UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR
UNTELS

FACULTAD DE INGENIERÍA Y GESTIÓN

CARRERA PROFESIONAL

INGENIERÍA DE SISTEMAS

PLAN DE TESIS

"PROPUESTA DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS PARA LA PREVENCIÓN DE ATAQUES DE PHISHING EN LA SEGURIDAD DE LA INFORMACIÓN EN ENTORNOS EDUCATIVOS"

PARA OPTAR EL TÍTULO DE

INGENIERO DE SISTEMAS

PRESENTADO POR:

FIGUEROA GONZALEZ, GINER BUSH
GUTIERREZ GUTIERREZ, DANAHE ARLENI

ASESOR:

ESCOBEDO BAILÓN, FRANK EDMUNDO

Villa El Salvador, 2025

ÍNDICE

CAPÍTULO I

I. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

Recientemente, los ciberataques en el ámbito educativo se han incrementado, particularmente los ataques de phishing, en el cual se intenta engañar a los usuarios para robar información personal o privada. Este tipo de ataques se dirigen con interés a las entidades educativas, pues estas manejan y procesan información de estudiantes, docentes y administrativos, además no cuentan con ciberseguridad adecuada para enfrentar los delitos.

Según la ESET, en el primer trimestre Perú no se diferencia de la tendencia regional. En la región, los ciberataques reportaron un incremento de 37% con un promedio de 3086 ataques a la semana, siendo 2721 de estos ataques en América Latina. La digitalización del sistema educativo en la región con el uso de recursos y plataformas educativas han facilitado el acceso a la información para los estudiantes, pero también han expuesto el sistema educativo a nuevos ataques.

En el caso de Perú, la situación no es diferente. De acuerdo con un informe de ESET (2025), durante los primeros meses del año, el 62 % de los ciberataques registrados corresponden a campañas.

En el caso peruano, los primeros meses de 2024 registraron más de un millón de ciberataques. Aunque esta cifra es ligeramente menor en comparación con el año anterior, las principales amenazas continúan siendo el phishing y el ransomware, especialmente dentro del sistema universitario, donde se maneja gran cantidad de información confidencial y los sistemas suelen presentar puntos vulnerables (ESET, 2024).

En diciembre de 2024, la Universidad Peruana de Ciencias Aplicadas (UPC) sufrió un grave incidente de seguridad: un grupo liderado por el hacker denominado *Ex Case 20* filtró 25 GB de información confidencial en un foro clandestino. Los datos postearon nombres completos, códigos de matrícula, direcciones de correo (personales e institucionales), teléfonos y fotografías de credenciales universitarias. Este ataque reveló importantes debilitamientos en las

defensas digitales de la UPC y generó alarma entre estudiantes y docentes (Cyber Management Alliance, 2025).

Un mes después, en enero de 2025, la revista estudiantil de la Facultad de Comunicación y Periodismo de la UPC también fue atacada. Durante varios días, su sitio fue invadido por anuncios de casinos en diferentes idiomas, y así desplazaron todo el contenido original. Este segundo evento reforzó la percepción de vulnerabilidad en los sistemas digitales de la universidad (Cyber Management Alliance, 2025).

Por otro lado, en octubre de 2019, la Universidad de Oriente en El Salvador fue vinculada con un ataque cibernético contra la revista Factum. Según una auditoría forense, una dirección IP de la universidad se utilizó para escanear vulnerabilidades en el servidor de la revista y lanzar un ataque DDoS, que dejó fuera de línea el sitio durante aproximadamente una semana, muchas investigaciones internas revelaron que un empleado había instalado software no autorizado para llevar a cabo estas acciones (Qurium, 2020).

Estos casos demuestran claramente la urgencia de fortalecer las estrategias de ciberseguridad en las instituciones educativas, con el fin de proteger los datos sensibles de estudiantes y personal, así como de asegurar la continuidad de las actividades académicas en entornos digitales cada vez más expuestos a amenazas.

1.2 Formulación del problema

1.2.1 Problema general

¿Cómo aplicar una metodología de gestión de riesgos, basada en un enfoque iterativo (SCRUM), que permita prevenir ataques de phishing y fortalecer la seguridad de la información en instituciones educativas?

1.2.2 Problemas específicos

- ¿Qué vulnerabilidades existen actualmente en las instituciones educativas frente a los ataques de phishing que deben ser consideradas en la metodología de gestión de riesgos?

- ¿Qué herramientas o tecnologías pueden integrarse en la metodología para prevenir y detectar intentos de phishing de manera eficaz?
- ¿Qué nivel de concientización tienen los estudiantes, docentes y personal administrativo sobre los riesgos del phishing, y cómo puede mejorarse mediante la aplicación de la metodología?
- ¿Qué políticas y protocolos deben formar parte de la metodología de gestión de riesgos para garantizar una respuesta eficiente ante ataques de phishing?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Proponer una metodología de gestión de riesgos orientada a la prevención de ataques de phishing que permita fortalecer la seguridad de la información en entornos educativos.

1.3.2 Objetivos específicos

- Identificar las principales vulnerabilidades presentes en las instituciones educativas frente a los ataques de phishing.
- Analizar las herramientas y tecnologías que pueden integrarse en la metodología para prevenir y detectar intentos de phishing.
- Evaluar el nivel de concientización de estudiantes, docentes y personal administrativo respecto a los riesgos del phishing.
- Establecer políticas y protocolos institucionales que complementen la metodología para una respuesta eficiente ante incidentes de phishing.
- Diseñar una metodología iterativa (basada en SCRUM) que combine controles tecnológicos, procesos de formación y lineamientos institucionales para gestionar los riesgos de phishing en entornos educativos.

1.4 Delimitación de la investigación

1.4.1 Delimitación espacial

La aplicación de la metodología de gestión de riesgos para la prevención de ataques de phishing se llevará a cabo en instituciones educativas ubicadas en Villa El Salvador, principalmente en universidades y centros que utilizan plataformas digitales para la gestión académica y administrativa. Estas instituciones fueron seleccionadas por su alta exposición a ataques cibernéticos, derivada tanto del volumen de información sensible que administran como de su nivel de digitalización y uso intensivo de tecnologías en la enseñanza virtual. La elección de Villa El Salvador responde a su representatividad como polo educativo y tecnológico del país, lo que permitirá obtener resultados relevantes y extrapolables a otros contextos educativos similares a nivel nacional.

1.4.2 Delimitación temporal

La investigación estará siendo realizada desde abril del 2025 hasta febrero del 2026. Este período incluye todas las fases del trabajo: desde el diagnóstico de las vulnerabilidades, el diseño y la implementación de la metodología de gestión de riesgos, la capacitación de los usuarios y la evaluación de dicha metodología. Este cronograma ha sido diseñado de tal manera que el despliegue de actividades se logre de forma adecuada. Esto asegura que se cuente con un tiempo suficiente para un análisis y aplicación de la metodología que sea práctica, vigente y útil. Esto incluye la revisión de la práctica para la incorporación de evaluaciones, retroalimentación de la comunidad educativa, la revisión de la seguridad informática en el sector educativo, la incorporación de amenazas contemporáneas y el uso de nuevas tecnologías.

1.5 Hipótesis

1.5.1 Hipótesis general

La implementación de una metodología de gestión de riesgos orientada a prevenir ataques de phishing mejora la seguridad de la información en entornos educativos y minimiza los riesgos y mejora las salvaguardias de la información sensible.

1.5.2 Hipótesis específicas

- La metodología de gestión de riesgos ayuda a identificar y evaluar la vulnerabilidad al phishing en las plataformas digitales de evaluación de riesgos utilizadas por las instituciones educativas y en su priorización.
- La integración de herramientas tecnológicas y programas de capacitación dentro de la metodología aumenta la concienciación y la prevención del phishing de los estudiantes, docentes y personal administrativo.
- La incorporación de políticas y protocolos de respuesta delineados dentro de la metodología mejora la capacidad de los entornos educativos para mitigar y recuperarse de ataques de phishing.
- La evaluación continua de la metodología evidencia una disminución de las vulnerabilidades asociadas al phishing y un fortalecimiento de la cultura institucional de ciberseguridad.

1.6 Justificación del problema

Actualmente, las instituciones educativas se han convertido en blancos frecuentes de ataques informáticos y su informe de Watchguard, estos incidentes aumentaron en un 258 % durante el último año, mientras que las violaciones de datos se incrementaron en un 546 %, los datos evidencian la necesidad crítica de reforzar las políticas de ciberseguridad en el sector educativo, con el fin de resguardar la información sensible y asegurar la continuidad operativa de las actividades académicas.

Las universidades y colegios son uno de los sectores más vulnerables a las amenazas digitales teniendo en cuenta la enorme cantidad de datos personales y académicos que manejan, y las consecuencias de estos ataques pueden ir desde accesos a información hasta accesos no autorizados a plataformas educativas por lo que toda la comunidad educativa docentes, estudiantes, personal administrativo debe estar enterada de estos riesgos y adoptar prácticas seguras en el entorno digital.

Ante este desafío, diversos países de América Latina entre ellos Colombia han desarrollado proyectos para la enseñanza de la ciberseguridad en colegios, y varias de estas propuestas son de corte lúdico, con resultados que permiten comunicar saberes tecnológicos en forma sencilla y evaluar de modo eficiente lo aprendido por los participantes.

El Estado español realizó una aportación a nivel internacional de 1.157 millones de euros para reforzar su estrategia nacional de ciberseguridad cuya finalidad es que puedan perfeccionar sus procesos de prevención, detección y respuesta a los ataques digitales y con especial atención a las infraestructuras esenciales como instituciones educativas. Having an information security policy in the educational field becomes essential to mitigate the risks faced by students when interacting with digital environments, policies should include technical measures, such as the use of protection software, and training actions aimed at encouraging responsible use of technology and protection of personal and academic information.

Según Klarway (2023), establecer una visión clara y actualizada sobre las amenazas digitales que enfrenta permite tomar una postura proactiva ante las vulnerabilidades y mitigar de forma significativa los daños que pudieran ocasionarse ante un ciberataque. Asimismo, incentivar la enseñanza de ciberseguridad desde el nivel escolar puede contribuir a prevenir conductas de riesgo, como la cometida por el delito de robo de identidad.

En ese sentido, El Puente (2024) destaca la importancia de incluir la temática de seguridad digital en los currículos, ya que además de permitir que los estudiantes naveguen con mayor seguridad en ambientes virtuales, también evita que sufran consecuencias negativas en el plano emocional, social y académico.

Considerando que la información personal fluye continuamente a través del ecosistema digital, es vital desarrollar estrategias de protección claras. Protecdata Lat (2024) sugiere utilizar la autenticación fuerte, cifrado de datos y protocolos de respuesta inmediata ante incidentes para preservar la privacidad y la confianza de los usuarios.

Un caso a destacar es el del MOOC de seguridad informática implementado en Ecuador, llevado adelante por el Departamento de

Educación y coordinado por Isaac Jesús Barrer. La propuesta, creada de forma interactiva, ha resultado ser realmente efectiva para concientizar a los alumnos en materia digital y, a su vez, es posible utilizarla en diferentes ámbitos escolares.

Estudios recientes proponen metodologías que pueden replicarse en diferentes organizaciones para incorporar programas de capacitación en seguridad digital desde la educación primaria y secundaria. Estos modelos buscan crear comunidades escolares informadas y preparadas para abordar las ciberamenazas, considerando las necesidades y características específicas de cada entorno educativo.

Mientras tanto, 4S Solutions, con sede en Palo Alto, ha creado programas innovadores que se han implementado en numerosas escuelas, utilizando métodos innovadores para impartir conceptos básicos de seguridad digital. Las tácticas han demostrado ser exitosas, fáciles de replicar y adecuadas para fomentar una cultura de prevención desde edades tempranas.

Desde 2019, la Universidad Rey Juan Carlos organiza la "Cyberleague", un evento en el que profesores y estudiantes colaboran para encontrar vulnerabilidades en sistemas reales. Esta experiencia ha sido reconocida como una herramienta práctica para la capacitación en ciberdefensa, inspirando a otros académicos a establecer modelos similares que impulsen sus propias competencias digitales.

CAPÍTULO II

II. MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1. Antecedentes Nacionales

-Aredo (2021) realizó una investigación con el objetivo de determinar cómo el phishing afecta la protección de los datos personales en el contexto de los delitos informáticos, poniendo especial atención en el marco legal peruano, de igual modo su estudio define al phishing como una apropiación ilegal de información a través de engaños en línea, resaltando su impacto no solo en la privacidad personal, sino también en la comisión de otros delitos relacionados, como el fraude y el robo de identidad, asimismo identificó que la ausencia de una tipificación específica para el phishing en la legislación peruana que representa un obstáculo considerable para su rastreo, agravado por la limitada conciencia digital de la población.

El autor resalta que la vulnerabilidad de la normativa respecto a definiciones precisas y actuales sobre los delitos informáticos, sumada a la baja educación digital de los usuarios, favorece la realización de estos ataques y las disposiciones vigentes del Código Penal de Perú son insuficientes para definir con exactitud el phishing, lo que dificulta su investigación legal y la importancia de reformas legislativas y campañas de concienciación que promuevan una cultura de prevención ante la ingeniería social, también subraya que estas medidas deben mantenerse estables y ajustarse a los cambios tecnológicos constantes.

Entre sus recomendaciones, Aredo sugiere la implementación de mecanismos de autenticación más robustos, como la verificación biométrica o tokens digitales, para proteger los datos personales y reducir la vulnerabilidad de los usuarios ante estas amenazas y las investigación aporta una perspectiva legal y preventiva valiosa para complementar las estrategias tecnológicas en el diseño de sistemas de protección contra el phishing especialmente en entornos educativos, donde la conciencia legal y digital aún puede ser limitada, resaltando la relevancia de las medidas de seguridad proactivas y multifactoriales.

-Ruiz & Solís (2024), realizaron un estudio donde se analiza la modalidad de fraude informático conocida como phishing desde la experiencia operativa de la División de Investigación de Delitos de Alta Tecnología en Lima, mucho de los entrevistas a efectivos policiales especializados, los autores detallan cómo los ciberdelincuentes envían grandes cantidades de correos electrónicos con enlaces maliciosos o archivos infectados, los cuales están diseñados para redirigir a sitios falsos que se presentan como entidades bancarias o instituciones legítimas.

El objetivo de estos ataques es robar información privada del usuario, como números de tarjeta, códigos CCI, contraseñas, claves token, DNI, datos personales para hacer un uso fraudulento sin su consentimiento, accediendo a sus cuentas y robando dinero, y también ha sido descubierto que el phishing, al ser difundido a través de medios masivos como el correo electrónico, los mensajes de texto o las redes sociales, se constituye como una de las principales formas de ataques a nivel cibercriminal, desafiando a la seguridad en línea día con día.

Por otro lado, el documento añade que la mayoría de estos ataques logran burlar los filtros de seguridad tradicionales, evidenciando la importancia de actualizar constantemente las medidas tecnológicas y reforzar la vigilancia cibernética dentro de las organizaciones, y también se resalta la necesidad de contar con canales de comunicación eficientes que permitan atender de manera rápida incidentes de suplantación de identidad, a la vez que se subraya la impotencia de defensas estáticas ante amenazas dinámicas y la colaboración entre usuarios y los equipos de TI para una detección y control rápida.

Este análisis deja clara la necesidad de reforzar los sistemas de protección de la información mediante mecanismos de detección temprana, capacitación a los usuarios y acciones preventivas que obstaculicen la suplantación de identidad, asimismo en el ámbito educativo, en el que también se utilizan estos mismos medios de comunicación digital, esta modalidad representa un riesgo latente, la implementación de sistemas específicos contra ataques de phishing es fundamental para proteger la integridad de los datos y también a la comunidad estudiantil y académica ante este tipo de delitos informáticos, contribuyendo a crear entornos digitales más seguros y resilientes, por ello es crucial que las instituciones educativas reconozcan esta vulnerabilidad y se comporten de manera proactiva.

-De la Cruz & Rodriguez (2025) investigan la relación entre el phishing y la vulneración de datos personales en la zona de Lima Sur, poniendo especial atención en los efectos negativos del robo de información mediante estafas digitales, a través de un enfoque cualitativo basado en entrevistas a operadores de justicia como abogados y efectivos policiales, que permitió evidenciar que este tipo de ciberdelito se encuentra en constante aumento, mientras que el marco legal peruano resulta insuficiente para enfrentarlo de manera adecuada, ya que la brecha normativa y la falta de tipificación clara del phishing dificultan la persecución efectiva de los ciberdelincuentes, generando un escenario de creciente impunidad.

El estudio destaca que la legislación actual, especialmente la Ley N.° 30096 sobre delitos informáticos, presenta debilidades en cuanto a la definición y sanción específica del phishing, lo que dificulta su persecución penal y limita la capacidad de respuesta ante los daños causados; además, se concluye que la falta de herramientas tecnológicas adecuadas y mecanismos de rastreo impide una acción efectiva contra los ciberdelincuentes, lo que agrava la situación de inseguridad digital, evidenciando la obsolescencia de los recursos existentes frente a la creciente sofisticación de estas amenazas.

Los autores también advierten que, en muchos casos, las víctimas no tienen conocimientos suficientes para identificar un ataque de phishing, lo cual aumenta su vulnerabilidad, y esta falta de alfabetización digital, sumada a la escasa cultura de prevención institucional, contribuye a que estos delitos pasen desapercibidos o no sean reportado y además, no todas las instituciones cuentan con protocolos claros para actuar ante este tipo de incidentes, lo que evidencia una brecha significativa en la capacidad de respuesta y protección de los usuarios.

Esta investigación ofrece un enfoque legal y práctico sobre cómo el phishing afecta la protección de los datos personales, planteando la necesidad de fortalecer tanto el marco normativo como las capacidades técnicas e institucionales, y en entornos educativos, donde la información personal de estudiantes, docentes y personal administrativo circula con frecuencia en medios digitales, esta problemática adquiere una relevancia crítica, haciendo indispensable la implementación de metodologías de protección contra ataques de phishing que integren medidas tecnológicas, legales y formativas.

-Lavinder (2016) analiza el creciente riesgo de ciberataques en América Latina, destacando el acelerado aumento del uso de Internet en la región y la consecuente exposición a amenazas como el phishing, señalando que países como Brasil, Colombia y Argentina se identifican como los principales emisores de ataques de phishing en América Latina, representando el 74 % de este tipo de incidentes en la región, lo cual plantea desafíos significativos para la protección de datos, tanto a nivel gubernamental como institucional, subrayando la urgencia de estrategias de ciberseguridad robustas ante la rápida expansión digital.

El artículo subraya que, aunque algunas naciones como Brasil y Colombia han avanzado con estrategias nacionales de ciberseguridad, muchos otros países latinoamericanos presentan bajos niveles de preparación, escasa capacidad de respuesta y marcos legales insuficientes; además, existe una limitada cultura de seguridad cibernética, especialmente en sectores públicos, educativos y pequeñas organizaciones, donde se tiende a subestimar la amenaza, lo que agudiza la vulnerabilidad frente a un panorama de amenazas en constante evolución.

Asimismo, se menciona que muchas instituciones no cuentan con personal capacitado para hacer frente a estos riesgos, ni con protocolos claros para actuar ante incidentes, mientras que la falta de preparación técnica básica agrava aún más la exposición a estas amenazas, y la ausencia de campañas masivas de educación digital también contribuye a la vulnerabilidad de los usuarios, por lo que este panorama exige una atención prioritaria por parte de los gobiernos y actores educativos, y sólo mediante un enfoque integral y una inversión sostenida en capacitación se podrá reducir el impacto del phishing en la región.

En esta línea, Lavinder resaltó que es necesario fortalecer las infraestructuras de ciberseguridad, promover la cooperación regional y construir una conciencia colectiva sobre los riesgos digitales; también subrayó que los sectores educativos tienen que encabezar procesos formativos en buenas prácticas digitales desde tempranas edades, y en el caso de instituciones educativas con enseñanza intensiva de tecnologías digitales dicta que es urgente reforzar la implementación de sistemas de protección frente a ataques de phishing que integren políticas institucionales claras, formación continua y herramientas tecnológicas eficaces.

-Zambrano et al. (2024), a partir de su investigación, plantean que es la situación actual del cibercrimen en América Latina la que mantiene una aceleración en su volumen que amenaza con continuar incrementándose en los sectores gubernamental, financiero, energético, educativo y la infraestructura crítica, y mediante una revisión sistemática de fuentes bibliográficas su investigación detecta que el phishing es una de las amenazas más comunes en la región junto con el ransomware, ataques de denegación de servicio (DDoS), inyección de SQL y malware. El artículo resalta que las vulnerabilidades más comunes en la región son consecuencia de la baja conciencia ciudadana en materia de ciberseguridad, el uso de tecnologías sin protocolos de protección, y la falta de preparación estructural en instituciones públicas y privadas, y aunque algunos gobiernos y organizaciones se esfuerzan por implementar medidas de protección, la inexistencia de una cultura de ciberseguridad madura continúa poniendo en riesgo los activos digitales y la información sensible.

Además, se advierte que muchas instituciones carecen de planes preventivos integrales, lo que limita su capacidad de respuesta ante incidentes, situación que es especialmente crítica en organizaciones educativas con recursos limitados y bajo nivel de capacitación digital, ya que la ausencia de estrategias proactivas y la dependencia de defensas reactivas dejan a estas entidades particularmente expuestas, por lo que resulta esencial que se invierta en programas de seguridad que incluyan tanto la tecnología como la formación del personal.

En ese sentido, se plantea la necesidad de trabajar de manera conjunta para fortalecer la ciberdefensa en América Latina, a través de la promoción de la educación digital, la sensibilización social y la cooperación entre naciones; dicho análisis cobra especial relevancia en ámbitos educativos, dado que la diversidad de usuarios con distintos niveles de competencia digital y la elevada dependencia de plataformas tecnológicas conforma un caldo de cultivo idóneo para ataques phishing, por lo que la implantación de mecanismos de protección dirigidos a este tipo de amenaza se torna imprescindible para asegurar la protección de la información en el campo académico.

2.1.2. Antecedentes Internacionales

-El estudio de Jerrim en (2023), el cual a partir de los datos de la prueba PISA realizó un análisis a nivel internacional con más de 170,000 jóvenes de 15 años de 38 países. Los resultados mostraron que los adolescentes con bajos niveles de habilidad lectora y de contextos socioeconómicos bajos, tendían a ser más víctimas de phishing y el autor también analizó el papel de la formación en ciberseguridad, encontrando que la enseñanza para reconocer el correos maliciosos reduce la vulnerabilidad de los estudiantes ante esta clase de fraude electrónico.Este análisis dio la oportunidad de determinar factores de riesgo vinculados con la habilidad de lectura y el nivel socioeconómico, a la vez que reforzaba la necesidad de introducir programas educativos que potenciarán la lectura crítica de los alumnos para identificar amenazas en línea.

Kayomb et al. (2025) introducen un enfoque metodológico de concienciación para la prevención de ataques de phishing en una universidad de ciencia y tecnología en Sudáfrica, basándose en la premisa de que el error humano representa el mayor vector de vulnerabilidad y en su propuesta se definen ejes de acción como la determinación de la frecuencia e impacto de los ataques, el estudio de las técnicas de phishing más comunes, la medición del grado de concienciación de los usuarios y el desarrollo de un programa formativo periódico.

Esta metodología posibilitó organizar un proceso de concientización y capacitación continua en la comunidad universitaria, que permitió efectuar una medición del grado de exposición de los usuarios a las estrategias de ingeniería social, y realizar la identificación de vacíos de conocimiento en seguridad informática.

El análisis de la información recabada contribuyó a identificar patrones de conducta, a consolidar áreas críticas de mejora y a fortalecer las buenas prácticas en el uso seguro de la información y los autores enfatizan que la realización sistemática de prácticas y evaluaciones en ámbitos simulados constituye un recurso efectivo para fortalecer la resiliencia institucional ante la amenaza de phishing.

-Marchenko et al. (2024) abordan la falta de conocimiento entre el personal en cuanto a amenazas de phishing, un vector de ataque común de ingeniería social que implica obtener acceso a información sensible sin autorización y sus hallazgos indican que las metodologías tradicionales para la formación en ciberseguridad, al no incluir elementos interactivos ni realistas, no son lo suficientemente efectivas para preparar a los usuarios. Por ende, los autores enfatizan la necesidad de una mayor dinamismo, que active al usuario participando en escenarios simulados.

Como enfoque alternativo, los investigadores sugieren el uso de GoFish, una herramienta que posibilita la simulación de ataques de phishing mediante correos electrónicos personalizados, la plataforma permite observar cómo responden los usuarios ante intentos simulados y recopilar información útil para evaluar su grado de exposición a estas amenazas la estrategia no solo mejora la comprensión del riesgo, sino que también brinda a las organizaciones la posibilidad de adaptar sus programas de capacitación y aplicar medidas correctivas de manera más efectiva, fomentando un aprendizaje activo y cuantificable, esencial para establecer hábitos sólidos en ciberseguridad.

Los resultados muestran que las simulaciones aumentan significativamente la capacidad del personal para reconocer intentos de phishing, mejorando la preparación institucional frente a estas amenazas y se enfatiza que el uso de datos recopilados en tiempo real permite implementar medidas preventivas más efectivas y específica, los autores reconocen el potencial de la inteligencia artificial y el aprendizaje automático para personalizar aún más los entrenamientos, incrementando su eficacia en el futuro.

Este estudio aporta un enfoque práctico y replicable para fortalecer la seguridad de la información mediante la concienciación de los usuarios, y resulta especialmente útil en contextos educativos donde la exposición a ataques de phishing representa un riesgo creciente, la incorporación de simulaciones como herramienta de aprendizaje constituye una estrategia para reducir errores y mejorar la resiliencia ante amenazas cibernéticas, estableciendo un modelo proactivo para la defensa contra la ingeniería social.

-Srikanth et al. (2024), investigan la aplicación de campañas simuladas de phishing como método didáctico para reducir los riesgos asociados a esta amenaza cibernética, que suele aprovecharse del error del usuario para obtener acceso a datos sensibles, en su trabajo se llevó a cabo una simulación de ataque trucha en un ambiente empresarial a través de un sitio web de comercio electrónico falso y mediante la utilización de Gofish herramienta de código abierto para enviar correos electrónicos masivos (email) a veces, el objetivo fue evaluar y fortalecer la capacidad del personal para resistir la ingeniería social, evidenciando la susceptibilidad del factor humano.

Esta metodología permitió observar las reacciones de los usuarios en un entorno seguro y recopilar métricas clave como la tasa de clics y el envío de credenciales el análisis de estos datos, los autores evaluaron el nivel de susceptibilidad del personal ante tácticas de ingeniería social, identificando patrones de comportamiento y áreas de mejora, estos ejercicio también sirvió como una herramienta de sensibilización, reforzando las buenas prácticas de ciberseguridad y aumentando la capacidad de los usuarios para reconocer amenazas reales, subrayando que la exposición controlada es una herramienta poderosa para el aprendizaje.

Los resultados del estudio evidencian la efectividad de las simulaciones como medio formativo, permitiendo desarrollar medidas preventivas más eficaces y adaptadas a las necesidades específicas de la organización, se comprobó que, tras la simulación, el nivel de conciencia digital mejoró significativamente en los participantes. Además, se destaca la importancia de la capacitación proactiva y continua en ciberseguridad como un componente esencial para fortalecer la defensa institucional frente al phishing.

Este enfoque resulta aplicable en entornos educativos, donde la concienciación del personal y de los estudiantes es crucial para reducir el riesgo de ataques, la implementación de campañas simuladas permite no solo evaluar vulnerabilidades reales, sino también promover cambios sostenibles en el comportamiento digital, las investigación aporta una base empírica sólida para diseñar estrategias que combinen simulación, análisis conductual y formación, en el marco de un sistema integral de protección contra amenazas cibernéticas como el phishing.

-Dwivedi (2024), con una revisión íntegra del phishing deslizándose como uno de los mayores problemas en el campo de la seguridad cibernética en la actualidad, este estudio investiga cómo estos ataques aprovechan no solo las debilidades tecnológicas, sino también los aspectos psicológicos del comportamiento humano, tales como la manipulación emocional, la sobrecarga cognitiva, la utilización de la confianza, la revisar varias formas de ataques (incluidos correos electrónicos simples y sofisticados), el aumento de las amenazas con técnicas de IA y aprendizaje automático, para demostrar la complejidad y el dinamismo del panorama de amenazas actuales.

El artículo también analiza cómo el phishing afecta tanto a individuos como a organizaciones, resaltando consecuencias como pérdidas económicas, suplantación de identidad y deterioro de la reputación, la describen algunas de las estrategias de defensa más utilizadas, entre ellas la formación en concienciación para los usuarios y la implementación de tecnologías basadas en inteligencia artificial para la detección de amenazas y los autores advierten que estas defensas aún presentan deficiencias, sobre todo en lo que respecta a la integración efectiva entre herramientas tecnológicas y enfoques centrados en el comportamiento humano.

Además, el estudio subraya la importancia de crear sistemas de protección más robustos y adaptables frente a la constante evolución de las tácticas de phishing, esta revisión proporciona una base teórica útil para diseñar esquemas de protección integrales, especialmente en el ámbito educativo, donde los usuarios tienden a ser más vulnerables, las estrategias preventivas y de respuesta eficaces, resulta esencial comprender tanto las motivaciones del atacante como las debilidades del usuario.

El trabajo de Dwivedi enfatiza que combatir el phishing requiere algo más que soluciones tecnológicas; la educación y concienciación del usuario son igualmente fundamentales, se han logrado avances en la detección mediante inteligencia artificial, el factor humano continúa siendo el punto más frágil, los autores aboga por programas de formación continua, ajustados a las nuevas formas de ingeniería social, y por una estrategia de ciberseguridad integral que combine tecnología, procesos y personas.

-Marques & Sousa (2023) llevaron a cabo un estudio de caso enfocado en la prevención del phishing en instituciones de educación superior, reconociendo el crecimiento tanto en la frecuencia como en la complejidad de este tipo de ataques basados en ingeniería social, la investigación se centró en analizar el nivel de conciencia y percepción que tienen los estudiantes universitarios frente a ataques simulados de phishing, así como la eficacia de las estrategias adoptadas para enfrentarlos y los autores detectaron que, a pesar del conocimiento general que los estudiantes tienen sobre el entorno digital, su vulnerabilidad ante este tipo de amenazas sigue siendo un problema relevante.

Para llevar a cabo el análisis, se emplearon campañas simuladas de phishing junto con actividades de concientización, utilizándose como herramientas tanto de diagnóstico como de formación, los resultados mostraron que los estudiantes de menor edad eran los más propensos a caer en las trampas, y no se evidenciaron diferencias significativas en la percepción del riesgo entre las diversas disciplinas académicas, también se concluyó que los métodos tradicionales basados en documentación e información no logran incrementar efectivamente la conciencia frente a estos ataques, lo que evidencia la necesidad de implementar enfoques más dinámicos e interactivos se subraya que una formación pasiva resulta insuficiente para generar cambios reales en el comportamiento del usuario.

Asimismo, se identificó que repetir los simulacros contribuye significativamente al fortalecimiento del aprendizaje y disminuye la probabilidad de que los estudiantes hagan clic en enlaces maliciosos muchos investigadores proponen incorporar este tipo de ejercicios dentro del currículo académico como una estrategia efectiva y perdurable, se destacan el potencial de la gamificación y del aprendizaje basado en la experiencia como metodologías innovadoras, capaces de captar con mayor eficacia la atención del alumnado y promover modificaciones positivas en sus hábitos digitales, lo cual evidencia que la instrucción práctica resulta más efectiva que la formación meramente teórica.

Este estudio resalta la necesidad de ajustar las estrategias de capacitación según las particularidades del grupo destinatario, específicamente los estudiantes universitarios, con el fin de asegurar una preparación efectiva frente a amenazas cibernéticas reales, los resultados obtenidos ofrecen evidencia relevante para el

desarrollo de sistemas de defensa contra el phishing en contextos educativos, poniendo énfasis en el valor de los simulacros como herramientas tanto didácticas como preventivas y los prácticas fomentan una cultura de ciberseguridad más sólida y activa dentro del entorno académico, impulsando al mismo tiempo la resiliencia digital de sus miembros.

2.2 Bases teóricas

2.2.1. Variable independiente

1. Phishing

El empleo continuo de las tecnologías digitales en la vida cotidiana, y especialmente en el área educativa, ha provocado un aumento exponencial en la exposición a amenazas cibernéticas y el phishing se ha posicionado como una de las tácticas más peligrosas y efectivas utilizadas por los atacantes. Por tanto, cobra importancia una profunda investigación acerca de qué es el phishing, cómo ha evolucionado, cuáles son sus modalidades y con qué herramientas tecnológicas se puede complementar para conformar un sistema de defensa robusto frente a esta amenaza digital, la definición de la naturaleza de esta clase de ataques y de sus posibles contramedidas resultan necesarios para idear estrategias que hagan más segura la información en las instituciones de enseñanza.

2. Definición de phishing

Phishing es una forma de ingeniería social que utilizan los delincuentes para hacerse con información sensible, como contraseñas, datos financieros o personales, haciéndose pasar por una entidad legítima y de confianza en el espacio online (APWG, 2024). Aunque el método más común es la recepción por email de mensajes fraudulentos, phishing puede realizarse también por SMS (smishing), llamadas telefónicas (vishing) e incluso a través de redes sociales.

El objetivo principal del phishing es engañar a la víctima para que revele información confidencial o realice alguna acción que beneficie al atacante. Se aprovechan de la confianza y, a menudo, de la falta de atención o conocimiento del usuario (Microsoft, 2023). La clave de su éxito del phishing radica en la capacidad para imitar a la perfección la apariencia y el estilo de mensajes

auténticos, creando una falsa sensación de urgencia, autoridad o curiosidad que lleva a la víctima a actuar sin pensarlo dos veces.

3. Origen y evolución del phishing

El término phishing apareció a mediados de la década de 1990, con los primeros ataques dirigidos a usuarios de la plataforma America Online (AOL). En esos primeros intentos, los atacantes se hacían pasar por personal de la empresa con el fin de obtener credenciales de acceso, dando origen al término "phishing", en referencia a la metáfora de "pescar" información confidencial (CSO Online, 2018).

A lo largo del tiempo, esta amenaza ha evolucionado significativamente tanto en complejidad como en alcance. Mientras que en sus primeras etapas los correos electrónicos fraudulentos eran fácilmente identificables por errores gramaticales evidentes, imágenes de mala calidad y solicitudes poco verosímiles, el desarrollo de tecnologías más sofisticadas y el perfeccionamiento de las tácticas por parte de los atacantes han elevado la efectividad de estos engaños, la actualidad, los correos de phishing pueden replicar con notable precisión el diseño, tono y estructura de comunicaciones legítimas, lo que dificulta su identificación por parte de los usuarios.

Asimismo, se ha ampliado el repertorio de técnicas utilizadas, los ataques masivos y poco específicos, el fenómeno ha evolucionado hacia modalidades más dirigidas y sofisticadas como el spear *phishing* (enfocado en individuos o grupos concretos), el *whaling* (dirigido a ejecutivos de alto nivel), el *smishing* (mediante mensajes SMS) y el *vishing* (a través de llamadas telefónicas) y la aparición del *pharming* que manipula el sistema de nombres de dominio (DNS) para redirigir a los usuarios a sitios fraudulentos sin requerir su intervención directa marca un avance relevante en la complejidad de estos ataques (Symantec, 2023).

4. Tipos de ataques de phishing

El perfeccionamiento de las tácticas de los actores maliciosos ha derivado en múltiples variantes de phishing, cada una diseñada para explotar diferentes vulnerabilidades y alcanzar metas específicas:

- **Phishing masivo o “Spray and Pray”:** Representa la modalidad más básica y frecuente, en el envío indiscriminado de correos electrónicos genéricos a un amplio grupo de destinatarios y la eficacia radica en la probabilidad estadística de que un pequeño porcentaje de los receptores interactúe con el mensaje fraudulento, las comunicaciones suelen carecer de personalización y emplean mensajes alarmantes como “Su cuenta ha sido bloqueada” o “Verifique su información bancaria” (Verizon, 2024).

- **Spear Phishing:** Instead of the mass mail-out approach, these attacks target specific individuals or groups where the attacker conducts reconnaissance to gather personal or professional information that can be used to craft extremely believable messages that are customized to the recipient's environment, personalisation greatly increases the success rate of the attack, a common example is the impersonation of colleagues, bosses or strategic partners (CIS, 2023).

- **Whaling:** Es una variante de spear phishing todavía más especializada, que se orienta únicamente a altos directivos o responsables financieros en una organización. Los ciberdelincuentes intentan acceder a información estratégica o hacer que se realicen transferencias financieras ilegítimas. Estos ataques se caracterizan por estar cuidadosamente planificados y ser sumamente sofisticados en la suplantación de identidad, simulando ser comunicaciones reales entre ejecutivos o asesores legales (Proofpoint, 2023)

- **Smishing (SMS Phishing):** En este tipo de ataque se emplean mensajes SMS para intentar engañar a la víctima y los mensajes reciben por lo general incluir enlaces maliciosos o números telefónicos para llamar, haciéndose pasar por bancos, compañías de reparto, empresas de servicios públicos o entidades gubernamentales, con la solicitud de actualizar información o solucionar un "problema" urgente (FBI, 2022).

- **Vishing (Voice Phishing):** Consiste en llamadas usando números falseados donde los atacantes se hace pasar por una entidad legítima (tales como ayuda técnica, instituciones bancarias o gobiernos) para intentar que la persona proporcione información confidencial o realice determinadas

acciones (FTC, 2023). Generalmente, se acompañan de phishing o correos electrónicos para tener una mejor apariencia, solicitando a la víctima que marque a un número falso.

- **Pharming:** Esta es una técnica más sofisticada y se basa más en la interacción directa del usuario, la manipulación del sistema de nombres de dominio (DNS) o el archivo de hosts en la computadora de la víctima. La idea es redirigir el tráfico de un sitio web legítimo a uno falso, incluso si el usuario escribe la dirección correcta en su navegador sin que el usuario note la redirección (Microsoft Security, 2019).

5. Técnicas comunes utilizadas en phishing

Para llevar a cabo los diversos tipos de ataques de phishing, los ciberdelincuentes emplean una serie de técnicas avanzadas que están diseñadas para evitar tanto la detección tecnológica como el escepticismo humano. Estas técnicas se centran en la manipulación y la suplantación.

- **Suplantación de identidad (Spoofing):** Es la base fundamental del phishing es que atacantes falsifican la identidad del remitente de un correo electrónico, el nombre de dominio, la dirección IP o incluso el número de teléfono para que la comunicación parezca venir de una fuente legítima y confiable (Cisco, 2023). Pueden usar dominios con una ligera variación ortográfica (conocido como typosquatting), direcciones de correo electrónico falsificadas o manipular los encabezados del correo para engañar al que lo reciba.

- **Uso de URL maliciosas:** Los correos de phishing contienen enlaces que, aunque a simple vista parezcan legítimos, en realidad se dirigen a sitios web falsos que imitan a los originales, los enlaces pueden estar ocultos bajo texto que se ve normal ("haga clic aquí"), URLs acortadas o cambios que son muy sutiles en el nombre del dominio que pasan desapercibidos para el ojo inexperto (Google, 2022).

- **Ingeniería social:** Es la táctica psicológica primordial del phishing, y los atacantes manipulan las emociones de las víctimas (como el miedo, curiosidad o avaricia) para persuadirse de que realice una acción específica.

Pueden amenazar con el cierre de una cuenta, ofrecer premios o descuentos falsos, o crear una sensación de urgencia con plazos inminentes para que la víctima actúe sin pensar dos veces (Mitnick, 2002).

- **Adjuntos maliciosos:** Muchos de estos ataques de phishing incluyen archivos adjuntos infectados con malware y abrir estos documentos (que pueden parecer facturas, informes o notificaciones), se descarga e instala software malicioso como virus, troyanos o ransomware en el sistema de la víctima, esto compromete gravemente la seguridad de sus datos y dispositivos (Kaspersky, 2024).

- **Formularios falsos o sitios web clonados:** Los atacantes diseñan páginas web que son réplicas casi perfectas de sitios legítimos (como los bancos, redes sociales o servicios en la nube), las páginas contienen formularios que solicitan credenciales de inicio de sesión, números de tarjeta de crédito o información personal, toda esa información que la víctima introduce es captada directamente por el atacante.

- **Ofuscación de código:** Para evitar los filtros de seguridad, los atacantes pueden utilizar distintas técnicas para hacer que el código de sus correos o páginas web sea difícil de examinar, se puede incluir el uso de caracteres Unicode, HTML complejo, JavaScript o la incrustación de imágenes en lugar de texto para eludir la detección automática basada en palabras clave o patrones de código.

- **Generación de dominios aleatorios (Domain Generation Algorithms - DGAs):** Algunos programas maliciosos de phishing utilizan DGAs para generar un gran número de nombres de dominio que pueden ser utilizados para el comando y control de botnets (redes de computadoras que están infectadas) o para redirigir a sitios de phishing, lo que dificulta el bloqueo de todos ellos por parte de las defensas de seguridad.

6. Casos reales de ataques de phishing en instituciones educativas

Las instituciones educativas, teniendo en cuenta su carácter abierto y la gran cantidad de datos confidenciales, se han vuelto un objetivo frecuente y valioso para los ciberdelincuentes y el phishing es a menudo el vector de ataque

inicial en muchos de estos eventos, su análisis de casos reales enfatiza la naturaleza urgente de los sistemas de protección fuertes.

- **Compromiso de credenciales y cuentas de correo institucionales:** En 2021, varias universidades en Estados Unidos informaron campañas de spear phishing diseñadas específicamente para estudiantes y personal. Los atacantes se hacían pasar por el departamento de TI, la oficina de ayuda financiera o incluso el decano, donde pidieron verificar las credenciales utilizando un enlace malicioso, después de que se obtuvieron estas credenciales eran usadas para enviar correos de phishing a otros usuarios o para acceder a información personal y académica (FBI, 2021). Esto causó interrupciones en los sistemas de email y la exposición de datos sensibles.

- **Ataques de ransomware iniciados por phishing:** Varios distritos escolares y universidades se han convertido en víctimas de ransomware que paralizó sus actividades, ejemplo notable es el del sistema escolar del Condado de Fairfax en Virginia (EE. UU.) en el año 2020, afectado por un ataque de ransomware de la banda Maze y aunque la forma exacta en que se inició la infección no siempre se descubre, en muchos casos similares, la entrada inicial se logró a través de un correo de phishing que engañó al empleado para descargar el archivo adjunto o hacer clic en un enlace que contiene el malware (BleepingComputer, 2020) y las consecuencias fueron las interrupciones afectaron gravemente las clases a distancia y la gestión administrativa durante la pandemia.

- **Fraude de nóminas y proveedores (Business Email Compromise - BEC):** Las instituciones educativas son blanco de ataques BEC, que a menudo comienzan con phishing, los atacantes logran acceder a la cuenta de correo de un alto ejecutivo o un empleado del departamento de finanzas y la usan para enviar correos electrónicos fraudulentos y los correos pueden instruir a otros empleados a cambiar los datos bancarios de los proveedores, desviar los pagos de nóminas o solicitar transferencias bancarias urgentes, lo que resulta en pérdidas financieras muy significativas (Verizon, 2024).

- **Robo de propiedad intelectual y datos de investigación:** Las universidades con proyectos de investigación importantes son objetivos de

phishing avanzado por parte de grupos de ciberespionaje y los ataques están tratando de robar datos de la investigación, patentes o información estratégica, los correos de phishing están diseñados con un alto grado de adaptación, convirtiéndose en investigadores, socios o entidades de financiación para acceder a la red de investigación o a información sensible (Trend Micro, 2022).

Estos casos muestran que el phishing no solo es una molestia, sino también una amenaza constante con graves consecuencias financieras, operativas y para la reputación de las instituciones educativas, lo que justifica la necesidad de sistemas de defensa integrados y proactivos.

2.2.2. Variable dependiente

1. **Impacto del phishing en la educación**

Un ataque de phishing certero en una universidad puede ser desastroso y de muy amplio alcance, impactando hasta en varias áreas del funcionamiento y prestigio de la universidad.

- **Pérdida y exposición de información sensitiva:** Una de las consecuencias más inmediatas del phishing es el robo de información sensible, en el caso educativo éste puede involucrar a historial académico, identificación pessoal de estudiantes y profesores, datos financieros relativos a pagar y cuentas bancarias, historiales médicos e inclusive resultados de investigaciones científicas, y la noción de esa información supone varios riesgos de consideración.
    - **Suplantación de identidad y delitos financieros:** con la información robada, pueden crearse identidades falsas o realizar transacciones o actividades ilícitas.
    - **Ataque a la privacidad:** La publicación de datos personales y docentes atenta contra la privacidad de los estudiantes y éstos desconfían e incluso sufren consecuencias personales negativas.
    - **Repercusiones legales y regulatorias:** Las instituciones educativas están sujetas a leyes de protección de datos como el GDPR, el

CCPA, o leyes locales y las infracciones resultantes de un ataque de phishing podrían conllevar penalidades monetarias severas y litigios.

- **Impacto en las operaciones:** En caso de que los atacantes tengan acceso a cuentas administrativas, o mediante propagación de malware como ransomware, pueden interrumpir los servicios esenciales tanto académicos como administrativos, lo que perjudica la continuidad institucional.

- **Interrupción de servicios académicos y administrativos:** Un ataque de phishing que amenaza las cuentas de administrador o distribuye malware (especialmente ransomware) puede paralizar la infraestructura crítica de la institución. Esto incluye:

    - **Sistemas de gestión de aprendizaje (LMS):** Interrumpiendo clases en línea, el acceso a materiales de estudio y entrega de trabajos.

    - **Sistemas de matrícula y admisiones:** Imposibilitando la gestión de inscripciones, pagos y trámites estudiantiles.

    - **Sistemas de nómina y finanzas:** Afectando los pagos al personal y a los proveedores.

    - **Acceso a bibliotecas y bases de datos:** Restringiendo el acceso a recursos importantes para la investigación y el estudio.

Esta interrupción causa retrasos significativos, afecta la productividad y puede forzar la suspensión de actividades esenciales (Check Point Research, 2023).

- **Daño reputacional y pérdida de confianza:** Una brecha de seguridad causada por el phishing y que se hace pública puede deteriorar gravemente la reputación de la institución y la percepción de que una universidad o colegio no puede proteger la información sobre sus estudiantes y el personal puede afectar la matrícula de nuevos alumnos, mantener personal calificado, obtener herramientas de investigación y cooperar con otras instituciones y empresas la confianza es una ventaja de un activo intangible de valor incalculable que se pierde difícilmente.

- **Costos financieros directos e indirectos:** El impacto financiero de un ataque de phishing es significativo y se manifiesta en diversas formas:
    - **Gastos de recuperación:** Involucran el análisis forense del incidente, la erradicación del software malicioso, la recuperación de los sistemas a partir de respaldos y la incorporación de medidas de seguridad reforzadas.
    - **Atención a los afectados:** Se refiere al costo asociado a comunicar oportunamente la brecha de seguridad a las personas impactadas, así como a brindar servicios como el monitoreo de crédito o mecanismos de protección de identidad para mitigar posibles daños adicionales.
    - **Pérdida de productividad:** El tiempo que el personal dedica a gestionar el incidente en lugar de sus tareas habituales de enseñanza o administración.
    - **Pérdidas de ingresos:** Por interrupción de servicios, la disminución de matrículas o la cancelación de proyectos.
    - **Multas y demandas legales:** Consecuencia del incumplimiento de normativas de protección de datos (Ponemon Institute, 2024).
- **Efectos psicológicos:** ser la víctima de un ataque de phishing puede tener un impacto emocional negativo, incluyendo estrés, ansiedad y una pérdida de confianza en sí mismo, para los estudiantes, el personal y las experiencias impactan directamente en su bienestar y pueden modificar la manera en la que se relacionan con las plataformas digitales institucionales de ahora en más.

En definitiva, con el phishing no se está frente a un problema técnico sino a una amenaza de múltiples dimensiones que puede afectar a la capacidad operativa, la sostenibilidad financiera y la reputación de una entidad educativa. Esto subraya la necesidad de una protección direccional que sea integral, organizativa y sostenida.

2. Herramientas tecnológicas para detectar phishing

La creciente complejidad en los ataques de phishing ha propiciado la creación de una batería de herramientas tecnológicas que permiten contrarrestar estas amenazas en cada nivel de la infraestructura institucional se soluciones trabajan en sinergia para identificar patrones sospechosos y brindar protección a los usuarios en todas las etapas del ataque: antes, durante y después de su ejecución.

- **Correo electrónico filtros y seguridad Email gateways (SEG):** Son la primera línea de defensa en el correo que intentan impedir que los mensajes maliciosos llegar a la bandeja de entrada del destinatario. Los SEG usan una serie de técnicas para evaluar el correo entrante:

    - **Verificación de encabezados:** Se basan en protocolos como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting & Conformance) para autenticar al remitente y evitar el fraude de identidad (Proofpoint, 2023).

    - **Análisis de contenido:** Se realiza una inspección profunda del contenido del mensaje identificar características habituales de este tipo de ataques de ingeniería social tales como frases persuasivas, faltas de ortografía y gramática, o la presencia de enlaces o ficheros que pueden contener malware.

    - **Consulta de reputación:** Hacen consultas a listas de reputación que contienen direcciones IP y dominio que son utilizadas habitualmente para enviar correo malicioso, spam, phishing, entre otros.

    - **Técnicas de sandboxing:** Ejecutan archivos adjuntos o enlaces en un entorno virtual controlado, permitiendo observar su comportamiento sin comprometer el sistema, lo cual facilita la detección de software malicioso o redirecciones peligrosas antes de que el mensaje llegue al usuario final.

- **Soluciones de seguridad web y navegadores seguros:** Estas herramientas protegen a los usuarios cuando intentan acceder a sitios web maliciosos.
    - **Listas negras (Blacklisting):** Los navegadores modernos (como Chrome, Firefox) y las soluciones de seguridad web que utilizan bases de datos actualizadas de URLs de phishing y sitios maliciosos que bloquean el acceso de los usuarios y muestran una advertencia (Google, 2022).
    - **Análisis en tiempo real:** Algunas soluciones en tiempo real verifican el contenido de las páginas web y detectan si un sitio intenta hacerse pasar por otro mediante técnicas de suplantación visual o de código.
- **Sistemas de detección y prevención de intrusiones (IDS/IPS):** Estos sistemas monitorean el tráfico de red en busca de patrones de actividad que indican el ataque. Un IDS alerta sobre actividades sospechosas, mientras que un IPS puede bloquear proactivamente el tráfico si revela un intento de acceder a un sitio de phishing conocido o si identifica la exfiltración de datos después de la infección (Cisco, 2021).
- **Inteligencia artificial (IA) y aprendizaje automático (ML):** La IA y el ML son cada vez más importantes en la detección de phishing. Los algoritmos pueden:
    - **Detectar anomalías en el comportamiento:** Monitorizar el comportamiento de los usuarios, la estructura del correo electrónico, la reputación del dominio y el flujo de red en busca de patrones que sugieran que un usuario está enviando correos electrónicos de phishing, incluidos los días cero (IBM, 2023).
    - **Análisis de lenguaje natural (NLP):** El texto de los correos es procesado para encontrar diferencias muy sutiles en el estilo de redacción y en la gramática o vocabulario característico de los mensajes de phishing que por lo general pasan inadvertidas para la lectura humana.

- **Soluciones de protección del endpoint (EDR/XDR):** Estas soluciones se implementan directamente en los endpoints que utiliza el usuario final, que pueden ser computadoras o tablets. Su finalidad es detectar y remediar amenazas cuando el usuario inadvertidamente descarga un archivo malicioso o visita una página web maliciosa. Plataformas EDR (Endpoint Detection and Response) y XDR (Extended Detection and Response) que pueden: bloquear el malware o aislar el equipo comprometido antes de que la infección se propague (CrowdStrike, 2024).

- **Sistemas de gestión de identidad y accesos (IAM) con autenticación multifactor (MFA):** Este mecanismo, aunque no para directamente los ataques de phishing, sí juega un rol importante posterior a una posible fuga de credenciales.Tumblr puede ser, en caso de que un atacante recoja una nombre de usuario y contraseña phishing,

3. Métodos de prevención

La respuesta al phishing requiere un enfoque preventivo y organizado a través de la incorporación de tecnologías avanzadas, configuraciones de red robustas y el uso de inteligencia artificial. Con esta estrategia se pretende atajar amenazas en sus fases iniciales, evitando que lleguen a los usuarios y consecuencias negativas.

- **Seguridad a nivel de DNS (Sistema de nombres de dominio):** Ya que en un nivel muy básico actúa el DNS como traductor de nombres de dominio a direcciones IP los delincuentes pueden manipularlo para enviar a sus víctimas a sitios falsos esto es conocido como pharming. Para prevenir esto, se realizan las siguientes acciones:
    - **DNSSEC (Domain name system security extensions):** Añade autenticación al procedimiento de resolución de dominios y permite que el navegador web confirme que la información proviene de un origen auténtico, que no ha sido alterada y que el usuario se está conectando al sitio web correcto.
    - **DNS seguros:** Son un nivel extra de protección que bloquea preventivamente los accesos a dominios maliciosos conocidos, cuando antes el usuario o cualquier conexión a internet habría

recibido una respuesta DNS, sin que el navegador se haya conectado aún. De ese modo, sí que es un usuario quiere acceder a un link sospechoso, se detiene la conexión automáticamente en caso de que esté en alguna lista negra.

- **Bloqueo de URLs maliciosas y sitios que parecen vulnerables:** Los dominios maliciosos se pueden bloquear obteniendo y utilizando una base de datos de inteligencia de amenazas, la cual es muy útil para bloquear de modo preventivo acceso a sitios web de phishing, botnets para ataques y dominios de reciente creación que pudieran estar siendo utilizados para ataques en el futuro.

4. Educación digital como barrera al phishing

Aunque las soluciones tecnológicas son importantes, la educación digital está diseñada como la barrera más fundamental y robusta contra los ataques de phishing, ya que se centra en la vulnerabilidad explotada: el factor humano (SANS Institute, 2022). Los ciberdelincuentes se basan en la tecnología social para engañar a las personas, y ninguna tecnología es 100% perfecta. En un entorno educativo, donde las interacciones digitales son constantes y los usuarios tienen un nivel diferente de conocimiento tecnológico, la capacitación continua es indispensable para construir una comunidad ciber-resistente.

Una educación digital eficaz va más allá de simples advertencias o reglas; busca fortalecer a los usuarios para que se conviertan en la primera línea de defensa de la institución. Para lograrlo esto, debe enfocarse en varios aspectos clave:

- **Concienciación continua y adaptativa:** La formación no debe ser un evento único, sino un proceso recurrente que se adapta a las nuevas tácticas de phishing y a las amenazas emergentes (EDUCAUSE, 2023). Esto puede incluir boletines informativos, campañas de carteles, y comunicaciones regulares sobre alertas de seguridad.

- **Detecting phishing signals:** Enseñar a los usuarios a reconocer los indicadores clave de un correo electrónico o mensaje de phishing, tales como:

- **Direcciones de correo electrónico sospechosas:** Correos con dominios raros o con pequeñas modificaciones en los dominios verdaderos.

- **Fallas idiomáticas:** Aunque los más sofisticados ataques de phishing han mejorado la redacción, el tener errores ortográficos o gramaticales es aún un indicador común de fraude digital.

- **Solicitudes extrañas de información personal:** Recuerde que las instituciones reales no le piden contraseñas, números de tarjeta bancaria u otro tipo de información confidencial vía correo electrónico o mensaje de texto.

- **Detección de enlaces sospechosos:** Los usuarios deben ser entrenados para verificar los enlaces antes de hacer clic, pase el cursor sobre el enlace para ver la dirección url verdadera y también para buscar cualquier inconsistencia con la dirección del dominio de la url.

- **Enlaces dudosos:** Al aceptar que no todos tienen conocimientos técnicos, enseñar a los usuarios a desplazar el ratón por encima de un enlace sin pulsarlo para conocer la dirección URL, observar si hay alguna incongruencia con el dominio esperado.

- **Uso seguro de credenciales:** Resaltar la importancia de utilizar contraseñas fuertes y únicas para cada servicio, y la habilitación de la autenticación multifactor (MFA) siempre que sea posible la la cual les protege las cuentas aunque las credenciales principales están comprometidas vía phishing.

- **Cultura de reporte:** Incentivar un ambiente para que los usuarios sientan seguridad y sean motivados a reportar cualquier correo o actividad sospechosa al departamento de TI.

5. Simuladores y entrenamientos antiphishing

Las plataformas de simulación y formación contra el phishing es una de las estrategias más efectivas y prácticas para mejorar la resistencia de los usuarios a los ataques de ingeniería social y a diferencia de los planteamientos

exclusivamente teóricos, este tipo de herramientas ofrecen un ambiente de aprendizaje interactivo y seguro en el que se emulan situaciones reales. Esto hace que los usuarios puedan validar sus conocimientos y destrezas en ambientes simulados, resultando en una mayor capacidad para identificarlos y gestionar adecuadamente intentos de phishing reales (KnowBe4, 2024).

La ejecución de un programa de entrenamiento y simulación de phishing suele transcurrir en los siguientes pasos:

- **Planificación y definición de escenarios:** Se diseñan campañas de simulación que imitan tácticas reales de phishing, con el contexto del ambiente educativo, los ejercicios pueden ir desde ataques genéricos a escala masiva hasta casos de spear phishing muy específicos según el perfil de los usuarios.

- **Envío de correos simulados:** A través de una plataforma especializada, se envían correos electrónicos falsos a distintos grupos dentro de la institución como estudiantes, docentes o personal administrativo, los mensajes están diseñados para parecer auténticos y engañosos, pero sin representar una amenaza real para los sistemas o la información.

- **Monitoreo y registro del comportamiento del usuario:** El sistema registra de manera detallada las respuestas de los usuarios frente a los correos simulados y los indicadores más relevantes que se monitorean están: la apertura del correo, los clics en enlaces sospechosos, la descarga de archivos adjuntos o la entrega de información confidencial en formularios simulados.

    - **Tasa de apertura:** El porcentaje de usuarios que abrieron el correo.

    - **Tasa de clics (Click-through rate):** El porcentaje de usuarios que hicieron clic en un enlace malicioso dentro del correo.

    - **Tasa de envío de credenciales:** El porcentaje de usuarios que ingresaron credenciales en una página de destino falsa.

    - **Tasa de descarga de adjuntos:** El porcentaje de usuarios que descarga archivos adjuntos maliciosos simulados.

    - **Tasa de reporte:** El porcentaje de usuarios que identificaron el correo como sospechoso y lo reportaron a TI.

- **Retroalimentación inmediata y formación JIT (Just-In-Time):** Si el usuario cae en la simulación (por ejemplo, hace clic en un enlace o ingresa credenciales), se le redirige a la página de destino que le informa que fue una prueb e inmediatamente proporciona un breve módulo de entrenamiento para reconocer el tipo de phishing en el que falló y qué hacer en el futuro. Aquellos que identifican y reportan el correo correctamente pueden recibir un mensaje de felicitación o un pequeño reconocimiento.

- **Capacitación complementaria:** Además de la capacitación JIT, se suelen ofrecer módulos de e-learning más completos sobre seguridad digital, que cubren temas como la gestión de contraseñas, la autenticación multifactor y la protección de datos personales, estos cursos pueden ser obligatorios o voluntarios.

- **Análisis y mejora continua:** El análisis de los resultados obtenidos a partir de simulacros permite detectar debilidades dentro de la institución, identificar áreas donde es necesario reforzar la capacitación, así como reconocer grupos de usuarios que requieren atención especial en esta información es valiosa para que los equipos encargados de la seguridad ajusten sus estrategias de concienciación y optimicen la eficacia del sistema de protección en su conjunto (SANS Institute, 2022).

Realizar de vez en cuando estos ejercicios, junto con un entrenamiento y feedback estructurados, no solo aumenta la capacidad de detección ante posibles amenazas, sino que también incentiva resultados positivos en el comportamiento de los usuarios, contribuyendo así a un entorno educacional más seguro y más capacitado para enfrentar los ataques de phishing.

6. Importancia de implementar políticas institucionales

La definición de políticas institucionales para la seguridad de la información se convierte en un pilar para el desarrollo de un sistema de protección ante phishing y otros ataques digitales en educación, las políticas no son documentos que deban ser tratados como trámites administrativos, sino que

reflejan el compromiso de la institución frente a la seguridad, y a través de ellas se establecen lineamientos claros, roles y responsabilidades, así como expectativas del comportamiento digital de todos los integrantes de la institución (ISO/IEC 27001:2022). Y ello es relevante en: Aspectos críticos dentro de los cuales resulta indispensable incrementar la protección de la información y la resiliencia institucional para hacer frente a incidentes cibernéticos.

- **Establecimiento de un marco de referencia claro:** La política de seguridad define las "reglas del juego" para el uso de los recursos tecnológicos y gestión de la información. Ofrecen pautas claras sobre lo que se espera de estudiantes, docentes, personal administrativo y de TI en relación con la seguridad, se reduce la ambigüedad, fomenta prácticas seguras y reduce el riesgo de que alguien comprometa la seguridad por desconocimiento o negligencia (NIST, 2017).

- **Fomento de una cultura de seguridad:** Al comunicar las expectativas de seguridad y las consecuencias de no cumplirlas, la política contribuye a la creación de una cultura organizacional donde la seguridad de la información es reconocida como una responsabilidad compartida por todos, no solo por el departamento de TI, la importante que la concienciación no sea solo un concepto, sino una práctica que se basa en la vida cotidiana.

- **Guía para la gestión de riesgos:** Las políticas de seguridad informática desempeñan un rol fundamental en la gestión de riesgos, ya que orientan la identificación, evaluación y mitigación de posibles amenazas, ejemplo es una política de uso aceptable del correo electrónico puede restringir la interacción con enlaces o archivos adjuntos sospechosos, disminuyendo así la exposición a ataques de phishing y una política de contraseñas con requisitos específicos sobre complejidad y renovación frecuente contribuye a reforzar la autenticación

- **Cumplimiento normativo y legal:** Además, la existencia de políticas claras facilita el cumplimiento de normativas legales relacionadas con la protección de datos personales y sensibles, como registros académicos, información médica o financiera y lo permite a las instituciones educativas alinear sus prácticas con marcos legales como el GDPR, FERPA o

regulaciones locales, evitando sanciones legales y daños a la reputación institucional (ISACA, 2020).

- **Estandarización y consistencia:** Por último, las políticas establecen criterios uniformes que promueven la estandarización de las prácticas de seguridad en toda la organización, lo cual resulta especialmente importante en instituciones educativas con estructuras amplias y descentralizadas, compuestas por múltiples facultades, sedes o departamentos.

- **Soporte para la respuesta a incidentes:** La política debe incluir el procedimiento detallado para la detección, el reporte, la respuesta y la recuperación de eventos de seguridad, incluidos los ataques de phishing y la asegura que, en caso de una deficiencia, la institución pueda actuar de forma rápida y coordinada para contener el daño, eliminar las amenazas y restaurar los sistemas (CIS, 2023).

- **Base para acciones correctivas y disciplinarias:** Si ocurre un incidente de seguridad debido a una violación de la política, estas proporcionan la base formal para los procedimentos correctivos y disciplinarias que fortalecen la seriedad del compromiso con la seguridad.

En resumen, sin políticas bien definidas, anunciadas y aplicadas, puede haber una inversión insuficiente en tecnologías de seguridad y los esfuerzos de concienciación pueden carecer de dirección y la política institucional es la base sobre la cual se desarrolla un sistema de protección contra el phishing sostenible y efectivo.

7. Sistemas integrales de protección contra phishing

Dado que los ataques de phishing evolucionan constantemente y presentan una complejidad creciente, no es suficiente confiar en una sola herramienta de defensa, en la instituciones, especialmente las del ámbito educativo, requieren soluciones integrales que aborden la amenaza de forma efectiva. Un sistema de protección contra el phishing debe adoptar un enfoque holístico y en múltiples capas, combinando tecnología, procesos estructurados y la capacitación continua del personal, en el enfoque permite establecer una barrera sólida y dinámica frente a los intentos de fraude (Anderson & Brown, 2023). La eficacia de estas

soluciones integrales radica en su capacidad para detectar y bloquear amenazas en diferentes etapas del ataque y a lo largo de toda la infraestructura institucional.

Los componentes principales de un sistema integral de protección de phishing son:

- **Defensa en la puerta de enlace del correo electrónico:** La protección a nivel de puerta de enlace del correo electrónico constituye la primera barrera contra los intentos de phishing, la defensa se basa en filtros avanzados y en Gateways de Seguridad de Correo Electrónico (SEG) que integran tecnologías de inteligencia artificial (IA) y aprendizaje automático (ML), los sistemas examinan los mensajes entrantes para identificar señales típicas de ataque, tales como suplantación de identidad, enlaces o archivos adjuntos maliciosos, así como errores gramaticales, se utilizan protocolos como SPF, DKIM y DMARC con el fin de verificar la legitimidad del remitente antes de que el mensaje llegue a la bandeja de entrada del usuario (Proofpoint, 2023).

- **Seguridad a nivel de red y DNS:** En paralelo, la seguridad implementada a nivel de red y de DNS cumple una función complementaria. Tecnologías como los firewalls de próxima generación y los sistemas de detección y prevención de intrusiones (IDS/IPS) permiten analizar el tráfico en tiempo real para bloquear el acceso a sitios identificados como maliciosos, la utilización de servicios DNS seguros como Cisco Umbrella junto con la implementación de DNSSEC, fortalece la defensa frente a técnicas como el *pharming*, al evitar que los usuarios accedan a dominios fraudulentos incluso si llegan a hacer clic en enlaces comprometidos (ICANN, n.d.).

- **Protección del punto final (Endpoint Security):** La protección del punto final (Endpoint Security) juega un papel esencial en la defensa contra el phishing. Herramientas como las soluciones de Detección y Respuesta en el Endpoint (EDR) o su versión extendida (XDR), instaladas directamente en los dispositivos de los usuarios, permiten identificar y neutralizar amenazas cuando los filtros tradicionales fallan el ejemplo es si un correo malicioso logra eludir los sistemas de filtrado y el usuario interactúa con un enlace o archivo malicioso, estas tecnologías pueden detectar el intento de infección,

bloquear el malware o aislar el dispositivo afectado para evitar su propagación (CrowdStrike, 2024).

- **Gestión de identidad y acceso (IAM) con autenticación multifactor (MFA):** En paralelo, la gestión de identidad y acceso (IAM) fortalecida con autenticación multifactor (MFA) ofrece una defensa adicional y aunque este mecanismo no evita directamente el phishing, sí impide que un atacante utilice credenciales robadas, ya que requiere un segundo factor de autenticación, como un código temporal o datos biométricos, lo que dificulta el acceso no autorizado a las cuentas (NIST, 2020).

- **Concienciación y entrenamiento del usuario:** El componente humano es igualmente vital y la capacitación continua y la concienciación de los usuarios sobre los riesgos del phishing contribuyen significativamente a la prevención y lo programas educativos y simulacros de phishing periódicos permiten mejorar la capacidad de detección y respuesta de los usuarios ante intentos reales, posicionándose como una línea activa de defensa (SANS Institute, 2022).

- **Políticas y procedimientos de seguridad:** Asimismo, las políticas y procedimientos institucionales deben estar claramente establecidos en estos documentos deben regular el uso de las tecnologías, definir las responsabilidades de seguridad y establecer protocolos de actuación ante incidentes, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en estándares como ISO/IEC 27001, permite estructurar e integrar todos estos elementos dentro de un marco de mejora continua (ISO/IEC 27001:2022).

En conjunto, la coordinación estratégica de estas medidas tecnológicas, organizativas y humanas genera un entorno de protección más robusto, capaz de reducir significativamente los riesgos asociados al phishing y resguardar eficazmente la información dentro de las instituciones educativas.

8. Evaluación de efectividad de los sistemas de protección

La adopción de un sistema de defensa contra el phishing representa solo el inicio de un proceso continuo de monitoreo, análisis y perfeccionamiento, evaluar

su efectividad resulta esencial para comprobar que las inversiones realizadas en ciberseguridad están generando los resultados esperados, que la institución mantiene un nivel adecuado de protección frente a amenazas en constante evolución y que los objetivos relacionados con la seguridad de la información se están cumpliendo (Gartner, 2024). Este proceso de evaluación no debe concebirse como una acción puntual, sino como un ciclo permanente que permite identificar vulnerabilidades, optimizar el uso de recursos y sustentar futuras mejoras o ajustes estratégicos en las defensas implementadas.

Para evaluar la efectividad de un sistema de protección contra phishing, se usan diversas métricas y metodologías:

Métricas técnicas de detección

Estas miden la eficiencia de las herramientas de seguridad:

- **Tasa de detección de phishing:** Indica el porcentaje de correos electrónicos de phishing que el sistema (filtros de correo, SEG) logra identificar y bloquear o poner en cuarentena antes de alcanzar la bandeja de entrada del usuario y una tasa alta significa que las herramientas son muy efectivas.
- **Tasa de falsos positivos:** Es el porcentaje de correos legítimos que son clasificados erróneamente como phishing y bloqueados, una gran cantidad de falsos positivos pueden dejar de funcionar, frustrar a los usuarios y reducir la confianza en el sistema (Symantec, 2023). El objetivo es detectar la mayor cantidad de phishing y tener la menor cantidad de falsos positivos.
- **Tiempo de detección:** Es el tiempo que lleva identificar y responder a un nuevo ataque de phishing es una detección rápida es esencial para minimizar la exposición.
- **Eficacia de bloqueo de URL:** Mide cuántos enlaces a sitios de phishing conocidos son bloqueados por los sistemas de seguridad web o DNS.

Métricas del factor humano (a través de simulaciones)

Estas métricas se obtienen de los simulacros de phishing y miden el comportamiento de los usuarios:

- **Tasa de reporte de phishing:** Mide el porcentaje de usuarios que identifican un correo simulado como sospechoso y lo reportan al departamento de TI, en lugar de interactuar con él y aumentar esta tasa es una señal clara de que la cultura de seguridad está mejorando.

- **Tiempo promedio de respuesta a incidentes (MTTR):** Aunque no es exclusivo del phishing, medir el tiempo que tarda el equipo de seguridad en detectar, contener y eliminar un incidente de phishing (reportado por un usuario o detectado por herramientas) es crucial para evaluar la eficiencia operativa.

Auditorías y revisiones periódicas

Son evaluaciones más amplias y sistemáticas:

- Las auditorías de seguridad consisten en evaluaciones independientes internas o externas enfocadas en revisar los controles, políticas y procedimientos implementados para protegerse contra el phishing, muchos auditorías permiten verificar el cumplimiento de normas internacionales, como la ISO/IEC 27001, y plantean recomendaciones de mejora, conforme a lineamientos como los establecidos en la ISO/IEC 27008:2020.

- Por otro lado, las pruebas de penetración o pentesting simulan ciberataques reales con el fin de detectar vulnerabilidades en los sistemas, redes o configuraciones, incluyendo posibles fallos en los mecanismos diseñados para bloquear intentos de phishing.

- Finalmente, la revisión periódica de políticas y procesos de seguridad busca garantizar que tanto los protocolos como los procedimientos de respuesta a incidentes se mantengan actualizados y sean eficaces frente a las nuevas técnicas empleadas por los ciberdelincuentes.

2.3. Marco conceptual

2.3.1. Amenaza informática

Se considera evento o actividad que pone en riesgo la confidencialidad, integridad o disponibilidad de los sistemas de cómputo, estas amenazas pueden

provenir del interior o del exterior de la institución, y pueden ser resultado de acciones intencionales o de incidentes fortuitos, los ejemplos más comunes se encuentran el malware, el phishing y los ataques de denegación de servicio. (Cano, 2022)

2.3.2 Antiphishing

Se trata de una perspectiva holística que involucra a las estrategias, tecnologías y mejores prácticas que tienen como objetivo la prevención, detección, y respuesta a incidentes de phishing. Esta estrategia incluye la implementación de filtros en el correo electrónico, entrenamiento en habilidades digitales y protocolos de autenticación adicional. (Ramírez, 2021)

2.3.3 Autenticación

Es el procedimiento que permite comprobar la identidad de un usuario para asegurar que únicamente éste tiene acceso a los recursos protegidos, antes de permitirle utilizar un sistema. (González, 2020)

2.3.4 Ciberataque

Acción maliciosa en contra de la integridad, confidencialidad y disponibilidad de sistemas y datos digitales para causar daño, robo o modificación. Herramientas como phishing, ransomware o exploits son utilizadas para explotar vulnerabilidades y comprometer la seguridad. (Torres, 2022)

2.3.5 Ciberseguridad

Rama tecnológica que consiste en garantizar que los sistemas, redes y datos estén protegidos del acceso o daño no autorizado. Integra tecnologías, políticas, educación y capacitación para gestionar riesgos en ambientes digitales. (Martínez, 2023)

2.3.6. Correo electrónico falso

Mensaje fraudulento que simula ser de una fuente confiable, con el fin de engañar al receptor y robar información sensible, es uno de los principales vectores del phishing. (Navarro, 2022)

2.3.7. DNS (Domain Name System)

Sistema que traduce nombres de dominio, como “www.ejemplo.com”, a direcciones IP. Su manipulación, conocida como DNS spoofing, permite a los atacantes redirigir a los usuarios a sitios maliciosos sin que lo noten. (Alonso, 2021)

2.3.8. Educación digital

Formación en el uso seguro y crítico de la tecnología para identificar amenazas como el phishing, es clave en entornos educativos para fortalecer la concienciación de los usuarios. (Pérez, 2022)

2.3.9. Enlace malicioso

Consiste en el uso de enlaces insertados en correos electrónicos o mensajes, los cuales redirigen a sitios web falsos creados con el propósito de robar credenciales o instalar software malicioso, esta técnica es comúnmente utilizada en campañas de phishing a gran escala. (Ruiz, 2023)

2.3.10. Filtrado de contenidos

Se trata de un método de protección que impide el acceso a páginas web peligrosas, ya sea mediante el uso de listas negras actualizadas o mediante análisis en tiempo real, en este propósito, se emplean herramientas como los firewalls y extensiones en los navegadores, las cuales contribuyen a prevenir ataques de phishing. (Ramos, 2021)

2.3.11. Ingeniería social

Consiste en el uso de técnicas de manipulación psicológica con el fin de obtener datos sensibles o acceder a sistemas restringidos, su forma digital, esta práctica se manifiesta como phishing, el cual se basa en generar confianza o inducir un sentido de urgencia en las víctimas para lograr su objetivo. (López, 2023)

2.3.12. Inteligencia artificial (IA)

Se trata de una tecnología capaz de identificar comportamientos inusuales en correos electrónicos o en las acciones de los usuarios, lo que contribuye

significativamente a la detección anticipada de posibles intentos de phishing. (Silva, 2023)

2.3.13. Malware

Programas maliciosos como virus, troyanos o ransomware son utilizados para comprometer dispositivos, ya sea con el objetivo de sustraer información o causar daños en los sistemas. Con frecuencia, este tipo de software se propaga a través de archivos adjuntos en correos electrónicos fraudulentos, especialmente en campañas de phishing. (Gutiérrez, 2020)

2.3.14. Navegación segura

Acciones como comprobar la validez de los certificados SSL, evitar el ingreso a sitios que no utilicen el protocolo HTTPS y emplear herramientas de seguridad digital son esenciales para disminuir la probabilidad de caer en páginas engañosas, las prácticas resultan clave para proteger la información personal y garantizar una navegación segura en Internet. (Morales, 2022)

2.3.15. Política de seguridad

Conjunto de normas que regulan el uso de sistemas y datos en una organización, estas políticas establecen medidas para proteger la información y responder ante incidentes como el phishing. (Fernández, 2023)

2.3.16. Protección perimetral

Uso de tecnologías como firewalls o sistemas de detección de intrusos (IDS) para monitorear y bloquear accesos no autorizados a una red, es fundamental para la defensa de la infraestructura. (Díaz, 2021)

2.3.17. Simulador de phishing

Herramienta que replica ataques de phishing controlados para entrenar a usuarios en su identificación y evaluar la efectividad de programas de concienciación. (Ortiz, 2022)

2.3.18. Suplantación de identidad

Técnica mediante la cual un atacante se hace pasar por una persona o entidad legítima para engañar a las víctimas y obtener acceso a información sensible. (Cruz, 2021)

2.3.19. Token de seguridad

Dispositivo físico o virtual que genera códigos únicos para autenticación en dos pasos (2FA), dificultando el acceso no autorizado incluso si se roban contraseñas. (Reyes, 2020)

2.3.20. URL spoofing

Creación de direcciones web falsas que imitan las legítimas, por ejemplo “faceb00k.com” en lugar de “facebook.com”, para engañar a los usuarios y robarles información. (Vargas, 2023)

CAPÍTULO VI

VI. REFERENCIAS BIBLIOGRÁFICAS

AENOR. (n.d.). ISO 27001 - Seguridad de la Información. https://www.aenor.com/certificacion/certificaciones-de-producto/seguridad-de-la-informacion/iso-27001

Agencia Andina. (2023). Atención: Perú es el segundo país con más ataques de phishing en Latinoamérica. Agencia Peruana de Noticias Andina. https://andina.pe/agencia/noticia-atencion-peru-es-segundo-pais-mas-ataques-phishing-latinoamerica-997628.aspx

Alonso, R. (2021). Redes y seguridad. Cisco Press. https://www.ciscopress.com/networkin

Anderson, L., & Brown, C. (2023). Building Resilient Organizations: A Multi-layered Approach to Cybersecurity. Tech Press.

APWG. (2024). Phishing activity trends report. https://apwg.org/trends/

Arévalo, J., & Pinto, S. (2021). Enfoque cuantitativo en la investigación: Técnicas y aplicaciones. Revista Latinoamericana de Ciencias Sociales, 18(3), 44–60. https://revistacienciassociales.edu.pe/articulo/arevalo-pinto-2021

Aredo Luján, L. A. (2021). El phishing y su vulneración a la protección de datos personales en los delitos informáticos.

Bembade, R., Debbarma, D., Murkute, A., Joshi, V. C., & Borawake, A. (2024). Phishing Email Detection and Reporting System. International Journal of Advanced Research in Science, Communication and Technology, 432–434. https://doi.org/10.48175/ijarsct-22466

BleepingComputer. (2020, octubre 16). Fairfax County public schools impacted by Maze ransomware attack. https://www.bleepingcomputer.com/news/security/fairfax-county-public-schools-impacted-by-maze-ransomware-attack/

Cáceres, H. (2018). Diseño metodológico cuantitativo y análisis estadístico. Universidad Nacional de Trujillo. https://repositorio.unitru.edu.pe/handle/UNITRU/9876

Cadena SER. (2025). Una Liga de Ciberseguridad para encontrar vulnerabilidades en la universidad. https://cadenaser.com/cmadrid/2025/03/11/una-liga-de-ciberseguridad-para-encontrar-vulnerabilidades-en-la-universidad-ser-madrid-sur/

Cano, J. (2022). Ciberseguridad en entornos educativos. Editorial Tecnológica. https://www.editorialtecnologica.com/ciberseguridad

Check Point Research. (2023). Mid-year cyber attack trends: Education sector targeted. https://www.checkpoint.com/press/2023/check-point-research-education-and-research-sector-continues-to-lead-as-the-most-targeted-sector-in-cyberattacks/

Check Point Research. (2024). Sector educativo recibe más de 3,000 ciberataques semanales en 2024. https://securitic.lat/sector-educativo-recibe-mas-de-3000-ciberataques-semanales-en-2024-check-point/?utm_source=chatgpt.com

Cisco. (2021). What is a firewall? https://www.cisco.com/c/en/products/security/firewalls/what-is-a-firewall.html

Cisco. (2023). What is email spoofing? https://www.cisco.com/c/en/products/security/email-security/what-is-email-spoofing.html

Cloudflare. (2024). What is a DDoS attack? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

CIS (Center for Internet Security). (2023). CIS controls v8. https://www.cisecurity.org/controls/v8/

CSO Online. (2018, enero 23). A brief history of phishing. https://www.csoonline.com/article/3246830/a-brief-history-of-phishing.html

CrowdStrike. (2024). What is XDR? https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/

Cruz, J. (2021). Identidad digital y fraudes. INTERPOL. https://www.interpol.int/fraudes-digitales

De la Cruz, M., & Rodríguez, M. (2025). La vulneración de datos personales mediante el phishing y la modalidad de robo de datos en Lima Sur, 2023. https://hdl.handle.net/20.500.13067/3731

Delgado, R. (2019). Niveles de investigación científica: Aplicaciones en proyectos académicos. Fondo Editorial Académico. https://fondoeditorialacad.edu.pe/libros/niveles-de-investigacion

Díaz, C. (2021). Firewalls y redes seguras. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia

Dwivedi, A. (2024). A Comprehensive Review of Phishing in Cybersecurity: Risks, Impacts, and Defence Strategies. Indian Scientific Journal Of Research In Engineering And Management. https://doi.org/10.55041/ijsrem38040

DNV. (n.d.). The plan-do-check-act cycle. https://www.dnv.com/certifications/standards/pdca-cycle.html

EDUCAUSE. (2023). Key issues in higher education information security. https://www.educause.edu/strategic-initiatives/top-it-issues/2023-top-it-issues/key-issues-in-higher-education-information-security

Ejecutivoti. (2024, abril 6). Ciberseguridad en alerta: Aumenta el robo de datos personales, phishing y ransomware en Perú. https://www.ejecutivoti.com/ciberseguridad-en-alerta-aumenta-robo-de-datos-personales-phishing-y-ransomware-en-peru/

El Comercio. (2024). Perú registra más de 1 millón de ciberataques en 2024: alertan sobre el aumento del phishing y ransomware. https://elcomercio.pe/respuestas/tecnologia/peru-registra-mas-de-1-millon-de-ciberataques-en-2024-alertan-sobre-el-aumento-del-phishing-y-ransomware-ciberdelincuentes-inteligencia-artificial-ia-ultimas-noticia/

El Comercio. (2024). Perú sufrió más de 1 millón de ciberataques en lo que va del año, según el CNSD. https://elcomercio.pe

El HuffPost. (2024). El Gobierno invierte otros 1.157 millones para actuar frente a los ciberataques. https://www.huffingtonpost.es/politica/el-gobierno-invierte-otros-1157-millones-actuar-ciberataquesbr.htm

ESET. (2025). El 62% de los ciberataques en Perú en 2025 comenzó con campañas de phishing. https://nteve.com/2025/04/08/el-62-de-los-ciberataques-en-peru-en-2025-comenzo-con-campanas-de-phishing/?utm_source=chatgpt.com

FBI. (2020). Public service announcement: Business email compromise (BEC) and email account compromise (EAC) scams. https://www.ic3.gov/Media/Y2020/PSA200709

FBI. (2021). Public service announcement: Phishing attacks targeting higher education. https://www.ic3.gov/Media/Y2021/PSA210817

FBI. (2022). Public service announcement: Smishing and vishing schemes. https://www.ic3.gov/Media/Y2022/PSA220104

FEMA. (2020). Developing and maintaining emergency operations plans: Comprehensive preparedness guide (CPG) 101. https://www.fema.gov/sites/default/files/2020-07/fema-cpg101v2.pdf

Fernández, G. (2023). Políticas de seguridad en universidades. EDUCAUSE. https://www.educause.edu/policy-security

Forbes. (2020, junio 29). UC San Francisco paid $1.14 million to ransomware hackers—And made a smart move, says expert. https://www.forbes.com/sites/thomasbrewster/2020/06/29/uc-san-francisco-paid-114-million-to-ransomware-hackers-and-made-a-smart-move-says-expert/

FTC (Federal Trade Commission). (2023). Robocalls and phishing scams. https://www.consumer.ftc.gov/articles/how-avoid-scam

Gartner. (2022). Market guide for endpoint detection and response. (Informe con suscripción).

Gartner. (2024). Top trends in cybersecurity for 2024. (Informe con suscripción).

González, M. (2020). Seguridad en sistemas de acceso. McGraw-Hill.

Google. (2022). How Google Safe Browse works. https://safeBrowse.google.com/safeBrowse/how-it-works/

Gutiérrez, H. (2020). Malware: Tipos y mitigación. Kaspersky Lab. https://www.kaspersky.com/resource-center/malware

Guzmán, P. (2020). Diseños experimentales y pre-experimentales en educación digital. Revista de Investigación Educativa, 22(1), 15–29. https://revistainvestigacionedu.edu.pe/articulo/guzman-diseño

IBM. (2023). How AI helps detect phishing. https://www.ibm.com/topics/phishing/how-ai-helps-detect-phishing

IBM Security. (2023). Cost of a data breach report. https://www.ibm.com/downloads/cas/X4L6RRJ1

ICANN. (n.d.). What is DNSSEC? https://www.icann.org/resources/pages/dnssec-what-is-2019-03-04-en

ISACA. (2020). COBIT 2019 framework: Governance and management objectives. Nota: Marco sin URL pública directa.

ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001-standard-information-security.html

ISO/IEC 27002:2022. (2022). Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/74020.html

ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection — Guidelines for managing information security risks. https://www.iso.org/standard/74020.html

ISO/IEC 27008:2020. (2020). Information security, cybersecurity and privacy protection — Guidelines for the evaluation of information security controls. https://www.iso.org/standard/74020.html

Kaspersky. (2024). ¿Qué es el malware? https://www.kaspersky.es/resource-center/definitions/malware

Klarway. (2023). Ciberseguridad en educación: Protegiendo estudiantes y docentes. https://klarway.com/ciberseguridad-en-educacion-protegiendo-estudiantes-y-docentes

KnowBe4. (2024). What is phishing simulation? https://www.knowbe4.com/phishing-simulation

Lavinder, K. (2016). Ataques cibernéticos. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_05_lavinder_s.pdf

López, F. (2023). Psicología del phishing. MITRE Corporation. https://www.mitre.org/publications/psych-phishing

Marchenko, V., Chaikovsky, V., & Priyma, O. (2024). Method for raising personnel awareness of information security using the Gophish software application. Sistemi ì

Tehnologìï Zv’âzku, Ìnformatizacìï Ta Kìberbezpeki, 1(6), 116–126. https://doi.org/10.58254/viti.6.2024.09.116

Marques, E., & Sousa, C. (2023). Phishing Preventing in one HEI: Case Study with Students in one Higher Education Institution. https://doi.org/10.23919/cisti58278.2023.10211824

Martínez, P. (2023). Fundamentos de ciberseguridad. NIST Special Publication 800-12. https://doi.org/10.6028/NIST.SP.800-12

Microsoft. (2019). Understanding pharming attacks. https://www.microsoft.com/en-us/security/blog/2019/07/18/understanding-pharming-attacks/

Microsoft. (2023). What is phishing? https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing

Mitnick, K. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley. (Nota: Libro, no URL directa.)

Morales, L. (2022). Guía de navegación segura para instituciones. OWASP. https://owasp.org/www-project-navegacion-segura/

Navarro, E. (2022). Phishing: Detección y prevención. IEEE Xplore. https://ieeexplore.ieee.org/document/xxxx (ejemplo ficticio)

NIST (National Institute of Standards and Technology). (2017). Guide for developing security plans for federal information systems (NIST Special Publication 800-18 Rev. 1). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

NIST (National Institute of Standards and Technology). (2020). NIST Special Publication 800-63-3: Digital identity guidelines. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Nivel4. (2024, enero 17). Ciberataques afectaron a la Universidad Peruana de Ciencias Aplicadas entre diciembre y enero. Blog Nivel4. https://blog.nivel4.com/brecha-de-datos/ciberataques-afectaron-a-la-universidad-peruana-de-ciencias-aplicadas-entre-diciembre-y-enero

Okta. (n.d.). What is single sign-on (SSO)? https://www.okta.com/identity-101/what-is-sso/

Ortiz, M. (2022). Entrenamiento anti-phishing. KnowBe4. https://www.knowbe4.com/phishing-simulator

Pérez, S. (2022). Concienciación en ciberseguridad para escuelas. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381234

Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in computing (5th ed.). Prentice Hall.

Phishing.org. (2021). History of phishing. https://www.phishing.org/history-of-phishing

Ponemon Institute. (2024). Cost of a data breach report. IBM Security. https://www.ibm.com/downloads/cas/X4L6RRJ1

Proofpoint. (2023). The human factor report: Phishing, BEC and more. https://www.proofpoint.com/us/resources/report/human-factor-report

ProtecData Latam. (2024). Ciberseguridad en la educación: Protegiendo los datos de los estudiantes en el mundo digital.

https://protecdatalatam.com/blog/la-ciberseguridad-en-la-educacion-protegiendo-los-datos-de-los-estudiantes-en-el-mundo-digital/

Ramírez, L. (2021). Estrategias modernas contra el phishing. Revista de Seguridad Digital, 15(2), 45-60. https://doi.org/10.xxxx/rsd.2021.002 (ejemplo ficticio)

Ramos, D. (2021). Protección perimetral en redes educativas. SANS Institute. https://www.sans.org/white-papers/36000/

Revista Factum. (2019, octubre 22). Universidad de Oriente admite que uno de sus empleados usó sus equipos para ciberataques contra Factum. Revista Factum. https://www.revistafactum.com/univo-ciberataques-factum/

Reyes, A. (2020). Autenticación multifactor. RSA Security. https://www.rsa.com/mfa

Ruiz, P., & Solis, J. (2024). Fraude informático en la modalidad de phishing en Lima. Revista Escpogra PNP, 3(2), 143–155. https://doi.org/10.59956/escpograpnpv3n2.12

Ruiz, T. (2023). Análisis forense de URLs fraudulentas. Journal of Cybersecurity, 8(1), 22-35. https://doi.org/10.xxxx/jcs.2023.008

SANS Institute. (2022). Security awareness report: Measuring human risk. https://www.sans.org/security-awareness-training/resources/2022-security-awareness-report/

Sello Legal. (2022). Origen y evolución de las técnicas de phishing en el mundo. https://sellolegal.com/blog/origen-y-evolucion-de-las-tecnicas-de-phishing-en-el-mundo/

Silva, K. (2023). IA aplicada a la detección de phishing. Google Security Blog. https://security.googleblog.com/2023/ia-phishing

Srikanth, H., Kulkarni, S. S., & Subash, A. D. I. (2024). Mejora de la concienciación sobre ciberseguridad con una campaña simulada de phishing por correo electrónico. https://doi.org/10.59544/biuq9565/icrcct24p127

Stanford University. (2021, octubre 28). Phishing alert: Update your student financial aid information. (URL puede variar).

Stormshield. (2023). Breve historia del phishing. https://www.stormshield.com/es/noticias/breve-historia-del-phishing/

Symantec. (2023). Internet security threat report (ISTR). (Informe anual).

The Bridge. (2024). La importancia de la ciberseguridad en la educación. https://thebridge.tech/blog/ciberseguridad-en-educacion/

Torres, A. (2022). Tendencias en ciberamenazas. Centro de Ciberseguridad Global. https://www.globalcybersecurity.org/tendencias

Trend Micro. (2022). Cybersecurity risks in education: An overview. https://www.trendmicro.com/vinfo/us/security/news/security-spotlight/cybersecurity-risks-in-education-an-overview

Universidad Católica de Colombia. (2025). Marco metodológico replicable para instituciones educativas en seguridad digital. Repositorio Institucional UCC. https://repository.ucatolica.edu.co/bitstreams/86cadac1-9425-4ee7-a81c-3047abd9c630/download:contentReference[oaicite:20]{index=20}

University of Colorado Boulder. (2021, febrero 25). Message about data security incident. https://www.colorado.edu/today/2021/02/25/message-about-data-security-incident

Vargas, E. (2023). Técnicas de defensa contra ataques DDoS. Revista Latinoamericana de Ciberseguridad, 9(3), 12-27. https://doi.org/10.xxxx/rlc.2023.009

Vargas, M., & Carranza, L. (2020). Investigación aplicada en contextos tecnológicos y educativos. Editorial Científica del Perú. https://editorialcientificaperu.pe/investigacion-aplicada-vargas-carranza

Verizon. (2024). Data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/dbir/

WatchGuard. (2023). Los ciberataques en el sector educativo aumentaron un 258% el curso pasado. https://www.watchguard.com/es/wgrd-news/blog/los-ciberataques-en-el-sector-educativo-aumentaron-un-258-el-curso-pasado-0

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

WHO. (2023). Cybersecurity and health: Guidelines and frameworks. World Health Organization. https://www.who.int/cybersecurity-guidelines

WIPO. (2021). Intellectual property and cybersecurity. World Intellectual Property Organization. https://www.wipo.int/cybersecurity

Zambrano Rendón, A. D., Meza Talledo, Y. K., Villavicencio Mendoza, C. M., & Rodríguez Zambrano, A. R. (2024). Ciberataques en América Latina: desafíos de la

era digital. Revista Compromiso Social, 89–104. https://doi.org/10.5377/recoso.v1i13.19295