigue a un empleado a través de una puerta desbloqueada, pero también puede adoptar una forma digital. Un ejemplo de esta variante es cuando alguien deja su computadora desatendida mientras permanece conectada a una red o cuenta privada. Este método destaca la importancia tanto de la seguridad física como de la ciberseguridad para prevenir el acceso no autorizado a áreas o información sensible [4].

Pretexting

En el Pretexting, el estafador fabrica una situación falsa y se presenta como la persona apropiada para resolverla. En muchos casos, irónicamente, el estafador afirma que la víctima ha sido afectada por una brecha de seguridad y ofrece resolver el problema a cambio de información de cuenta importante o control sobre el sistema o dispositivo de la víctima. Técnicamente hablando, casi todos los ataques de Ingeniería Social involucran algún nivel de Pretexting. Esta táctica subraya la importancia de ser cauteloso y verificar cuidadosamente la autenticidad de las situaciones antes de compartir información sensible o tomar acciones en respuesta a solicitudes inesperadas [4] [15].

Quid pro quo

En una estafa Quid pro quo, los hackers ofrecen un bien o servicio deseable a cambio de información confidencial de la víctima. Ejemplos de tácticas Quid pro quo incluyen el ganar un concurso falso o recompensas de fidelidad aparentemente inofensivas ("gracias por su pago, tenemos un regalo para usted"). Este enfoque manipulativo explora la predisposición de las personas a recibir beneficios inmediatos, a menudo sin cuestionar la autenticidad de la oferta. La conciencia y la precaución son esenciales para evitar caer en este tipo de estafas y proteger la información personal y confidencial [28].

Scareware

El Scareware, también considerado una forma de programa maligno, es software que utiliza el miedo como táctica para manipular a las personas y lograr que compartan información confidencial o descarguen más programa maligno. Este tipo de software a menudo se presenta en forma de advertencias falsas, como un aviso de la policía que acusa al usuario de un delito, o un mensaje de soporte tecnológico falso que alerta al usuario sobre la presencia de programa maligno en su dispositivo. La estrategia principal es generar temor en la víctima para que tome acciones impulsivas que beneficien al atacante, resaltando la importancia de la educación en ciberseguridad para reconocer y evitar estas amenazas [29].

Ataque de abrevadero (watering hole)

Siguiendo la metáfora de "alguien ha envenenado el abrevadero", en los ataques de abrevadero, los hackers inyectan código malicioso en una página web legítima frecuentada por sus objetivos. Estos ataques son responsables de una amplia gama de consecuencias, desde el robo de credenciales hasta descargas involuntarias de ransomware. La estrategia aquí es comprometer un lugar en línea confiable para aprovechar la confianza de los usuarios y ejecutar acciones maliciosas en sus dispositivos, subrayando la importancia de mantenerse alerta y protegerse contra amenazas cibernéticas incluso en sitios web aparentemente seguros [30].

Phishing

Los ataques de phishing son mensajes, ya sea digitales o de voz, que buscan manipular a los destinatarios para que compartan información confidencial, descarguen software malicioso, transfieran dinero o activos a personas equivocadas, o realicen alguna otra acción perjudicial. Estos ataques suelen utilizar tácticas engañosas, como correos electrónicos que aparentan ser de fuentes confiables o llamadas telefónicas que simulan ser de instituciones legítimas, con el objetivo de obtener información sensible o inducir a las víctimas a realizar acciones no deseadas. La conciencia y la capacitación en ciberseguridad son esenciales para prevenir caer en este tipo de trampas [31].

Tipos de estafas de Phishing:

- Los correos electrónicos de Phishing en masa se envían a millones de destinatarios al mismo tiempo. Parecen enviados por una gran empresa u organización reconocida, como un banco nacional o global o un gran minorista online, y realizan una solicitud genérica como "estamos teniendo problemas para procesar su compra; por favor, actualice su información de crédito" [32]
- El spear Phishing se dirige a una persona específica, normalmente alguien con acceso con privilegios a la información del usuario, la red de sistemas o fondos corporativos. El Whaling es un tipo de spear Phishing dirigido a una persona de alta visibilidad, como un director ejecutivo o una figura política. En el Business Email Compromise (BEC), el hacker utiliza credenciales comprometidas para enviar mensajes de correo electrónico desde la cuenta de correo electrónico real de una figura de autoridad, lo que hace que la estafa sea mucho más difícil de detectar [32].
- El Phishing de voz o vishing, es un Phishing realizado a través de llamadas telefónicas. La forma más frecuente de vishing son llamadas grabadas amenazantes que afirman ser del FBI (Federal Bureau of Investigation). Pero X-Forcé de IBM (International Business Machines) recientemente determinó que agregar Vishing a una campaña de Phishing dirigida puede aumentar el éxito de la campaña hasta 3 veces [28].
- El Phishing por SMS, o smishing, es Phishing a través de mensajes de texto.
- En el Phishing de motor búsqueda los hackers crean sitios Web maliciosos que tienen un buen posicionamiento en los resultados de búsqueda en Google por términos de búsqueda populares.
- El Angler Phishing es Phishing a través de cuentas falsas en Redes Sociales que se hacen pasar por la cuenta oficial del servicio al cliente o de equipos de soporte al cliente de empresas fiables [32].

1.4 Objetivos

1.4.1 Objetivo general

Definir una estrategia para prevenir y reducir la incidencia de fraudes de Angler-Phishing basados en Ingeniería Social

1.4.2 Objetivos específicos

- Caracterizar el ámbito de ataques Angler-Phishing llevados a cabo en la actualidad.
- Identificar instrumentos TI utilizados para prevenir y reducir la incidencia de ataques basados en Ingeniería Social.
- Integrar instrumentos TI estratégicamente para prevenir y reducir la incidencia de ataques Angler-Phishing basados en Ingeniería Social.
- Evaluar experimentalmente la aplicabilidad de la estrategia definida.

CAPÍTULO II.- METODOLOGÍA.

2.1 Materiales

El material con el cual se recopilo la información de la presente investigación es una encuesta compuesta por 10 preguntas. Estas preguntas abarcaron una variedad de formatos, incluyendo opciones cerradas, selección múltiple y el empleo de la escala de Likert.

Encuesta dirigida al público en general sobre Ingeniería Social y Angler-Phishing

Encuestador: Ariel Jinde

Objetivo: Determinar el nivel de conocimiento que tienen las personas que usan redes sociales acerca de los ataques fraudulentos de angler phishing e ingeniera social.

Indicaciones: Seleccionar la respuesta con la mayor sinceridad posible.

1. **¿Cuál es su edad?**

    - Menor a 18
    - 18 años a 24 años
    - 25 años a 34 años
    - 35 años a 44 años
    - 45 años a 54 años
    - Mas de 54

2. **¿Con qué género se identifica?**

    - Masculino
    - Femenino
    - Prefiero no contestar

3. **¿Con qué fin utiliza las redes sociales?**

    - □ Entretenimiento
    - □ Educativo
    - □ Informativo
    - □ Trabajo
    - □ Ventas
    - □ Compras
    - □ Otros:

4. ¿Con que frecuencia utiliza las siguientes redes sociales?

	Nunca	Casi nunca	En Ocasiones	Casi todos los días	Todos los días
Facebook	O	O	O	O	O
YouTube	O	O	O	O	O
Instagram	O	O	O	O	O
TikTok	O	O	O	O	O
WhatsApp	O	O	O	O	O
LinkedIn	O	O	O	O	O
Snapchat	O	O	O	O	O
X-Twitter	O	O	O	O	O

5. ¿Alguna vez ha sido víctima de un intento de ingeniería social, como engaño, manipulación o suplantación de identidad en línea?

- Sí
- No

6. ¿Puede identificar alguno de los siguientes ataques de ingeniería social?

	Nada	Poco	Algo	Suficiente	Mucho
Phishing	O	O	O	O	O
Suplantación de identidad	O	O	O	O	O
Pretexting	O	O	O	O	O
Angler-phishing	O	O	O	O	O
Tailgaiting	O	O	O	O	O
Vishing	O	O	O	O	O
Smishing	O	O	O	O	O
Encuestas Falsas	O	O	O	O	O

7. ¿Qué medidas toma habitualmente para protegerse contra estas técnicas de ingeniería social?

	Nunca	Casi nunca	En ocasiones	Cada mes	Una vez por semana
Configurar la privacidad en las redes sociales	O	O	O	O	O
Informar y aprender sobre este tipo de amenazas.	O	O	O	O	O
Usar una contraseña segura.	O	O	O	O	O
Configurar la autenticación en dos pasos	O	O	O	O	O
Prestar atención a cualquier persona que te pida información personal.	O	O	O	O	O
Aplicaciones de seguridad	O	O	O	O	O
Extensiones del navegador	O	O	O	O	O

8. ¿Qué tan importante considera recibir capacitación sobre cómo identificar posibles intentos de ataques de ingeniería social y protegerse de ellos?

Nada Importante	Poco Importante	Algo Importante	Importante	Muy Importante
O	O	O	O	O

9. ¿Cuánto confía en su capacidad para evitar intentos de ingeniería social en línea?

	Pobre	Cuestionable	Aceptable	Buena	Excelente
Phishing	O	O	O	O	O
Scareware	O	O	O	O	O
Pharming	O	O	O	O	O
Engaño en Redes Sociales	O	O	O	O	O
Angler-phishing	O	O	O	O	O
Pretexting	O	O	O	O	O

Spear phishing	O	O	O	O	O

10. ¿En qué medida los siguientes factores le hacen más propenso hacer clic en un enlace de un mensaje de redes sociales?

	Nada Propenso	**Poco Propenso**	**Neutral**	**Propenso**	**Muy Propenso**
El mensaje parece ser de una fuente conocida o de confianza	O	O	O	O	O
El mensaje ofrece un premio o una recompensa atractiva	O	O	O	O	O
El mensaje es urgente o parece que se estaría perdiendo de algo	O	O	O	O	O
El mensaje genera curiosidad o trata temas populares	O	O	O	O	O
El mensaje aparenta provenir de figuras de autoridad	O	O	O	O	O

¡Gracias por su colaboración!

Esta encuesta de 10 preguntas fue elaborada y difundida al público mediante el formulario que ofrece Google Forms.

2.2 Métodos

2.2.1 Modalidad de la investigación

Investigación Bibliográfica – Documental en la obtención de información que pueda servir de sustento para el proyecto, indagando acerca de problemas similares y sus respectivas propuestas de solución que se hayan establecido con anterioridad.

Investigación de campo porque se recopilaron datos de fuentes primarias, como lo son investigaciones previas realizadas con similitudes en el tema planteado.

Investigación de Modalidades Especiales ya que se realizará una novedosa y creativa estrategia que brinde una solución ante la problemática.

2.2.2 Población y muestra

Población

Para la presente investigación se tomó como población infinita debido a que no se puede contabilizar el número de usuarios activos en redes sociales en la actualidad.

Tabla 1. Población de usuarios en redes sociales

Población	Numero	Porcentaje
Usuarios de redes sociales	Indefinido	100%
Total:	Indefinido	100%

Muestra

Para el cálculo del tamaño de la muestra representativa de una población infinita se utilizó un nivel de confianza deseado de 95% y un margen de error de 9.8% aplicando la siguiente fórmula:

$$\textbf{Tamaño de la muestra (n)} = \frac{z^2 * p * (1-p)}{e^2}$$

Tabla 2. Cálculo de muestra representativa.

Variable	Definición	Datos
N	Población	Indefinida
NC	Nivel de confianza deseado	95%
Z	Puntuación de valor z según NC	1.96
P	Probabilidad de éxito	0.5
E	Margen de error	9.8%

$$\mathbf{n} = \frac{1.96^2 * 0.5 * 0.5}{0.098^2} \quad \mathbf{n = 100}$$

De la población infinita de usuarios en redes sociales con un nivel de confianza de 95% y un margen de error 9.8% la fórmula estadística arrojo un tamaño de muestra de 100 usuarios.

2.2.3 Recolección de información

Se recolectó información a través de la encuesta aplicada al público en general que usa redes sociales, para analizar los problemas y dificultades que presenta ante una posible amenaza de angler-phishing.

Validación del Instrumento

Alfa de Cronbach en la encuesta

El coeficiente Alfa de Cronbach es una fórmula general para estimar la fiabilidad y la validez de un instrumento en el que la respuesta a los ítems es dicotómica o tiene más de dos valores como lo es la escala de Likert[33].

Para obtener este coeficiente se utilizó el programa estadístico Statistical Package for the Social Sciences (SPSS versión 29.0.1.0) que permite calcular el coeficiente alfa de Cronbach de manera sencilla.

Los datos fueron extraídos en un formato .xlsx desde el formulario de Google Forms, luego estos fueron procesados para posteriormente ser leídos en SPPS y finalmente obtener el valor de confiabilidad.

Para realizar los cálculos del coeficiente se realiza los siguientes pasos[33]:

1. En primer lugar, seleccionar la opción Analizar del menú principal. Este apartado permite calcular estadísticos descriptivos, correlaciones, reducción de dimensiones, entre otros. Dentro de la opción Analizar, seleccionar Escala, y a continuación **Análisis de la fiabilidad**.
2. Seleccionar los ítems del cuestionario que queramos analizar, pasarlos a la casilla Elementos pulsando la flecha en horizontal.
3. A continuación, en la parte superior derecha, pulsar Estadísticos y seleccionar aquellos que interesan para el estudio:
    - Descriptivos: elemento, escala y escala si se elimina el elemento.
    - Inter elementos: para correlaciones y covarianzas.
    - Resúmenes: medias, varianzas, covarianzas y correlaciones
4. Y pulsamos Continuar.

5. Eso retorna a la pantalla anterior —donde se habían seleccionados los ítems del cuestionario—y puede apreciarse que, en la parte inferior, la casilla Modelo tiene seleccionado por defecto **Alfa**. Pulsar la tecla Aceptar y aparecen los resultados en el Visor de resultados.

En la Tabla 3 se representa la escala del Alfa de Cronbach para calificar la validez del cuestionario que se realizó.

Tabla 3. Interpretación escala de alfa de Cronbach.

Alfa de Cronbach	Interpretación
0,9	Excelente
0,9 - 0,8	Buena
0,8 - 0,7	Aceptable
0,7 - 0,6	Débil
0,6 - 0,5	Pobre
< 0,5	Inaceptable

Se pude visualizar el procedimiento en las siguientes figuras:

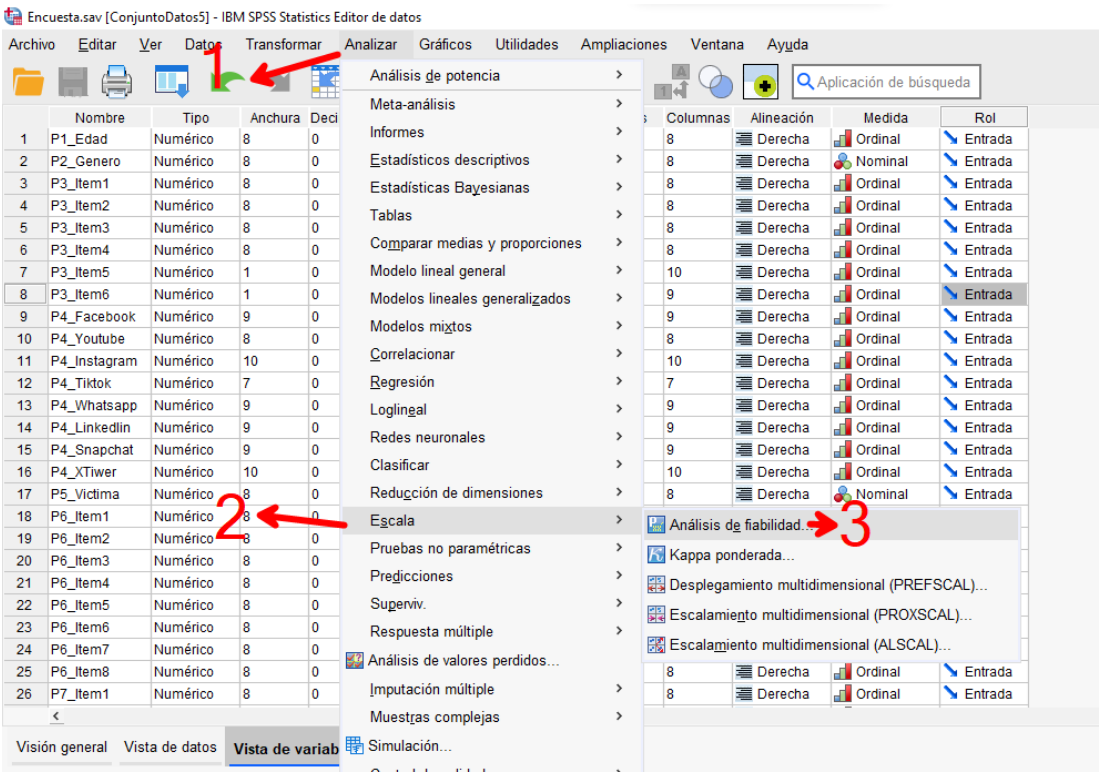

Figura 1. Cuadro de dialogo para realizar el análisis de fiabilidad parte 1

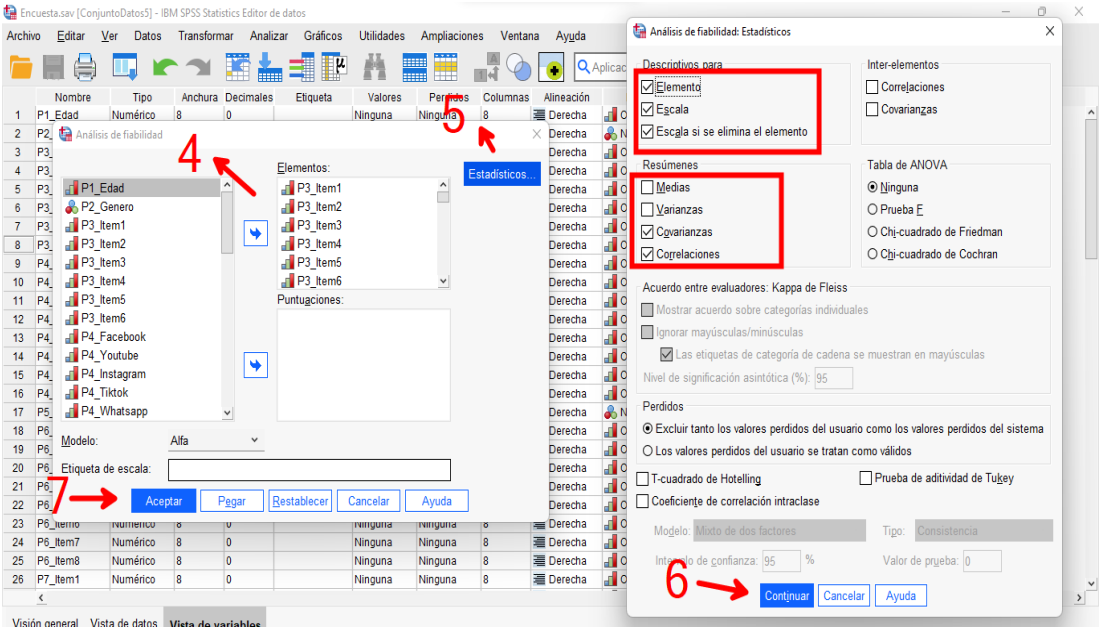

Figura 2. Cuadro de dialogo para realizar el análisis de fiabilidad parte 2

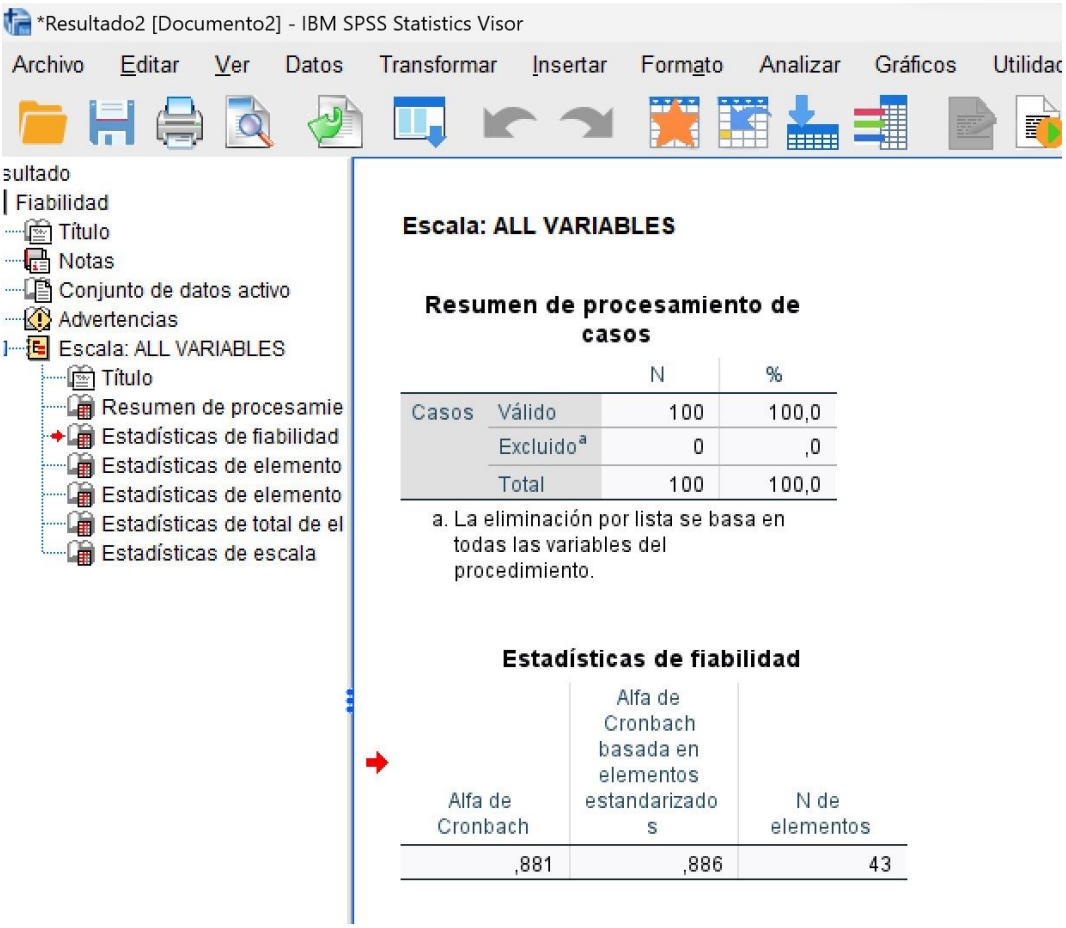

Figura 3. Resultados de estadísticas de fiabilidad.

- Coeficiente obtenido para la pregunta 2 y pregunta 5.

Tabla 4. Resumen de procesamiento de casos

		N	%
Casos	**Válido**	100	100
	Excluido	0	0
	Total	100	100

Tabla 5. Confiabilidad Alfa de Cronbach en la encuesta pregunta 2 y 5

Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0,929	0,929	2

Como se muestra en la tabla anterior, el resultado en el alfa de Cronbach da un valor de **0,929**, considerando la confiabilidad de las respuestas dentro del rango excelente.

- Coeficiente obtenido para la pregunta 1, pregunta 3, pregunta 4, pregunta 6, pregunta 7, pregunta 8, pregunta 9 y pregunta 10.

Tabla 6. Confiabilidad Alfa de Cronbach en la encuesta preguntas restantes

Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0,881	0,886	43

Como se muestra en la anterior, el resultado en el alfa de Cronbach da un valor de **0,886**, considerando la confiabilidad de las respuestas dentro del rango aceptable.

a. Resultados de la encuesta aplicada sobre ingeniería social y angler-phishing.

Pregunta 1: ¿Cuál es su edad?

Tabla 7. Resultados de rango de edades

Indicador	Frecuencia	Porcentaje
18 años a 24 años	49	49%
25 años a 34 años	43	43%
35 años a 44 años	4	4%
Menor a 18	2	2%
45 años a 54 años	2	2%

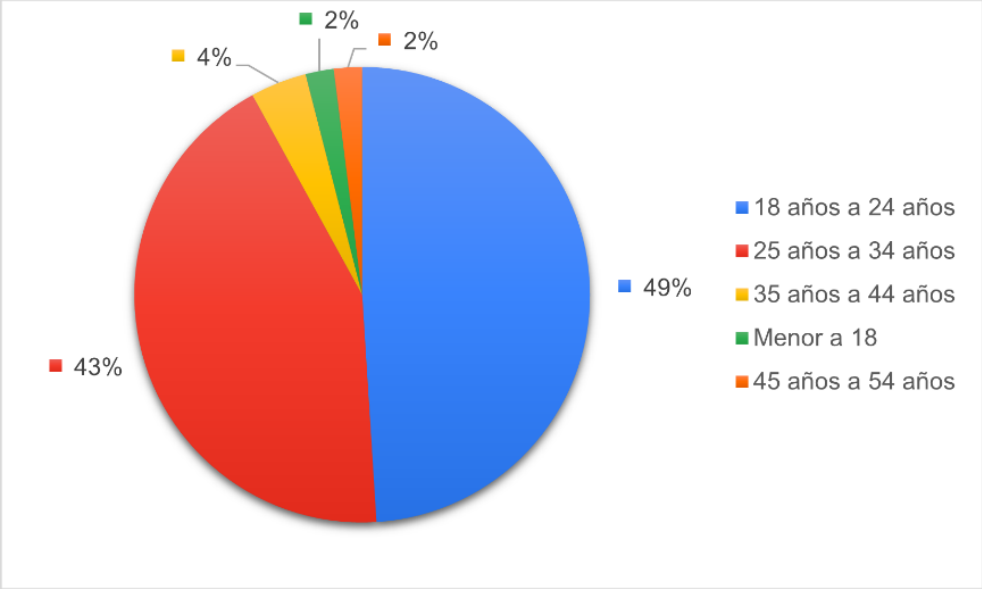

Figura 4. Resultados rango de edades

Análisis e interpretación de resultados

Con los resultados obtenidos en la **Figura 4** , se observa que de los 100 encuestados 49 pertenecen al grupo de 35 años a 44 años representando el 49%, 43 encuestados pertenecen al grupo de 25 años a 34 años representando el 43%, 4 encuestados pertenecen al grupo de 35 años a 44 años representando el 4%, 2 encuestados pertenecen al grupo de menor a 18 años representando el 2%. Como resultado se evidencia que la mayor parte de la muestra se encuentra entre 18 y 34 años, entendiendo que son jóvenes adultos que trabajan o estudian.

Pregunta 2: ¿Con qué género se identifica?

Tabla 8. Género de los encuestados

Indicador	Frecuencia	Porcentaje
Femenino	63	63%
Masculino	37	37%
No contestar	0	0%
Total	100	100%

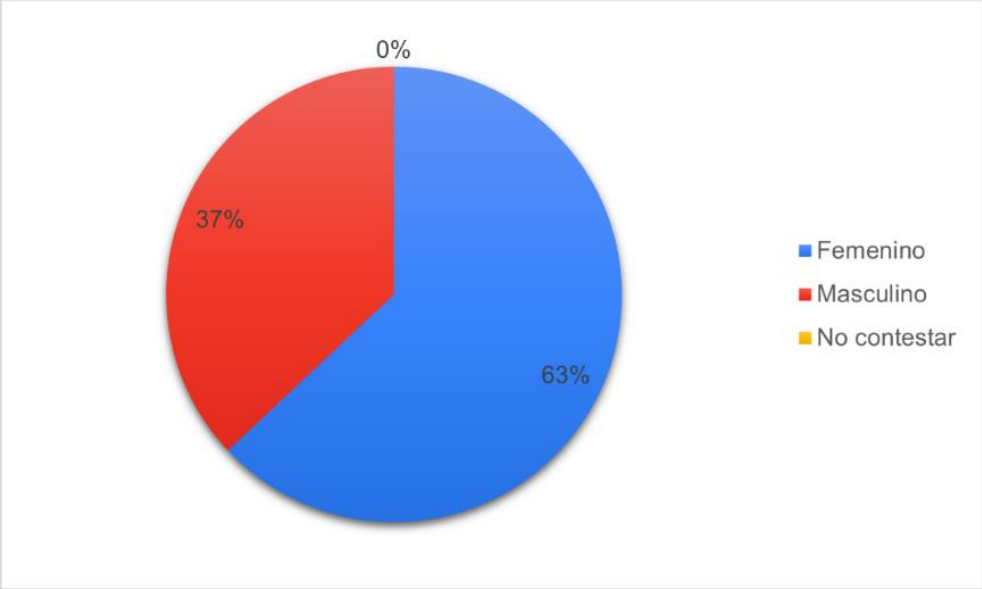

Figura 5. Género de los encuestados

Análisis e interpretación de resultados

En la **Figura 5,** se puede detectar que el 63% de los encuestados corresponden al género Femenino mientras que el 37% corresponden al género masculino, determinando así que la mayor parte de los encuestado son mujeres. El 0% respondió prefirió no contestar.

Pregunta 3: ¿Con qué fin utiliza las redes sociales?

Tabla 9. Género de los encuestados

Ítems	Frecuencia	Porcentaje
Ventas	24	8%
Compras	30	10%
Trabajo	34	11%

Ítems	Frecuencia	Porcentaje
Educativo	63	21%
Informativo	64	21%
Entretenimiento	86	29%
Total	301	100%

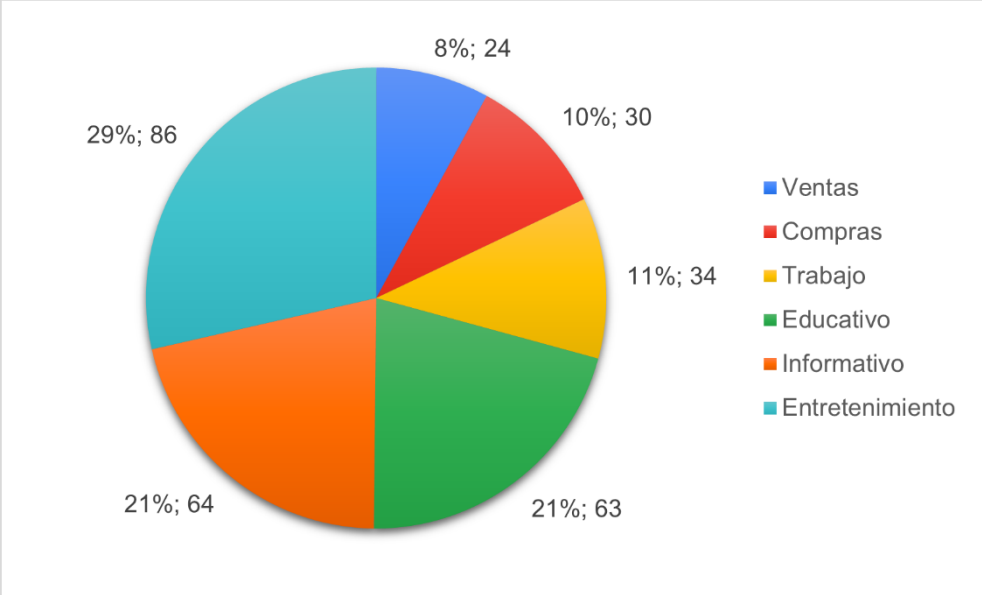

Figura 6. Utilidad de redes sociales

Análisis e interpretación de resultados

- Entretenimiento (86 interacciones, 29%): La categoría de entretenimiento es la más grande en términos de porcentaje, lo que sugiere que gran parte de los encuestados ve contenido en redes sociales.
- Informativo (64 interacciones, 21%): Las interacciones informativas también tienen un porcentaje importante. Esto podría indicar que las personas utilizan las redes sociales para ver contenido que ofrece información.
- Educativo (63 interacciones, 21%): Esta categoría tiene un porcentaje significativo de interacciones. Puede indicar que todos los encuestados están interesado en contenido educativo.
- Trabajo (34 interacciones, 11%): Las interacciones en la categoría de trabajo podrían estar relacionadas con la promoción de empleo, anuncios de vacantes o interacciones profesionales. El 11% sugiere que el contenido laboral también es una parte relativamente pequeña en redes sociales.

- Compras (30 interacciones, 10%): Esto representa interacciones relacionadas con compras o adquisiciones de productos o servicios.
- Ventas (24 interacciones, 8%): Estas interacciones están relacionadas con la promoción o venta de productos o servicios. El porcentaje es relativamente bajo en comparación con otras categorías, lo que indica que las ventas en redes sociales no son el enfoque principal de las personas encuestadas.

Pregunta 4: ¿Con que frecuencia utiliza las siguientes redes sociales?

Tabla 10. Escala de Likert frecuencia para la pregunta 4

Opciones	Valor
Nunca	1
Casi Nunca	2
En Ocasiones	3
Casi todos los días	4
Todos los días	5

Tabla 11. Frecuencia y porcentaje del uso de redes sociales

	1		2		3		4		5		Total
	f.	%	f.	%	f.	%	f.	%	f.	%	
Facebook	6	6%	13	13%	41	41%	25	25%	15	15%	100%
YouTube	2	2%	7	7%	49	49%	32	32%	10	10%	100%
Instagram	11	11%	14	14%	26	26%	26	26%	23	23%	100%
TikTok	5	5%	17	17%	29	29%	28	28%	21	21%	100%
WhatsApp	0	0%	0	0%	16	16%	25	25%	59	59%	100%
LinkedIn	54	54%	15	15%	23	23%	6	6%	2	2%	100%
Snapchat	55	55%	18	18%	23	23%	2	2%	2	2%	100%
X-Twitter	42	42%	25	25%	21	21%	6	6%	6	6%	100%

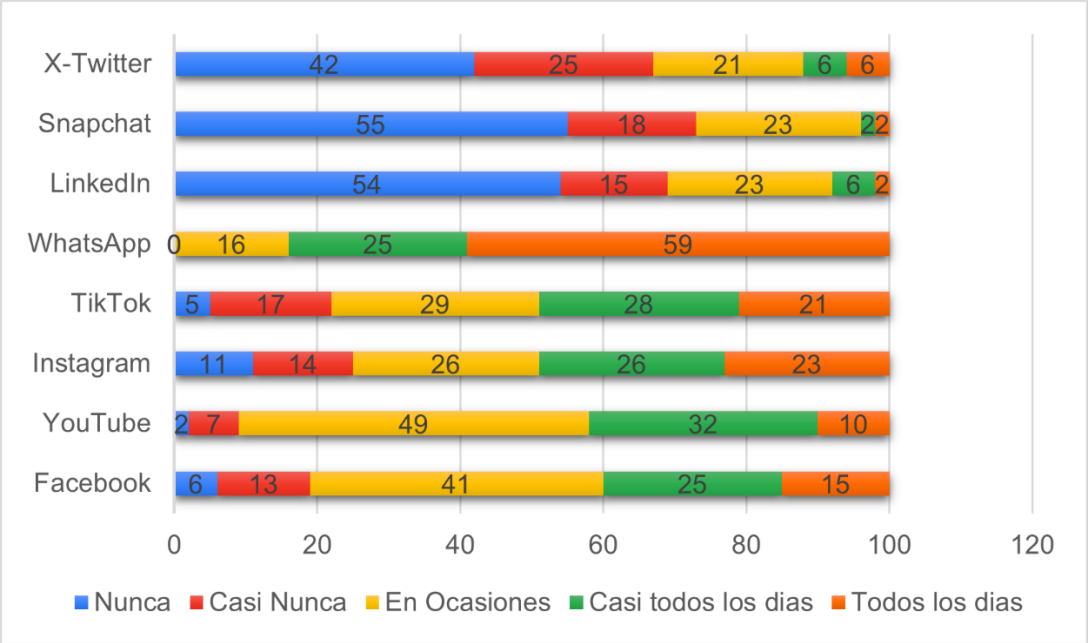

Figura 7. Uso de redes sociales

Análisis e interpretación de resultados

- WhatsApp: WhatsApp es una plataforma ampliamente utilizada, con un 59% de usuarios que lo utilizan "Todos los Días". Esto refleja su importancia como plataforma de mensajería instantánea.
- Facebook: La mayoría de los usuarios (41%) utilizan Facebook "En Ocasiones", seguido de un 25% que lo utilizan "Casi Todos los Días". Esto sugiere que Facebook es una plataforma de uso común, aunque no necesariamente a diario.
- YouTube: YouTube es muy utilizado, con un 49% de usuarios que lo utilizan "En Ocasiones" y un 32% que lo utilizan "Casi Todos los Días". Esto refleja la popularidad de YouTube como plataforma de video.
- Instagram: Al igual que YouTube, Instagram es ampliamente utilizado, con un 26% de usuarios que lo utilizan "En Ocasiones" y un 23% que lo utilizan "Casi Todos los Días".
- TikTok: TikTok es utilizado "En Ocasiones" por un 29% de los usuarios y "Casi Todos los Días" por un 28%. Esto muestra que TikTok ha ganado popularidad y es utilizado tanto de manera ocasional como regular.
- LinkedIn: LinkedIn es principalmente utilizado "En Ocasiones" por el 23% de los usuarios, pero ha disminuido en uso diario ("Todos los Días" y "Casi Todos los Días" suman solo un 8% en total).

- Snapchat: Snapchat ha disminuido en uso, con un 55% que lo utiliza "Nunca" y un 18% que lo utiliza "Casi Nunca". Solo un 4% de los usuarios lo utilizan "Todos los Días" o "Casi Todos los Días".
- X-Twitter: La plataforma denominada "X-Twitter" también ha disminuido en uso, con un 42% que lo utiliza "Nunca" y un 25% que lo utiliza "Casi Nunca".

En resumen, estos datos muestran que plataformas como Facebook, YouTube, Instagram y TikTok son utilizadas de manera más frecuente, mientras que LinkedIn, Snapchat y la plataforma X-Twitter han disminuido en popularidad. WhatsApp destaca como una plataforma esencial para la comunicación diaria, debido a su uso muy frecuente es una aplicación que puede ser utilizada para realizar diversos ataques o fraudes.

Pregunta 5: ¿Alguna vez ha sido víctima de un intento de ingeniería social, como engaño, manipulación o suplantación de identidad en línea?

Tabla 12. Resultados pregunta 5

Indicadores	Frecuencia	Porcentaje
No	53	53%
Si	47	47%
Total	100	100%

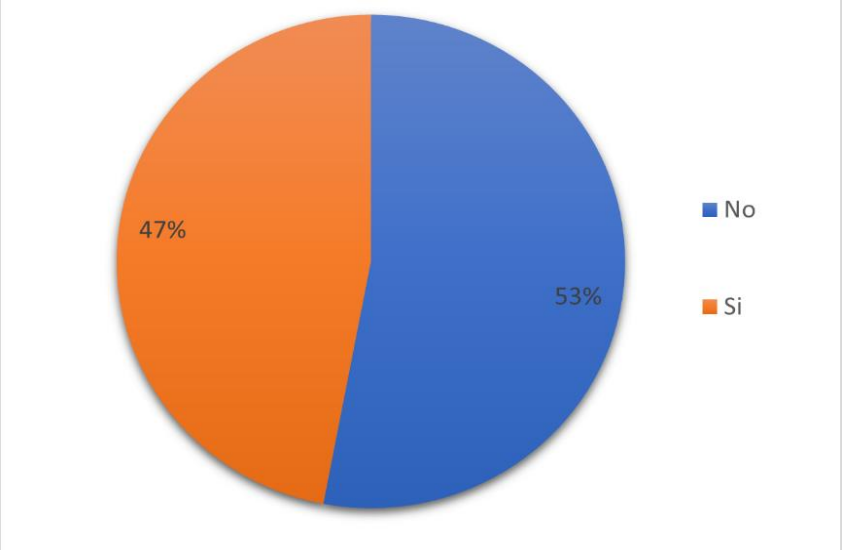

Figura 8. Resultados de la pregunta 5

Análisis e interpretación de resultados

El 53% de las personas encuestadas respondieron que no han sido víctimas de intentos de ingeniería social. Esto sugiere que más de la mitad de las personas encuestadas no han experimentado este tipo de problema.

El 47% de las personas encuestadas respondieron que sí han sido víctimas de intentos de ingeniería social. Esto indica que un porcentaje significativo de las personas encuestadas han experimentado en algún momento intentos de manipulación o engaño con el propósito de obtener información confidencial o cometer fraude.

El análisis de estos resultados sugiere que la ingeniería social es una preocupación real y que un número considerable de personas han experimentado intentos de este tipo. Esto resalta la importancia de la concienciación sobre la ingeniería social y de tomar medidas para protegerse contra estos ataques.

Pregunta 6: ¿Puede identificar alguno de los siguientes ataques de ingeniería social?

Tabla 13. Escala de Likert frecuencia para la pregunta 6

Opciones	Valores
Nada	1
Poco	2
Algo	3
Suficiente	4
Mucho	5

Tabla 14. Frecuencia y porcentaje de ataques de ingeniería social

	1		2		3		4		5		Total
	f.	%	f.	%	f.	%	f.	%	f.	%	
Phishing	56	56%	26	26%	6	6%	6	6%	6	6%	100%
Suplantación de identidad	39	39%	21	21%	19	19%	11	11%	10	10%	100%
Pretexting	55	55%	29	29%	12	12%	4	4%	0	0%	100%
Angler-phishing	54	54%	22	22%	22	22%	2	2%	0	0%	100%

	f.	%	f.	%	f.	%	f.	%	f.	%	Total
Tailgaiting	59	59%	25	25%	14	14%	0	0%	2	2%	100%
Vishing	58	58%	24	24%	16	16%	2	2%	0	0%	100%
Smishing	59	59%	25	25%	12	12%	4	4%	0	0%	100%
Encuestas Falsas	22	22%	25	25%	32	32%	18	18%	3	3%	100%

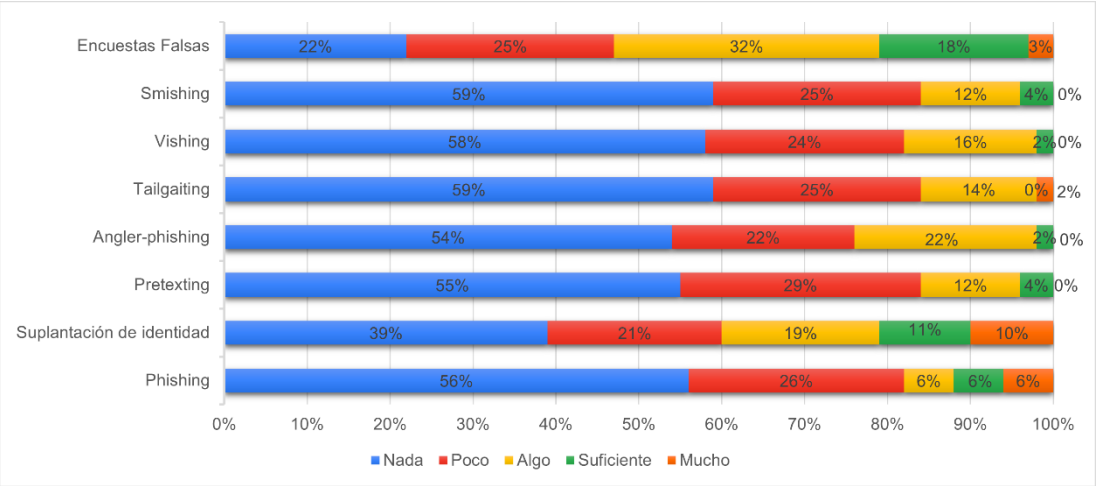

Figura 9. Frecuencia y porcentaje de ataques de ingeniería social

Análisis e interpretación de resultados

Phishing:

- El 56% de las personas encuestadas reportaron que no han experimentado phishing.
- El 26% indicó que han experimentado phishing en una medida "Poco".
- El 6% experimentó phishing en una medida "Algo".
- El 6% experimentó phishing en una medida "Suficiente".
- El 6% experimentó phishing en una medida "Mucho".

La mayoría de las personas informan que no han experimentado phishing, pero un porcentaje significativo ha experimentado este tipo de ataque en cierta medida.

Suplantación de Identidad:

- El 39% de las personas no han experimentado la suplantación de identidad.

- El 21% informó haber experimentado la suplantación de identidad en una medida "Poco".
- El 19% experimentó esto en una medida "Algo".
- El 11% experimentó la suplantación de identidad en una medida "Suficiente".
- El 10% experimentó esto en una medida "Mucho".

Interpretación: Un número considerable de personas ha experimentado suplantación de identidad en diferentes grados.

Pretexting:

- El 55% no ha experimentado pretexting.
- El 29% ha experimentado pretexting en una medida "Poco".
- El 12% experimentó esto en una medida "Algo".
- El 4% experimentó pretexting en una medida "Suficiente".
- El 0% experimentó esto en una medida "Mucho".

La mayoría de las personas no han experimentado pretexting, y solo un pequeño porcentaje lo ha experimentado en cierta medida.

Otros Tipos de Ataques (Angler-phishing, Tailgaiting, Vishing, Smishing, Encuestas Falsas):

En general, la mayoría de las personas informaron que no han experimentado estos tipos de ataques o los han experimentado en una medida "Nada" o "Poco".

En resumen, los resultados indican que la mayoría de las personas encuestadas no han experimentado la mayoría de los tipos de ataques de ingeniería social, pero algunos han experimentado phishing y suplantación de identidad en diferentes grados.

Pregunta 7: ¿Qué medidas toma habitualmente para protegerse contra estas técnicas de ingeniería social?

Figura 10. Escala de Likert frecuencia para la pregunta 7

Opciones	Nunca	Casi nunca	En ocasiones	Cada mes	Una vez por semana
Valor	1	2	3	4	5

Tabla 15. Frecuencia y porcentaje de medidas y técnicas contra ataques de ingeniería social

	1		2		3		4		5		Total
	f.	%	f.	%	f.	%	f.	%	f.	%	
Configurar privacidad en redes sociales	6	6%	13	13%	50	50%	20	20%	11	11%	100%
Informar y aprender sobre este tipo de amenazas.	8	8%	15	15%	50	50%	16	16%	11	11%	100%
Usar una contraseña segura.	4	4%	5	5%	49	49%	25	25%	17	17%	100%
Configurar autenticación en dos pasos	5	5%	17	17%	37	37%	28	28%	13	13%	100%
Prestar atención cuando pidan información personal.	10	10%	11	11%	31	31%	27	27%	21	21%	100%
Aplicaciones de seguridad	4	4%	23	23%	34	34%	22	22%	17	17%	100%
Extensiones del navegador	12	12%	19	0,19	34	34%	25	25%	10	10%	100%

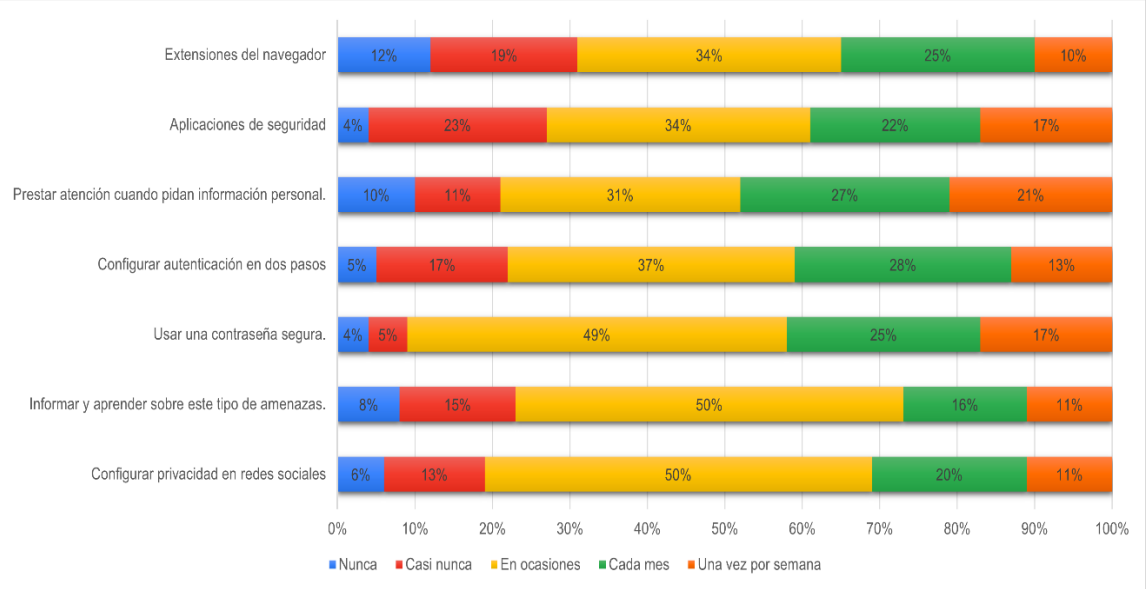

Figura 11. Frecuencia y porcentaje de medidas y técnicas contra ataques de ingeniería social

Análisis e interpretación de resultados

Los datos proporcionados representan la frecuencia con la que las personas toman medidas para proteger su seguridad en línea en diferentes categorías de acciones, desde "Nunca" hasta "Una vez por semana".

- **Configurar privacidad en redes sociales**: La mayoría de las personas (50%) lo hacen "En ocasiones". Un 20% lo hace "Cada mes". El 11% lo hace "Una vez por

semana". La configuración de la privacidad en redes sociales es una práctica común para la mayoría de las personas, aunque no todos la realizan con regularidad.

- **Informar y aprender sobre este tipo de amenazas**: El 50 %personas lo hacen "En ocasiones". Un 16% lo hace "Cada mes". La mitad de las personas se informa sobre amenazas en línea en ocasiones, pero aún hay margen para una mayor concienciación.
- **Usar una contraseña segura:** La mayoría de las personas (49%) lo hacen "En ocasiones". Un 25% lo hace "Cada mes". Utilizar contraseñas seguras es una práctica común para la mayoría de las personas, pero menos personas lo hacen con frecuencia.
- **Configurar autenticación en dos pasos:** La mayoría de las personas (37%) lo hace "En ocasiones". Un 28% lo hace "Cada mes". La autenticación en dos pasos es una medida de seguridad que se utiliza comúnmente, aunque no todos la utilizan con regularidad.
- **Prestar atención cuando pidan información personal:** La mayoría de las personas (31%) lo hace "En ocasiones". La precaución al compartir información personal es una práctica común para muchas personas, pero no todos son consistentes en esta medida.
- **Aplicaciones de seguridad:** El 34% de las personas las utilizan "En ocasiones". El uso de aplicaciones de seguridad es utilizado con regularidad.
- **Extensiones del navegador:** El 34% de las personas las utilizan "En ocasiones". La mayoría de las personas utilizan extensiones del navegador en ocasiones, cada mes o una vez por semana. El uso de extensiones del navegador ayuda a mejorar la seguridad en línea.

En general, los resultados indican que la mayoría de las personas están tomando medidas para proteger su seguridad en línea, pero no todos son consistentes en estas prácticas. Es importante destacar que la seguridad en línea es crucial en la era digital, y se recomienda tomar medidas para protegerse de amenazas cibernéticas.

Pregunta 8: ¿Qué tan importante considera recibir capacitación sobre cómo identificar posibles intentos de ataques de ingeniería social y protegerse de ellos?

Tabla 16. Escala de Likert importancia para la pregunta 8

Opciones	Frecuencia	Porcentaje
Nada Importante	2	2%
Poco Importante	4	4%
Algo Importante	5	5%
Importante	31	31%
Muy Importante	58	58%
Total	100	100%

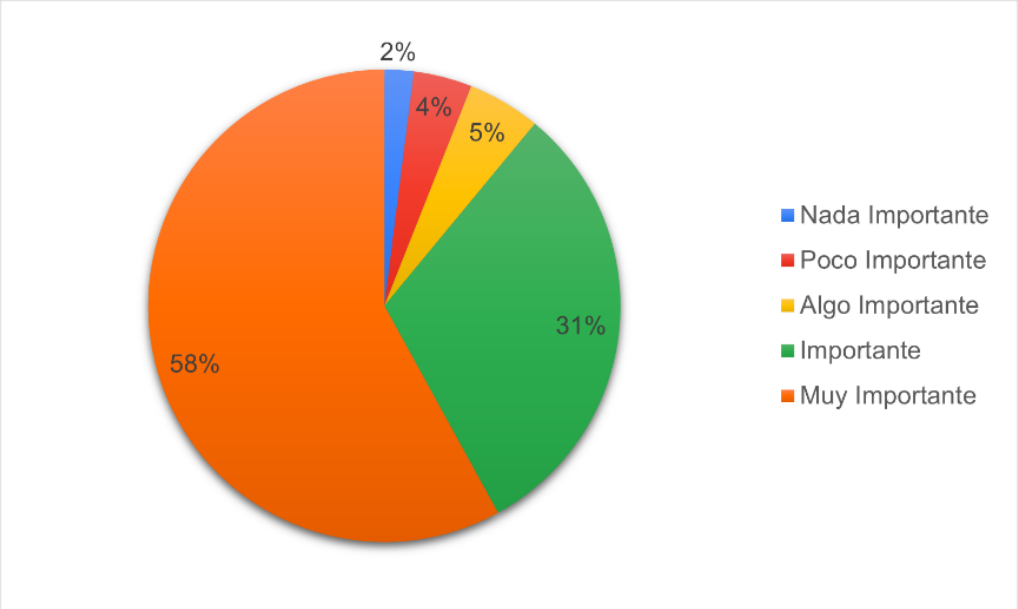

Figura 12. Resultado en porcentaje de la pregunta 8

Análisis e interpretación de resultados

- Muy Importante (58%, 58 personas): La mayoría de las personas encuestadas considera que recibir capacitación es muy importante. Esto indica que la capacitación en seguridad cibernética es de alta importancia para una gran parte de la muestra.
- Importante (31%, 31 personas): Un porcentaje significativo de personas considera que recibir capacitación es importante. Esto sugiere que muchas personas ven la capacitación en seguridad cibernética como una cuestión relevante.

- Algo Importante (5%, 5 personas): Un número ligeramente mayor de personas considera que recibir capacitación es algo importante. Esto indica que algunas personas le dan un grado de importancia, pero no es crítica.
- Poco Importante (4%, 4 personas): Otra minoría considera que recibir capacitación es poco importante. Aunque un poco más que en el primer grupo, sigue siendo un porcentaje bajo.
- Nada Importante (2%, 2 personas): Solo un pequeño porcentaje considera que recibir capacitación en este tema es nada importante. Esto sugiere que un número limitado de personas no valora la capacitación en seguridad cibernética y protección contra ataques de ingeniería social.

La mayoría de las personas encuestadas considera que recibir capacitación sobre cómo identificar posibles intentos de ataques de ingeniería social y protegerse de ellos es muy importante. Esto resalta la concienciación de la importancia de la educación en seguridad cibernética y la protección contra ataques de ingeniería social. Las respuestas nada importante y poco importante son minoritarias, lo que sugiere que la mayoría de las personas valoran la capacitación en este tema.

Pregunta 9: ¿Cuánto confía en su capacidad para evitar intentos de ingeniería social en línea?

Tabla 17. Escala de Likert importancia para la pregunta 9

Opciones	Valor
Pobre	1
Cuestionable	2
Aceptable	3
Buena	4
Excelente	5

Tabla 18. Frecuencia y porcentaje para evitar contra ataques de ingeniería social

	1		2		3		4		5		Total
	f.	%	f.	%	f.	%	f.	%	f.	%	
Phishing	23	23%	41	41%	25	25%	5	5%	6	6%	100%

	f.	%	f.	%	f.	%	f.	%	f.	%	Total
Scareware	24	24%	34	34%	29	29%	11	11%	2	2%	100%
Pharming	25	25%	41	41%	23	23%	9	9%	2	2%	100%
Engaño en Redes Sociales	4	4%	41	41%	31	31%	16	16%	8	8%	100%
Angler-phishing	22	22%	44	44%	23	23%	9	9%	2	2%	100%
Pretexting	21	21%	41	41%	25	25%	11	11%	2	2%	100%
Spear phishing	21	21%	47	47%	21	21%	9	9%	2	2%	100%

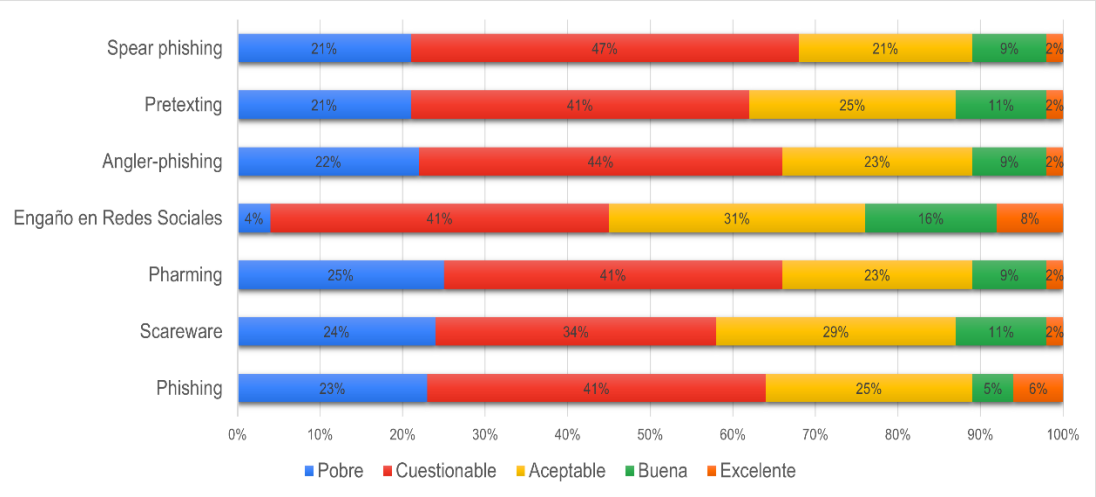

Figura 13. Frecuencia y porcentaje para evitar contra ataques de ingeniería social

Análisis e interpretación de resultados

- Phishing: la mayoría de las personas se sienten cuestionables en su capacidad para evitar el phishing (41%), seguido por un 25% que se siente aceptable.
- Scareware: la mayoría se siente cuestionables (34%) o aceptable (29%) en su capacidad para evitar el Scareware.
- Pharming: las respuestas son bastante variadas, pero la mayoría se siente cuestionables (41%) o aceptable (23%) en su capacidad para evitar el Pharming.
- Engaño en redes sociales: la mayoría se siente cuestionables (41%) en su capacidad para evitar el engaño en redes sociales, seguido por un 31% que se siente aceptable.
- Angler-phishing: la mayoría se siente cuestionables (44%) en su capacidad para evitar el angler-phishing.
- Pretexting: la mayoría se siente cuestionables (41%) o aceptable (25%) en su capacidad para evitar el pretexting.

- Spear phishing: la mayoría se siente cuestionables (47%) en su capacidad para evitar el spear phishing.

Los resultados muestran que la mayoría de las personas se sienten cuestionables o aceptables en su capacidad para evitar diferentes tipos de intentos de ingeniería social en línea. Esto puede reflejar una conciencia de la amenaza, pero también la percepción de que siempre existe un cierto nivel de riesgo. Solo una minoría se siente buena o excelente en su capacidad para evitar estos ataques, lo que indica que hay margen para la mejora en la educación y concienciación en seguridad cibernética.

Pregunta 10: ¿En qué medida los siguientes factores le hacen más propenso hacer clic en un enlace de un mensaje de redes sociales?

Tabla 19. Escala de Likert importancia para la pregunta 10

Opciones	Valor
Nada Propenso	1
Poco Propenso	2
Neutral	3
Propenso	4
Muy Propenso	5

Tabla 20. Frecuencia y porcentaje de factores para hacer clic en un enlace

	1		2		3		4		5		Total
	f.	%	f.	%	f.	%	f.	%	f.	%	
Procede de una fuente conocida o de confianza	21	21%	24	24%	20	20%	29	29%	6	6%	100%
Ofrece un premio o una recompensa atractiva	46	46%	17	17%	10	10%	20	20%	7	7%	100%
Urgente o parece que se estaría perdiendo de algo	35	35%	21	21%	15	15%	23	23%	6	6%	100%
Genera curiosidad o trata temas populares	33	33%	24	24%	14	14%	23	23%	6	6%	100%
Proviene de figuras de autoridad	27	27%	30	30%	16	16%	19	19%	8	8%	100%

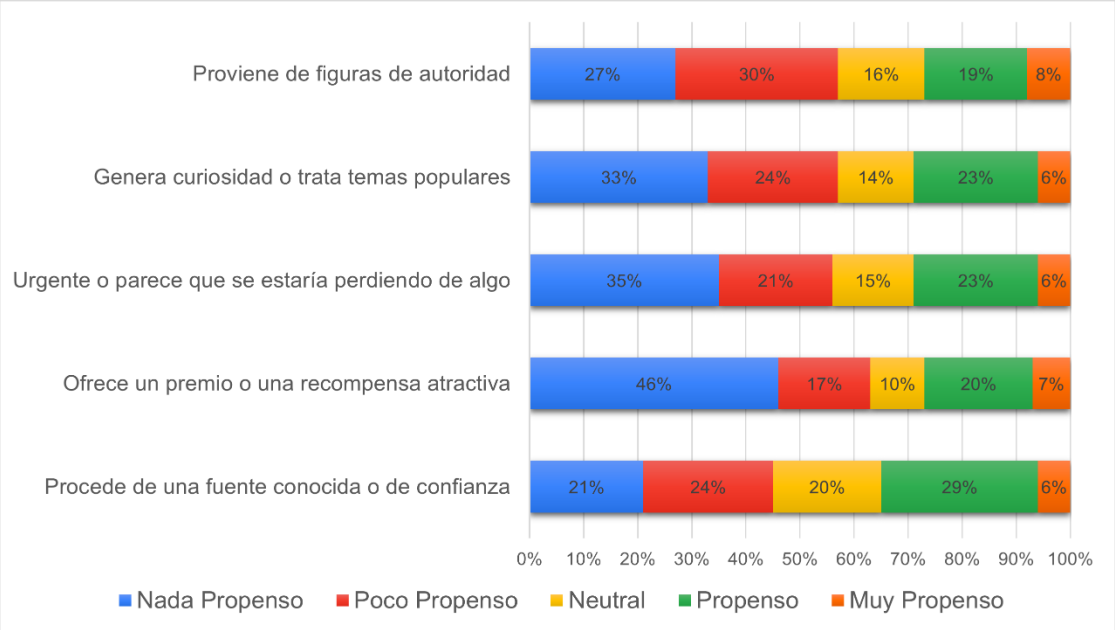

Figura 14. Frecuencia y porcentaje de factores para hacer clic en un enlace

Análisis e interpretación de resultados

- **Procede de una fuente conocida o de confianza:** La mayoría de las personas se siente poco propenso (24%) o nada propenso (21%) a hacer clic en un enlace si proviene de una fuente conocida o de confianza. Esto indica un grado de precaución en cuanto a la procedencia de los enlaces.
- **Ofrece un premio o una recompensa atractiva**: La mayoría de las personas se siente poco propenso (46%) a hacer clic en un enlace si ofrece un premio o una recompensa atractiva, lo que refleja una desconfianza hacia las ofertas de este tipo.
- **Urgente o parece que se estaría perdiendo de algo**: La mayoría de las respuestas están distribuidas entre poco propenso (21%), nada propenso (35%), y neutral (15%). Esto indica que una parte significativa de las personas es cautelosa con los enlaces que parecen urgentes o que insinúan que se perderían algo si no hacen clic.
- **Genera curiosidad o trata temas populares:** La mayoría de las personas se siente poco propenso (24%) o nada propenso (33%) a hacer clic en un enlace si genera curiosidad o trata temas populares. Esto sugiere que, aunque la curiosidad puede ser un factor, muchas personas son cautelosas al respecto.
- **Proviene de figuras de autoridad**: La mayoría de las personas se siente nada propenso (27%) o poco propenso (30%) a hacer clic en un enlace si proviene de

figuras de autoridad. Esto indica una cierta desconfianza en las supuestas figuras de autoridad en las redes sociales.

Los resultados indican que la mayoría de las personas son cautelosas a la hora de hacer clic en enlaces de redes sociales, especialmente si los enlaces prometen premios o recompensas atractivas. Las fuentes conocidas o de confianza pueden influir en cierta medida, pero la desconfianza en general hacia los enlaces sospechosos parece ser común. Esta actitud precautoria es importante para protegerse contra posibles intentos de ingeniería social y ataques en línea.

2.2.4 Procesamiento y análisis de datos

De acuerdo con la encuesta aplicada se determinaron los siguientes aspectos relacionados con el nivel de conocimiento que tiene las personas sobre la detección del Angler-Phishing y la factibilidad de realizar una estrategia de concientización como es la capacitación para el mejor entendimiento sobre la ciberseguridad que conlleva la Ingeniería Social.

- Muy pocas personas no entienden o no se han relacionado con el término de Ingeniería Social o Angler-Phishing por lo que es importante que conozcan que es, en que consiste, y como estos tipos de ataques cuando son exitosos pueden ser perjudiciales en ámbito educativo, como el profesional
- Estos datos reflejan una preocupación por la seguridad en línea y la ingeniería social, así como una actitud cautelosa hacia los mensajes y enlaces recibidos en las redes sociales. La educación en seguridad cibernética es percibida como Muy Importante, y la confianza en la capacidad para evitar ataques de ingeniería social varía en su mayoría por lo que es importante que las personas reciban educación para reducir el temor y preocupación por posibles ataques.
- Una de las Redes Sociales más utilizadas por las personas es WhatsApp como una plataforma esencial para la comunicación diaria, debido a su uso muy frecuente es una aplicación que puede ser utilizada para realizar ataques de ingeniera social.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

3.1.1 Ataques más frecuentes de ingeniería social.

Los datos recopilados sugieren una combinación de tendencias y creencias con respecto a la seguridad en línea, la exposición a la manipulación de las redes sociales y los peligros percibidos al interactuar con material en las redes sociales.

Frecuencia de recepción y uso de redes sociales: Facebook, YouTube y WhatsApp son plataformas populares para la recepción y uso frecuente de noticias. También se utilizan con frecuencia plataformas como Instagram, TikTok y Snapchat.

Experiencia en ingeniería social: casi la mitad de los encuestados han sido víctimas de algún tipo de intento de ingeniería social. Este alto porcentaje indica la prevalencia de estas amenazas en línea.

Importancia de la formación en ciberseguridad: Existe consenso sobre la importancia de la educación para detectar y prevenir ataques de ingeniería social. Estos conocimi entos son importantes para mejorar la concienciación sobre la seguridad en línea.

Factores de riesgo al hacer clic en enlaces: La mayoría de las personas tienden a no c onfiar en enlaces que ofrecen un precio atractivo, tienen inmediatez o provienen de u na fuente desconocida. Esta precaución es positiva porque reduce la exposición a am enazas potenciales.

A continuación, se presenta una tabla donde se realiza un análisis de los ataques de ingeniería social, esto implica comprender las herramientas y técnicas utilizadas por los atacantes para manipular a las personas y obtener información confidencial o acceso no autorizado a sistemas, cunetas bancarias, cuentas de redes sociales entre otros.

Tabla 21. Ataques de ingeniería social

Tipo de ataque	Métodos de utilizados	Nivel de gravedad	Factores de Riesgo	Impacto Potencial
Phishing por email	Correos electrónicos, sitios web falsos.	Alto	Falta de conciencia en seguridad	Pérdida de datos sensibles, acceso no autorizado
Vishing	Llamada telefónica, mensajes de voz engañosos, suplantación de identidad.	Medio	Falta de autenticación sólida	Robo de información personal, acceso no autorizado
Smishing	Mensaje de texto	Medio	Falta de protección telefónica	Divulgación de información confidencial por teléfono
Phishing de pescador	Mensaje directo	Alto	Falta de conciencia en seguridad	Pérdida de datos sensibles, acceso no autorizado
Baiting	Oferta de incentivo	Medio	Falta de protección en navegación	Acceso a sitios falsos, robo de datos sensibles
Pretexting	Creación de historia falsa	Medio	Conexiones inseguras en red	Intercepción de datos sensibles, espionaje
Spear phishing	Correo electrónico personalizado	Alto	Falta de autenticación sólida	Robo de información personal, acceso no autorizado
Whaling	Correo electrónico dirigido a altos ejecutivos	Alto	Falta de actualizaciones y respaldo	Pérdida de datos, daño financiero

De acuerdo con el análisis realizado en la **0,** la ingeniería social es una táctica utilizada por los ciberdelincuentes para manipular psicológicamente a las personas y obtener acceso a información y sistemas confidenciales. Para combatir esta amenaza, es importante comprender las herramientas de ataque utilizadas y tomar las precauciones

adecuadas. Las herramientas de ataque más comunes incluyen phishing, phishing de pescador, vishing y pharming.

Los factores de riesgo asociados con estos ataques suelen ser la falta de conciencia de seguridad, la falta de autenticación sólida, la falta de actualizaciones y la falta de protección al navegar y comunicarse.

El impacto potencial de un ataque de ingeniería social puede ser devastador, incluida la pérdida de datos confidenciales, el acceso no autorizado y el daño económico.

3.1.2 Mentalidad de precaución y monitoreo constante

Al mantener una conciencia constante, se promueve un enfoque proactivo hacia la seguridad digital, donde la educación continua y la adaptación a las amenazas en evolución son cimientos básicos para lograr un enfoque integral que no solo fortalece las defensas individuales, sino que contribuye a la construcción de una comunidad en línea más segura y resiliente.

Tabla 22. Análisis de la mentalidad de precaución y monitoreo constante

Ventajas	Desventajas
• Detección Temprana Al estar alerta y consciente de posibles intentos de fraude, las organizaciones y las personas pueden identificar y abordar rápidamente cualquier actividad sospechosa **[34]**.	• Paranoia Excesiva Una mentalidad excesivamente cautelosa puede llevar a la paranoia, lo que puede afectar la productividad y hacer a las personas desconfiadas.
• Educación y Conciencia Las personas se vuelven más conscientes de los posibles riesgos y son menos propensas a caer en trampas.	• Carga de Trabajo Adicional La necesidad de monitoreo constante puede generar una carga adicional para los equipos de seguridad [14].
• Adaptabilidad A medida que evolucionan las técnicas de fraude, las personas y las organizaciones pueden ajustar sus estrategias de seguridad para abordar las amenazas emergentes **[27].**	• Posibles Falsos Positivos Se puede generar distracciones innecesarias y potencialmente dañar la confianza dentro de una organización [15].

Ventajas	Desventajas
• Prevención Proactiva La identificación temprana de actividades sospechosas puede llevar a la implementación de medidas preventivas antes de que ocurra un fraude **[35]**.	• Costos Financieros La implementación y el mantenimiento de sistemas de monitoreo constante pueden generar costos financieros significativos [36]

La mentalidad de precaución y el monitoreo constante son estrategias importantes para prevenir fraudes de ingeniería social, pero como cualquier enfoque, tienen ventajas y desventajas. Donde lo esencial equilibrarlas con la eficiencia operativa y la necesidad de mantener un ambiente de trabajo saludable para la educación continua y la adaptabilidad son clave para maximizar los beneficios de estas estrategias y mitigar sus posibles desventajas.

3.1.3 Seguridad en línea

La seguridad en línea es una preocupación importante en la era digital, ya que cada vez más aspectos de nuestra vida están conectados a internet por lo cual el uso de las herramientas para la seguridad en línea es muy importante. A continuación, se detallan las más comunes:

Tabla 23. Herramientas para seguridad en línea

Herramienta	Descripción
Contraseñas seguras	Crear contraseñas que sean únicas y difíciles de adivinar, utilizando una combinación de letras mayúsculas y minúsculas, números y caracteres especiales ayuda mejorar el nivel de seguridad
Autenticación de dos factores (2FA)	Es un refuerzo de la capa de seguridad ya que al requerir dos métodos de verificación para acceder a una cuenta al utilizar un código único enviado a tu dispositivo móvil o generado por una aplicación de autenticación hace que sea más difícil para los ciberdelincuentes acceder incluso si obtienen tu contraseña.
Firewall y software antivirus	Un firewall actúa como una barrera entre tu red y posibles amenazas externas, bloqueando el acceso no autorizado y controlando el tráfico.

Herramienta	Descripción
	Complementariamente, un software antivirus protege tu sistema contra programas malignos, virus y otras amenazas detectando, bloqueando o eliminando software malicioso
Redes Wi-Fi seguras	Para prevenir accesos no autorizados y proteger la privacidad de tus datos es necesario evitar conectarse a redes wifi-desconocidas o libres pues estas no suelen encriptar la información y no brindan seguridades de si terceros están accediendo a nuestra información

Las medidas y herramientas que han surgido en los últimos años resaltan con énfasis la naturaleza dinámica y en constante evolución del entorno digital, subrayando la dominante necesidad de poseer una educación en ingeniería social como un medio para mantenerse no solo a la par, sino por delante de los astutos delincuentes cibernéticos [37]

3.1.4 Simulaciones de Phishing y Pruebas de Seguridad

La convergencia de simulaciones de phishing, pruebas de seguridad y programas de concientización representa de manera significativa una postura de seguridad en la cual se ofrece un vistazo práctico para la capacidad de identificar y resistir ataques cibernéticos, mientras que las pruebas de seguridad desentrañan vulnerabilidades sistémicas, permitiendo una corrección precisa en las cuales estos esfuerzos se ven respaldados por programas de concientización sobre las últimas amenazas y mejores prácticas de seguridad, que fortalecen la primera línea de defensa [38].

Las simulaciones de phishing y las pruebas de seguridad son componentes notables de una estrategia integral de ciberseguridad pues estas prácticas ayudan a evaluar la preparación frente a posibles amenazas. Al combinar simulaciones de phishing con pruebas de seguridad exhaustivas, se puede identificar posibles puntos de vulnerabilidad y mejorar la capacidad de respuesta ante posibles amenazas cibernéticas o ataques. En última instancia, estas prácticas contribuyen a fortalecer la postura de seguridad y respuesta de las personas en un entorno digital en constante evolución.

Tabla 24. Análisis de factores de simulación y pruebas seguridad

Factores	Descripción
Simulaciones de Phishing	Evaluar la capacidad de los empleados para reconocer y resistir ataques de phishing.
	Enviar correos electrónicos simulados que imitan posibles ataques de phishing para medir la tasa de clics y evaluar la conciencia de seguridad.
Concientización del Personal	Educar a los empleados sobre las amenazas de seguridad y las mejores prácticas.
	Realizar sesiones de capacitación regulares para sensibilizar al personal sobre los riesgos y las tácticas utilizadas por los atacantes.
Informes y Retroalimentación	Proporcionar informes detallados sobre los resultados de las simulaciones y pruebas de seguridad.
	Desarrollar informes que destaquen las áreas de mejora, los éxitos y proporciona recomendaciones específicas para fortalecer la postura de seguridad.
Participación de expertos	Involucrar a expertos externos para obtener una evaluación imparcial de la seguridad.
	Contratar servicios de empresas de seguridad especializadas para realizar auditorías y pruebas de seguridad independientes.
Seguimiento de Indicadores de Compromiso (IoC)	Monitorear continuamente los IoC para detectar actividad maliciosa.
	Utilizar herramientas de monitoreo de seguridad y análisis de registros para identificar posibles amenazas en tiempo real

La mitigación efectiva de fraudes de ingeniería social implica una combinación de tecnología avanzada, políticas claras y una cultura de seguridad arraigada en la educación y la colaboración continua a través de la cual mitigar fraudes de ingeniería social que requiere de la implementación de estrategias sólidas que aborden tanto los aspectos técnicos como los comportamentales de la seguridad digital.

3.1.5 Análisis de estrategias para mitigar fraudes

Tabla 25. Estrategias para mitigación de fraudes

Estrategias	Análisis	Beneficios
Concientización y Educación	Una comprensión profunda de las tácticas de ingeniería social es esencial. La educación y la concientización regular pueden ayudar a los usuarios a reconocer señales de alerta y a tomar decisiones informadas	Reducción de la probabilidad de caer en trampas de ingeniería social, fortalecimiento de la cultura de seguridad y creación de una línea de defensa más sólida desde el nivel de usuario.
Simulaciones de Phishing y Pruebas de Seguridad	Realizar simulaciones de ataques de phishing ayuda a evaluar la preparación de los empleados frente a amenazas reales. Las pruebas regulares de seguridad identifican vulnerabilidades en la infraestructura.	Identificación temprana de debilidades en la seguridad, mejora de las políticas y procedimientos de respuesta a incidentes.
Actualizaciones y Parches de Seguridad	Mantener sistemas y software actualizados es crucial para cerrar vulnerabilidades conocidas	Reducción del riesgo de explotación de vulnerabilidades, mejora de la resistencia ante amenazas comunes.
Colaboración y Compartición de Información	Fomentar la colaboración entre organizaciones y la compartición de información sobre amenazas puede fortalecer las defensas colectivas.	Mayor conocimiento de las tácticas de ingeniería social, posibilidad de anticipar y prevenir amenazas compartidas
Implementación de Tecnologías de Seguridad Avanzadas	El uso de tecnologías como inteligencia artificial, análisis de comportamiento y sistemas de prevención de intrusiones puede elevar las defensas contra ataques sofisticados.	Mayor capacidad para detectar y mitigar amenazas avanzadas, reducción del riesgo de éxito de ataques de ingeniería social

Una estrategia integral para fortalecer la concientización y preparación frente a amenazas cibernéticas, especialmente angler phishing, se basaría en la combinación de concientización y simulaciones interactivas. Dado que el 58% de las personas encuestadas considera la capacitación como muy importante, por lo cual se define la estrategia, implementar un programa de concientización que incluya sesiones educativas interactivas sobre la identificación de ataques de angler phishing. Esta estrategia no solo elevaría la conciencia general sobre la ciberseguridad, sino que también brindaría a los usuarios la experiencia práctica necesaria para reconocer y evitar posibles amenazas en el futuro. Además, la recopilación de datos de las simulaciones permitiría evaluar el nivel de preparación de la organización y ajustar las iniciativas de concientización según sea necesario.

3.1.6 Selección de instrumentos y servicios TI

a. Servicio virtualizado

Los servicios virtualizados en la nube son aquellos que permiten crear y gestionar máquinas virtuales (VM) en un entorno de nube, ofreciendo recursos informáticos flexibles y escalables según las necesidades de los usuarios. Algunos de los principales proveedores de servicios virtualizados en la nube son Google Cloud Platform (GCP), DigitalOcean y Amazon Web Services (AWS).

A continuación, se presenta un cuadro comparativo entre estos tres proveedores, basado en algunos criterios como el precio, el rendimiento, la disponibilidad, la facilidad de uso y el soporte.

Tabla 26. Análisis comparativo de servicios virtualizados.

Criterio	GCP	Digitalicen	AWS
Precio	Plan gratuito con una VM f1-micro y un crédito de $300 para nuevos usuarios. El precio de las VM varía según la región, el tipo y el uso [39].	Plan gratuito con una VM básica y un crédito de $100 para nuevos usuarios. El precio de las VM es fijo y depende del tamaño y las características.	plan gratuito con una VM t2. Micro y un crédito de $100 para nuevos usuarios. El precio de las VM varía según la región, el tipo y el uso [40]

Rendimiento	Alto rendimiento y velocidad, con una infraestructura global y una red de fibra óptica [35].	Buen rendimiento y velocidad, con una infraestructura distribuida y una red de baja latencia [40].	Gran rendimiento y velocidad, con una infraestructura robusta y una red de alta disponibilidad [40].
Disponibilidad	Alta disponibilidad y fiabilidad, con una garantía de nivel de servicio (SLA) del 99.99% para las VM [35].	Buena disponibilidad y fiabilidad, con una garantía de nivel de servicio (SLA) del 99.99% para las VM.	Excelente disponibilidad y fiabilidad, con una garantía de nivel de servicio (SLA) del 99.99% para las VM.
Facilidad de uso	Ofrece una interfaz de usuario intuitiva y amigable, con una	Ofrece una interfaz de usuario simple y clara, con un panel de control	Ofrece una interfaz de usuario compleja y avanzada, con una consola web y una
Criterio	**GCP**	**Digitalicen**	**AWS**
	consola web y una línea de comandos.	y una línea de comandos [35].	línea de comandos [40].
Soporte	Ofrece un soporte técnico y de atención al cliente, con diferentes planes y opciones según el nivel de servicio [40].	Ofrece un soporte técnico y de atención al cliente, con un plan básico gratuito y planes premium de pago según el nivel de servicio [35].	Ofrece un soporte técnico y de atención al cliente, con diferentes planes y opciones según el nivel de servicio [40].

Para el presente proyecto se eligió la Plataforma GCP, ya que es una excelente opción para servidores en la nube. Esta solución facilita el lanzamiento y la ampliación a medida que el proyecto crece ya que es un software escalable.

b. Distribuciones GNU/Linux

Los sistemas operacionales basados en Linux son aquellos que utilizan el núcleo de Linux, un software libre y de código abierto que gestiona los recursos del hardware y las interacciones con el usuario. Existen muchas distribuciones o variantes de Linux, que se diferencian en aspectos como la interfaz gráfica, el gestor de paquetes, el

software incluido y el soporte técnico. Algunas de las distribuciones más populares son Ubuntu, Fedora, Debian, CentOS y Red Hat [41] [42].

Tabla 27. Análisis Comparativo de los Sistemas Operacionales basados en Linux

Distribución	Base	Entorno de escritorio	Gestor de paquetes	Software	Soporte
Ubuntu	Debian	GNOME, KDE, XFCE, entre otros	APT, Snap	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
Fedora	Independiente	GNOME, KDE, XFCE, entre otros	DNF, RPM	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
Distribución	**Base**	**Entorno de escritorio**	**Gestor de paquetes**	**Software**	**Soporte**
Debian	Independiente	GNOME, KDE, XFCE, entre otros	APT, DPKG	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
CentOS	Red Hat	GNOME, KDE, XFCE, entre otros	YUM, RPM	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
AlmaLinux	Red Hat	GNOME, KDE, XFCE, entre otros	YUM, RPM	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
Rocky Linux	Red Hat	GNOME, KDE, XFCE, entre otros	YUM, RPM	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, comunidad, foros
Red Hat	Independiente	GNOME, KDE, XFCE, entre otros	YUM, RPM	LibreOffice, Firefox, Thunderbird, entre otros	Oficial, pago, foros

Después de comparar las distintas distros de Linux en una variedad de factores, se puede concluir que para el levantamiento de servidores según el tipo de necesidad de este proyecto se va a trabajar con un clon Red Hat que es Rocky Linux.

c. Hosting web

Un hosting o alojamiento web es un servicio que proporciona un espacio en un servidor para almacenar los archivos y datos de un sitio web, y hacerlos accesibles a través de Internet. Existen muchos proveedores de hosting que ofrecen diferentes planes y características según las necesidad de cada proyecto web [43].

A continuación, se presenta un cuadro comparativo de los hostings más usados en la actualidad, basado en algunos criterios como el precio, el rendimiento, la disponibilidad, la facilidad de uso y el soporte.

Tabla 28. Hostings más usados en la actualidad

Hosting	Precio	Rendimiento	Disponibilidad	Facilidad de uso	Soporte
Hostinger	Desde $1.49/mes	Alto, utiliza la tecnología LiteSpeed	99.99% de uptime garantizado	Fácil, cuenta con un panel de control patentado	24/7 vía chat, email y teléfono
Acens	Desde $4.39/mes	Bueno, incluye herramienta de auto instalación	99.99% de uptime garantizado	Fácil, cuenta con una interfaz intuitiva y amigable	24/7 vía chat, email y teléfono
Raiola Networks	Desde $5.95/mes	Bueno, ofrece discos SSD NVMe	99.99% de uptime garantizado	Fácil, cuenta con cPanel y Softaculous	24/7 vía chat, email y teléfono
Dinahosting	Desde $3.57/mes	Bueno, ofrece discos SSD	99.99% de uptime garantizado	Fácil, cuenta con cPanel y Softaculous	24/7 vía chat, email y teléfono
Loading	Desde $3.99/mes	Alto, ofrece discos SSD NVMe	99.99% de uptime garantizado	Fácil, cuenta con cPanel y Softaculous	24/7 vía chat, email y teléfono
Arsys	Desde $2/mes	Bueno, ofrece discos SSD	99.99% de uptime garantizado	Fácil, cuenta con cPanel y Softaculous	24/7 vía chat, email y teléfono

Para el presente proyecto se utilizó Hostinger porque tiene un excelente rendimiento a un bajo costo. Se compró el dominio cursophiser.tech.

d. Plataformas de aprendizaje

Las plataformas de aprendizaje LMS (Learning Management System) de código abierto son aquellas que permiten crear y gestionar cursos virtuales, utilizando un software libre y modificable. Algunas de las ventajas de estas plataformas son su bajo costo, su flexibilidad, su personalización y su comunidad de usuarios y desarrolladores [44] [45].

A continuación, se presenta un cuadro comparativo de algunas de las plataformas LMS de código abierto más populares y usadas en la actualidad, basado en algunos criterios como el precio, el rendimiento, la disponibilidad, la facilidad de uso y el soporte [46] [47] .

Tabla 29. Análisis de plataformas de aprendizaje LMS.

Plataforma	Precio	Rendimiento	Disponibilidad	Facilidad de uso	Soporte
Moodle	Gratis, se paga por el hosting y el dominio	Alto, utiliza la tecnología LiteSpeed	99.99% de uptime garantizado	Fácil, cuenta con una interfaz intuitiva y amigable	Oficial, comunidad, foros
Chamilo	Gratis, se paga por el hosting y el dominio	Bueno, ofrece discos SSD	99.99% de uptime garantizado	Fácil, cuenta con una interfaz simple y clara	Oficial, comunidad, foros
Canvas	Gratis, se paga por el hosting y el dominio	Alto, ofrece discos SSD y caché	99.99% de uptime garantizado	Fácil, cuenta con un panel de control propio	Oficial, comunidad, foros
Open edX	Gratis, se paga por el hosting y el dominio	Alto, ofrece discos SSD y caché	99.99% de uptime garantizado	Medio, cuenta con una interfaz compleja y avanzada	Oficial, comunidad, foros
Sakai	Gratis, se paga por el hosting y el dominio	Bueno, ofrece discos SSD	99.99% de uptime garantizado	Medio, cuenta con una interfaz compleja y avanzada	Oficial, comunidad, foros

Después de comparar varias plataformas LMS se escogió a moodle para utilizarla en el presente proyecto como herramienta para realizar un curso de capacitación sobre angler phishing.

e. Inteligencia Artificial

La inteligencia artificial (IA) es una rama de la informática que se ocupa de crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento, la percepción o la toma de decisiones [48].

La IA puede aplicarse a la educación y la capacitación de usuarios sobre angler phishing, que es una técnica de ingeniería social que consiste en suplantar la identidad de una entidad legítima, como una empresa, una organización o una persona, a través de las redes sociales, con el fin de engañar a los usuarios y obtener información personal, financiera o de acceso [49].

Aplicaciones de la IA para la educación y la capacitación de usuarios sobre angler phishing:

- Crear sistemas de detección y prevención de angler phishing, que puedan identificar y bloquear los perfiles falsos, los mensajes sospechosos y los enlaces maliciosos que usan los atacantes, y alertar a los usuarios sobre los posibles intentos de estafa [50].
- Crear sistemas de simulación y entrenamiento de angler phishing, que puedan generar escenarios realistas y personalizados para que los usuarios puedan practicar sus habilidades de seguridad, reconocer y evitar los ataques, y aprender de sus errores [51].
- Crear sistemas de evaluación y retroalimentación de angler phishing, que puedan medir el nivel de conocimiento, conciencia y comportamiento de los usuarios frente a los ataques, y proporcionarles consejos y recomendaciones para mejorar su seguridad.

En el ámbito de la educación y el desarrollo, las herramientas de tecnología de la información (TI) son recursos que facilitan la creación, el acceso, el almacenamiento y el procesamiento de información digital. Estas herramientas pueden tener distintas funciones y características, según el tipo de actividad que se quiera realizar. Después

de comparar distintos métodos, procesos, acciones y mediante una investigación bibliográfica se escogieron varios instrumentos que fueron seleccionados por sus características que ayudarán a resolver la problemática planteada y cumpliendo con el objetivo propuesto, a continuación, se presentan las herramientas seleccionadas que se van a utilizar:

Tabla 30. Herramientas TI seleccionadas para el proyecto

Herramienta	**Descripción**	**Nombre/Versión**
Moodle	Una plataforma de educación virtual que ofrece múltiples herramientas para la formación en línea, como tareas, foros, cuestionarios y recursos.	Moodle 3.4
Servidor en la nube GCP	Un servicio de Google Cloud Platform que permite alojar aplicaciones web, bases de datos, almacenamiento y otros recursos en la nube.	Google Cloud Platform
Hosting	Un servicio que proporciona espacio en un servidor para almacenar y publicar sitios web.	Hostinger
IA	La inteligencia artificial es la disciplina que estudia cómo crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de imágenes, el procesamiento de lenguaje natural o el aprendizaje automático.	Chat GPT Bing IA

En este trabajo se realizará cuatro simulaciones de ataque mediante una clonación de páginas que estarán dentro de una plataforma moodle, estas se integran a un curso de capacitación para evaluar las reacciones de las personas ante estas páginas clonas. Estos servicios estarán alojados en un servidor de Google Cloud Platform y se podrán acceder desde el internet a través de un dominio llamado cursophisher.tech.

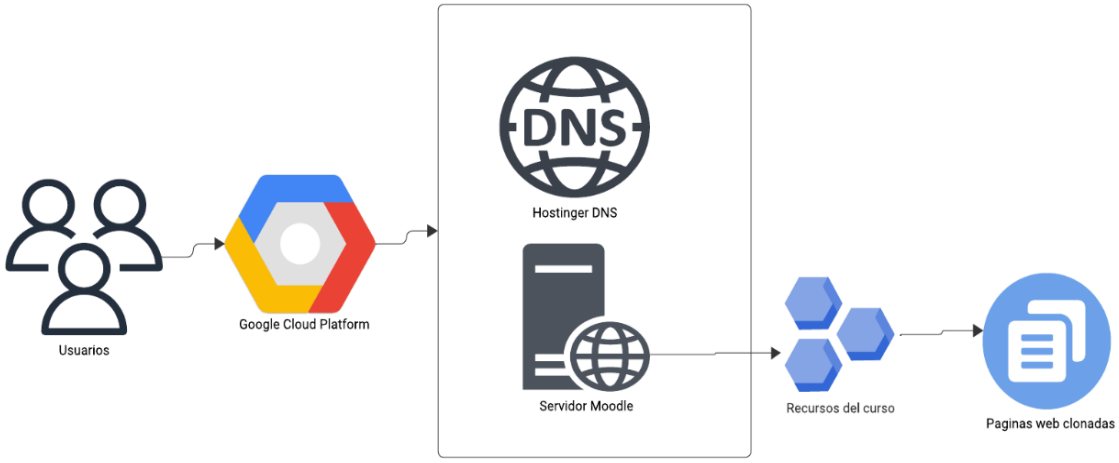

Figura 15. Diagrama de servicio virtualizo para moodle

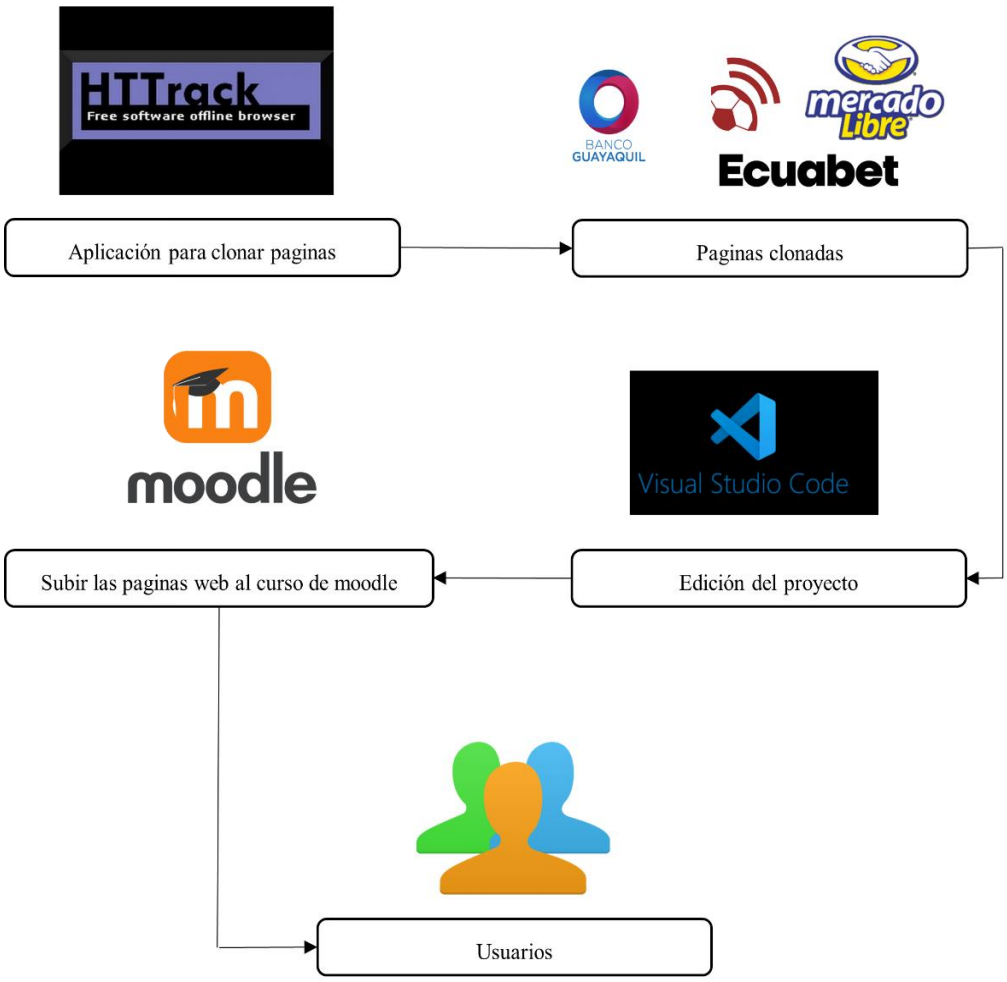

Figura 16. Esquema de simulación

f. Respaldo legal

Para encasillar a la simulación de ataque Angler Phishing dentro de los parámetros de legalidad o ilegalidad hay que tener claro dos conceptos primordiales: delito y hacking ético.

Según la legislación ecuatoriana un delito es una acción antijurídica, culpable o dolosa que es sancionada con una pena [52]. Ahora bien, un hackeo ético se lo puede definir como el análisis de vulnerabilidades con el único propósito de favorecer y prevenir ataques malintencionados.

Una vez aclarada la definición de delito y hackeo ético; la simulación de ataque Phishing para este estudio hace parte de un hackeo ético y no se encuentra penado por la ley ecuatoriana, la cual es muy relevante en cuanto a intrusiones y robo de información usando herramientas como pharming, Phishing, tapering, entre muchas otras, sancionando así el hecho de robar información, estafar al cliente y romper seguridades causando perjuicio a la víctima [53]

En definitiva, la constitución ecuatoriana no contempla la posibilidad de que alguien haga uso de herramientas diseñadas en gran porcentaje, para explotar las vulnerabilidades, en beneficio de los sistemas de destino, transformando las mismas herramientas en parte de la solución y no del problema [53].

g. Compromiso Ético

El presente trabajo de integración curricular documenta el siguiente compromiso: Toda la información recolectada será usada con fines estrictamente académicos, será cuidadosamente custodiada, anonimizada dentro del proyecto de investigación. Los datos originales se destruirán una vez procesados.

3.1.7 Metodologías para seguridad informática

Para el desarrollo de la propuesta, es esencial elegir la metodología que se utilizará, la cual nos permita realizar los procesos y tareas de forma ágil y eficiente, se procede a realizar un cuadro comparativo entre las metodologías: Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST) y Penetration Testing Execution Standard (PTES).

Tabla 31. Metodologías para seguridad informática

Metodología	Enfoque	Alcance	Proceso
OSSTMM	Medir la seguridad operacional, evitando suposiciones y evidencias anecdóticas [54].	Seguridad de las personas, física, inalámbrica, de las comunicaciones y de las redes de datos [54] .	Se divide en cinco fases: definición, enumeración, análisis, verificación y reporte [54] .
OWASP	Identificar y mitigar los riesgos más comunes y críticos de las aplicaciones web, siguiendo una guía de buenas prácticas y estándares [55].	Seguridad de las aplicaciones web, incluyendo aspectos como la autenticación, la autorización, la sesión, la entrada, la salida, la criptografía, la lógica de	Se divide en cuatro fases: planificación, descubrimiento, ataque y reporte [55].
Metodología	**Enfoque**	**Alcance**	**Proceso**
		negocio y la configuración [55].	
NIST	Evaluar y mejorar la gestión de la seguridad de los sistemas de información, siguiendo un marco de referencia y un ciclo de vida [56].	Seguridad de los sistemas de información, incluyendo aspectos como la identificación, la protección, la detección, la respuesta y la recuperación [56].	Se divide en siete fases: planificación, exploración, examen, análisis, explotación, post-explotación y reporte [56].
PTES	Simular ataques reales a los sistemas, siguiendo un proceso estructurado y documentado [57].	Seguridad de los sistemas, incluyendo aspectos como la inteligencia, el modelado de amenazas, la vulnerabilidad, el análisis, la explotación y el reporte [57].	Se divide en siete fases: pre-interacción, inteligencia, modelado de amenazas, análisis de vulnerabilidad, explotación, post-explotación y reporte [57].

Mediante el análisis realizado en la Tabla 31, de las metodologías para realizar pruebas de seguridad, se eligió a la metodología OSSTMM considerando sus beneficios y características con lo cual ayuda a cumplir con los requerimientos y funcionalidades del desarrollo de la estrategia.

3.2 Desarrollo de la propuesta

Para el desarrollo del proyecto se aplicarán 4 fases que posee la metodología OSSTMM (Open Source Security Testing Methodology Manual) es un conjunto de

procedimientos para realizar pruebas de seguridad exhaustivas y precisas en diferentes canales, como redes, aplicaciones, personas, procesos, entre otros [58].

3.2.1 Metodología OSSTMM

Para realizar una estrategia una estrategia para prevenir y reducir la incidencia de fraudes de Angler-Phishing basados en Ingeniería Social que es una forma de phishing que utiliza las redes sociales para engañar a las víctimas, se debe adaptar las siguientes fases de la metodología OSSTMM:

- Fase de inducción: En esta fase, se debe definir el alcance, los objetivos, las limitaciones y el tipo de prueba que se va a realizar. También se debe revisar la cultura, las normas, las políticas y la legislación aplicables a la entidad que se va a auditar [58].
- Fase de interacción: En esta fase, se debe determinar los puntos de acceso, la visibilidad y la confianza de los objetivos dentro del alcance. Se debe medir la amplitud y la profundidad de la interacción, la autenticación y la respuesta de los objetivos [58].
- Fase indagatoria: En esta fase, se debe analizar la información obtenida en la fase anterior, identificar las vulnerabilidades, los riesgos y las amenazas, y evaluar el nivel de seguridad operativa de los objetivos. Se debe utilizar el análisis de confianza y el pensamiento crítico de seguridad para validar los hallazgos [58].
- Fase de intervención: En esta fase, se debe reportar los resultados de la auditoría, proponer las medidas de mitigación y prevención, y realizar un seguimiento de la implementación de las recomendaciones. Se debe incluir una capacitación para concienciar y educar a los usuarios sobre los riesgos y las buenas prácticas de seguridad [58].

3.2.2 Fase de Inducción

a. Evaluación del Conocimiento y Concientización Actual:

- **Encuestas y Entrevistas:** Se realizó una encuesta al público en general para evaluar su nivel de conocimiento sobre Angler-Phishing e Ingeniería Social.

Resultados:

La información de la encuesta aplicada esta detallada en el Capítulo II punto 2.2.4 donde se explica los resultados obtenidos sobre el conocimiento actual de las personas en relación con los riesgos de Angler-Phishing y la Ingeniería Social.

b. Diseño del Curso de Capacitación en Moodle:

- **Identificación de Contenidos Clave:** Determinar los temas críticos a abordar en el curso, incluyendo conceptos de Ingeniería Social, tácticas de Angler-Phishing y buenas prácticas de seguridad.

Tabla 32. Contenidos clave para el curso de Angler-Phishing

Módulo	Tema	Contenido Clave
Módulo 1	Introducción a Angler-Phishing	- Definición de Angler-Phishing y sus variantes. - Impacto y consecuencias de los ataques de phishing.
Módulo 2	Ingeniería Social	- Fundamentos de Ingeniería Social. - Psicología detrás de los ataques de phishing.
Módulo 3	Identificación de Angler-Phishing	- Características comunes de angler-phishing. - Reconocimiento de enlaces maliciosos y adjuntos.
Módulo 4	Herramientas TI	- Implementación de simulaciones de angler phishing.
Módulo 5	Evaluación y Mejora Continua	- Retroalimentación y actualización de contenidos.

En la Tabla 32 se proporciona un marco para identificar y priorizar las necesidades de capacitación relacionadas con la prevención de ataques de Ingeniería Social. La información recopilada es esencial para desarrollar un programa de capacitación efectivo y adaptado a las circunstancias específicas.

- **Desarrollo de Materiales:** Crear materiales de capacitación efectivos, que pueden incluir módulos interactivos, presentaciones y casos de estudio.

Tabla 33. Materiales de los módulos del curso

Módulo	Material
Módulo 1	- Documento descargable con definiciones clave y estadísticas relevantes.
Módulo 2	- Infografía que explique los conceptos básicos de la Ingeniería Social de manera visual y fácil de entender. - Ejemplos prácticos de situaciones de Ingeniería Social.
Módulo 3	- Video tutorial sobre cómo identificar elementos sospechosos en correos electrónicos. - Escenarios de simulación interactiva para practicar la identificación de amenazas.
Módulo 4	- Demostración práctica en video sobre el uso de herramientas TI específicas.
Módulo 5	- Gráficos y tablas interactivas que presenten métricas de seguridad.

En la Tabla 33 se proporciona una estructura para el desarrollo de materiales que incorporan diversos formatos multimedia para mantener la participación y la retención del conocimiento entre los participantes del curso. La combinación de videos, documentos descargables y actividades prácticas contribuirá a una experiencia de aprendizaje completa y efectiva. Todos los materiales que contiene el curso se detallan en el (Anexo A.).

- **Configuración del Curso en Moodle:** Establecer un curso en la plataforma Moodle.

Tabla 34. Aspectos de configuración del curso en moodle

Aspecto de Configuración	Detalles
Configuración General	- Título del curso: “Capacitación de Angler-Phishing”.
	- Duración estimada: Periodo sugerido para completar.
	- Fecha de inicio y finalización del curso.
Acceso al Curso	- Restringir acceso: Solo personal autorizado.
	- Método de inscripción: Aprobación manual.
Formato del Curso	- Formato: Por módulos.
	- Navegación: Libre.
Recursos y Actividades	- Documentos descargables: PDF, videos, infografías.
	- Foros de discusión: Para preguntas y discusiones.
	- Evaluaciones: Cuestionarios al final de cada módulo.
Evaluación y Calificación	- Ponderación de evaluaciones y participación.
	- Notificaciones automáticas de calificaciones.

Comunicación	- Anuncios: Información importante y actualizaciones.
Soporte Técnico	- Contacto de soporte técnico y política de respuesta.
	- Enlaces a recursos de ayuda en Moodle.
Seguridad	- Restricciones de acceso a materiales sensibles.
	- Copias de seguridad regulares del contenido del curso.
Participantes	- Lista de participantes y roles asignados.
	- Monitoreo de participación y progreso.
Foros y Colaboración	- Moderación de foros para un ambiente seguro.
	- Grupos de discusión para colaboración.
Informes y Analíticas	- Estadísticas de participación y calificación.
	- Reportes automáticos de actividad del curso.

Todos los aspectos de la configuración del curso en la plataforma moodle se puede visualizar en el Anexo C.

3.2.3 Fase Indagatoria

a. Diseño del Curso en Moodle:

- **Definición de Objetivos de Aprendizaje:** Establecer claramente los objetivos de aprendizaje del curso en relación con la prevención de Angler-Phishing.

Tabla 35. Objetivos de aprendizaje de los módulos del curso

Módulo o Tema	Objetivo de Aprendizaje
Introducción a Angler Phishing	Comprender qué es Angler Phishing y sus principales características.
Tipos de Ataques	Identificar diferentes tipos de ataques de Angler Phishing y sus métodos asociados.
Técnicas de Ingeniería Social	Comprender las tácticas utilizadas en Ingeniería Social para engañar a los usuarios.
Simulaciones Angler-Phishing	Participar en simulaciones para poner en práctica la detección y prevención.
Evaluación y Medición del Aprendizaje	Demostrar la capacidad de aplicar conocimientos mediante evaluaciones y pruebas prácticas.

- **Creación de Contenidos de Capacitación:** Desarrollar módulos de capacitación específicos para abordar las brechas de conocimiento identificadas durante la indagación.

Tabla 36. Esquema de curso de capacitación en moodle

Módulo	Tema	Contenido
Módulo 1	Introducción a Angler-Phishing	- Definición de Angler-Phishing
		- Ejemplos de ataques exitosos
Módulo 2	Ingeniería Social	- Conceptos básicos de Ingeniería Social
		- Técnicas comunes utilizadas por los atacantes
Módulo 3	Identificación de Angler-Phishing	- Ejercicios prácticos de retroalimentación
Módulo 4	Escenarios simulados	- Descripción y uso de casos de estudio con escenarios simulados
		- Simulaciones de páginas clonas.
Módulo 5	Evaluación y Mejora Continua	- Monitoreo de métricas y seguimiento de curso
		- Retroalimentación y actualización del curso

3.2.4 Fase de Intervención

a. Desarrollo e Implementación del Curso en Moodle

- **Creación del Curso en Moodle:**

  Configurar un servidor con Rocky Linux en Google Cloud Platform (GCP) e instalar Moodle con MariaDB implica varios pasos. A continuación, se describen los pasos que se utilizó para lograr esto:

  Nota: Antes de comenzar, hay que tener una cuenta en Google Cloud Platform y haber creado un proyecto.

1. Crear una instancia de Máquina Virtual (MV) en GCP con Rocky Linux:

- Acceder al [Google Cloud Console](https://console.cloud.google.com/).
- Seleccionar el proyecto con el que se va a trabajar.
- Dirigirse a “Compute Engine" y luego a "Instancias de MV".
- Hacer clic en "Crear instancia".
- Configurar la instancia con el nombre, región, y configuración que desees.
- Seleccionar "Rocky Linux" como imagen del sistema operativo.

- Configurar el tamaño de la instancia y otras opciones según tus necesidades.
- Permitir el tráfico HTTP/HTTPS en la configuración del firewall.

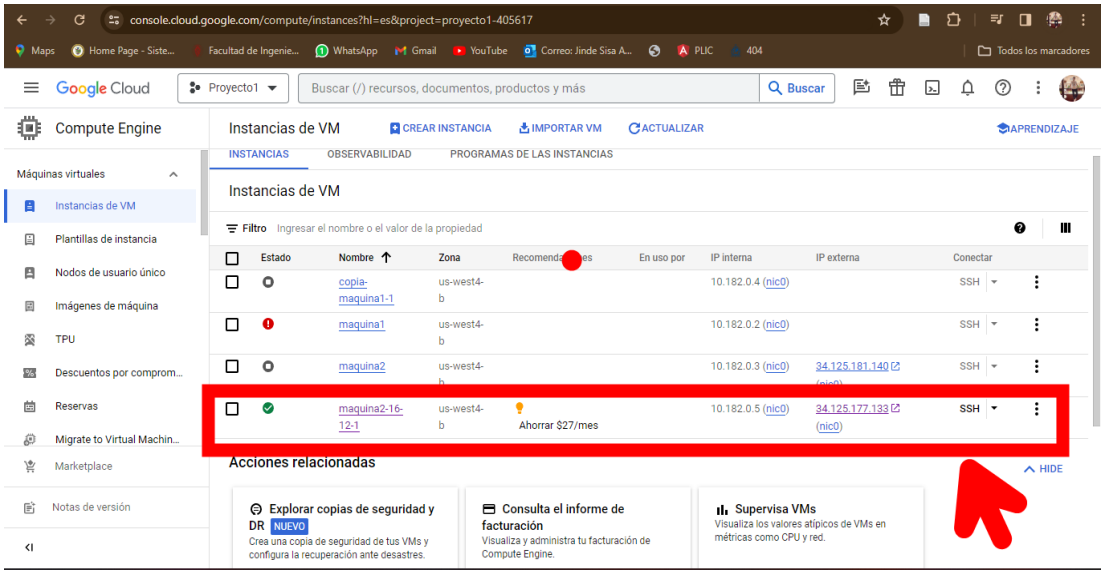

Figura 17. Instancia de MV creada

2. Conectarse a la instancia de Rocky Linux:

- Utilizar SSH para conectarse a la instancia de VM de Rocky Linux.

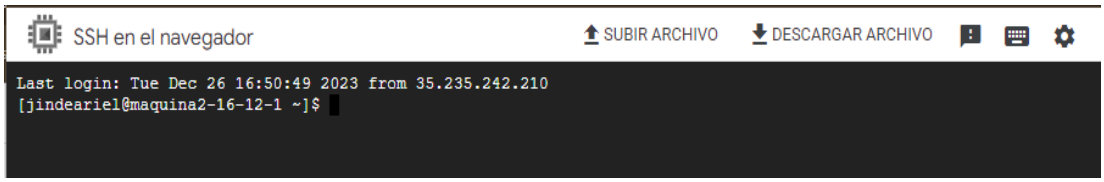

Figura 18. Conexión SHH a MV

3. Instalar y configurar MariaDB:

- Actualizar el sistema:

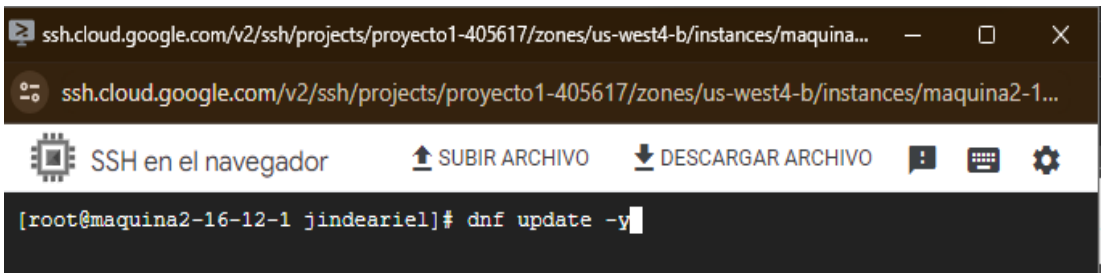

Figura 19. Comando actualizar la MV

- Instalar MariaDB:

Figura 20. Comando para instalar el servidor de base de datos

- Iniciar el servicio y habilitar el inicio automático:

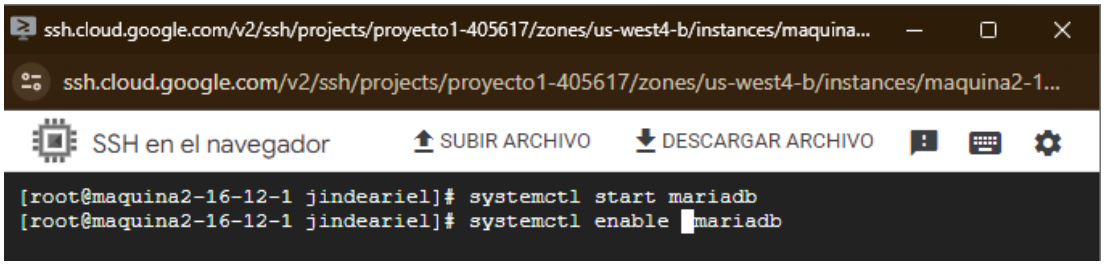

Figura 21. Comandos para iniciar y habilitar el servidor de base de datos

- Ejecutar el script de seguridad de MariaDB para configurar opciones de seguridad:

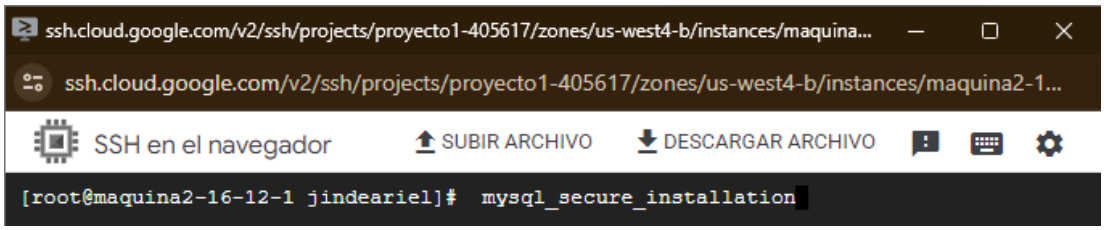

Figura 22. Configuración de seguridad de MariaDB

4. Instalar y configurar Moodle:

- Descargar Moodle:

Figura 23. Comando para instalar moodle con wget

- Extraer el archivo y mover al directorio de tu elección:

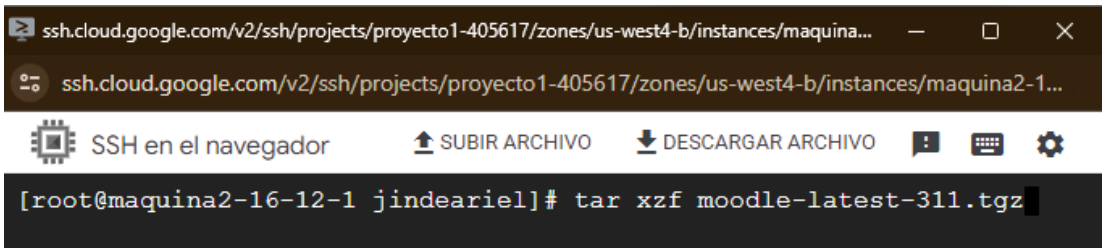

Figura 24. Extracción del archivo con el comando tar.

- Crear una base de datos y un usuario para Moodle en MariaDB:

```
sudo mysql -u root -p

CREATE DATABASE moodle DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'moodleuser'@'localhost' IDENTIFIED BY 'tu_contrasena';
GRANT ALL PRIVILEGES ON moodle.* TO 'moodleuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Figura 25. Creación de base de datos y usuario con privilegios.

- Configurar los permisos del directorio de Moodle:

Figura 26. Asignar propietario a la carpeta moodle.

5. Configurar Apache y SELinux:

- Instalar Apache:

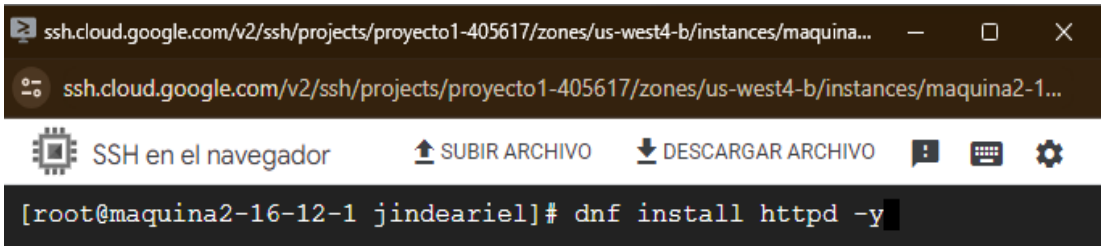

Figura 27. Comando para instalar apache.

- Iniciar el servicio y habilitar para que se inicie en el arranque:

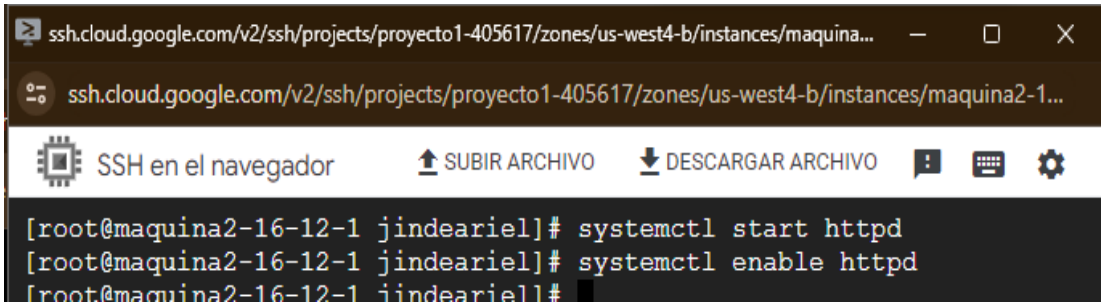

Figura 28. Comandos para iniciar y habilitar el servidor web.

- Configurar SELinux para permitir conexiones web:

Figura 29. Configuración la seguridad extendida de Linux

6. Configurar el dominio con Hostinger:

- Registrar el dominio en Hostinger.

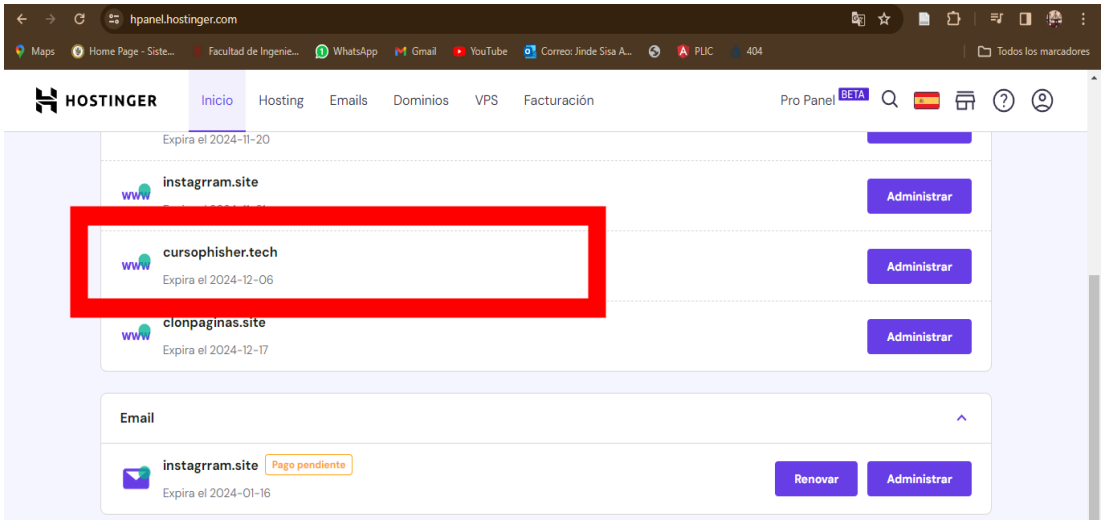

Figura 30. Dominio comprado cursophisher.tech

- Configura el servidor virtual de Apache para reconocer el dominio:

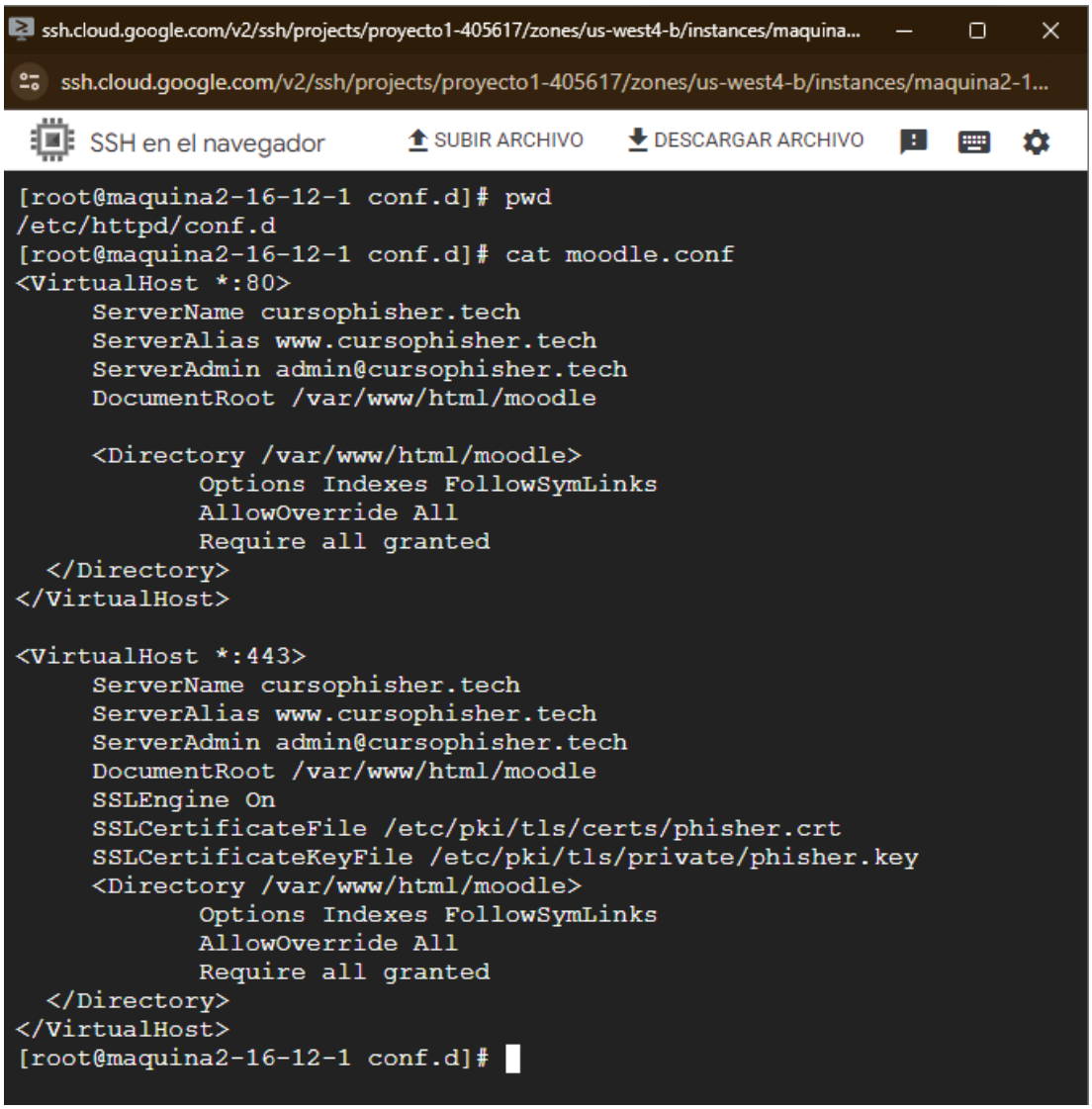

Figura 31. Contenido del host virtual para moodle

Guardar el archivo y reiniciar Apache.

- Crear una zona en Google Cloud Platform (GCP) y añadir los registros vinculando la ip publica con el dominio de cursophisher.tech

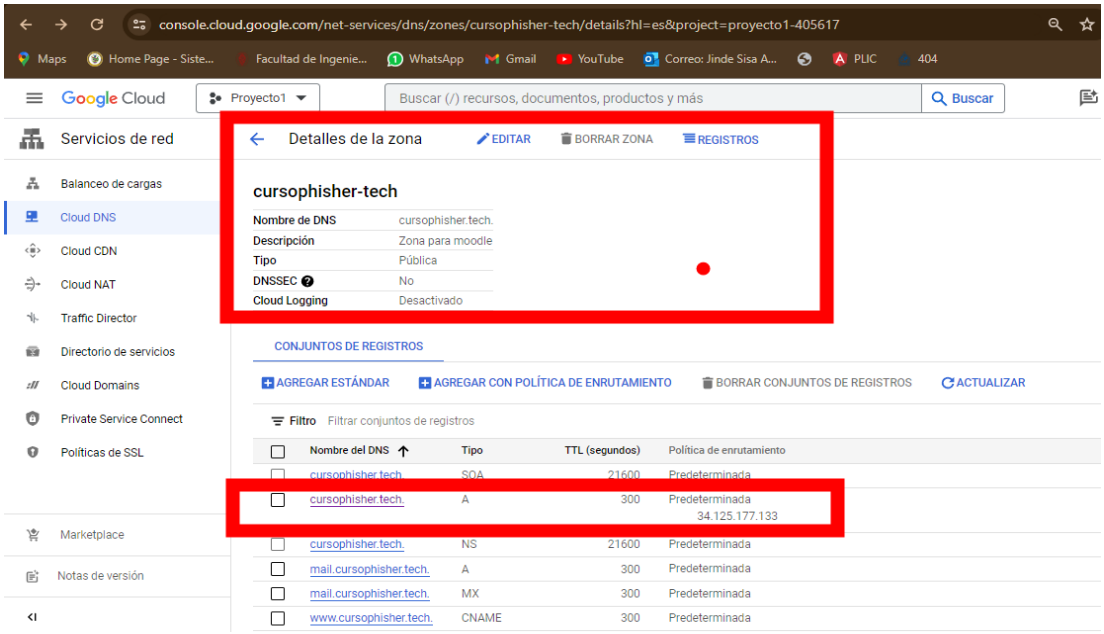

Figura 32. Zona en Cloud DNS para el dominio cursophisher.tech

7. Configurar Moodle:

- Acceder a Moodle a través del navegador web:

Nota: La dirección ip que se muestra en las siguientes figuras no es la misma que está registrada en la zona de Cloud DNS de Google debido a que en un inicio era una ip efímera, posteriormente se cambió a un ip publica fija.

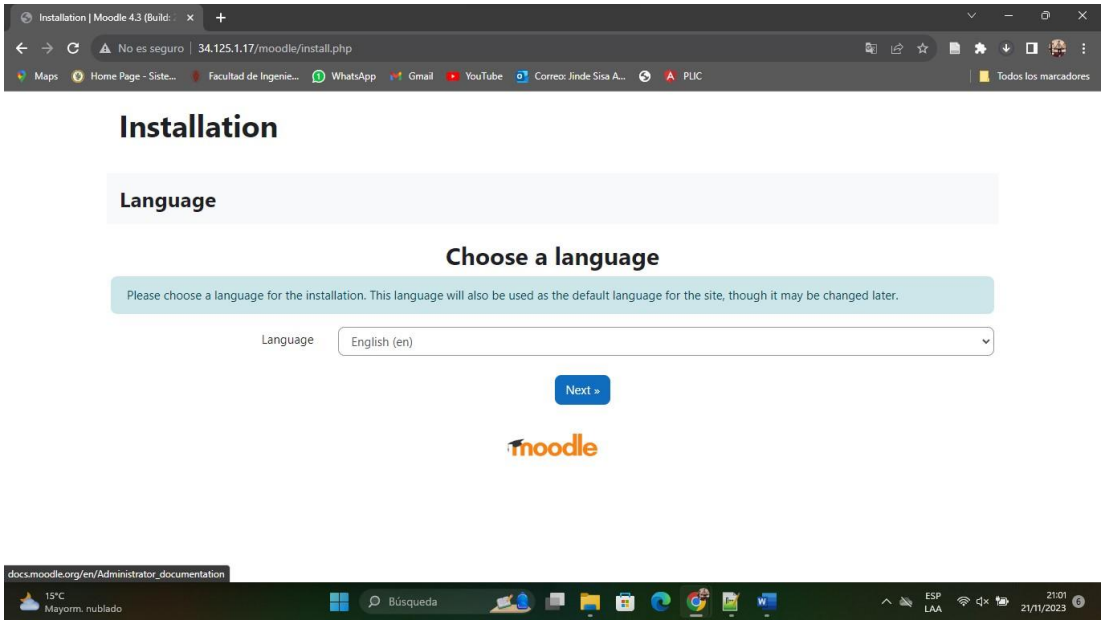

Figura 33. Instalación de moodle vía web.

- Sigue el asistente de instalación de Moodle y completa la configuración, incluyendo la conexión a la base de datos y otros parámetros específicos de tu entorno.

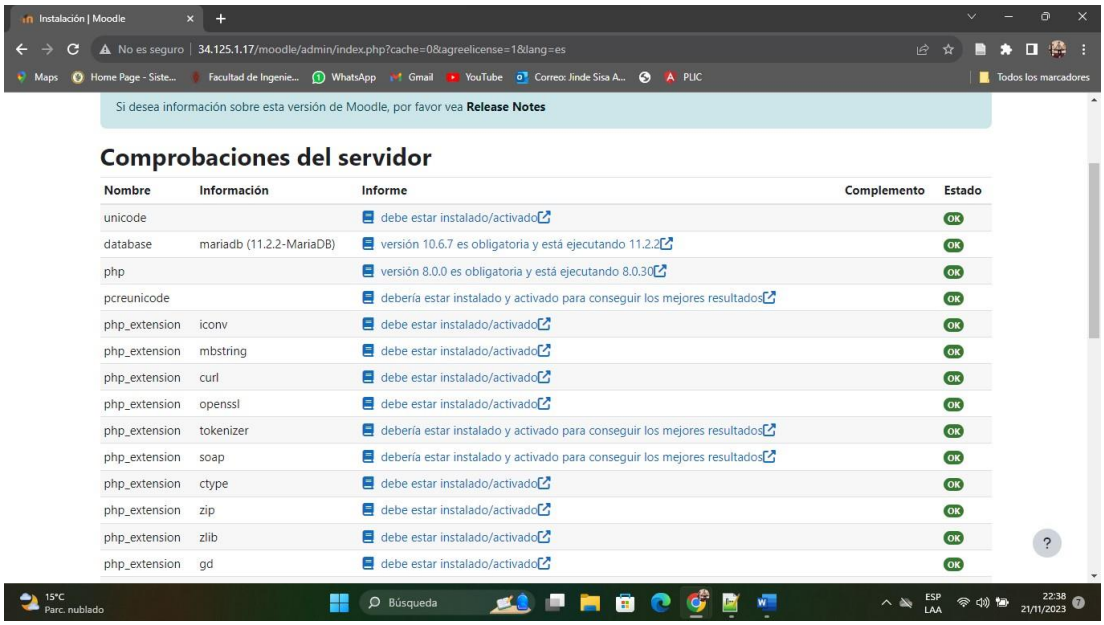

Figura 34. Comprobación del servidor

- Una vez completada la instalación, Moodle debería estar accesible en tu dominio.

Figura 35. Visualización de la página moodle a través del dominio

3.2.5 Fase de Interacción

a. Evaluación de la Aprendizaje del Curso en Moodle:

- **Revisión de Resultados del Curso**: Evaluar las calificaciones y comentarios de los participantes en el curso de Moodle.

Resultados del Test Inicial

Para medir los conocimientos de los usuarios que van a realizar el curso en la plataforma moodle se realizó al inicio un test que contiene preguntas (Anexo D.) para saber el porcentaje de información que conocen los participantes sobre angler-phishing.

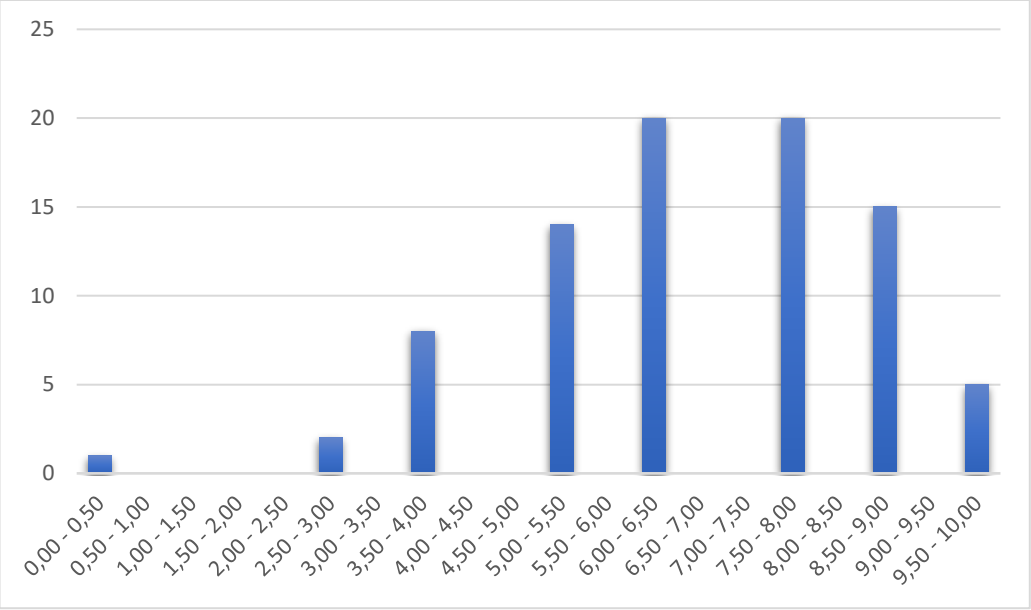

Figura 36. Resultados del test inicial

La mayoría de los participantes obtuvieron calificaciones en los rangos medios y superiores. En particular, hay un grupo significativo con calificaciones entre 6,00 y 8,00.

Un número considerable de participantes obtuvo calificaciones en los extremos: 20 participantes con calificaciones entre 6,00 y 6,50, y otros 20 con calificaciones entre 7,50 y 8,00. Esto sugiere que hay dos grupos distintos de participantes con conocimientos notables en el tema.

Hay participantes con calificaciones en los extremos más bajos (1 participante con calificación entre 0,00 y 0,50), pero también hay grupos en los que ningún participante obtuvo calificaciones (por ejemplo, entre 1,00 y 2,00, entre 3,00 y 3,50, entre 4,00 y 4,50, entre 4,50 y 5,00, y entre 9,00 y 9,50).

La distribución general de las calificaciones sugiere que algunos participantes pueden tener un conocimiento sólido sobre angler-phishing, mientras que otros pueden necesitar mejorar sus conocimientos.

En resumen, estos datos indican que hay una variabilidad significativa en las calificaciones de los participantes en el test inicial. Sería útil analizar más a fondo las áreas específicas donde los participantes pueden necesitar refuerzo y diseñar estrategias de enseñanza o recursos adicionales para abordar esas áreas.

Resultados del Test Final

A continuación, se presenta los resultados del test de finalización del curso, mediate el cual se analiza el aprendizaje o refuerzo de los participantes que realizaron el curso mediante preguntas.(Anexo D.)

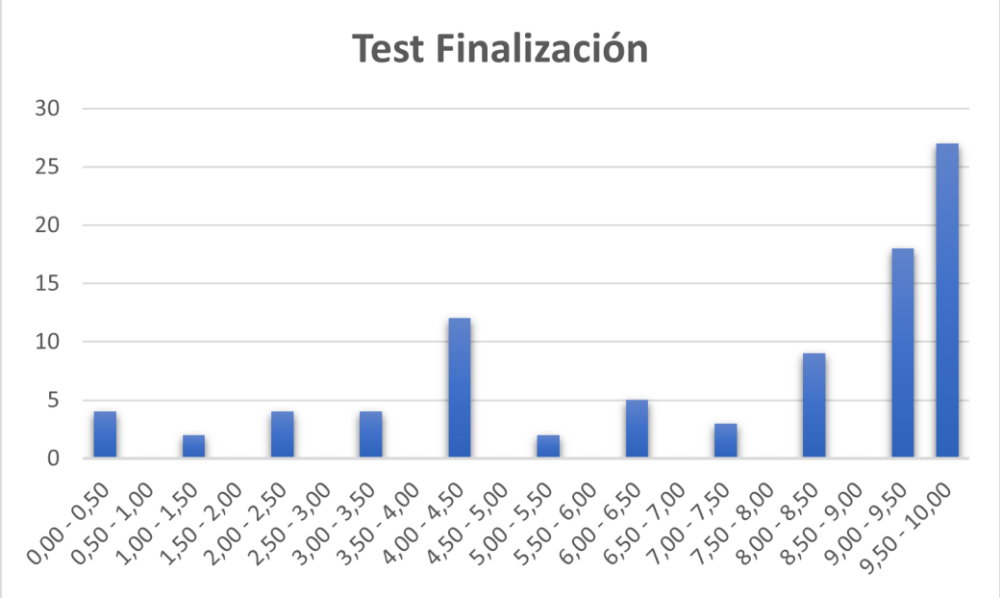

Figura 37. Resultados del test de finalización

La mayoría de los participantes (27) obtuvieron una calificación entre 9,50 y 10,00, lo que sugiere que un gran número de ellos tuvo un rendimiento excepcional.

Los participantes con calificaciones entre 4,00 y 4,50 también son numerosos (12), indicando un rendimiento sólido, pero no tan alto como el grupo superior.

Hay varios grupos en los que no hay participantes, como los que tienen calificaciones entre 0,50 y 1,50, entre 1,50 y 2,00, entre 2,50 y 3,00, entre 3,50 y 4,00, entre 4,50 y 5,00, entre 5,50 y 6,00, entre 6,50 y 7,00, entre 7,50 y 8,00, y entre 8,50 y 9,00.

La distribución general parece sesgada hacia las calificaciones más altas, ya que hay más participantes en los rangos superiores.

En resumen, parece que la mayoría de los participantes tuvieron un rendimiento bastante bueno en el curso, con un énfasis particular en calificaciones altas. Sin embargo, también hay algunos grupos de calificaciones donde no hubo participantes. Estos datos proporcionan una visión general de cómo se desempeñaron los participantes en el curso de angler-phishing.

Comparando los resultados del test inicial y el test de finalización proporcionados anteriormente, se pueden observar algunas diferencias notables en la distribución de las calificaciones y en el rendimiento general de los participantes en el curso de angler-phishing.

- Test Inicial:

En el test inicial, hay una variabilidad significativa en las calificaciones, con un énfasis particular en los rangos medios y superiores (6,00 - 8,00).

Algunos participantes obtuvieron calificaciones extremadamente altas (20 participantes con calificaciones entre 7,50 y 8,00), indicando un conocimiento sólido desde el principio.

Hay grupos de calificaciones (por ejemplo, entre 1,00 y 2,00, entre 3,00 y 3,50, entre 4,00 y 4,50, entre 4,50 y 5,00, y entre 9,00 y 9,50) donde no hubo participantes.

- Test de Finalización:

En el test de finalización, la mayoría de los participantes obtuvieron calificaciones altas, con un número significativo en el rango más alto (27 participantes con calificaciones entre 9,50 y 10,00).

En comparación con el test inicial, el rendimiento en el test de finalización parece haber mejorado, ya que hay más participantes en los rangos superiores y menos en los rangos bajos.

La distribución general en el test de finalización parece estar sesgada hacia calificaciones más altas, sugiriendo un mejor entendimiento y aplicación de los conceptos de angler-phishing al final del curso.

Delta t" (cambio en el tiempo)

Se calcula restando la puntuación del test final de la puntuación del test inicial para cada participante ver Anexo F, la fórmula sería:

Delta t = Puntuación del test final − Puntuación del test inicial

Tabla 37. Rango obtenido delta t”

Rango Delta t”	Cantidad
-8,75; -6,75	2
-6,75; -4,75	5
-4,75; -2,75	8
-2,75; -0,75	9
-0,75; 1,25	18
1,25; 3,25	22
3,25; 5,25	12
5,25; 7,25	4
7,25; 9,25	1
Total	81

Al analizar el delta de los test del curso, se observó la distribución de los cambios en las puntuaciones entre el test inicial y el test final en cada rango:

- Mayoría de participantes con mejoras moderadas: La mayor proporción de participantes se encuentra en los rangos de delta T entre -1.25 y 3.25, lo que indica que la mayoría experimentó mejoras moderadas en sus puntuaciones entre los dos test.
- Distribución simétrica alrededor de cero: La distribución de los recuentos muestra una simetría alrededor de cero, lo que sugiere que hay una cantidad similar de participantes que experimentaron mejoras y empeoramientos en sus puntuaciones.

Sin embargo, la proporción de participantes con mejoras es ligeramente mayor que aquellos con empeoramientos.

- Pocos participantes con cambios extremos: Hay pocos participantes en los extremos de la distribución, es decir, aquellos con cambios muy negativos (por debajo de -4.75) o muy positivos (por encima de 5.25). Esto sugiere que los cambios drásticos en las puntuaciones son menos comunes y que la mayoría de los participantes experimentaron cambios más moderados.
- Proporción significativa de participantes con mejoras pequeñas: Aunque la mayoría de los participantes experimentaron mejoras moderadas, también hay una proporción significativa que experimentó mejoras pequeñas (entre -0.75 y 1.25). Esto indica que incluso cambios pequeños en las puntuaciones pueden ser significativos en el contexto del curso.

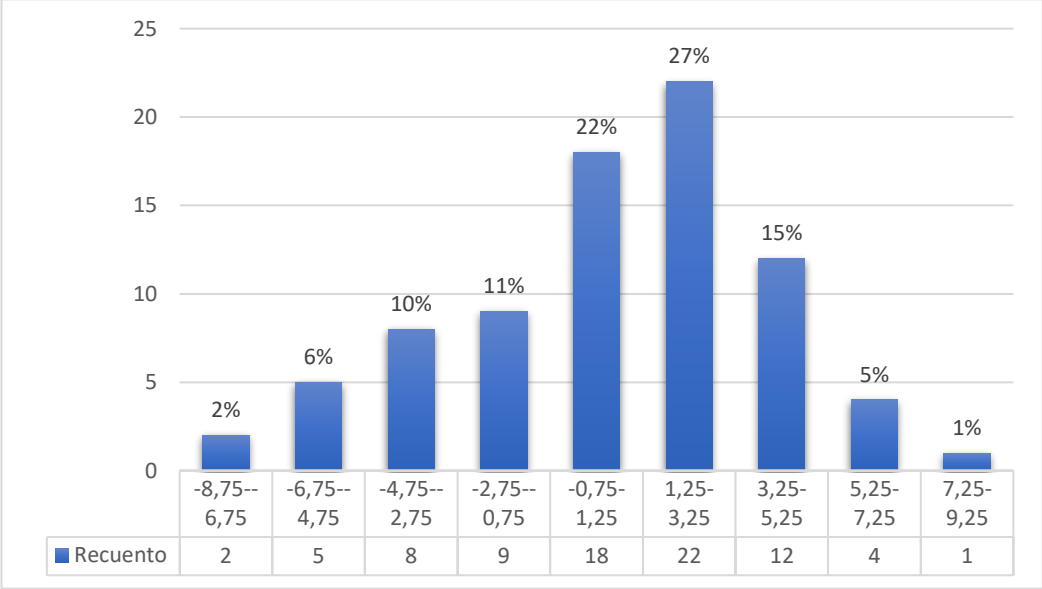

Figura 38. Rangos de puntuación de delta t”

En resumen, estos datos sugieren que el curso pudo haber tenido un impacto positivo en las puntuaciones de los participantes, con la mayoría experimentando mejoras moderadas en sus habilidades y conocimientos. Sin embargo, también hubo una proporción significativa de participantes cuyas puntuaciones apenas cambiaron o incluso disminuyeron, lo que indica áreas potenciales para mejorar el curso en futuras iteraciones.

- **Análisis de Participación:** Analizar la participación, la finalización del curso y cualquier retroalimentación recibida.

Finalización del curso

Estos datos indican la distribución de participantes en función de finalización del curso.

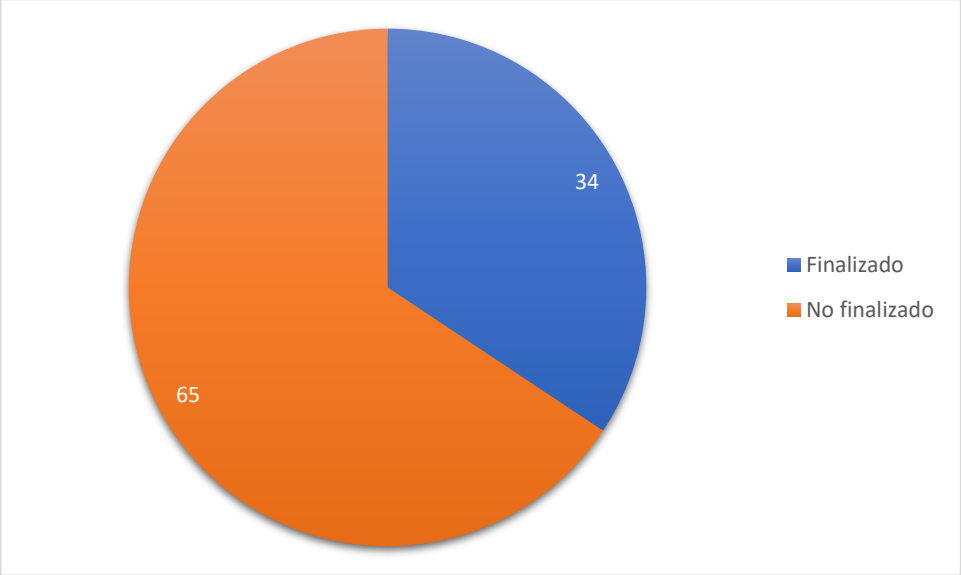

Figura 39. Cantidad de participantes que finalizaron y no finalizaron el curso.

- Cantidad de personas que completaron el curso: Un total de 34 personas finalizaron el curso, lo que representa aproximadamente el 34.36% del total de participantes.

- Cantidad de personas que no completaron el curso: Por otro lado, 65 personas no finalizaron el curso, lo que equivale aproximadamente al 65.65% del total de participantes.
- Comparación de finalizados y no finalizados: La cantidad de personas que completaron el curso es considerablemente menor que la cantidad de personas que no lo hicieron. Esto sugiere que una proporción significativa de participantes no logró finalizar todas las actividades del curso. Porcentaje completado del curso de cada uno de los participantes en el Anexo E.

Participación General

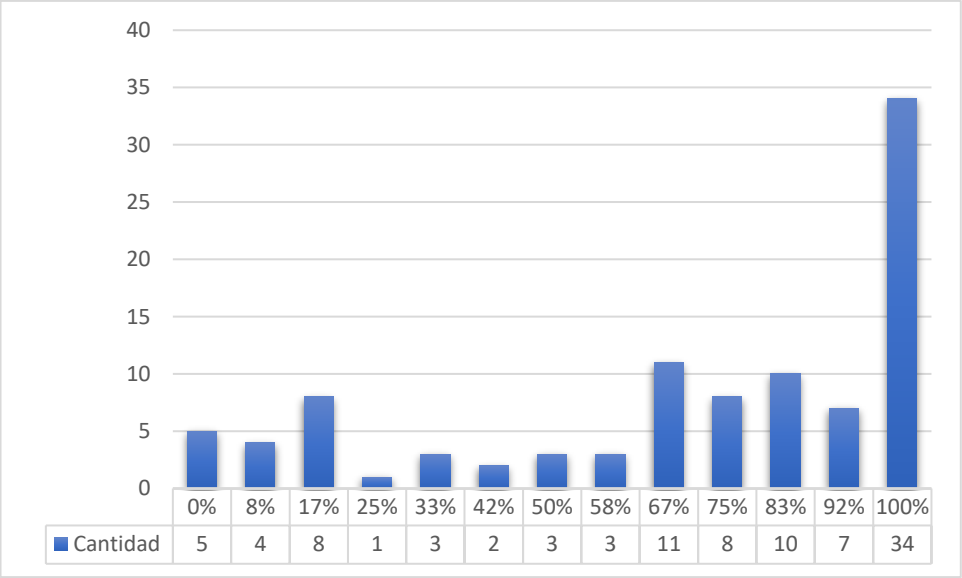

Figura 40. Porcentaje de actividades finalizadas.

- Mayoría de participantes completaron el curso: La mayor cantidad de participantes (34) completaron el curso al 100%, lo que representa un 28.81% del total de participantes. Esto indica que una proporción significativa de los participantes logró finalizar todas las actividades y alcanzar el máximo porcentaje del curso.
- Distribución en otras categorías de finalización: Además del grupo que completó el curso al 100%, observamos que hay una distribución en otras categorías de finalización. Por ejemplo, 11 participantes completaron el 67% del curso, seguido de 10 participantes que alcanzaron el 83%, y así sucesivamente.
- Pocos participantes en las categorías extremas: Hay una menor cantidad de participantes en las categorías de finalización más baja (0% y 25%) y más alta (92%). Esto podría indicar que algunos participantes abandonaron el curso temprano, mientras que otros tuvieron un alto nivel de compromiso y completaron la mayoría del curso.
- Distribución equilibrada en algunas categorías intermedias: Las categorías intermedias, como el 50% y el 75%, tienen una cantidad similar de participantes, lo que sugiere que hubo un progreso consistente para algunos participantes hasta ciertos puntos del curso.

CAPITULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En el cierre de este estudio sobre la ciberseguridad y la prevención de ataques Angler-Phishing basados en Ingeniería Social, es gratificante destacar que se han cumplido satisfactoriamente todos los objetivos planteados en las siguientes conclusiones:

- Se ha logrado una comprensión actualizada de las tácticas, técnicas y procedimientos empleados por los ciberdelincuentes en los ataques de Angler-Phishing. La información recopilada proporciona una base para el desarrollo de una estrategia defensiva, efectiva y adaptativa. La estrategia resultante se caracteriza por su capacidad de respuesta, permitiendo afrontar las constantes evoluciones en el panorama de la ciberseguridad con eficacia y anticipación.

- Se ha identificado y evaluado un conjunto variado de herramientas TI diseñadas específicamente para la detección y prevención de ataques basados en Ingeniería Social. Lo cual sugiere que la implementación estratégica de estas herramientas puede ser efectiva para mitigar el riesgo asociado a los ataques Angler-Phishing.

- La estrategia ha sido desarrollada en base a la metodología OSSTMM, se distingue por la implementación de varias soluciones tecnológicas. Entre ellas se destaca el despliegue de un servidor Moodle, el diseño de un curso en línea y la replicación de páginas web. Esta implementación refuerza de manera considerable la capacidad de reacción y defensa de las personas ante posibles amenazas cibernéticas.

- La aplicabilidad de la estrategia propuesta ha sido evaluada mediante pruebas con usuarios que utilizaron la plataforma Moodle, sometiéndolos a un test inicial y un test final donde los resultados indican una eficacia y viabilidad de la estrategia en términos de aprendizaje y aplicación de conocimientos, proporcionando evidencia empírica de su capacidad para mitigar los ataques de Angler-Phishing.

- El curso diseñado registró un índice de cumplimiento del 70%, indicando que la mayoría de los participantes completaron exitosamente el programa. Estos resultados favorables respaldan la aplicabilidad práctica de la estrategia, también refuerzan la confianza en su capacidad para defenderse y protegerse eficientemente contra amenazas derivadas de Ingeniería Social.

4.2 Recomendaciones

- Mantener una vigilancia constante sobre las tendencias emergentes en los ataques Angler-Phishing para adaptar rápidamente las estrategias defensivas.

- Impartir programas de formación y concientización para mejorar la capacidad de reconocer y resistir los intentos de Ingeniería Social de las personas.

- Mantener una actualización regular de todos los contenidos del curso para abordar posibles vulnerabilidades y garantizar una completa concientización en los usuarios que participen del curso.

- Realizar simulacros periódicos de ataques de ingeniería social para poner a prueba a los usuarios mejorando su nivel de respuesta en caso de un ataque real.

- Explorar y adoptar tecnologías emergentes, como inteligencia artificial y aprendizaje automático, para mejorar la capacidad predictiva y preventiva contra ataques de Ingeniería Social.

REFERENCIAS BIBLIOGRÁFICAS

[1] J. Rojas, «¿Qué son las TIC y para qué sirven?», Telefónica. Accedido: 23 de octubre de 2023. [En línea]. Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/que-son-las-tic-y-para-que-sirven/

[2] «Importancia de las tecnologías de la información y la comunicación | Indeed.com México». Accedido: 23 de octubre de 2023. [En línea]. Disponible en: https://mx.indeed.com/orientacion-profesional/desarrollo-profesional/importancia-tecnologias-informacion-comunicacion

[3] E. U. Mediterrani, «Hoy hablamos de Redes Sociales», Mediterrani. Accedido: 23 de octubre de 2023. [En línea]. Disponible en: https://mediterrani.com/hoy-hablamos-de-redes-sociales/

[4] «¿Qué es la ingeniería social? | IBM». Accedido: 23 de octubre de 2023. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/social-engineering

[5] admin, «¿Existe la Ingeniería Social en el Ecuador?», La Competencia S.A. Accedido: 23 de octubre de 2023. [En línea]. Disponible en: https://www.competencia.com.ec/corporativo/existe-la-ingenieria-social-en-el-ecuador/

[6] «Ecuador lidera la lista de países más vulnerados por los ciberataques», Primicias. Accedido: 24 de octubre de 2023. [En línea]. Disponible en: https://www.primicias.ec/noticias/tecnologia/ciberataques-latinoamerica-elevan-pirateria-trabajo-remoto/

[7] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, y M. A. Ibrahim, «Social Engineering Attacks Prevention: A Systematic Literature Review», *IEEE Access*, vol. 10, pp. 39325-39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[8] J. Alzas Hernandez, «Estudio de fraudes basados en la técnica de Ingeniería Social», jun. 2023, Accedido: 6 de febrero de 2024. [En línea]. Disponible en: https://openaccess.uoc.edu/handle/10609/148147

[9] L. I. C. Machaca, «Estrategias para evitar ataques de Phishing en Empresas», *INF-FCPN-PGI Rev. PGI*, pp. 65-68, 2020.

[10] R. Tejada y L. Fernando, «El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático».

[11] D. F. A. Toapanta, M. O. U. Mayorga, y R. O. A. Paredes, «Análisis y Diseño de un Modelo Predictivo para Detección de Phishing Basado en Url y Corpus del Correo Electrónico», *Rev. Politécnica*, vol. 50, n.º 3, Art. n.º 3, dic. 2022, doi: 10.33333/rp.vol50n3.03.

[12] I. Collins y J. Muhammad, «Phishing Attack Awareness», *ADMI 2022 Symp. Comput. Minor. Inst.*, ene. 2022, Accedido: 6 de febrero de 2024. [En línea]. Disponible en: https://par.nsf.gov/biblio/10344955-phishing-attack-awareness

[13] «Repositorio de la Universidad de Fuerzas Armadas ESPE: Error interno del sistema». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://repositorio.espe.edu.ec/bitstream/21000/32745/1/T-ESPE-052520.pdf

[14] D. J. M. Gómez, J. C. A. Vargas, y A. Á. Quiceno, «Análisis del estado actual de la seguridad informática en tiempos de pandemia, entregando un conjunto de buenas prácticas, para fomentar la seguridad informática en las organizaciones de la ciudad de Medellín», *Rev. CIES Escolme*, vol. 13, n.º 1, Art. n.º 1, abr. 2022.

[15] O. C. MANUEL JOSÉ, *Ciberseguridad. Manual práctico*. Ediciones Paraninfo, S.A., 2021.

[16] R. N. Barazarte Mastropietro, «Creación de políticas de seguridad informática, mediante el análisis de propuestas teóricas y del estándar ISO 27001, de acuerdo con los recursos tecnológicos, para la mejora estructural tecnológica en la empresa Produsoft, a partir del 2020», sep. 2020, Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://repositorio.ulatina.ac.cr/handle/20.500.12411/297

[17] «Diseño de un Plan de Recuperación ante Desastres DRP para la Gobernación de Casanare». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/12031

[18] «Soluciones de Ciberseguridad Kaspersky para hogar y negocio | Kaspersky | Kaspersky». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://latam.kaspersky.com/

[19] «¿Qué es la Seguridad de TI? - Seguridad de la tecnología de la información», Cisco. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-it-security.html

[20] O. D. A. Gomez, «EL ABC DE LA SEGURIDAD INFORMATICA GUIA PRACTICA PARA ENTENDER LA SEGURIDAD DIGITAL».

[21] «Seguridad en internet: ¿Qué es la seguridad en internet?», GCFGlobal.org. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-la-seguridad-en-internet/1/

[22] Conzultek, «Computación en la nube: ¿qué es y cuáles son sus alcances?» Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://blog.conzultek.com/teletrabajo/que-es-computacion-nube-sus-alcances

[23] «¿Qué es la seguridad de aplicaciones web? | Seguridad web», Cloudflare. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/security/what-is-web-application-security/

[24] «Qué son las políticas de seguridad informática y por qué son importantes», Informática para empresas. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.gadae.com/blog/politicas-de-seguridad-informatica/

[25] G. B. Urbina, *Introducción a la seguridad informática*. Grupo Editorial Patria, 2017.

[26] «Ciberdelincuencia». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

[27] «Ingeniería social | INCIBE | INCIBE». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.incibe.es/aprendeciberseguridad/ingenieria-social

[28] K. Petrosyan, «¿Qué son y en qué consisten los ataques cibernéticos Quid Pro Quo?», EasyDMARC. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://easydmarc.com/blog/es/que-son-y-en-que-consisten-los-ataques-ciberneticos-quid-pro-quo/

[29] «¿Qué es el scareware? Detección, prevención y eliminación», ¿Qué es el scareware? Detección, prevención y eliminación. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.avast.com/es-es/c-scareware

[30] «Ataques 'Watering hole': en qué consisten y cómo protegerse | Empresas | INCIBE». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.incibe.es/empresas/blog/ataques-watering-hole-consisten-y-protegerse

[31] «¿Qué es el phishing? | Cómo protegerse de los ataques de phishing», Malwarebytes. Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://es.malwarebytes.com/phishing/

[32] «¿Qué es el phishing? | IBM». Accedido: 29 de diciembre de 2023. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/phishing

[33] J. Rodríguez-Rodríguez y M. Reguant-Álvarez, «Calcular la fiabilidad de un cuestionario o escala mediante el SPSS: el coeficiente alfa de Cronbach», *REIRE Rev. Innovació Recer. En Educ.*, vol. 13, n.º 2, Art. n.º 2, jul. 2020, doi: 10.1344/reire2020.13.230048.

[34] P. González y G. Arley, «Análisis de amenazas presentes en los entornos computacionales, vinculando sistemas operativos, redes y bases de datos como estrategia defensiva ante ciber-ataques sobre plataforma Windows.», abr. 2021, Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/40337

[35] P. M. Foster, «Protección y privacidad de la información», Tesis, Universidad Nacional de La Plata, 2020. doi: 10.35537/10915/124284.

[36] C. N. Torres Artos, «Afectación de la privacidad por el uso de marketing en redes sociales», bachelorThesis, PUCE - Quito, 2022. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.puce.edu.ec:80/handle/22000/20166

[37] R. G. Pérez, *El dilema de la IA*. Ediciones Rialp, S.A., 2023.

[38] G. de la T. Gómez y J. María, «Reorientación estratégica de una empresa de servicios de seguridad de la información orientada a prestar servicios a instituciones del sector financiero», masterThesis, Quito, EC: Universidad Andina Simón Bolívar,

Sede Ecuador, 2023. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: http://repositorioslatinoamericanos.uchile.cl/handle/2250/8128969

[39] «AWS Vs. Microsoft Azure Vs. Google Cloud ¿Cuándo Usar Cada Uno?» Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://codster.io/blog/servicios-nube-aws-vs-microsoft-azure-vs-google-cloud/

[40] «Google Cloud vs AWS en 2023 (Comparación de los gigantes)», Kinsta®. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://kinsta.com/es/blog/google-cloud-vs-aws/

[41] «Debian vs Fedora: Comparación entre titanes». Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://laboratoriolinux.es/index.php/-noticias-mundo-linux-/distribuciones/23043-debian-vs-fedora-comparacion-entre-titanes.html

[42] A. Junior, «Fedora vs. Ubuntu: ¿Cuál distro de Linux es mejor? » Adictec», Adictec - Adicción por la tecnología. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://adictec.com/fedora-vs-ubuntu-mejor-distro/

[43] «Los 10 Mejores Servicios de Hosting Web Para Tu página web 2024», Website Planet. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://www.websiteplanet.com/es/web-hosting/

[44] «Las mejores plataformas LMS de código abierto de 2023». Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://www.onlyoffice.com/blog/es/2023/01/mejores-plataformas-lms-de-codigo-abierto

[45] M. G. Almonte, «Plataformas LMS: qué son, características, tipos y diferencias con otros sistemas», Aprendizaje en Red - Elearning y Diseño Instruccional. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://aprendizajeenred.es/plataformas-lms-definicion-caracteristicas-tipos-diferencias/

[46] admin, «Cuadro comparativo de plataformas LMS Cuadros Comparativos», Cuadros Comparativos. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://juegaconpalabras.com/cuadro-comparativo-de-plataformas-lms/

[47] «Top 5 Herramientas LMS de código abierto para negocios en 2021». Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://blog.containerize.com/es/top-5-open-source-lms-tools-for-business-in-2021/

[48] Informática, «Angler Phishing: qué es y cómo protegernos de esta amenaza», CEC. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://www.cec.es/angler-phishing-que-es-y-como-protegernos-de-esta-amenaza/

[49] K. Petrosyan, «¿Qué es el phishing de Angler y cómo puedes evitarlo?», EasyDMARC. Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://easydmarc.com/blog/es/que-es-el-phishing-de-angler-y-como-puedes-evitarlo/

[50] «La Inteligencia Artificial en Educación y la aplicabilidad de ChatGPT | UNIR». Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://www.unir.net/educacion/revista/inteligencia-artificial-educacion-chatgpt/

[51] «La inteligencia artificial en la educación | UNESCO». Accedido: 30 de diciembre de 2023. [En línea]. Disponible en: https://www.unesco.org/es/digital-education/artificial-intelligence

[52] «CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

[53] «t2244ti.pdf». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/38430/1/t2244ti.pdf

[54] H. R. González Brito y R. Montesino Perurena, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web», *Rev. Cuba. Cienc. Informáticas*, vol. 12, n.º 4, pp. 52-65, dic. 2018.

[55] «Open Source Security Testing Methodology Manual (OSSTMM) | Cyberzaintza». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-osstmm

[56] «Metodologías Existentes | Alonso Caballero / ReYDeS». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.reydes.com/d/?q=Metodologias_Existentes

[57] «INVESTIGACIÓN». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.isecom.org/research.html

[58] «Fases de la metodología OSSTMM - Metodología OSSTMM». Accedido: 2 de enero de 2024. [En línea]. Disponible en: https://1library.co/article/fases-de-la-metodolog%C3%ADa-osstmm-metodolog%C3%ADa-osstmm.yeo0km4q

ANEXOS

Anexo A. Desarrollo de materiales.

En las siguientes figuras se muestra las diapositivas sobre conceptos básicos de Ingeniería Social.

Figura A1. Diapositiva 1

Figura A2. Diapositiva 2

.

Figura A3. Dispositiva 3

Figura A4. Dispositiva 4

Figura A5. Dispositiva 5

Figura A6. Dispositiva 6

Figura A7. Dispositiva 7

- Diapositivas sobre Angler-Phishing

Figura A8. Dispositiva 8

Figura A9. Dispositiva 9

Figura A10. Dispositiva 10

Ejemplos de casos de angler phishing

Publicación de red social falsa

Los atacantes crean publicaciones aparentemente legítimas que contienen enlaces maliciosos, engañando a los usuarios para que hagan clic y revelen información confidencial.

Emails engañosos

Se envían correos electrónicos falsos que parecen provenir de empresas o servicios de confianza, solicitando información personal o credenciales de inicio de sesión.

Sitios web falsos

Los atacantes crean réplicas de sitios web legítimos para engañar a los usuarios y obtener sus datos de inicio de sesión o información financiera.

Figura A11. Dispositiva 11

Riesgos y consecuencias del angler phishing

Pérdida de datos personales

El angler phishing puede resultar en el robo de información personal como contraseñas, números de tarjetas de crédito y datos de identificación.

Robo de identidad

Los ciberdelincuentes pueden utilizar la información robada para suplantar la identidad de las víctimas y llevar a cabo actividades fraudulentas en su nombre.

Pérdida financiera

Las personas pueden ser víctimas de estafas financieras, con consecuencias que van desde cargos no autorizados en tarjetas de crédito hasta el vaciado de cuentas bancarias.

Figura A12. Dispositiva 12

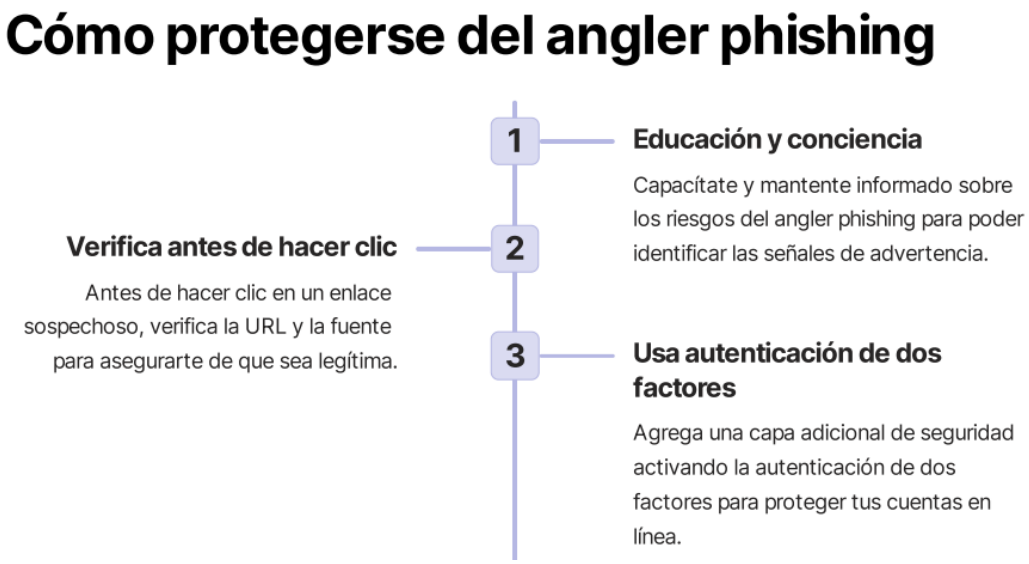

Figura A13. Dispositiva 13

Figura A14. Dispositiva 14

- Diapositivas de cómo funciona Angler-Phishing en redes sociales.

Figura A15. Dispositiva 15

Figura A16. Dispositiva 16

Figura A17.Dispositiva 17

Figura A18. Dispositiva 18

Anexo B. Paginas clonadas

En la Figura B1. Se muestra una simulación de chat que solicita información personal.

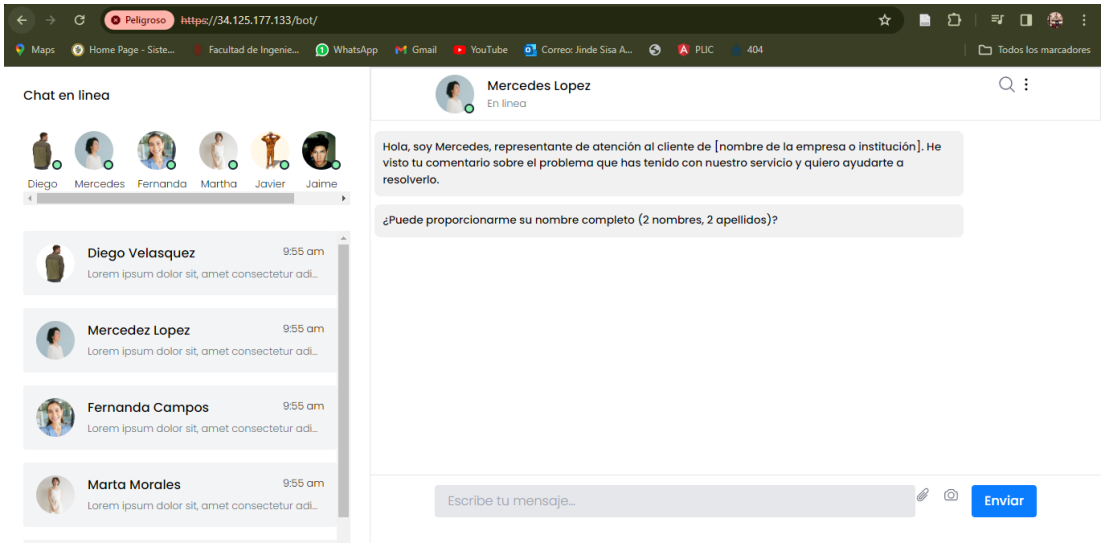

Figura B1. Simulación de chat phishing.

En la Figura B2. Se muestra una página clonada de una entidad bancaria que contiene una pequeña publicidad.

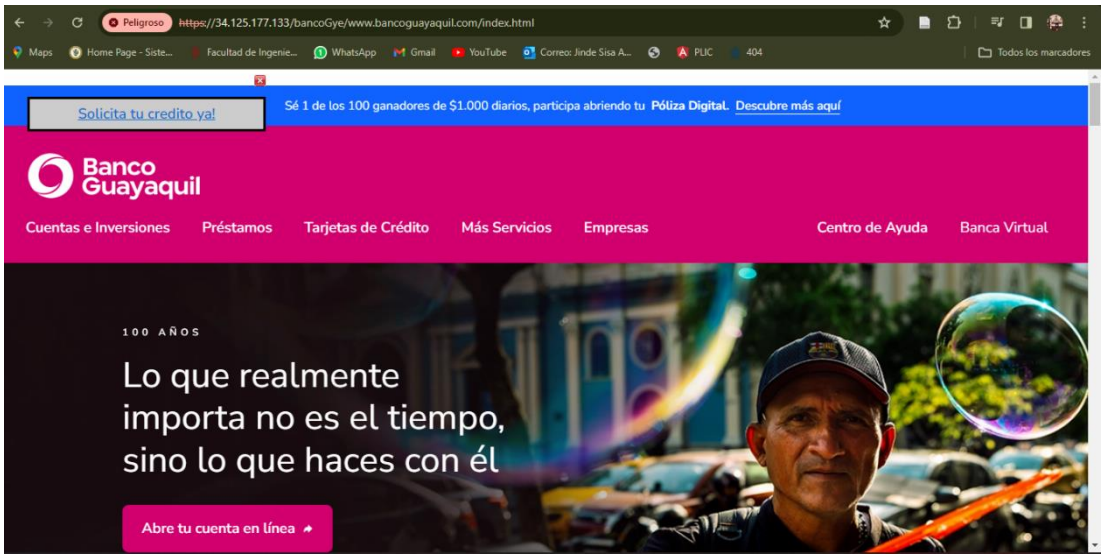

Figura B2. Simulación página web entidad bancaria.

En la Figura B3. Se muestra una página clonada para iniciar sesión de una entidad bancaria.

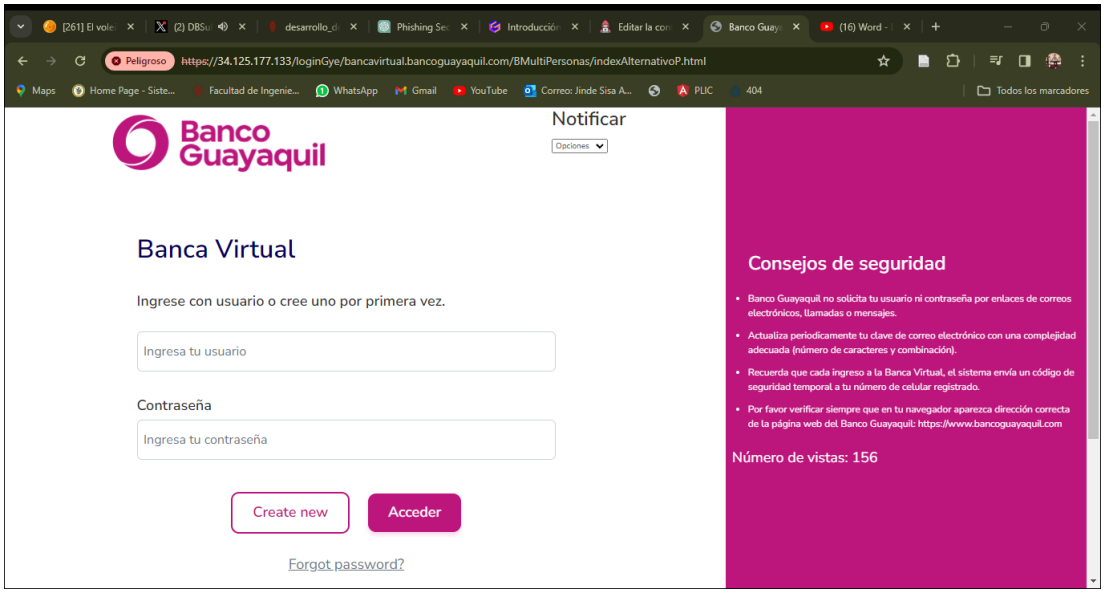

Figura B3. Simulación login falso para entidad bancaria.

En la Figura B4. Se muestra una página clonada de información deportiva que contiene una ventana que solicita cometarios.

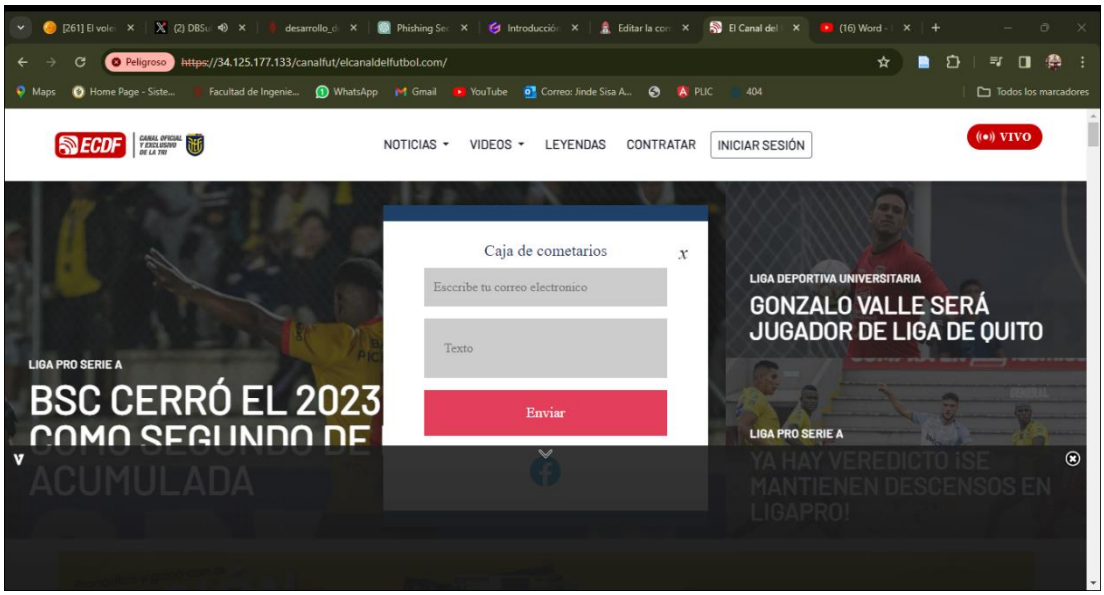

Figura B4. Pagina clonada de un sitio de información deportiva.

En la Figura B5. Se muestra una página clonada para iniciar sesión de la página deportiva mostrada en la Figura B3.

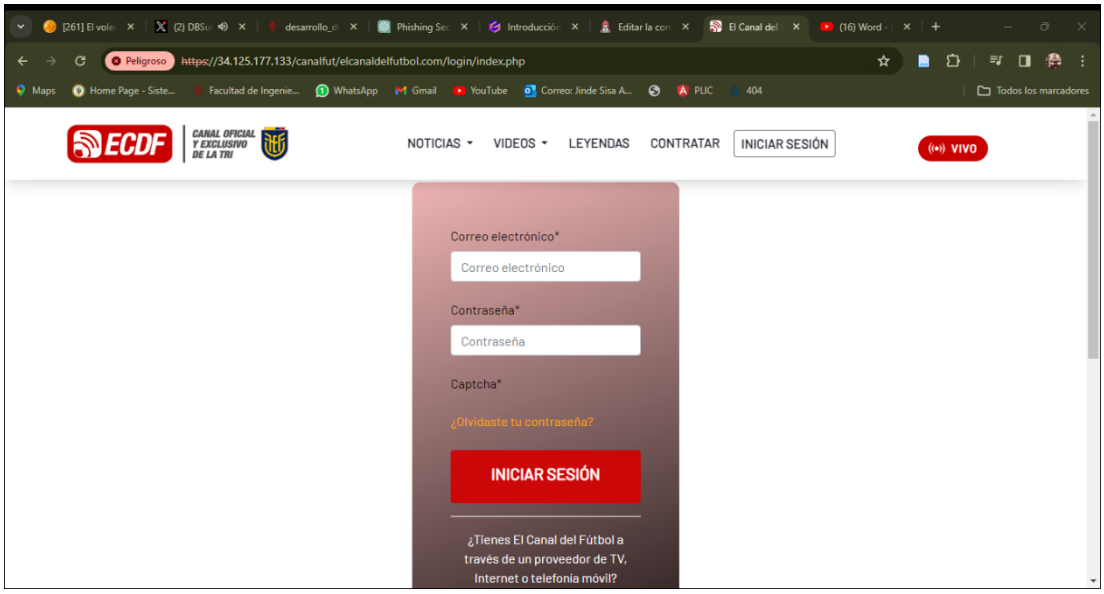

Figura B5. Inicio de sesión falso de la página deportiva.

En la Figura B6. Se muestra una página clonada de un sitio de compras en línea con una pequeña publicad que sugiere un descuento.

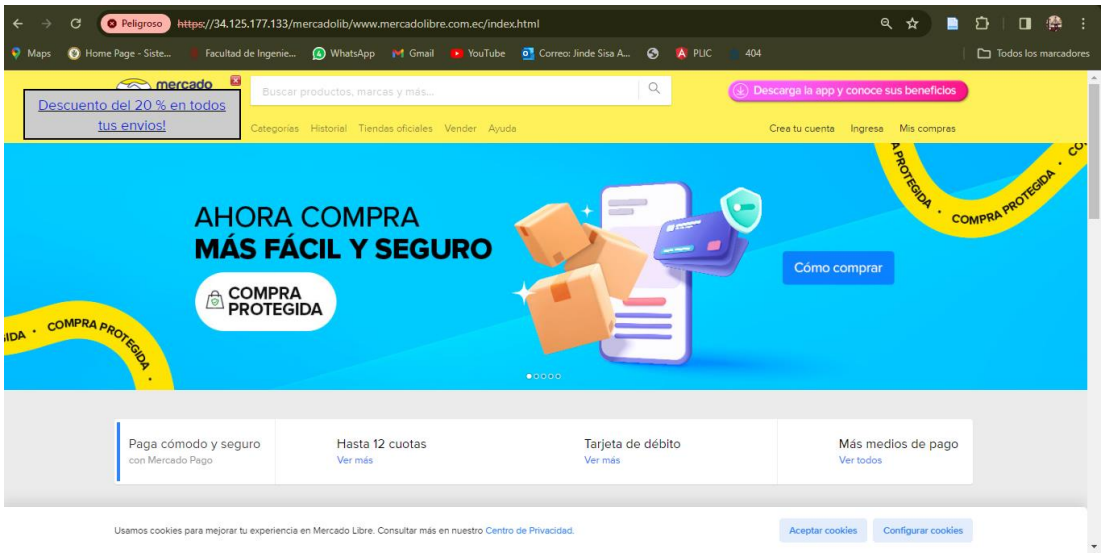

Figura B6. Página clonada de un sitio de compras en línea.

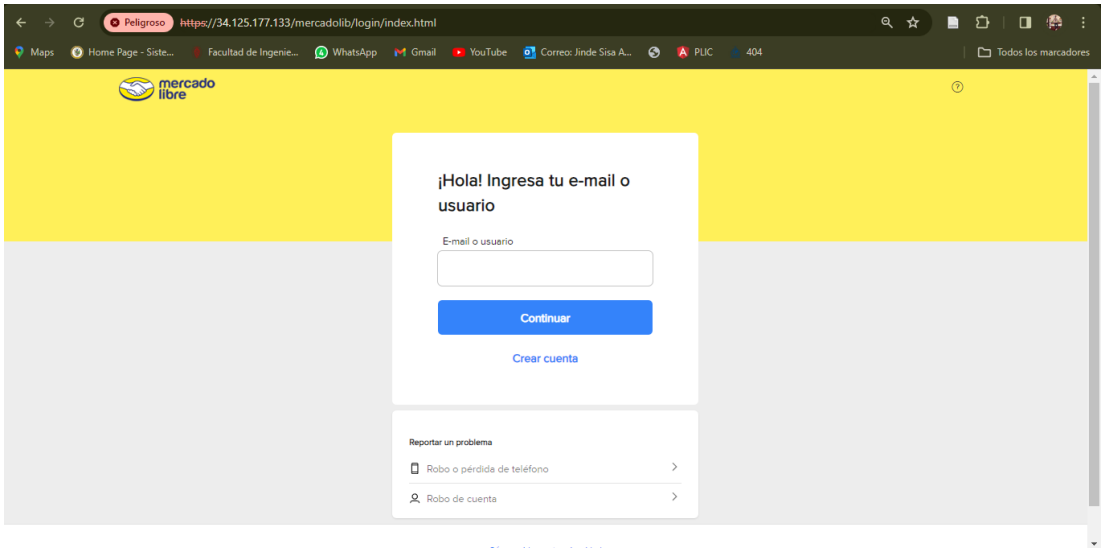

Figura B7. Inicio de sesión falso de un sitio de compras en línea.

Anexo C. Configuración del curso en moodle.

En las siguientes figuras se muestra la configuración de creación del curso en moodle.

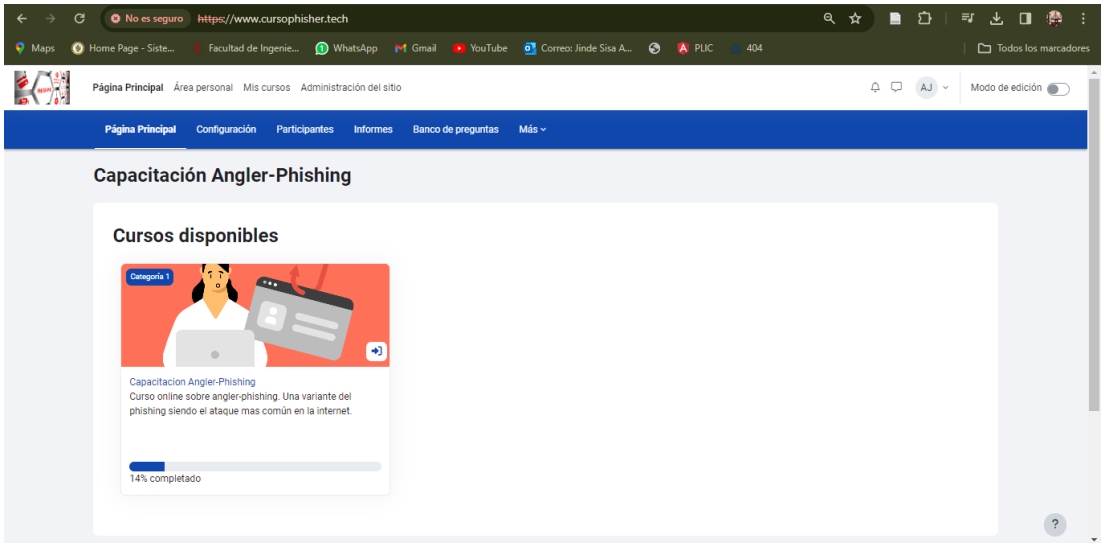

Figura C1. Curso Angler-Phishing

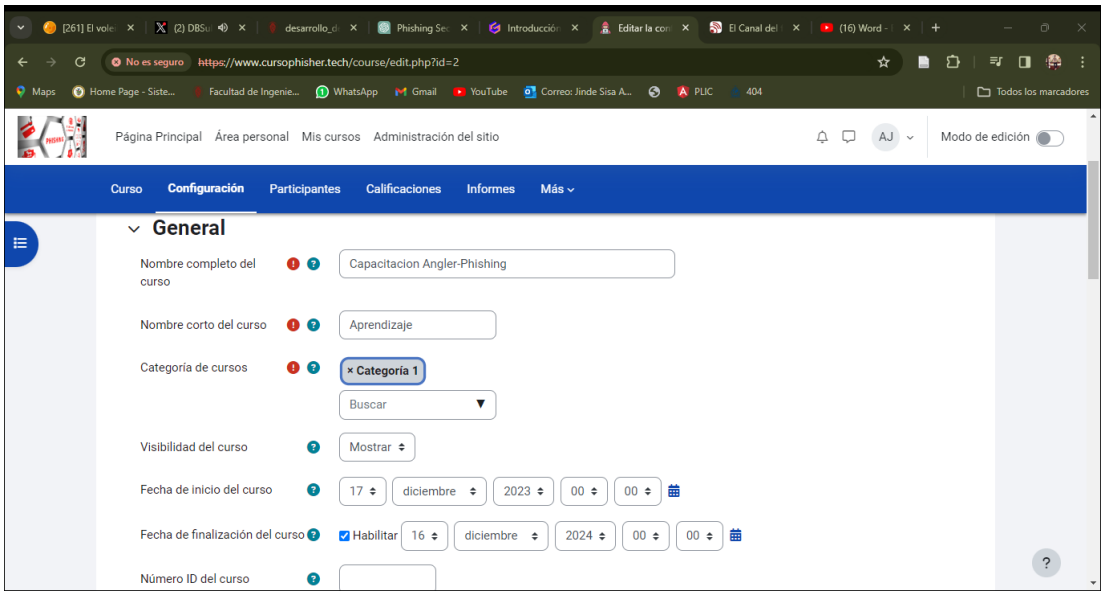

Figura C2. Configuración curso Angler-Phishing

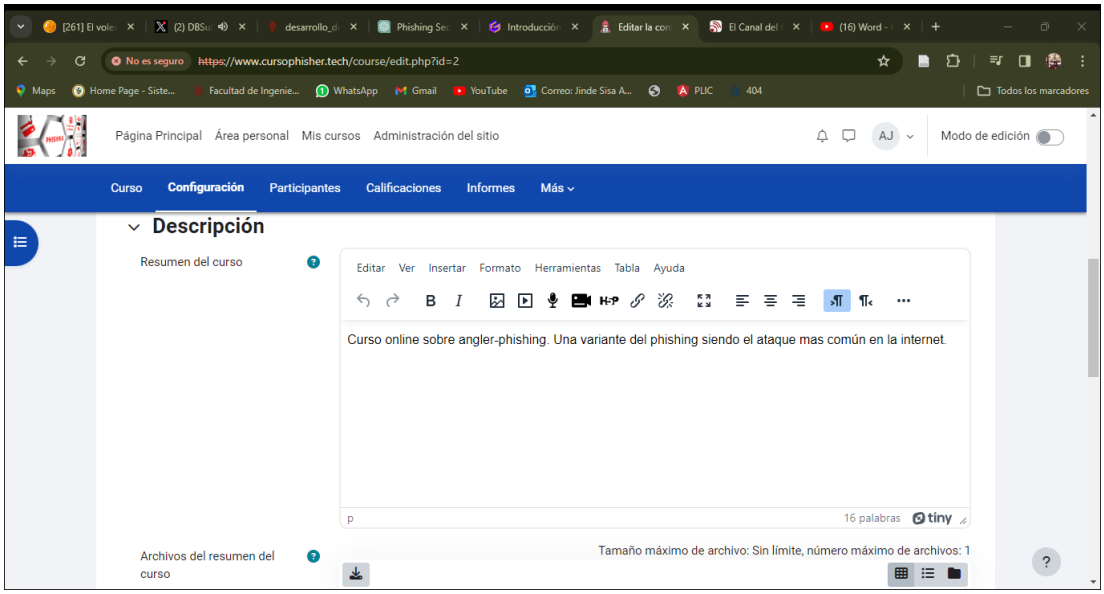

Figura C3. Descripción curso Angler-Phishing

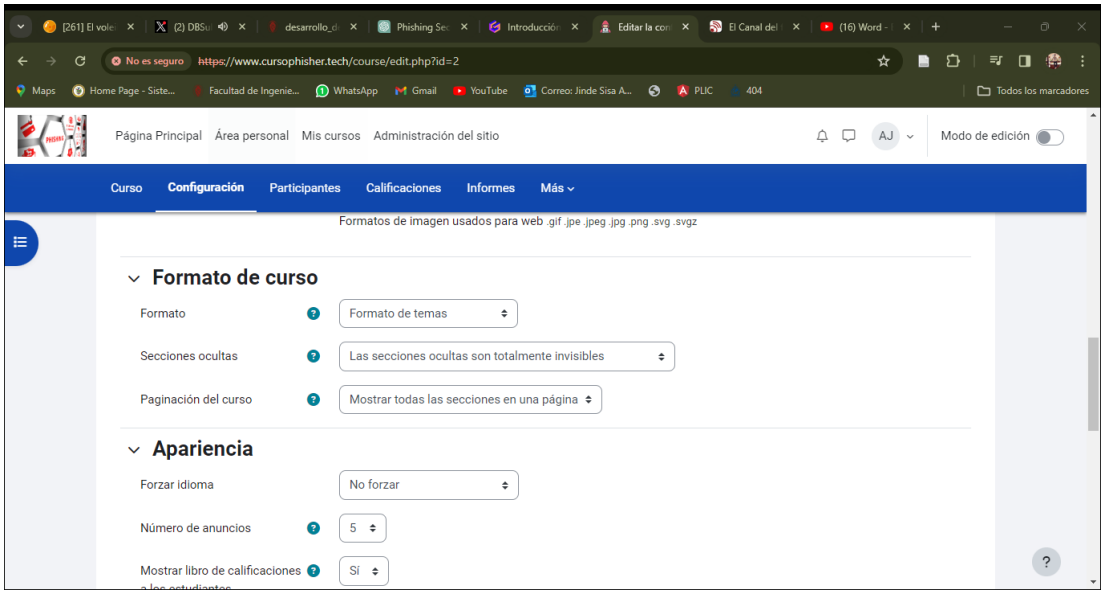

Figura C4. Formato y apariencia curso Angler-Phishing

Anexo D. Cuestionario de preguntas Test Inicial y Test Final

- Preguntas del Test Inicial

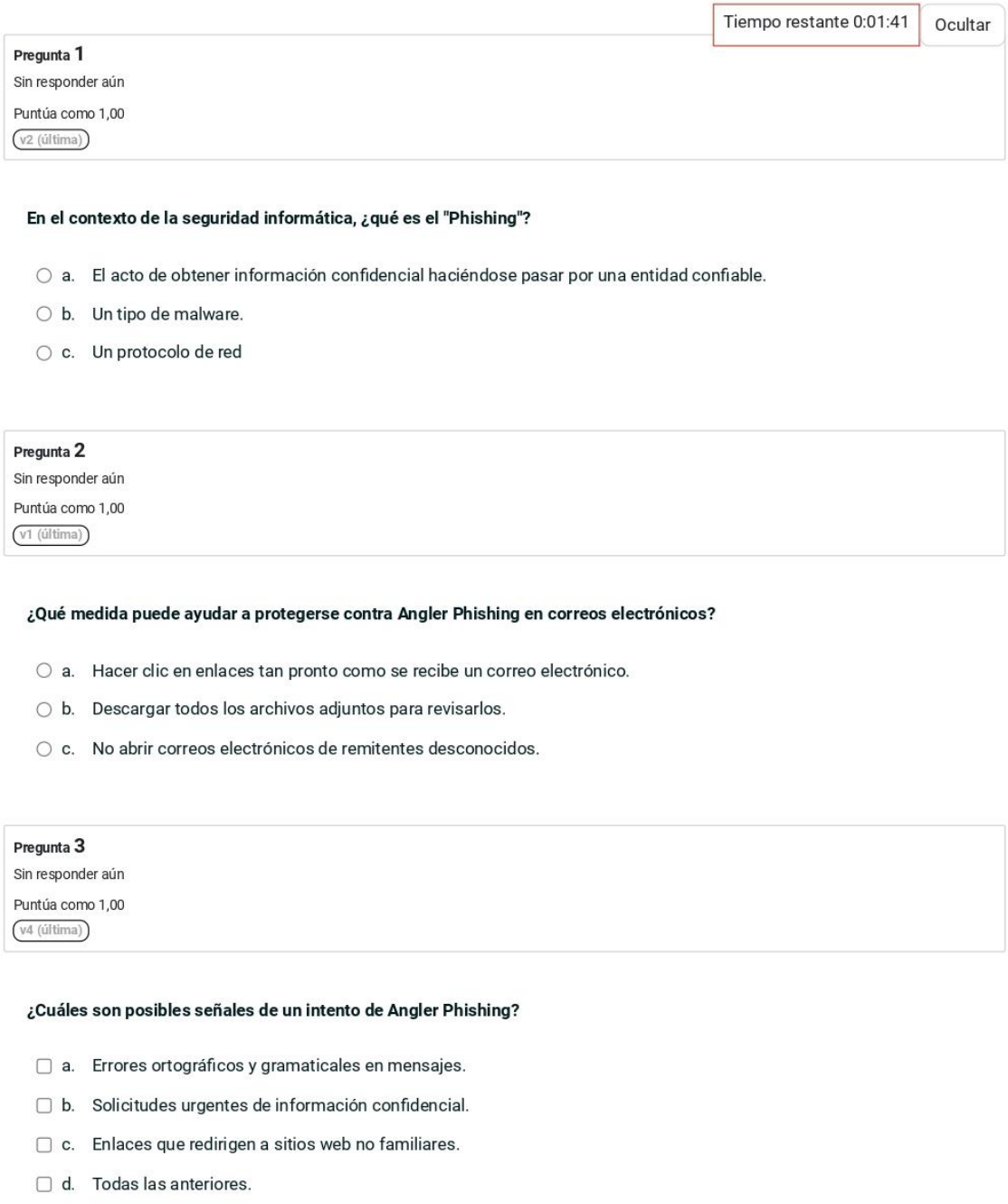

Figura D1. Preguntas 1,2,3 del test inicial.

Pregunta 4
Sin responder aún
Puntúa como 1,00
v1 (última)

¿Cómo podría verificar la autenticidad de un enlace antes de hacer clic en él?

- a. Ignorando el enlace y buscándolo en un motor de búsqueda.
- b. Haciendo clic y verificando la URL después.
- c. Pasando el cursor sobre el enlace para ver la URL antes de hacer clic.

Pregunta 5
Sin responder aún
Puntúa como 1,00
v2 (última)

¿Cuál de las siguientes situaciones podría ser un ejemplo de Angler Phishing?

- a. Un protocolo de red.
- b. Un mensaje en una red social que ofrece un enlace para ganar un premio.
- c. Un correo electrónico que solicita cambiar la contraseña de una cuenta bancaria.

Pregunta 6
Sin responder aún
Puntúa como 1,00
v1 (última)

¿Por qué es importante verificar la autenticidad de los enlaces antes de hacer clic en ellos?

- a. Para mejorar la velocidad de carga de la página.
- b. Para evitar errores de redirección
- c. Para protegerse contra sitios web maliciosos.

Pregunta 7
Sin responder aún
Puntúa como 1,00
v1 (última)

¿Cómo podría alguien ser víctima de Angler Phishing en plataformas de redes sociales?

- a. Al descargar archivos adjuntos de correos electrónicos desconocidos.
- b. Al responder a preguntas personales en comentarios públicos.
- c. Al hacer clic en enlaces maliciosos en mensajes o publicaciones.

Figura D2. Preguntas 4,5,6,7 del test inicial.

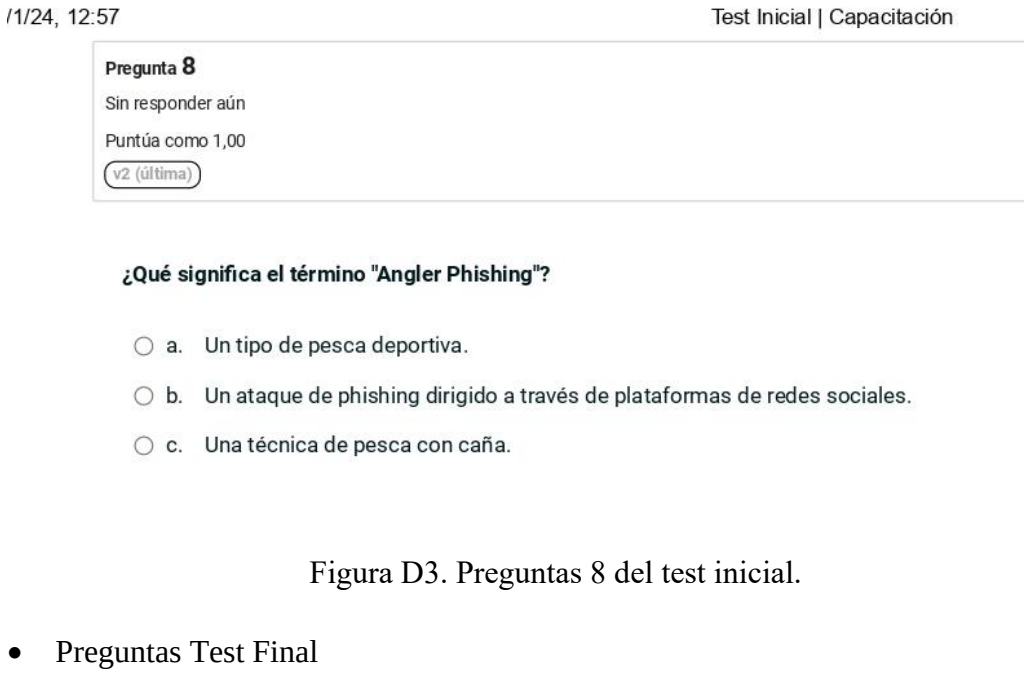

Figura D3. Preguntas 8 del test inicial.

- Preguntas Test Final

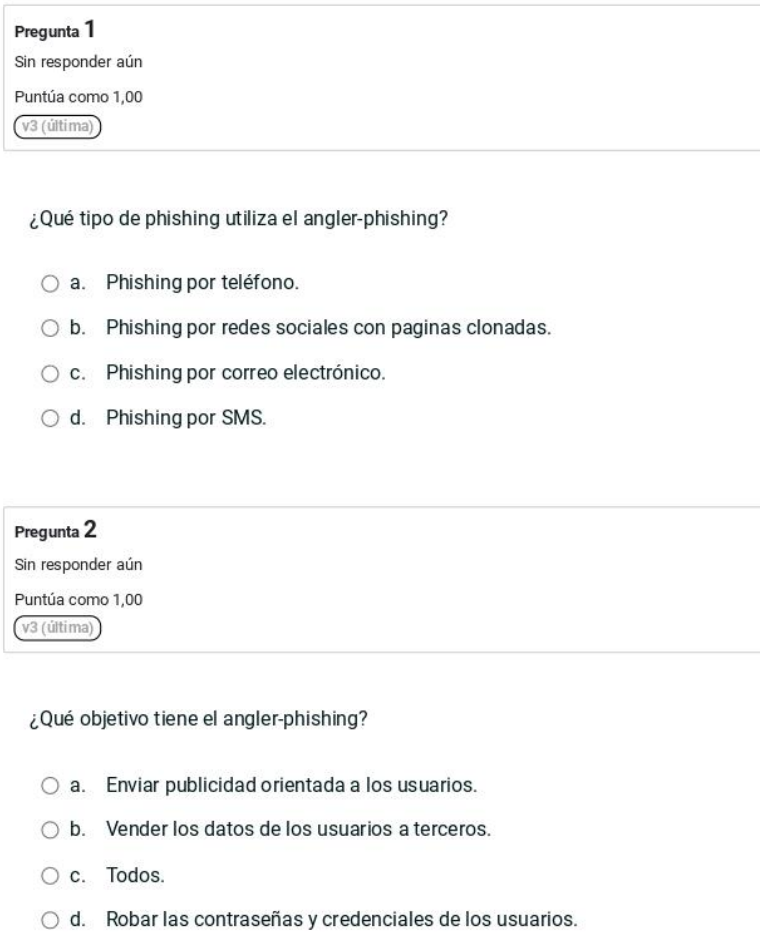

Figura D4. Preguntas 1,2 del test final.

Pregunta 3

Sin responder aún

Puntúa como 1,00

v5 (última)

¿Cómo se realiza un ataque de angler-phishing?

- a. Los ciberdelincuentes crean una página web falsa que simula ser la página oficial de una empresa o organización y envían un enlace malicioso a los usuarios.
- b. Todos.
- c. Los ciberdelincuentes utilizan técnicas de ingeniería social para convencer a los usuarios de que revelen información confidencial o hagan clic en enlaces maliciosos.
- d. Los ciberdelincuentes se dirigen a los clientes descontentos de una empresa y se hacen pasar por representantes de atención al cliente o entidades de confianza.

Pregunta 4

Sin responder aún

Puntúa como 1,00

v4 (última)

¿Qué técnica usan los estafadores para hacerse pasar por una empresa o institución legítima en las redes sociales?

- a. Usan llamadas telefónicas.
- b. Crean cuentas falsas con nombres, fotos y descripciones similares a los oficiales.
- c. Usan mensajes con enlaces web que han sido suplantados o clonados.
- d. Usan cuentas reales que han sido compradas.

Figura D5. Preguntas 3,4 del test final.

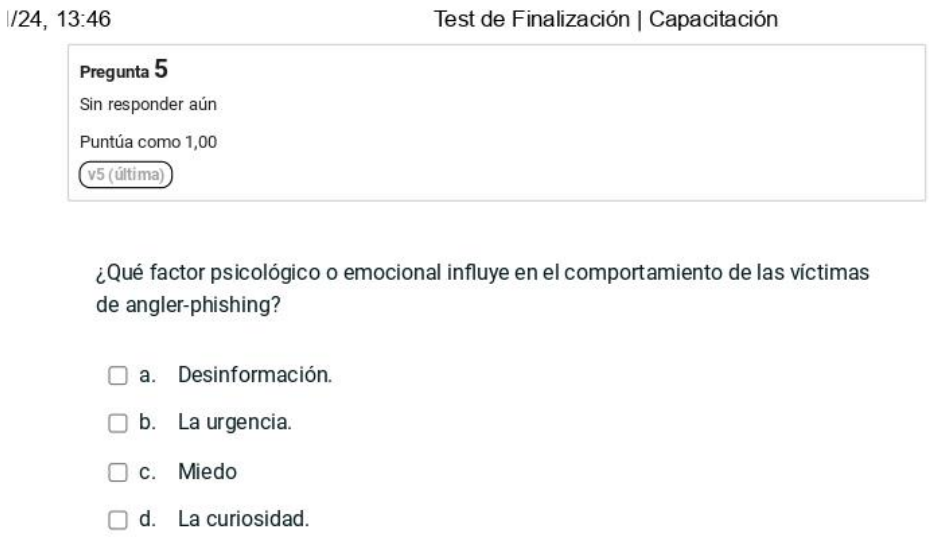

Figura D6. Preguntas 5 del test final.

Anexo E. Porcentaje de actividades y curso completado.

Dirección de correo	Test Inicial	Conceptos basicos sobre ingenieria social	Cómo Funciona Angler Phishing	Escenario: Entidad Bancaria	Retroalimentación: Entidad Bancaria	Escenario: Pagina Deportiva	Preguntas sobre la pagina de noticias deportivas	Escenario: Pagina de compras en línea	Retroalimentación: Compras en línea	Escenario: Chat simulado	Retroalimentación: Escenario 4	Test de Finalización	Actividades finalizadas	Activiades No finalizadas	Total	Porcentaje Curso	Curso Finalizado
enriqueminigua	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
cristalacosta18	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
kiup082005@gr	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
sanderinfante72	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
jbalarez@gmail.	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	1	11	12	8%	No finalizado
catalinassalced	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
edinsonbonilla@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
piedadb90@gm	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
ocalderon3322(	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
scaroc21@gma	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
munircastromu	Finalizado (no h	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
katerincecen20	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	1	11	12	8%	No finalizado
martha123@gm	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	0	12	12	0%	No finalizado
falesesha@gma	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	10	2	12	83%	No finalizado
3robtichachaloj	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
chambak099@g	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
edisonchancus	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	0	12	12	0%	No finalizado
elizabcha2016(	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
christian.chico2	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	0	12	12	0%	No finalizado
chitoomar45@g	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
fresasconchocc	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
jessicaregistrad	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	11	1	12	92%	No finalizado
juanmanucobo(	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	10	2	12	83%	No finalizado
nacontrerasg@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
coparamarlonm	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
karinamishell.14	Finalizado (ha a	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
aleshili21@gma	Finalizado (ha a	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	11	1	12	92%	No finalizado
juanahumadaf(	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
yedicar@gmail.	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
erikadorado112	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
julian1912@gm	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	11	1	12	92%	No finalizado
alexesco234@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
damian.jona@g	Finalizado (ha a	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	4	8	12	33%	No finalizado
crissvfc@gmail.	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	7	5	12	58%	No finalizado
jaimegaitanq@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	10	2	12	83%	No finalizado
gamingmanquit	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	Finalizado	10	2	12	83%	No finalizado
cegcontador@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
remanos2012@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
leninjoel386@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
estebanguanolu	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
alejo23guzman(	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
marlonisaac200	Finalizado (ha a	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
jindeariel@hotn	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	0	12	12	0%	No finalizado
jindeerick76@g	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	0	12	12	0%	No finalizado
arieljindes@gm	Finalizado (no h	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado

Figura E1. Cuadro de finalización de las actividades 1.

randyjinde@gm	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	7	5	12	58%	No finalizado
jindeariel@gma	Finalizado (ha a	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	Finalizado	7	5	12	58%	No finalizado
2juanlaguaquiz	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
saulleonc@gma	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
wilsonlpez@gm	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
wilmermacas12	Finalizado (ha a	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	3	9	12	25%	No finalizado
maciasandy655	Finalizado (no h	No finalizado	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	9	3	12	75%	No finalizado
yesid.malaver@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
hmaldo59@gma	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	10	2	12	83%	No finalizado
mimartinezp@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
famase55@gma	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
matamen3023@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
paul05futbol@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	6	6	12	50%	No finalizado
cmbouzas1@gr	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
mishelpilamung	Finalizado (ha a	No finalizado	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	9	3	12	75%	No finalizado
milemorafe@gr	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	11	1	12	92%	No finalizado
jaminsonmoren	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
moyolemakarer	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
isa.0617@gmai	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
gaotmusica@gr	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
dianaorozco01(	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
enriquotero@gr	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	1	11	12	8%	No finalizado
otojonathan47@	Finalizado (no h	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	10	2	12	83%	No finalizado
paolapadilla010	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	No finalizado	5	7	12	42%	No finalizado
johnpalate991@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
eramirez.aseso	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
meliperezb@gn	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
edupi1002@gm	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	4	8	12	33%	No finalizado
jesusmiriam969	Finalizado (no h	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	2	10	12	17%	No finalizado
myriampilamun	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	4	8	12	33%	No finalizado
quintanaisrael0	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	Finalizado	10	2	12	83%	No finalizado
fernandoiid@gn	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	10	2	12	83%	No finalizado
maraes@gmail.	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
stevenreal832@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
richi2869@gma	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
felika76@gmail	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	Finalizado	6	6	12	50%	No finalizado
katta2918@gm	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
roldanp2021@g	Finalizado (no h	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	6	6	12	50%	No finalizado
jeffersonamado	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	10	2	12	83%	No finalizado
emmabeatrizsis	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	Finalizado	2	10	12	17%	No finalizado
charlisol002@g	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	No finalizado	Finalizado	1	11	12	8%	No finalizado
sofia2004tapia(	Finalizado (no h	No finalizado	No finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	Finalizado	No finalizado	Finalizado	5	7	12	42%	No finalizado
rosa30toapanta	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
wilfridotoapanta	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
uuussuario1@g	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
anyulurrea@gm	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
cvalenciaaldana	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	11	1	12	92%	No finalizado
cesarvanegasr@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	10	2	12	83%	No finalizado
jimena.vargas@	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	8	4	12	67%	No finalizado
ing.leydyvargas	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado

Figura E2. Cuadro de finalización de las actividades 2.

juanfernandov1	Finalizado (ha a	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	11	1	12	92%	No finalizado
anahivillegas14	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	12	0	12	100%	Finalizado
vizcainobejaran	Finalizado (ha a	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	No finalizado	Finalizado	9	3	12	75%	No finalizado
arrozmorenozz5	Finalizado (no h	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	Finalizado	No finalizado	Finalizado	11	1	12	92%	No finalizado

Figura E3. Cuadro de finalización de las actividades 3.

Anexo F. Delta t” entre el test inicial y final.

Apellido(s)	Nombre	Dirección de correo	Calificación/ 10,00 test final	Calificación/ 10,00 test inicial	Delta T
3221	MixiGame	iqueminiguano@gmail.c	9	7,5	1,5
Acosta López	Cristal Yanela	istalacosta184@gmail.co	3	7,5	-4,5
Acurio	Dario	kiup082005@gmail.com	10	7,5	2,5
Arroba	Alexander	nderinfante720@gmail.c	5	7,5	-2,5
horquez Salce	Catalina	talinassalcedo@gmail.co	10	6,25	3,75
Bonilla Jimene	Edinson	dinsonbonilla@gmail.cor	8	7,5	0,5
BUSTOS	PIEDAD	piedadb90@gmail.com	10	7,5	2,5
Calderon	Oscar	calderon3322@gmail.co	9	6,25	2,75
CARO CAMELO	SANDRA	scaroc21@gmail.com	9	6,25	2,75
CASTRO	MUNIR	nircastromunoz@gmail.c	4	6,25	-2,25
Cervantes	Leidys	falesesha@gmail.com	10	7,5	2,5
Chachalo	Joseph	tichachalojoseph@gmail	2	8,75	-6,75
Chamba	Kevin	chambak099@gmail.com	5	3,75	1,25
Chaves Zafra	Elizabeth	lizabcha2016@gmail.cor	9	5	4
Chito	Omar	chitoomar45@gmail.com	4	6,25	-2,25
Chocolates	Fresas	sconchocolates2@gmail	10	10	0
uentes Martir	Jessica Liseth	icaregistraduria@gmail.c	10	7,5	2,5
Cobos	Juan Manuel	anmanucobo@gmail.co	10	6,25	3,75
ontreras Guac	Nubia Amparo	nacontrerasg@gmail.com	9	7,5	1,5
Cunuhay	Karina	inamishell.1409@gmail.c	0	7,5	-7,5
David	Alex	aleshili21@gmail.com	2	8,75	-6,75
DE LA CRUZ	AN ADALBER	uanahumadaf@gmail.cor	9	5	4
Diaz	enis DelCarme	yedicar@gmail.com	9	6,25	2,75
Dorado Suarez	Erika Mayerly	kadorado1127@gmail.co	9	6,25	2,75
Escobar	Alex	alexesco234@gmail.com	9	8,75	0,25
Escobar	Jonathan	damian.jona@gmail.com	0	8,75	-8,75
FORIGUA CAR	RISTINA VANE	crissvfc@gmail.com	10	7,5	2,5
aitan Quimba	Jaime Alberto	aimegaitanq@gmail.com	9	8,75	0,25
Gaming	Manquitos	mingmanquitos@gmail.c	3	3,75	-0,75
Garcia	Cristian	cegcontador@gmail.com	10	6,25	3,75
NZALEZ SANC	JUAN MIGUEL	emanos2012@gmail.cor	9	3,75	5,25
Guaman	Lenin	leninjoel386@gmail.com	6	8,75	-2,75
Guanoluisa	Esteban	anguanoluisa2002@gma	1	5	-4
Guzmán	Alejandro	ejo23guzman@gmail.co	0	5	-5
Isaac	Marlon	arlonisaac2002@gmail.c	3	7,5	-4,5
Jinde	Hernan	arieljindes@gmail.com	10	2,5	7,5
Jinde Sisa	Ariel	jindeariel@gmail.com	10	8,75	1,25
Laguaquiza	Juan	uanlaguaquiza@gmail.co	4	7,5	-3,5
Len	Saul Orlando	saulleonc@gmail.com	10	7,5	2,5
LOPEZ BERNA	WILSON	wilsonlpez@gmail.com	9	6,25	2,75
MACAS	WILMER	ilmermacas12@gmail.co	4	7,5	-3,5
Macias	Andy	aciasandy659@gmail.co	1	2,5	-1,5
Malaver Sanche	Wilfer Yesid	esid.malaver@gmail.cor	9	5	4

Figura F1. Cuadro de calculo de delta t” del test inicial y final 1.

Maldonado	Hernando	hmaldo59@gmail.com	4	6,25	-2,25
Martinez	Milton	mimartinezp@gmail.com	10	8,75	1,25
Martinez Serp	Fabian Alfonso	famase55@gmail.com	10	6,25	3,75
Mata	Daniel	hatamen3023@gmail.co	4	10	-6
Medina	Jan Paul	paul05futbol@gmail.com	8	8,75	-0,75
Mendez Bouza	Carolina	cmbouzas1@gmail.com	9	5	4
Mishel	Beautyby	helpilamunga68@gmail.c	4	8,75	-4,75
MORALES	CONSTANZA	milemorafe@gmail.com	6	5	1
oreno Rodrigu	Jaminson	minsonmoreno@gmail.co	10	7,5	2,5
Murillo	Isabel	isa.0617@gmail.com	9	6,25	2,75
OCAMPO	GABRIEL	gaotmusica@gmail.com	6	6,25	-0,25
Orozco	Diana Maritza	ianaorozco01@gmail.co	10	3,75	6,25
Oto	Jonathan	tojonathan47@gmail.co	4	6,25	-2,25
palate	john	ohnpalate991@gmail.co	2	8,75	-6,75
Pea	duardo Ramre	mirez.asesorias@gmail.c	10	6,25	3,75
Perez	Beatriz Meliss	meliperezb@gmail.com	7	6,25	0,75
Quintana	Israel	ntanaisrael070@gmail.c	6	5	1
Ramirez	Luis	fernandoiid@gmail.com	8	5	3
Ramrez	Mauricio Andr	maraes@gmail.com	9	5	4
Real	Steven	tevenreal832@gmail.co	9	8,75	0,25
odrguez Garc	Ricardo	richi2869@gmail.com	10	6,25	3,75
Rojas	Yanet	felika76@gmail.com	10	7,5	2,5
Rojas Leon	Sofia Lorena	katta2918@gmail.com	10	7,5	2,5
Roldan	Oscar	roldanp2021@gmail.com	3	6,25	-3,25
Sierra	efferson Amad	fersonamados@gmail.co	10	3,75	6,25
Tapia	Sofia	ofia2004tapia@gmail.co	0	3,75	-3,75
Toapanta	Rosa	a30toapanta08@gmail.c	4	5	-1
Toapanta	Wilfrido	ridotoapanta06@gmail.c	10	10	0
Uno	Usuario	uuussuario1@gmail.com	8	7,5	0,5
Urrea Prez	Anyul	anyulurrea@gmail.com	8	8,75	-0,75
alencia Aldan	Camilo Andres	alenciaaldana@gmail.co	10	7,5	2,5
anegas Ramir	Cesar Augusto	esarvanegasr@gmail.co	9	8,75	0,25
Vargas Mayo	Maria	mena.vargas@gmail.co	7	6,25	0,75
VARGAS SOLE	LEYDY JOHAN	g.leydyvargas@gmail.co	10	5	5
Villarreal	Juan	nfernandov111@gmail.c	8	8,75	-0,75
Villegas	Anahi	ahivillegas1422@gmail.c	4	5	-1
zcaino Bejara	Jesus	nobejarano.jesus@gmai	10	3,75	6,25
Zambrano	Daniel	ozmorenozz555@gmail.c	6	5	1
Promedio			7,09	6,63580247	0,45061728

Figura F2. Cuadro de cálculo de delta t” del test inicial y final 2.

Figura G1. Capacitación mediante el curso en moodle día 1.

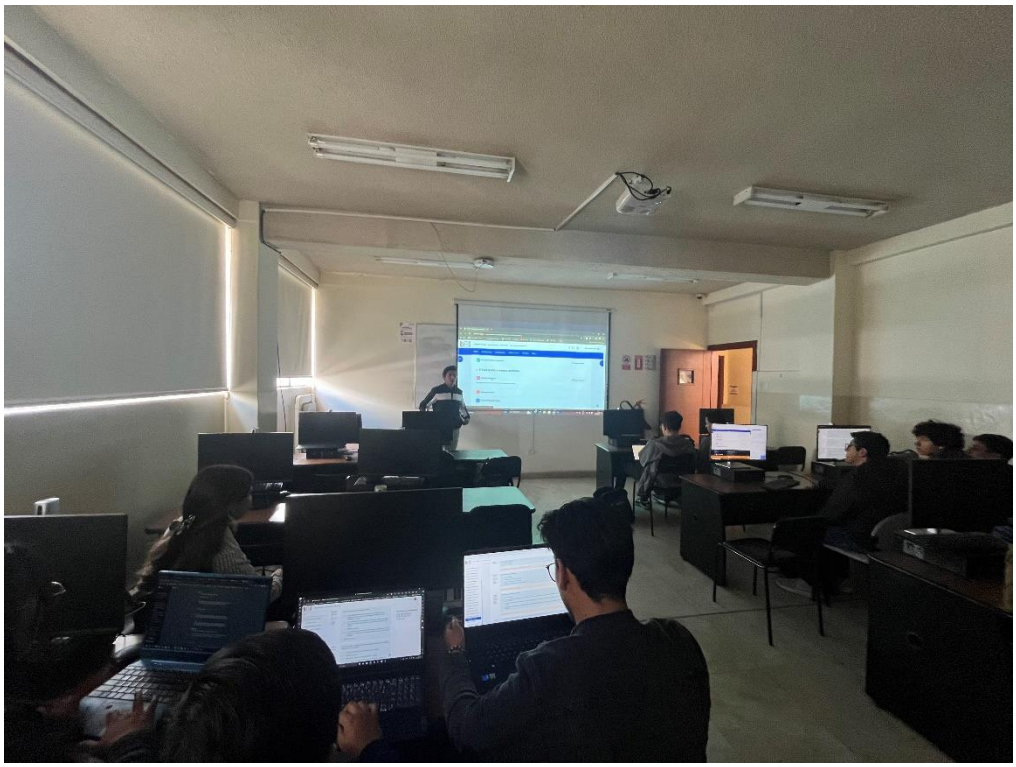

Figura G2. Capacitación mediante el curso en moodle día 2.

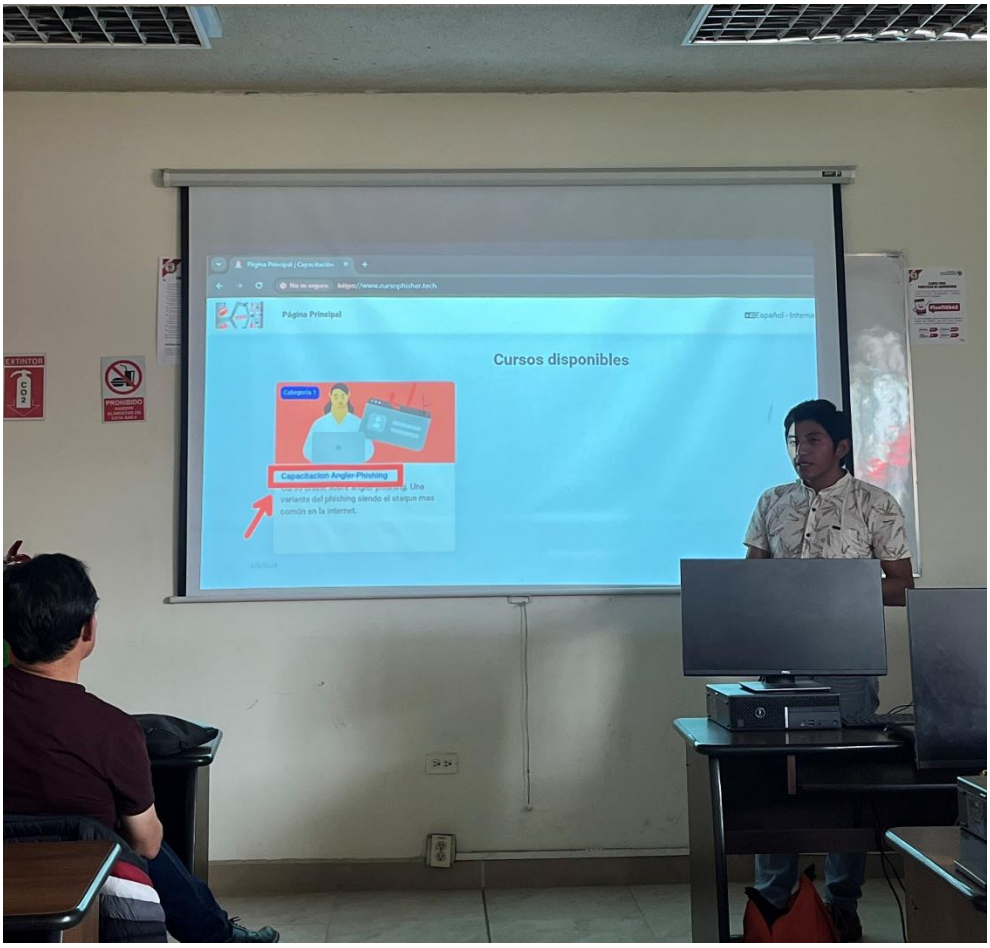

Figura G3. Capacitación mediante el curso en moodle día 3.

Figura G4. Evaluación mediante el curso en moodle día 3.

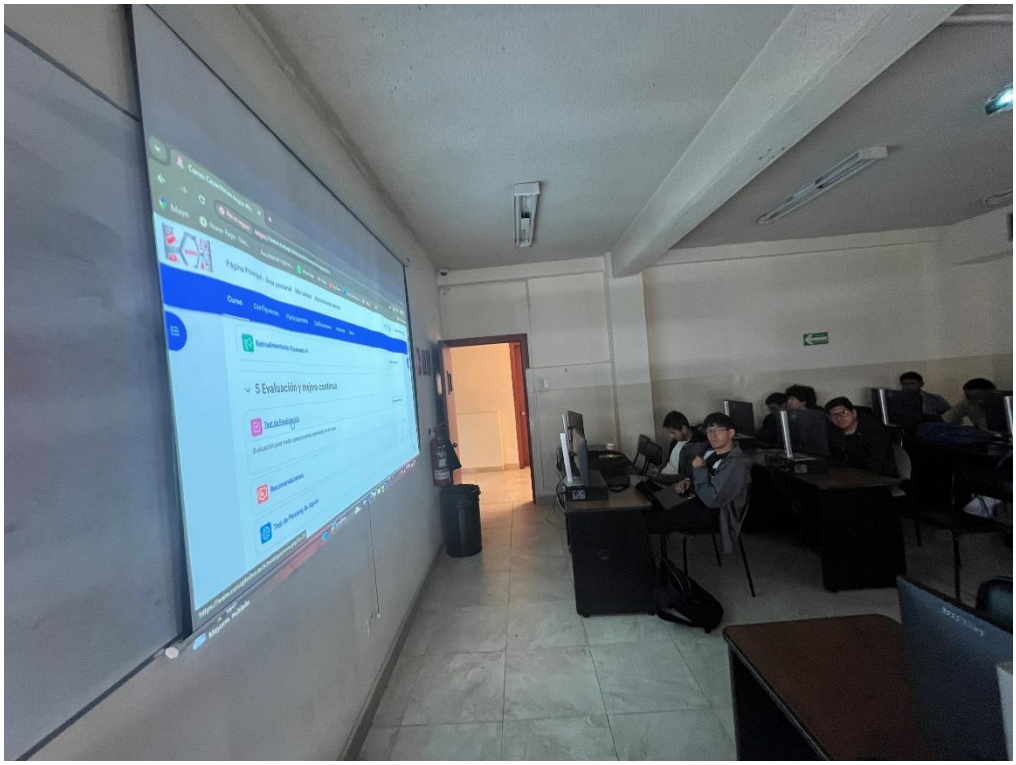

Figura G5. Evaluación mediante el curso en moodle día 1.