UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"PROGRAMA DE SEGURIDAD INFORMÁTICA ANTE CIBERATAQUES DE INGENIERÍA SOCIAL PARA EMPLEADOS DE UNA ENTIDAD BANCARIA EN LIMA, 2024"

PARA OPTAR:

TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR:

Bach. STANY EDGAR PASTOR HELFER

TACNA – PERÚ

2025

UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"PROGRAMA DE SEGURIDAD INFORMÁTICA ANTE CIBERATAQUES DE INGENIERÍA SOCIAL PARA EMPLEADOS DE UNA ENTIDAD BANCARIA EN LIMA, 2024"

Tesis sustentada y aprobada el 09 de octubre de 2025; estando el jurado calificador integrado por:

PRESIDENTE	**:**	**Mtra. HAYDEE RAQUEL SISA YATACO**
SECRETARIO	**:**	**Mtro. ENRIQUE FELIX LANCHIPA VALENCIA**
VOCAL	**:**	**Dr. RENZO ALBERTO TACO COAYLA**
ASESOR	**:**	**Mtro. HUGO MARTIN ALCÁNTARA MARTÍNEZ**

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Stany Edgar Pastor Helfer en calidad de: Bachiller de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de la Universidad Privada de Tacna, identificado con DNI 71248892, así como Hugo Martín Alcántara Martínez con DNI 00486155; declaramos en calidad de autor y asesor que:

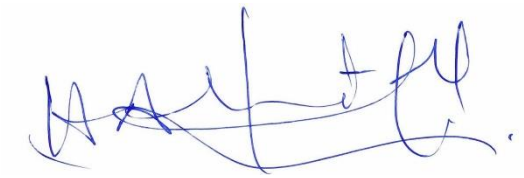
1. Somos los autores de la tesis titulada*: Programa de seguridad informática ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024*, la cual presento para optar al Título *Profesional de Ingeniero de Sistemas*.
2. La tesis es completamente original y no ha sido objeto de plagio, total ni parcialmente, habiéndose respetado rigurosamente las normas de citación y referencias para todas las fuentes consultadas.
3. Los datos presentados en los resultados son auténticos y no han sido objeto de manipulación, duplicación ni copia.

En virtud de lo expuesto, asumimos frente a La Universidad toda responsabilidad que pudiera derivarse de la autoría, originalidad y veracidad del contenido de la tesis, así como por los derechos asociados a la obra.

En consecuencia, nos comprometemos ante a La Universidad y terceros a asumir cualquier perjuicio que pueda surgir como resultado del incumplimiento de lo aquí declarado, o que pudiera ser atribuido al contenido de la tesis, incluyendo cualquier obligación económica que debiera ser satisfecha a favor de terceros debido a acciones legales, reclamos o disputas resultantes del incumplimiento de esta declaración.

En caso de descubrirse fraude, piratería, plagio, falsificación o la existencia de una publicación previa de la obra, aceptamos todas las consecuencias y sanciones que puedan derivarse de nuestras acciones, acatando plenamente la normatividad vigente.

Tacna, 9 de octubre del 2025.



Stany Edgar Pastor Helfer
DNI: 71248892

Hugo Martín Alcántara Martínez
DNI: 0048615

DEDICATORIA

La dedicatoria en este trabajo de investigación es para mis padres Edgar y Rosario y también para mi hermana Zarella, que siempre me apoyaron desde el momento en que decidí empezar en esta carrera y fueron parte importante de mi crecimiento, no solo profesional sino también como persona. También quiero hacer una mención para mis mascotas Carlitos y Chavo, que siempre me acompañaron en todos estos años de estudio y trabajo.

Stany Edgar Pastor Helfer

AGRADECIMIENTO

Agradezco a los docentes encargados de brindarnos la información necesaria para cumplir con el trabajo de investigación y hacerlo de manera óptima, también agradezco a mi asesor, el Ing. Martín Alcántara, por su apoyo en el desarrollo de mi investigación.

Stany Edgar Pastor Helfer

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

Esta investigación se llevó a cabo con el objetivo de determinar la influencia de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social en empleados de una entidad bancaria en Lima, durante el año 2024. El estudio se enmarcó en un enfoque cuantitativo, de tipo aplicado, con diseño cuasi-experimental, aplicando una evaluación pretest y postest a una muestra de 100 colaboradores del área de tecnología. Se implementó un programa de formación estructurado en tres módulos temáticos, orientados a reforzar conocimientos sobre ingeniería social, phishing y protección de información confidencial. Este programa cuya finalidad no fue solo impartir conocimientos técnicos, sino también promover la concienciación y buenas prácticas en seguridad informática, con el fin de mejorar la capacidad de respuesta de los colaboradores ante intentos de manipulación o fraude. Los resultados obtenidos a través del software SPSS, mostraron diferencias significativas entre las evaluaciones que se realizaron previas y posteriores a la intervención, lo que evidencia una influencia en la preparación y capacidad de respuesta de los colaboradores. Asimismo, se logró identificar que el nivel de comprensión y la capacidad para aplicar medidas de seguridad aumentó considerablemente tras la aplicación del programa de capacitación. En conclusión, el programa de seguridad informática tuvo una influencia positiva y significativa en la preparación de los colaboradores frente a ciberataques de ingeniería social, esto se ve reflejado en los resultados estadísticos obtenidos luego de la comparación entre el pretest y el postest, en donde en el 99% de los casos se vio un aumento en el puntaje promedio obtenido por los colaboradores, solo 1% de los colaboradores obtuvieron el mismo puntaje y nadie obtuvo un promedio más bajo. Fortaleciendo así la cultura de seguridad en la organización y aportando un valor estratégico en la protección de los activos de información de la entidad bancaria.

Palabras clave: seguridad informática; ingeniería social; ciberataques; programa educativo; prevención.

ABSTRACT

This study was conducted to determine the impact of an IT security program on the preparedness and decision-making of employees at a bank in Lima in response to social engineering cyberattacks in 2024. The study employed a quantitative, applied approach with a quasi-experimental design, using pre- and post-tests on a sample of 100 employees in the technology department. A training program structured into three thematic modules was implemented, aimed at reinforcing knowledge about social engineering, phishing, and the protection of confidential information. The purpose of this program was not only to impart technical knowledge but also to promote awareness and best practices in cybersecurity, with the goal of improving employees' ability to respond to attempts at manipulation or fraud. The results obtained using SPSS software showed significant differences between the assessments conducted before and after the intervention, indicating an impact on employees' preparedness and response capabilities. Furthermore, it was found that the level of understanding and the ability to apply security measures increased considerably following the implementation of the training program. In conclusion, the cybersecurity program had a positive and significant impact on employees' preparedness to deal with social engineering cyberattacks, This is reflected in the statistical results obtained after comparing the pre-test and post-test, where in 99% of cases there was an increase in the average score obtained by employees, only 1% of employees obtained the same score, and no one obtained a lower average. This strengthens the security culture within the organization and provides strategic value in protecting the bank's information assets.

Keywords: computer security; social engineering; cyberattacks; educational program; prevention.

INTRODUCCIÓN

En la presente investigación denominada “Programa de seguridad informática ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024”, se buscó abordar la crítica problemática de la ciberseguridad en el sector financiero. Esta investigación se estructuró en cinco capítulos, donde se examinó las amenazas diarias que enfrenta la entidad bancaria, las cuales ponen en riesgo la confidencialidad, integridad y disponibilidad de la información, pilares principales de la norma ISO/IEC 27001.

En el primer capítulo se desarrolló el planteamiento del problema, detallando la naturaleza de las amenazas de ingeniería social y su impacto en la continuidad del negocio. Aquí se enuncian el problema general y específicos, así como la justificación de la investigación, que subraya la necesidad de un enfoque proactivo en la gestión de riesgos de seguridad de la información, alineado con los principios de la ISO 27001.

En el segundo capítulo, se construye un marco teórico que incluye antecedentes de investigación a nivel internacional y nacional, seguido de bases teóricas relevantes. Este capítulo profundiza en conceptos clave como el análisis de riesgos y la gestión de vulnerabilidades, presentando un glosario de términos que son esenciales para comprender el contexto de la investigación.

El tercer capítulo presenta el marco metodológico del estudio, que define el tipo y diseño del estudio, la población y muestra, así como la operacionalización de variables y el procesamiento de información

En el cuarto capítulo se presentan los resultados de obtenidos tras la aplicación del programa de seguridad informática en los empleados de la entidad financiera.

Finalmente, el quinto capítulo presenta la discusión de resultados, destacando la efectividad de la aplicación del programa de seguridad informática en los empleados de la entidad financiera y como su preparación ante ataques de ingeniería social ha mejorado notablemente, alineándose con los objetivos de mejora continua de la ISO 27001.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

Según IBM, (2024), la ingeniería social resulta atractiva para los ciberdelincuentes porque les permite acceder a redes digitales, dispositivos y cuentas sin necesidad de realizar laboriosos esfuerzos técnicos para eludir cortafuegos, software antivirus y otras protecciones de ciberseguridad. Esto convierte a la ingeniería social en un método muy atractivo para los ciberdelincuentes. Según el estudio “The State of Cybersecurity” de (ISACA, 2022) , afirma que la ingeniería social es la principal fuente de incidentes de red en la actualidad. Esta es una de las razones por las que la ingeniería social es la principal causa de violaciones de la red. Según las conclusiones del informe “El coste de una violación de datos en 2024” de IBM, las violaciones de datos más costosas fueron las provocadas por técnicas de ingeniería social. Estas técnicas incluían el phishing y el hackeo de correos electrónicos empresariales.

De acuerdo con Albladi y Weir (2018), bajo el panorama actual, las organizaciones se han visto obligadas a implementar soluciones tecnológicas en todos o gran parte de sus procesos, con el fin de ser más competitivas, esto también ha significado la oportunidad para que los ciberdelincuentes encuentren formas nuevas y también más sofisticadas para explotar las vulnerabilidades de estos activos informáticos. En este contexto, es necesario entender los factores que tiene influencia sobre la capacidad de los usuarios para detectar amenazas, si pretendemos construir un perfil de usuarios susceptibles, desarrollar programas de asesoramiento y capacitación adecuados, y en general para ayudar a las personas con mayor probabilidad de convertirse en objetivo de ataques de ingeniería social en redes sociales.

Por lo que se puede decir que la seguridad de la información se ha convertidos en parte fundamental de una organización moderna. Según Scientific Knowledge Publisher (2024) para mantenerse a la vanguardia ante un panorama de amenazas cada vez más cambiante, los procedimientos de seguridad están actualizándose constantemente. Los atacantes identifican las fallas tecnológicas más recientes y de acuerdo a esto se encargan de crear métodos sofisticados para explotar dichas vulnerabilidades. Para mitigar estos nuevos peligros, los expertos en ciber seguridad deben actualizar sus conocimientos constantemente y cambiar sus enfoques.

Este trabajo de investigación brinda un modelo con la preparación necesaria para enfrentar preventivamente estas amenazas y para mantener a los colaboradores de la entidad financiera preparados y actuando sobre la marcha en situaciones de riesgo relacionadas específicamente a ciberamenazas de ingeniería social, lo cual dio pie a la implementación de un programa de seguridad informática que no solo brinde información general acerca de estos peligros sino que también ataca situaciones puntuales que puedan darse en una entidad bancaria y en el día a día de los colaboradores, mejorando de esa manera su desempeño ante este tipo de amenazas y por lo tanto, fortaleciendo la confidencialidad e integridad de los datos de los usuarios y clientes.

1.2 Formulación del problema

1.2.1 Problema general

¿Como influye un Programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social a los empleados de una entidad bancaria en Lima, 2024?

1.2.2 Problemas específicos

a. ¿Cómo influye la gestión de vulnerabilidades y riesgos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?

b. ¿Cómo influye las políticas y procedimientos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?

c. ¿Cómo influye el compromiso de datos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?

d. ¿Cómo influyen las medidas de seguridad de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?

1.3 Justificación e importancia

1.3.1 Justificación

La presente investigación se justifica desde tres niveles fundamentales: teórico, metodológico y práctico, en el marco del desarrollo de la ciberseguridad en organizaciones del sector financiero, particularmente ante amenazas de ingeniería social.

A nivel teórico, esta investigación contribuye al cuerpo de conocimiento existente sobre la seguridad de la información, con énfasis en el enfoque preventivo ante ciberataques de ingeniería social. Aporta evidencia empírica sobre la efectividad de programas de capacitación específicos en contextos laborales sensibles, y se alinea con los estándares internacionales de gestión de seguridad, como la norma ISO/IEC 27001 y el marco COBIT 2025, integrando principios de mejora continua, concienciación y control de riesgos humanos.

A nivel metodológico, la tesis propone y valida un diseño cuasi-experimental con aplicación de pretest y postest en un entorno real corporativo. El uso de una muestra estadísticamente representativa, el desarrollo de instrumentos de evaluación con criterios de validez y confiabilidad, y el tratamiento estadístico riguroso mediante pruebas no paramétricas como Wilcoxon, representan una contribución relevante para futuras investigaciones aplicadas en ciberseguridad organizacional.

A nivel práctico, esta investigación tiene un impacto directo en la protección de activos informáticos críticos en la banca, sector altamente expuesto a ataques sofisticados. La implementación del programa propuesto permite mejorar la preparación, la cultura preventiva y la capacidad de respuesta de los empleados ante situaciones reales de manipulación o engaño. Sus resultados ofrecen evidencia concreta sobre la reducción del riesgo humano, y pueden ser escalados o adaptados en otras áreas funcionales o instituciones con necesidades similares.

Es posible que la tecnología digital afecte a la forma en que las personas ven el mundo y se relacionan con su entorno. En ese sentido, Pashentev et al. (2019), nos dice que en general el uso de la tecnología digital, tiene gran influencia en la mentalidad y en la conciencia de las personas llevado a cualquier esfera de la sociedad. Adicionalmente el uso de tecnologías de la información en cualquier organización es parte fundamental en para el desarrollo de las mismas, convirtiéndose en un activo de gran valor, por lo que su uso conlleva también a grandes riesgos en la seguridad y privacidad de la información para personas y organizaciones, por lo que es blanco de cibercriminales que valiéndose de métodos y herramientas destinadas a burlar los

controles y vulnerar las debilidades de seguridad informática en las empresas pretenden mediante la manipulación y engaño obtener el recurso más importante para una organización que es la información.

Según IBM (2024) el rubro de finanzas y seguros se situó en el segundo lugar como el sector que recibió la mayor cantidad de ciberataques en 2023 por tercer año consecutivo, representado el 18,2% de los incidentes que reportó la plataforma de seguridad de IBM X-Force. El malware fue la amenaza más común, representando el 38% de los incidentes dentro de la industria de finanzas y seguros, y el ransomware representó el 25% de los casos. Los casos de acceso al servidor ocuparon el segundo lugar con el 25% de los ataques, mientras que el uso de herramientas legítimas con fines maliciosos fue la tercera acción más observada en el objetivo, representando el 19% de los incidentes.

1.3.2 Importancia de la investigación

La investigación tiene una importancia significativa en múltiples dimensiones. Para empezar, la evaluación de la eficacia del proceso de implantación de un programa de seguridad informática ante ciberataques de ingeniería social ayuda a mejorar la seguridad de la información de la organización y prevención para salvaguardar sus recursos más valiosos. Además, contribuye al cuerpo de conocimientos sobre seguridad de la información y sirve como valioso recurso para otras organizaciones que pretendan adoptar o mejorar este punto de referencia. Desde la asignación de recursos hasta la planificación de acciones futuras, los resultados facilitarán una toma de decisiones bien informada. Además, al promover prácticas seguras y el cumplimiento de la normativa. Por último, esta investigación podrá ayudar a la implementación de modelos teóricos que sirvan de ejemplo a las organizaciones para adaptarse y saber cómo responder efectivamente en la prevención y preparación de sus empleados ante ciberataques de ingeniería social.

1.4 Objetivos

1.4.1 Objetivo general

Identificar como influye un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

1.4.2 Objetivos específicos

a. Conocer cómo influye la gestión de vulnerabilidades y riesgos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
b. Conocer cómo influyen las políticas y procedimientos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
c. Conocer cómo influye el compromiso de datos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
a) Conocer cómo influyen las medidas de seguridad de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

1.5 Hipótesis

1.5.1 Hipótesis general

El programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

1.5.2 Hipótesis específicas

a. La gestión de vulnerabilidades y riesgos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
b. Las políticas y procedimientos de un programa de seguridad informática influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
c. El compromiso de datos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
d. Las medidas de seguridad de un programa de seguridad informática influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 A nivel nacional

Marchand (2020) desarrolló la tesis titulada *Cultura de seguridad de información en la protección de activos informáticos en la Universidad Nacional Agraria de la Selva, 2018-2020*. El propósito de este estudio era investigar la naturaleza de la conexión que existe entre los aspectos de cumplimiento, concienciación y apropiación que se asocian a la cultura de seguridad de la información y los aspectos que se asocian a la protección de activos. El nivel corresponde a una investigación descriptiva correlacional explicativa, y el tipo de investigación es aplicada ya que se pretendió abarcar temas particulares, con la aplicación del conocimiento científico, así como la aplicación; y el nivel es investigación aplicada. Por esta razón, se realizó una encuesta a una población de 79 usuarios para establecer el diagnóstico, y se utilizaron métodos de ingeniería social durante todo el procedimiento. Fue factible llegar a la conclusión de que existe una relación entre las variables de estudio que presenta un alto nivel de significación.

Orihuela (2022), desarrolló la tesis titulada “Programa de seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima”, de la Pontificia Universidad Católica del Perú. Con la ayuda de un programa de capacitación, el propósito de la investigación es lograr el desarrollo de los empleados de una empresa de telecomunicaciones en Lima, Perú, con conocimientos relacionados a la seguridad de la información. Estos conocimientos permitirán a los empleados facilitar la detección y reacción positiva ante intentos de ataques cibernéticos de ingeniería social. El nivel básico, relacional y el diseño experimental son los tipos de estudios que se están llevando a cabo. A la luz de esto, se tomaron en consideración el uso de cuestionarios, los datos recibidos del curso y las entrevistas como metodologías de medición. El piloto ha demostrado que existe una preocupación genuina por la seguridad de la información dentro de la organización, y que es de suma importancia cultivar en los trabajadores el conocimiento de la seguridad de la información para asegurar que se comporten y piensen de buena manera al interactuar con Internet.

Alfaro y Perez (2023), desarrollaron la tesis *Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de ingeniería social en el rubro empresarial*, *de la Universidad Cesar Vallejo*. El objetivo principal de la investigación era desarrollar e implementar un módulo de extensión de seguridad que

permitiera identificar y prevenir los ataques de ingeniería social en el sector comercial. Para llevar a cabo el estudio, se seleccionó el uso del marco Vue.js y el enfoque en cascada. La evaluación se basó en tres indicadores: el tiempo medio de confirmación, la capacidad de reacción y la tasa de detección. Tras el análisis, se determinó que el módulo de extensión había logrado los objetivos establecidos para la identificación y prevención de ataques de ingeniería social. Se determinó que el indicador del tiempo medio de confirmación tenía una media de 0,1320 milisegundos, el indicador de la tasa media de detección tenía una media del 91,73 % y el indicador de la capacidad media de reacción también tenía una media del 91,73 %. Al final del día, se descubrió que los indicadores habían logrado resultados considerables y positivos como consecuencia directa de la adopción del módulo de seguridad.

Rodas y Sánchez (2024), desarrollaron la tesis *La implementación de un protocolo de prevención contra ransomware para optimizar la seguridad del servidor en la empresa BBTI S.A.C entre el año 2022*. En este trabajo, intentaremos encontrar una solución a un problema que amenaza la integridad de BBTI S.A.C., así como su capacidad para continuar con sus operaciones. La organización ha sido objeto de ataques de ransomware a lo largo de los últimos tres años, lo que ha provocado un daño significativo a la seguridad de sus sistemas. El método utilizado en esta investigación en particular fue la investigación explicativa. Se llevó a cabo una encuesta a una muestra representativa de veintitrés personas de una de sus oficinas, además de utilizar un diseño de estudio experimental. Se utilizaron varias pruebas estadísticas, como las pruebas de Shapiro-Wilk, Spearman y ANOVA, para verificar la hipótesis. Estas pruebas permitieron verificar la relación existente entre las variables. En conclusión, los resultados obtenidos fueron aceptables. Se demostró que la implementación de un protocolo de prevención de ransomware está directamente relacionada con el grado de seguridad del servidor. Esto llevó a la conclusión de que la adopción de un protocolo de prevención de ransomware dio lugar a una mejora en la seguridad del servidor.

Palomino et al. (2024), desarrollaron la tesis *Modelo de desarrollo de reglas de correlación para la detección y alerta de ransomware*. El objetivo de esta investigación era implementar un modelo de reglas de correlación en el Sistema de Gestión de Información y Eventos de Seguridad (SIEM) para detectar, prevenir y mitigar eficazmente los ataques de ransomware. Este era el objetivo general del estudio. La creación de un enfoque de vanguardia para este fenómeno y la validación de un modelo que satisfaga el objetivo especificado anteriormente llevaron a la selección de un diseño mixto como metodología para el estudio. Se descubrió que el modelo sugerido, basado en la base de conocimientos MITRE ATT&ACK, proporciona mecanismos que permiten

detectar, prevenir y mitigar con éxito los ataques de ransomware. Este fue uno de los descubrimientos o resultados más importantes que se obtuvieron. La planificación, el diseño, la construcción y la mejora son las cuatro etapas cíclicas que componen el modelo. Es importante comprender que el modelo se compone de estas fases. Una revisión de la bibliografía relevante reveló que actualmente existen cuatro formas principales de este virus. Esto se descubrió tras la revisión de la bibliografía. En resumen, la investigación demostró que es posible desarrollar un modelo de reglas de correlación capaz de identificar y notificar casos de ransomware. Esto puede considerarse importante tanto desde el punto de vista teórico como práctico, especialmente si se tienen en cuenta las pérdidas sustanciales que provocan este tipo de ataques.

2.1.2 A nivel internacional

Flores (2023), desarrolló la tesis titulada *Análisis de vulnerabilidades en el uso de las redes sociales en ciberataques de ingeniería social para fortalecer la seguridad de la información en la Facultad de Ciencias Humanas Y De La Educación, de la Universidad Técnica de Ambato*. La ingeniería social es un conjunto de métodos que permiten obtener información sensible manipulando a otras personas para acceder a dicha información. En un sentido más tangible, es una capacidad que utilizan algunos individuos para adquirir conocimientos, acceder a sistemas de información que les permitan llevar a cabo alguna acción perjudicial para el individuo o la organización implicada, o que los exponga a un peligro potencial. Para el desarrollo de este proyecto se utilizó la plataforma DigitalOcean para el servicio de nube virtualizada, el framework Gophish para la creación, planificación y ejecución de la simulación de ataques, la técnica de Phishing y la herramienta Hunter.io para el descubrimiento y recolección de correos electrónicos. La evaluación de la seguridad de los sistemas informáticos que manejan información perteneciente a la institución es de suma importancia. Sin embargo, el elemento humano que manipula esta información puede convertirse en una fuente de exposición de la misma, lo que puede ser útil para un atacante. En consecuencia, es de suma necesidad determinar la cantidad de conocimientos sobre ciberseguridad que poseen tanto los alumnos como los instructores. El objetivo principal de estos exámenes es aumentar la Seguridad de la Información de la institución mejorando la concienciación en materia de seguridad de los alumnos y profesores de la Facultad de Ciencias Humanas y de la Educación. Esto puede lograrse preparándolos para enfrentarse a una variedad de escenarios de riesgo que podrían surgir en caso de un ataque verdadero.

Peñafiel (2022) desarrolló la tesis titulada *Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales*, *de la Universidad Estatal Península de Santa Elena*. El proyecto propone determinar posibles vulnerabilidades mediante la recopilación de información en una institución de educación superior de la provincia de Santa Elena a través del uso de la ingeniería social empleando técnicas computacionales y no computacionales. El objetivo final del proyecto es generar un informe sobre los datos descubiertos y complementarlo con una guía de buenas prácticas para las personas que trabajan en dicha institución. La técnica de investigación exploratoria y de diagnóstico que se utilizó en la preparación de este informe fue útil para recopilar información sobre la institución de educación superior. Esta información se recopiló mediante la realización de una encuesta a los estudiantes y al profesorado de la institución. De manera similar, se utilizó una metodología genérica, que se modificó para identificar vulnerabilidades a través de ataques de ingeniería social. Esta metodología consta de las siguientes fases: la identificación y selección de técnicas de ingeniería social, la implementación de técnicas de ingeniería social, el análisis de resultados y la presentación de resultados. Lo último que se hizo fue llevar a cabo ataques de ingeniería social, que tuvieron éxito y demostraron las debilidades que se descubrieron en esa institución. En la misma línea, se sugirió una guía de buenas prácticas, que será de gran utilidad para quienes no estén familiarizados con el tema.

Villacís (2023), desarrolló la tesis titulada *Diseño de una campaña de ataques de ingeniería social, de la Pontificia universidad católica de Ecuador*. En concreto, la investigación se centra en la ingeniería social y cómo afecta a las personas en términos de la información personal que poseen, así como los peligros a los que se enfrentan en caso de ser objeto de uno de estos ataques. Con el fin de elaborar una campaña de ingeniería social, se llevó a cabo un ataque de phishing controlado a pequeña escala con la intención de evaluar la situación actual. Durante el transcurso de este estudio, se utilizó un enfoque descriptivo para determinar los elementos que hacen a las personas susceptibles a un ataque de ingeniería social e ilustrar las etapas que se utilizan en la ejecución de este tipo de ataque. Los resultados obtenidos demostraron que el primer paso, que es la fase de investigación, es de suma importancia para lograr el éxito con el público objetivo. Todas las personas que enviaron sus datos utilizaron contraseñas débiles relacionadas con su información personal o con dificultades sociales. Esto se descubrió porque no se impusieron restricciones en el campo de la contraseña, por lo que cualquiera podía introducir sus datos. Como parte de este proyecto, se llevó a cabo con éxito una iniciativa de ingeniería social. Esto fue posible gracias a la concienciación

que se transmitió a cada dirección de correo electrónico registrada. No solo recomendamos llevar a cabo ataques de phishing para futuros estudios, sino que también proponemos probar diferentes tácticas de ingeniería social para determinar cuáles son las que más probabilidades tienen de engañar a las personas.

Rocohano y Silva (2021), desarrollaron la tesis titulada *Detección de vulnerabilidades en el comportamiento de las personas para evitar que sean víctimas de ataques de ingeniería social*, *de la Universidad de las fuerzas armadas de Ecuador*. El presente estudio se orienta a proponer un modelo que permita identificar a las personas que, por sus conductas o hábitos, presentan una mayor susceptibilidad frente a técnicas de Ingeniería Social. Los hallazgos obtenidos pueden servir posteriormente como insumo para que instituciones o individuos reconozcan a dichos usuarios en condición de riesgo y diseñen estrategias de sensibilización respecto a las amenazas que representan estos ataques.

La investigación se enmarca en un enfoque cuantitativo y de tipo descriptivo, dado que busca caracterizar las actitudes y comportamientos de usuarios vinculados al uso de Tecnologías de la Información, a través de la recopilación de datos relacionados con los principios de la Seguridad de la Información. Asimismo, pretende examinar la relación entre determinadas conductas y actitudes presentes en distintos colectivos, tales como estudiantes, docentes, administradores y personal militar.

Los resultados evidenciaron que los estudiantes constituyen el grupo con mayor vulnerabilidad frente a ataques de Ingeniería Social, lo cual se asocia a su exceso de confianza y limitada experiencia en la gestión de información. En contraste, docentes, administradores y militares, al estar familiarizados con la manipulación de datos sensibles y conscientes de los riesgos asociados, presentan una menor propensión a ser víctimas de estos ataques. Finalmente, el análisis demostró que el incremento en las horas de exposición a dispositivos digitales eleva el nivel de riesgo, y que este se intensifica cuando el usuario muestra comportamientos permisivos o carece de cautela.

Campoverde (2022), desarrolló la tesis titulada *Implementación de técnicas en ingeniería social en un gobierno autónomo descentralizado de la provincia de Santa Elena*. Debido a que estos ataques se llevan a cabo directamente contra los usuarios, esta propuesta busca determinar la herramienta adecuada para el hacking ético con el fin de realizar un análisis de la seguridad de la información que manejan los operadores de diversos departamentos del gobierno municipal. Este análisis permitirá comprometer la información mediante el uso de herramientas de ingeniería social. Utilizando el enfoque de la ingeniería social, se diseñaron y llevaron a cabo dos escenarios de prueba

en diversos departamentos del gobierno municipal. El objetivo de estos escenarios era recrear condiciones controladas en caso de que se llevara a cabo un ataque a la seguridad de la información. En el primer escenario, los empleados que trabajaban en uno de los departamentos fueron objeto de un ataque de phishing, en el que se replicó la página de inicio de sesión de Gmail, lo que permitió a los atacantes obtener las credenciales de logueo de las personas a las que se dirigía el ataque. En el segundo caso, se envió por correo electrónico un archivo que incluía un virus con un título que hacía referencia al área de trabajo. Este archivo fue recibido por miembros del personal de Municipal Gad, lo que provocó una conexión remota al ordenador y comprometió la información que se estaba procesando. Como consecuencia de la implementación de técnicas de ingeniería social, se formularon recomendaciones para un plan de seguridad de la información destinado a prevenir ataques que pudieran comprometer la ética del Gobierno Municipal. Estas recomendaciones incluían instruir a los miembros del personal de diversos departamentos sobre cómo actuar en caso de ser objeto de un ataque de ingeniería social.

2.2 Bases teóricas

2.2.1 Seguridad informática

De acuerdo con CIBERTEC (2024), la seguridad informática es un campo de estudio que abarca un conjunto de prácticas, tecnologías, métodos y procedimientos diseñados para proteger los sistemas informáticos, las redes, los dispositivos y los datos digitales contra el acceso no autorizado, los ciberataques, las fugas, la manipulación y otras amenazas que pueden comprometer la confidencialidad, la integridad y la disponibilidad de la información.

Según IBM (2025), la seguridad informática es el proceso de proteger los activos de tecnología de la información de una organización, como sus sistemas, redes, dispositivos y datos, contra el acceso no autorizado, las violaciones de datos, los ciberataques y el comportamiento delictivo mediante el uso de una combinación de tecnologías y soluciones de seguridad. Esta protección incluye medidas de seguridad tanto digitales como físicas. Algunos ejemplos de medidas de seguridad digitales son los cortafuegos, el software antivirus y la autenticación multifactorial. Otros ejemplos son las cerraduras, las cámaras y las restricciones de acceso.

Según Gómez (2006), el término seguridad informática se define como cualquier método que impide que se realicen operaciones ilegales en un sistema informático o una red. Estas operaciones podrían causar daños a la información, los equipos o el

software. Esta definición proviene de una perspectiva académica. De acuerdo con Kissel (2012), la protección de accesos no deseados a la información y a los sistemas que los sostienen es lo que se conoce como seguridad de la información.

2.2.1.1 Gestión de la seguridad en TI

De acuerdo con Stallings y Brown (2015), a lo largo de las últimas décadas, el subcampo de la gestión de la seguridad de la información ha experimentado un importante desarrollo. Como resultado de la rápida expansión y dependencia de los sistemas de información en red, así como del consiguiente aumento de las amenazas a estos sistemas, esto se ha hecho como reacción. A lo largo de los últimos diez años, se han publicado una serie de normas nacionales e internacionales. Estas directrices son el resultado de un acuerdo sobre los procedimientos más eficaces en este ámbito. Muchas de estas normas han sido evaluadas e incluidas en la serie ISO 27000 por la Organización Internacional de Normalización (ISO), que también las ha revisado y consolidado.

2.2.2 Programa de seguridad informática

Según Whitman y Mattord (2018), los programas de seguridad de la información tienen un enfoque metódico y planificado para salvaguardar los activos de información de una organización mediante la implementación de políticas, procedimientos y controles tecnológicos. Estos programas también se conocen como programas de seguridad de la información. El objetivo de esta iniciativa es garantizar que la información se mantenga segura, intacta y accesible a pesar de la presencia de una amplia variedad de vulnerabilidades y amenazas. La identificación de riesgos, la implementación de acciones preventivas y correctivas, y el cumplimiento de normas y estándares de seguridad deben incluirse en este programa. Además, debe contar con métodos de evaluación y revisión continuas para responder a los cambios en el entorno de amenazas, así como a los cambios en la infraestructura técnica.

2.2.2.1 La seguridad de la información está limitada por factores sociales y culturales

De acuerdo con Nieles et al. (2017), la forma en que las personas comprenden y utilizan los sistemas está influenciada por cuestiones sociales, lo que a su vez repercute en la

seguridad de la información utilizada por los sistemas y la empresa. Personas diferentes tienen métodos diferentes de ver, razonar y tomar decisiones basadas en el riesgo. Por consiguiente, para resolver este problema, las empresas deben definir las funciones de la seguridad de la información de forma clara, intuitiva y comprensible. Además, la impartición de formación periódica en materia de sensibilización sobre la seguridad contribuye a reducir el impacto de las diferencias individuales en la percepción del riesgo. La forma en que una empresa lleva a cabo su actividad puede funcionar como un elemento cultural que debe tenerse en cuenta al abordar la seguridad de la información, al igual que las variables sociales. La reacción de una organización ante la seguridad de la información puede verse influida por la cultura de la propia empresa. Mediante una descripción detallada de los riesgos asociados a los procesos empresariales, es posible contribuir a la transparencia y la aceptabilidad de los procedimientos de seguridad de la información recomendados.

Si miramos el panorama general, la conexión entre la seguridad y los estándares culturales no siempre tiene por qué ser adversa. Las normas de la sociedad pueden tener tanto un efecto beneficioso como negativo en la seguridad de la información. Un ejemplo de comportamiento que podría tener un efecto perjudicial en la seguridad de la información es cuando un usuario escribe sus contraseñas y las guarda cerca de su ordenador. Una implantación más generalizada de la autenticación multifactorial, en la que el usuario debe proporcionar más de una forma de autenticación para cambiar su contraseña (por ejemplo, enviando un mensaje de texto al usuario o utilizando un token físico), podría tener una influencia beneficiosa. Mediante el suministro de información más precisa y fiable, así como una mayor disponibilidad del sistema, la seguridad tiene el potencial de mejorar el flujo de datos e información, así como el acceso a los mismos. Además, los métodos de seguridad, como el cifrado, pueden ayudar a las personas a proteger mejor su privacidad. Es posible que algunas técnicas de seguridad, como el inicio de sesión único, introduzcan nuevas vulnerabilidades. Por lo tanto, es esencial reflexionar sobre las formas en que las soluciones de seguridad pueden implementarse de manera que se maximicen los objetivos sociales más amplios.

2.2.3 El modelo ADDIE

De acuerdo con Peterson (2003), el proceso de diseño instruccional ADDIE, es una técnica popular que se utiliza con frecuencia en el proceso de desarrollo de cursos instruccionales y programas de capacitación. Mediante el uso de esta estrategia, los instructores cuentan con fases útiles y claramente definidas con el fin de implementar

la educación de manera eficaz. El marco ADDIE, que consta de cinco etapas, se utilizó de dos maneras diferentes a lo largo del proceso de desarrollo de un curso de diseño instruccional para estudiantes que cursaban una maestría. El marco ADDIE se utilizó en las primeras etapas del proceso de planificación del curso de diseño instruccional. Posteriormente, se comprobó que el marco era beneficioso como andamiaje para los estudiantes que estaban construyendo proyectos multimedia como requisito final del curso. A lo largo de toda la clase, se utilizó el modelo ADDIE, que se centraba en el estudiante en lugar de mantener un enfoque centrado en el profesor. En lo que respecta a la creación del curso, el análisis de los alumnos se convirtió en un componente clave, y también fue un componente esencial para los alumnos mientras desarrollaban sus propios proyectos multimedia. El marco ADDIE dio vida al curso de diseño instruccional y a los proyectos al ofrecer un mecanismo que involucraba activamente a los desarrolladores en la resolución de problemas. Esto permitió que el curso fuera más eficaz.

Podemos comprender mejor su importancia si nos remitimos a su acrónimo, que representa los cinco principios en los que se basa:

A (Análisis): Identifica el problema.

D (Diseño): Creación del roadmap del plan de formación.

D (Desarrollo): Crear las herramientas y recursos requeridos.

I (Implementación): Ejecutar el plan de comunicación y brindar las clases.

E (Evaluación): Evaluar y detectar de puntos de mejora.

2.2.4 Capacitación en seguridad de la información

La formación y sensibilización del personal en materia de ciberseguridad es un proceso educativo cuyo objetivo es informar y preparar a los trabajadores sobre los riesgos digitales a los que se enfrentan. De acuerdo con Kaspersky (2023), el objetivo final de este proceso es capacitar a los empleados para que puedan defenderse a sí mismos y a la empresa frente a los ciberataques. Debido a que muchas violaciones de seguridad son el resultado de errores humanos o de la falta de concienciación sobre métodos comunes como el phishing, que es uno de los ataques más frecuentes y exitosos, esta formación es muy necesaria.

Según MetaCompliance (2024), esta formación suele ser impartida por las organizaciones mediante cursos específicos, simulaciones de ataques, difusión

constante de información sobre los riesgos y normas de seguridad explícitas. Además, es fundamental que la formación sea continua y se adapte a las distintas características de los empleados de la organización, desde los usuarios normales hasta los profesionales de la seguridad.

En resumen, de acuerdo a lo indicado por Fortinet (2024), proporcionar formación a los empleados y mejorar sus conocimientos sobre ciberseguridad es un método esencial para reducir los riesgos causados por errores humanos, reforzar las defensas contra los ciberataques y fomentar una cultura de la seguridad dentro de la empresa.

2.2.5 Norma ISO/IEC 27001

Según la información que tenemos sobre la norma ISO/IEC 27001, International organization of standardization & International Electrotechnical Commission (2022), nos dice que esta se ha desarrollado con el fin de permitir a las empresas de cualquier tipo, tamaño e industria construir, ejecutar, supervisar, evaluar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Según lo establecido por ICONTEC (2017), el propósito de la norma ISO/IEC 27001 es garantizar que los componentes del sistema de gestión de seguridad de la información (SGSI) estén de acuerdo con lo requerido por la empresa.

La norma ISO 27001 promueve un enfoque basado en procesos mediante la adopción del modelo Deming, que recomienda un ciclo de mejora continua a través de la repetición de las etapas «Planificar-Hacer-Verificar-Actuar», a menudo conocido como PDCA. Este ciclo se conoce como mejora continua.

2.2.6 Políticas y procedimientos en seguridad de la información

Raza et al.(2024), nos dice que para establecer una base sólida para la seguridad de la información, es necesario crear normas y procedimientos de seguridad que sean explícitos y estén bien definidos. Cuando se trata de preservar los activos de información, estos acuerdos establecen las normas, las obligaciones y las mejores prácticas que deben seguirse. Proporcionan a las partes interesadas y a los trabajadores un marco que pueden cumplir, lo que garantiza que las medidas de

seguridad se apliquen de manera coherente y se desarrolle una cultura dentro de las empresas que sea consciente de la seguridad.

De manera similar OSTEC (2024), las políticas y procedimientos de seguridad de la información son un conjunto de normas, estándares, directrices y procesos definidos por una organización con el fin de proteger sus activos de información dentro de la empresa. Con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos frente a amenazas tanto internas como externas, estas normas describen la forma en que se debe manejar, proteger y utilizar la información.

Por otro lado Grupo Atico34 (2024), nos dice que Las políticas de una organización suelen ser documentos que han sido aprobados por la alta dirección. Estas políticas describen los procedimientos y controles que son esenciales para evitar, detectar y reaccionar ante incidentes de seguridad. Las políticas también describen el compromiso de la empresa con la seguridad de la información. Complementando el concepto previo, UNIR (2024), nos dice que los procedimientos proporcionan un desglose exhaustivo de las acciones específicas que deben realizar el personal y los usuarios para cumplir con las normas que se han desarrollado. Estos procedimientos incluyen rutinas de copia de seguridad, control de acceso, uso permitido de los sistemas y gestión de incidentes.

2.2.6.1 Normas, directrices y procedimientos

De acuerdo a Nieles et al. (2017), las organizaciones también establecen normas, reglas y procedimientos que proporcionan a los usuarios, gerentes, administradores de sistemas y otras personas una forma más clara de aplicar las políticas y alcanzar los objetivos de la organización. Esto se debe a que las políticas se expresan a un nivel general. Las tecnologías y los procedimientos que se deben utilizar para proteger los sistemas se especifican en normas y recomendaciones. Los procedimientos son procesos adicionales más específicos que deben realizarse para completar las actividades relacionadas con la seguridad. Una organización puede difundir sus normas, reglas y procesos en toda la organización mediante manuales, reglamentos o guías.

- Es importante señalar que los estándares organizacionales, que no deben confundirse con las Normas Nacionales Americanas, las Normas Federales de Procesamiento de la Información ni ninguna otra norma nacional o internacional, estipulan la aplicación coherente de determinadas tecnologías, parámetros o

procesos en situaciones en las que dicha aplicación uniforme resultaría ventajosa para una organización. Un buen ejemplo sería la estandarización de las tarjetas de identificación en toda la empresa. Esto facilitaría la circulación de los empleados y automatizaría los procedimientos de acceso y salida. El establecimiento de normas suele ser obligatorio dentro de una institución.

- Las directrices proporcionan a los usuarios, a los trabajadores que trabajan en TI y a otras personas la asistencia para proteger adecuadamente sus sistemas. Por otra parte, la naturaleza de las directrices reconoce de inmediato que los sistemas difieren significativamente entre sí y que la imposición de normas no siempre es factible, aceptable o rentable. Un ejemplo de ello sería el uso de una directriz organizativa para ayudar a desarrollar procedimientos estándar específicos para un sistema. Las directrices se utilizan a menudo para ayudar a garantizar que no se descuiden determinadas medidas de seguridad, a pesar de que pueden aplicarse de diversas maneras, algunas de las cuales son más adecuadas que otras.

- Los procedimientos, son las instrucciones para poner en práctica las políticas, normas y recomendaciones de seguridad pertinentes. Para ejecutar una determinada actividad, los usuarios, el personal de operaciones del sistema u otras personas deben seguir una serie de etapas específicas. Por ejemplo, para preparar nuevas cuentas de usuario y asignar los permisos pertinentes, se deben seguir estos procedimientos.

2.2.7 Análisis de riesgos

De acuerdo a Chicano (2014), en las organizaciones, los sistemas de información cuentan con múltiples recursos susceptibles ante ataques de seguridad. Es por este motivo que se toma como parte fundamental de las medidas de seguridad de activos de información, poner en práctica de estrategias y herramientas que nos brinden la información pertinente para poder descubrir posibles ataques y las incidencias que podrían perjudicar a la organización, las herramientas de gestión de riesgos han sido diseñadas para cumplir con las siguientes funciones: facilitan la identificación de los recursos críticos dentro de la organización, los riesgos a los que están expuestos y el impacto que podrían sufrir si se materializa alguna amenaza.

Según Romero et al. (2018), la dirección de una empresa y los responsables de cada departamento no ejercen una influencia significativa en la protección de la infraestructura de gestión de la información. Este también es el caso cuando se considera la perspectiva corporativa. Es de suma importancia adoptar un punto de vista adecuado; el análisis de riesgos debe concentrarse en gran medida en las amenazas que tienen un impacto en los objetivos de la empresa, en lugar de concentrarse únicamente en los dispositivos. Tanto si los objetivos de la organización están relacionados con las ventas, la fabricación o los servicios públicos, entre otras cosas, es esencial determinar los elementos que podrían impedir su progreso hacia el logro de esos objetivos. Por esta razón, cuando se trata de establecer medidas de seguridad para los equipos, los jefes de los distintos departamentos deben trabajar juntos para identificar los riesgos que podrían influir en sus actividades y diseñar planes eficientes de resiliencia tecnológica.

2.2.8 Incidentes de seguridad

En su análisis de ciberataques e incidentes alrededor del mundo IBM (2014) nos da un mayor alcance acerca de las incidencias de seguridad de la información. Al examinar los datos presentados, se observa que la gran cantidad de eventos de seguridad se reduce a un número mucho más manejable de incidentes. Sin embargo, de estos incidentes, ¿cuántos son realmente "significativos" y tienen el potencial de causar un impacto considerable en el negocio? Según el Equipo de Respuesta a Incidentes de Seguridad Informática de IBM, solo el tres por ciento de todos los incidentes analizados alcanza un nivel de gravedad suficiente para ser considerados "notables", siendo el impacto más común la divulgación o el robo de datos, esto calza perfectamente con la posibilidad de que los ataques más comunes sean los relacionados a ingeniería social.

Es interesante, aunque preocupante, que más del 95 por ciento de los incidentes investigados identifican el "error humano" como un factor contribuyente. Los errores más comunes incluyen configuraciones incorrectas del sistema, mala gestión de parches, uso de id de usuario y contraseñas predeterminados o fáciles de adivinar, pérdida de portátiles o dispositivos móviles, y divulgación de información sensible al utilizar una cuenta de correo electrónico incorrecta. ¿El error humano más frecuente? Dar clic en un archivo adjunto infectado o en un enlace inseguro.

2.2.9 Gestión de vulnerabilidades

Según Harris y Maymi (2020), la gestión de vulnerabilidades es un proceso continuo de identificación, evaluación, priorización y remediación de vulnerabilidades en los sistemas de información de una empresa. Este proceso implica el escaneo regular de sistemas para detectar posibles debilidades de seguridad, evaluar los riesgos asociados a estas vulnerabilidades y aplicar medidas apropiadas para mitigar o eliminar los riesgos. Una gestión eficaz de vulnerabilidades ayuda a las organizaciones a proteger sus activos al asegurar que las vulnerabilidades sean abordadas antes de que puedan ser vulneradas por atacantes. También incluye mantener un inventario actualizado de vulnerabilidades, aplicar parches y actualizaciones, y verificar la efectividad de los esfuerzos de remediación.

Acerca de la detección de vulnerabilidades, Raza et al. (2024), nos dice que las aplicaciones, las redes y los sistemas pueden tener fallos de seguridad que pueden detectarse mediante herramientas de análisis de vulnerabilidades. Para identificar posibles vulnerabilidades, se revisan y analizan la configuración del sistema, las versiones del software y las vulnerabilidades detectadas. La gestión de parches es el proceso de aplicar parches de seguridad y actualizaciones en el momento adecuado para corregir las vulnerabilidades detectadas y reducir la probabilidad de que sean explotadas.

2.2.10 Las amenazas, vulnerabilidades y riesgos

En ciberseguridad existen conceptos fundamentales, entre los cuales se encuentran las amenazas y vulnerabilidades; una vulnerabilidad se define como una debilidad en un sistema, la cual puede presentarse en sus medidas de seguridad, en controles internos o en su implementación, que puede ser aprovechada por diferentes amenazas como los ciberdelincuentes.

De acuerdo a lo dicho por Pavon et al. (2024) , define los conceptos de amenaza, vulnerabilidad y riesgo como:

Una amenaza se puede entender como una situación indeseada que debe ser reconocida con anticipación para poder tomar decisiones en caso de que ocurra. En el ámbito de la ciberseguridad, una amenaza se refiere a un posible ataque malicioso que busca obtener acceso no permitido a un sistema de información, comprometiendo su

seguridad y realizando acciones perjudiciales para la organización. Por ejemplo, un ciberdelincuente que intenta infiltrarse en la red wifi de una empresa representa una amenaza.

A menudo, estas amenazas surgen porque el sistema presenta vulnerabilidades. Pero, ¿qué es una vulnerabilidad?

La vulnerabilidad se define como una debilidad o defecto en el diseño, implementación o proceso de un sistema, ya sea por fallos en su origen o por una configuración incorrecta, que puede ser aprovechada por factores externos. En ciberseguridad, este término suele referirse a una brecha de seguridad en los componentes del sistema de información (software, hardware o red) que, al ser explotada, afecta negativamente los principios fundamentales de la ciberseguridad. Las vulnerabilidades pueden manifestarse como errores de software, configuraciones inadecuadas, controles de seguridad deficientes e incluso fallos humanos. Siguiendo el ejemplo anterior, una vulnerabilidad sería tener una contraseña débil en la red wifi, que sea fácil de adivinar.

Con estos conceptos de amenaza y vulnerabilidad aclarados, es importante definir el riesgo, ya que los tres están interrelacionados en el campo de la ciberseguridad. Cuando una amenaza logra explotar una vulnerabilidad, existe la probabilidad de que los activos de una organización puedan resultar dañados o perderse. Esto es lo que se entiende por el término «riesgo». En el ejemplo, esto implicaría la posibilidad de que el ciberdelincuente descifrara la contraseña de la red wifi, accediendo así a la red de la organización y, potencialmente, a información sensible.

Así también según, Romero et al. (2018), el riesgo puede definirse como la probabilidad de que ocurra algo desfavorable, lo que resultará en la destrucción de recursos físicos o intangibles y, como consecuencia, obstaculizará el crecimiento de la actividad profesional.

Las vulnerabilidades de seguridad son fallos en los sistemas de seguridad o en los sistemas que el usuario utiliza para llevar a cabo actividades que permitirían que una amenaza tuviera éxito en causar una incidencia. Las amenazas son eventos que tienen el potencial de causar daño a procesos o recursos, mientras que las vulnerabilidades son fallos en los sistemas de seguridad. La responsabilidad principal de un gerente de seguridad es evaluar los riesgos determinando las vulnerabilidades y

amenazas, y luego, sobre la base de este conocimiento, evaluar los riesgos asociados con las actividades y los recursos.

De igual manera Nieles et al. (2017), indica que estas vulnerabilidades exponen los sistemas a diversas actividades que pueden resultar en pérdidas financieras, reputacionales, operativas, a veces irreversibles, para individuos, grupos u organizaciones. Estas pérdidas pueden variar desde un archivo dañado en una computadora, dispositivo móvil o incluso en servidores, hasta la violación de bases de datos completas en un centro de operaciones. Con las herramientas y el conocimiento adecuados, un atacante puede aprovechar las vulnerabilidades del sistema para acceder a la información que contiene. El daño a los sistemas comprometidos puede diferir dependiendo de la fuente de la amenaza.

Finalmente, Whitman y Mattord (2018), nos dice que es necesario conocerse a uno mismo para poder proteger la información de su empresa. Esto significa que se debe estar familiarizado con la información que debe protegerse, así como con los sistemas que la almacenan, transportan y procesan. Además, debe ser consciente de los riesgos a los que se enfrenta. Es necesario que la dirección sea consciente de los diferentes peligros que pueden afectar al personal, las aplicaciones, los datos y los sistemas de información de una organización para poder tomar decisiones inteligentes en materia de seguridad de la información. En el contexto de la seguridad de la información, una amenaza es cualquier entidad, ya sea una persona, un objeto u otra entidad, que supone un riesgo persistente para un activo.

Los investigadores han realizado entrevistas a expertos en seguridad de la información en activo y han revisado la bibliografía sobre seguridad de la información con el fin de analizar la gran variedad de peligros que prevalecen en el mundo conectado. A pesar de que las clasificaciones pueden diferir, las amenazas han sido objeto de numerosos estudios y, como resultado, se conocen muy bien. Existe un consenso generalizado en que el peligro que representan las fuentes externas se amplifica cuando una organización tiene conexión a Internet. Se estima que alrededor del 26 % de los 6800 millones de habitantes del mundo, es decir, 1700 millones de personas, tienen acceso a Internet de una forma u otra. El número de personas que utilizan Internet sigue aumentando.

2.2.11 El Ciberataque

De acuerdo a Whitman y Mattord (2018), un ataque se define como un acto que explota una vulnerabilidad para comprometer un sistema. Este es realizado por un agente amenazante que causa daño o roba información y activos físicos de una organización. Una vulnerabilidad es una debilidad reconocida en un sistema gestionado, donde los controles son inexistentes o han dejado de funcionar eficazmente. A diferencia de las amenazas, que están siempre presentes, los ataques solo ocurren cuando un acto específico puede resultar en una pérdida. Por ejemplo, la amenaza de daños por tormentas eléctricas está presente durante todo el verano en muchos lugares, pero un ataque y el riesgo de pérdida asociado solo se manifiestan mientras la tormenta está activa.

Entonces, de acuerdo con Perez (2019) se puede afirmar que un ciberataque es la manifestación de una o varias ciber amenazas. Así, el ciber riesgo se refiere a la posibilidad de que ocurra un ciberataque y a la gravedad del daño que este pueda causar; en otras palabras, es la posible pérdida resultante de la materialización de uno o varios ciberataques. Los ciberataques pueden provocar diversos tipos de daños, incluyendo la posibilidad de un efecto dominó que afecte a diversas entidades o partes de la cadena productiva.

De manera similar Vega (2021), nos dice que somos susceptibles a agresiones que provienen de una amplia gama de direcciones y perspectivas. Cuando examinamos qué define precisamente un ataque, podemos categorizarlo según el tipo de ataque que representa, el riesgo que plantea y los controles que podemos emplear para reducir el riesgo.

Cuando observamos los tipos de ataques a los que podríamos enfrentarnos, generalmente podemos clasificarlos en una de estas cuatro categorías: interceptación, modificación, interrupción, y fabricación.

2.2.12 La ingeniería social

De acuerdo a Romero et al. (2018), la aplicación de algunos conocimientos psicológicos y sociológicos fundamentales es la base sobre la que se construyen los conceptos de ingeniería social. Esto significa que no se trata de un conocimiento extremadamente complejo, ya que el atacante generalmente no tiene muchos detalles sobre su víctima y debe basarse en generalidades que son estadísticamente válidas para lograr resultados positivos en la misma proporción. Los conceptos de psicología individual que son

fundamentales y pueden verificarse mediante análisis estadísticos constituyen la base de la ingeniería social. Entre dichos conceptos, hay cuatro que hacen a las personas más susceptibles a este tipo de tácticas:

• No decir “NO”.

• Confianza excesiva.

• Halagos hacia la persona, no naturales o excesivos.

• Empatizar.

Así también IBM (2014) afirma que las técnicas de ingeniería social permiten a los atacantes dirigirse a empresas específicas para acceder a datos valiosos. Estos delincuentes roban directorios telefónicos internos y luego contactan a empleados de interés. Su objetivo es persuadir a las víctimas para que instalen voluntariamente software de administración remota que los hackers usarán para acceder a su red. Suplantándose como personal de seguridad interna o de TI, les indican que descarguen un software conocido para resolver un "problema crítico del sistema" o que se unan a una videoconferencia y cedan el control a los atacantes.

Una vez que consiguen el control del sistema, instalan malware para establecer una conexión persistente, elevan privilegios y penetran en la red. Dado que muchas empresas no tienen un sistema para verificar llamadas, esta estrategia se ha vuelto muy efectiva para infiltrarse en los sistemas internos, especialmente cuando los atacantes comprenden los procesos de las víctimas y los utilizan para convencerlas de actuar rápidamente.

Finalmente podemos decir que la ingeniería social los ataques de ingeniería social tienen como objetivo principal a las personas de una organización que cuentan con los privilegios necesarios a la data requerida por los ciber delincuentes. Es por ello que una vez logrado su objetivo es muy difícil interceptar el ataque a tiempo, pudiendo vulnerar cualquier tipo de activo, incluyendo datos financieros fundamentales para la continuidad del negocio. Es por ello que ni siquiera las organizaciones con un alto grado de prevención y buenas prácticas son inmunes a este tipo de ataque. Es por ello que la capacitación a los colaboradores acerca de este tipo de amenazas es fundamental.

2.2.12.1 Defensa contra la ingeniería social

Pueden prevenirse este tipo de ataques de ingeniería social mediante la formación y educación de las personas en sus hogares, universidades y lugares de trabajo, con el

fin de minimizar los riesgos que pueden surgir en los sistemas informáticos. Esta técnica puede utilizarse para protegerse contra los ataques de ingeniería social. En consecuencia, permite tomar medidas preventivas con respecto a la información y elimina la posibilidad de perder datos, ya sea en su totalidad o en parte. De acuerdo con lo indicado por Sandoval (2011), existen mecanismos que nos permite defendernos de estos ataques, como son los siguientes:

- Bajo ninguna circunstancia debe proporcionar información privada a personas desconocidas o en áreas públicas (como redes sociales, anuncios, sitios web, etc.).
- Si tiene motivos para creer que alguien está intentando cometer un fraude, debe exigirle que revele su identidad y hacer todo lo posible por revertir la situación obteniendo toda la información posible del sospechoso sin llamar su atención sobre el problema.
- Es importante garantizar que todos los trabajadores de la empresa conozcan las medidas de seguridad que se han implementado dentro de la corporación para reducir la probabilidad de comportamientos peligrosos.
- Es importante realizar inspecciones de seguridad física con el fin de reducir el riesgo inherente para las personas.
- Para identificar fallos de seguridad de este tipo, es necesario llevar a cabo auditorías periódicas y pruebas de penetración que hagan uso de la ingeniería social.
- Implementar iniciativas que aumenten el conocimiento sobre la seguridad de la información.

2.2.13 Ataques de ingeniería social

2.2.13.1 Phishing

Pande (2017) , define al phishing como un proceso que implica la obtención de información personal y confidencial de una persona a través del correo electrónico, haciéndose pasar por una entidad confiable en la comunicación digital. El objetivo del phishing es el robo de identidad, y datos personales como el nombre de usuario, la contraseña y el número de tarjeta de crédito pueden ser utilizados para sustraer dinero de la cuenta del usuario. Cuando se utiliza un teléfono para llevar a cabo el robo de identidad, se denomina vishing (phishing por voz). Otra variante es el smishing, que utiliza mensajes de texto para atraer a los usuarios.

De manera similar Romero et al. (2018), dice que uno de los métodos más populares de utilizar la ingeniería social para atacar infraestructuras informáticas es recopilar información personal sobre los trabajadores de una empresa. Esta es una de las formas más comunes en que se utiliza la ingeniería social. La disponibilidad de este tipo de información puede facilitar el acceso a contraseñas y a otros sitios prohibidos. Además, la ingeniería social se utiliza en la ejecución de campañas fraudulentas por correo electrónico, también conocidas como phishing, que tienen como objetivo transferir malware, por ejemplo.

El ransomware es un tipo de software malicioso que cifra datos y luego exige un rescate a cambio de descifrarlos. Uno de los métodos más comunes para distribuir ransomware es la ingeniería social. Es posible que el phishing tenga éxito porque los correos electrónicos que se envían parecen auténticos. Estos correos electrónicos imitan la identidad corporativa de empresas conocidas, siendo especialmente frecuentes las suplantaciones de proveedores de servicios telefónicos y empresas de servicios públicos. Una variante, conocida como espía Phishing, no se distribuye masivamente; en su lugar, utiliza correos electrónicos elaborados específicamente para engañar a una persona en particular.

Frecuentemente, se suplanta a un miembro de la empresa con un cargo alto, a un proveedor o a un cliente, creando así una narrativa coherente que logra engañar a la víctima mediante técnicas de ingeniería social.

2.2.13.2 Vishing o phishing de voz

El vishing es un tipo de ataque de ingeniería social que se lleva a cabo a través de llamadas telefónicas. En este tipo de estafa, el ciberdelincuente se hace pasar por una persona, empresa u organización de confianza con el fin de engañar a la víctima y obtener información confidencial, como datos personales, información financiera u otro tipo de información personal. Este método se caracteriza por el uso de la voz mediante llamada o mensajes de voz para controlar a la persona y persuadirla de que facilite datos como contraseñas, números de tarjetas, PIN o cualquier otra información que pueda utilizarse para cometer fraude o robo de identidad. El término “vishing” es una combinación de los términos “voz” y “phishing”, y se caracteriza por la capacidad de manipular a la persona. Con el fin de robar datos, instalar malware o realizar pagos fraudulentos, los atacantes suelen crear una sensación de urgencia o confianza para

bajar la guardia de la víctima. Para ello, pueden hacerse pasar por bancos, técnicos informáticos, empresas de mensajería o incluso familiares.

2.2.13.3 Smishing o phishing por SMS

El smishing es un tipo de ataque de ingeniería social que consiste en el uso de mensajes de texto (SMS) para engañar a las personas y obtener información personal. Esta información puede incluir credenciales de inicio de sesión en aplicaciones, datos personales o datos bancarios. Mediante técnicas de ingeniería social, que intentan explotar la sencilles de este tipo de comunicación y suelen aprovechar el miedo infundido en las personas ante situaciones de emergencia como por ejemplo la filtración de datos o incluso desastres naturales, el ciberdelincuente se hace pasar por una entidad legítima como un banco, una red social o una institución pública, con el fin de inducir a la víctima a realizar acciones como hacer clic en enlaces maliciosos, descargar aplicaciones fraudulentas o compartir información privada. El término “smishing” proviene de la combinación de “SMS” y “phishing”, y se basa en técnicas de ingeniería social. Los mensajes de este tipo suelen crear una sensación de urgencia o se aprovechan de la confianza del usuario para instarle a resolver un problema ficticio, reclamar una recompensa o verificar información confidencial. Al final, el objetivo es robar información crítica o generar reclamaciones financieras falsas.

2.2.13.4 Suplantación de identidad

De acuerdo con ESET (2021), suplantar a un tercero con el fin de obtener información o acceso a una persona, empresa o sistema informático es un ejemplo de robo de identidad, que se define como la práctica de suplantar a un tercero. Los piratas informáticos utilizan diferentes tácticas, como realizar llamadas telefónicas, enviar correos electrónicos o utilizar aplicaciones de mensajería como Whatsapp, para lograr estos objetivos. En muchos casos, los autores del ataque eligen nombres de la alta dirección de la empresa y redactan un correo electrónico que da la impresión de haber sido enviado por un directivo.

2.2.13.5 Scareware

Se le denomina scareware a un programa malicioso que tiene como objetivo asustar al usuario enviándole alertas engañosas o exageradas sobre falsos problemas de

seguridad en su dispositivo. Estos problemas pueden incluir infecciones por virus, fallos graves o amenazas inminentes. El scareware está diseñado para engañar a los usuarios y hacerles realizar acciones impulsivas, como instalar un software no deseado, comprar una solución de seguridad falsa o revelar información personal y financiera. El objetivo principal del scareware es engañar a los usuarios para que realicen este tipo de acciones.

2.2.13.6 Estafas de soporte técnico

De acuerdo con ESET (2021), las estadas de soporte técnico están estrechamente relacionadas con los fraudes relacionados a asistencia técnica. Por otro lado, a diferencia del scareware, estos programas hacen creer que proceden de una empresa de renombre, como Microsoft. No comienzan a buscar malware en su equipo de forma inmediata. En su lugar, le instan a abrir determinados archivos y, a continuación, le explican que dichos archivos demuestran que existe un problema, que en realidad no existe. Las estafas relacionadas con la asistencia técnica son habituales, según la Comisión Federal de Comercio (FTC) de los Estados Unidos de América. La (FTC) recibió más de 100 000 denuncias de estafas de este tipo en el año 2019.

2.2.14 Compromiso de datos

De acuerdo con Andress (2011),En el proceso de garantizar la seguridad de nuestras operaciones, la primera etapa, que también se considera la fase más crucial, consiste en determinar cuáles de nuestros activos de información son los más importantes. A pesar de que podríamos dedicar una cantidad significativa de tiempo a identificar cada pequeño dato que pudiera tener la más mínima importancia, esta etapa concreta del proceso de seguridad de las operaciones no tiene por objeto hacer eso. Dentro de cada organización, ya sea una empresa, una persona, una operación militar, un procedimiento o un proyecto, siempre hay al menos unos pocos datos esenciales que dependen de todo lo demás. Por ejemplo, para una empresa que fabrica refrescos, puede ser nuestra fórmula secreta; para una empresa que proporciona servicios de aplicaciones, puede ser nuestro código fuente; para una operación militar, puede ser nuestro calendario de asalto; y así sucesivamente. Estamos obligados a identificar estos activos porque son los que necesitan mayor seguridad y los que nos causarán mayor daño si se revelan.

Por ejemplo, si somos una empresa de software que ha determinado que el código fuente de uno de nuestros principales productos se considera información importante, podemos llegar a la conclusión de que los peligros más significativos de su divulgación serían la exposición a nuestros competidores y a aquellos que intentarían perjudicarnos. Si los atacantes tuvieran acceso al código fuente, podrían descubrir el método que utilizamos para generar las claves de licencia de nuestros productos con el fin de evitar la piratería. A continuación, podrían utilizar esta información para crear una herramienta capaz de generar claves auténticas, lo que provocaría una pérdida de ingresos debido a ello. En el caso de nuestros competidores, podrían copiar partes importantes de nuestro programa y venderlo por si mismos, o podrían utilizar el acceso a nuestro código fuente para copiar funciones y utilizarlas en sus propias aplicaciones. Ambas opciones son posibles.

De acuerdo con Information Comissioner's Officers UK (2023),en su forma más básica, la protección de datos de acuerdo con el concepto de integridad implica la implementación de medidas de seguridad por parte de las organizaciones con el fin de evitar que los datos se vean comprometidos o corruptos, preservar su integridad y confidencialidad, y garantizar que sean accesibles para los usuarios autorizados siempre que sea necesario. Además, las empresas deben demostrar que son responsables y capaces de cumplir con estos procedimientos, que incluyen la gestión de riesgos y la respuesta a incidentes.

2.2.15 Medidas de seguridad

De acuerdo con INCIBE (2015), es responsabilidad de todos y cada uno de los empleados de una empresa garantizar que se mantenga un nivel satisfactorio de seguridad. Por este motivo, es fundamental establecer una cultura de seguridad y formar al personal. Esto es algo que se aprecia fácilmente en el día a día y, para ilustrarlo, analizaremos dos ejemplos: la empresa A, que ha implementado programas de concienciación sobre seguridad, y la empresa B, que no imparte formación en materia de concienciación a sus usuarios.

Es necesario seguir un procedimiento seguro, como el uso de trituradoras de papel, para desechar documentos privados o material que contenga datos personales identificables. Si no se sigue un procedimiento de destrucción seguro, se puede dañar gravemente la reputación de la empresa y provocar pérdidas económicas por no seguir los procesos adecuados para desechar información confidencial. Tener hábitos de trabajo seguros, como bloquear la sesión al abandonar el ordenador, es consecuencia

de comprender bien la situación y reduce el riesgo de acceso no autorizado a los sistemas de información.

Así también INCIBE (2015), nos dice que es posible evitar el acceso no deseado a la información mediante la implementación adecuada de una política de escritorio limpio. La formación de los empleados debe incluir temas relacionados con el uso del correo electrónico. En este sentido, es fundamental enseñarles a reconocer un correo electrónico falso y qué medidas deben tomar en tal caso para evitar intentos de phishing. Las redes sociales son cada vez más populares entre los trabajadores, especialmente por motivos personales y profesionales. Sin embargo, para proteger la imagen online de la empresa, es necesario crear y aplicar normas de uso adecuado.

2.2.16 Ransomware

Según Serra et al. (2022) El ransomware es un tipo de software malicioso que cifra datos o desactiva y bloquea partes del sistema para extorsionar a los usuarios de un ordenador infectado. El ransomware exige un pago después de desactivar y bloquear partes del sistema. El atacante ofrece una opción para erradicar el daño producido por el virus en caso de que la víctima decida pagar por ello. Este pago puede hacerse a menudo mediante transferencias bancarias en bitcoins o por mensajes de texto con cargos adicionales. Para ser más específicos, un criptovirus es un tipo de software malicioso que cifra datos mediante el uso de criptografía. La mayoría de las veces, utilizan algoritmos criptográficos asimétricos o híbridos, que impiden a la víctima acceder al contenido de los archivos cifrados, ya que no tienen la clave privada.

Así también Paniagua (2022) , nos dice que, en la última década, ha habido una evolución continua en el ámbito del ransomware, tanto en términos tecnológicos como sociológicos. Los grupos delictivos se han multiplicado y se han profesionalizado de manera significativa. Para alcanzar este nivel de profesionalización, es necesario utilizar estrategias de gestión operativa, herramientas y soluciones especializadas que a menudo se utilizan en el ámbito de la programación o la seguridad. Algunos atacantes han sido capaces de fijar objetivos más ambiciosos, como empresas o instituciones, y someterlos a un seguimiento exhaustivo para conocer mejor a la víctima. Esto incluye determinar qué datos podrían verse comprometidos, la importancia de esta información, cuánto estarían dispuestos a pagar y otra información. Además, estos ataques son cada vez más sofisticados y efectivos, ya que son capaces de cifrar una gran cantidad de archivos ubicados en una variedad de lugares dentro de una red empresarial o de robar información importante. Esta última estrategia añade una faceta más al proceso de

extorsión, ya que amenazan con poner esta información a disposición del público en general. Además, existe la posibilidad de que se lance un ataque distribuido de denegación de servicio (también conocido como ataque DDoS) con la intención de derribar un servidor en particular.

2.3 Definición de términos

2.3.1 Ciberseguridad

De acuerdo a lo indicado por Pérez (2019), la Organización Internacional de Normalización (ISO) define la ciberseguridad como la protección de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Esta definición se puede encontrar en la norma ISO/IEC 270323. Esta última se entiende como el entorno complejo que surge de la interacción entre personas, software y servicios en Internet, utilizando dispositivos tecnológicos y redes conectadas, sin tener una forma física específica.

De igual manera, la Iniciativa Nacional para la Profesionalización y Estudios en Ciberseguridad (NICCS, en inglés), del Departamento de Seguridad Nacional de EE. UU., define la ciberseguridad como un conjunto de actividades, procesos, habilidades o estados que aseguran que los sistemas de información y comunicación, así como los datos que contienen, estén protegidos y defendidos contra daños, accesos o modificaciones no autorizadas, así como su explotación.

2.3.2 Educación en Seguridad

Según Whitman y Mattord (2018), todos en una organización deben recibir capacitación y concienciación sobre seguridad de la información, pero no todos los miembros de la organización necesitan un título formal o un certificado en seguridad de la información. Cuando la dirección considera que la educación formal es apropiada, un empleado puede investigar los cursos disponibles en instituciones locales de educación superior o educación continua.

Varias universidades ofrecen cursos formales en seguridad de la información. Para aquellos interesados en investigar programas formales de seguridad de la información, hay recursos disponibles, como los Centros de Excelencia en Educación de Aseguramiento de la Información identificados por la NSA (National Security Agency).

2.3.3 Ataques de seguridad

De acuerdo con Whitman y Mattord (2018), un ataque es definido como un acto que explota una vulnerabilidad para poner en riesgo un sistema controlado. Este acto es realizado por un agente amenazante que puede dañar o robar información o activos físicos de una organización. Una vulnerabilidad es una debilidad detectada en un sistema controlado, donde los controles son inexistentes o han dejado de funcionar adecuadamente. A diferencia de las amenazas, que son constantes, los ataques solo ocurren cuando un acto específico puede resultar en una pérdida. Por ejemplo, aunque la amenaza de daños por una tormenta eléctrica está presente durante todo el verano en muchas regiones, un ataque y el riesgo de pérdida relacionados solo se producen mientras la tormenta está activa.

2.3.4 Hacker malicioso

Según Nieles et al. (2017), cuando se hace referencia a una persona u organización que hace uso de su experiencia en sistemas informáticos, redes y programación para obtener acceso no autorizado a sistemas informáticos, causar daños a sistemas informáticos o robar información, se utiliza la frase «pirata informático malintencionado». Si una empresa es capaz de comprender las razones que hay detrás de un pirata informático malintencionado, estará mejor preparada para aplicar las medidas de seguridad adecuadas, lo que reducirá el riesgo de que se produzca una violación del sistema. El término «pirata informático malintencionado» hace referencia a una amplia categoría de amenazas hostiles que pueden subdividirse en categorías más precisas en función de los actos o intenciones particulares del pirata informático malintencionado. Algunas de las subcategorías que se han adoptado de la Guía para la seguridad de los sistemas de control industrial (ICS) incluida en la Publicación Especial 800-82 del NIST son las siguientes:

2.3.4.1 Malware

Según Stallings y Brown (2015), el software malicioso, también conocido como malware, es sin duda una de las categorías más importantes de amenazas para los sistemas informáticos. El malware puede entenderse como un tipo de software que se introduce en un sistema de manera oculta o no autorizada, con el propósito de afectar la confidencialidad, integridad o disponibilidad de la información, las aplicaciones o el propio sistema operativo de un usuario. Su acción también puede orientarse a alterar el

funcionamiento normal del sistema o interrumpir las actividades de la víctima. El malware es un tipo de software desarrollado con la intención de causar daño a un sistema informático. Por ello, nos preocupa el peligro que representa el malware para los programas de aplicación, las aplicaciones de utilidad como editores y compiladores, y los programas que se ejecutan a nivel del núcleo. Además, nos preocupa su uso en sitios web y servidores que han sido pirateados o son maliciosos, así como en correos electrónicos no deseados u otras comunicaciones que han sido diseñadas específicamente para engañar a los usuarios y que divulguen información personal crítica sobre ellos mismos.

2.3.4.2 Phishers

De acuerdo con Nieles et al. (2017), los phishers son personas o grupos reducidos que llevan a cabo ataques de phishing para robar identidades o información con el fin de obtener beneficios económicos. También pueden emplear spam y software espía o malware para alcanzar sus metas.

2.3.4.3 Spammers

De acuerdo con Nieles et al. (2017), para vender cosas, llevar a cabo estafas de phishing, transmitir spyware o malware, o atacar a empresas (como en los ataques de denegación de servicio), los spammers son personas o grupos que envían correos electrónicos molestos que incluyen material engañoso o incorrecto.

2.3.4.4 Autore de spyware/código malicioso

De acuerdo con Nieles et al. (2017), personas u organizaciones que realizan ataques maliciosos contra usuarios mediante la creación y distribución de spyware y malware. Entre los virus destructivos y gusanos que han causado daños en archivos y discos duros se encuentran el Virus Macro Melissa, el gusano Explore.Zip, el Virus CIH (Chernobyl), Nimda, Code Red, Slammer y Blaster.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 Diseño de la investigación

El enfoque es de tipo cuantitativo, ya que se realizó la recopilación de datos numéricos mediante el instrumento de pruebas estandarizadas de conocimiento y su análisis respectivo, con el objetivo de establecer la relación entre las variables al utilizar métodos estadísticos. Esto nos permitió identificar como influye el programa de seguridad informática y obtener resultados objetivos. De acuerdo con Hernández et.al (2014), cuando se lleva a cabo un estudio cuantitativo, la muestra es un subconjunto de la población de interés que servirá como fuente de los datos que sera recopilada. Es necesario definirla y delimitarla con precisión de antemano, y también es importante que sea representativa de la población.

El tipo de investigación del presente trabajo es de tipo aplicada, debido a que se buscó influir en los conocimientos y preparación de los empleados de una entidad bancaria para enfrentar ataques de ingeniería social en su entorno de trabajo. De acuerdo con De Vecchi y Grossi (2016), a diferencia de la investigación básica, que busca únicamente nuevos conocimientos, la investigación aplicada se enfoca en descubrir respuestas eficaces a circunstancias particulares, como la mejora de productos o la invención de nuevas tecnologías. La investigación aplicada se distingue de la investigación básica por su énfasis en el uso de los conocimientos existentes para abordar problemas reales.

Se considera el tipo de diseño de la investigación como cuasi experimental en donde se manipula la variable independiente programa de seguridad informática realizando un pretest y un post test para validar su efecto sobre la variable independiente ciberataques de ingeniería social. De acuerdo con Shadish et al. (2002), los estudios que examinan el efecto de una intervención sin asignar aleatoriamente a los participantes son ejemplos de diseños que se consideran cuasi experimentales. Se utilizan en casos en los que no es posible ejercer un control total sobre un experimento y cuando se intenta establecer relaciones de causa y efecto ajustándose a las condiciones que se dan en la vida real.

El nivel de investigación es explicativo, debido a que se buscó medir como influye un programa de seguridad informática sobre la preparación de los empleados ante ciberataques de ingeniería social. De acuerdo con Hernández (2014), el objetivo de los estudios explicativos es proporcionar una explicación de las razones que

subyacen a la ocurrencia de acontecimientos y fenómenos físicos o sociales. Los estudios explicativos van más allá de la mera descripción de ideas o fenómenos o de la creación de correlaciones entre conceptos. Cuando se trata de describir por qué ocurre un fenómeno y en qué circunstancias se manifiesta, o por qué dos o más variables están conectadas entre sí, se centran principalmente en explicar por qué se dan determinadas condiciones.

Por último, se consideró la investigación como longitudinal, ya que lo que se buscó recolectar datos en periodos de tiempo distintos con el fin de evaluar los cambios, los factores que los provocan y sus implicaciones. De acuerdo con Arias (2006), en la investigación longitudinal se estudian los cambios y la evolución de una variable o un fenómeno a lo largo del tiempo. Este tipo de estudio implica recopilar datos en varios momentos para examinar cómo se desarrolla la variable o el fenómeno.

3.2 Acciones y actividades

Para el desarrollo del programa de capacitación en seguridad informática se utilizó la metodología ADDIE, ya que es reconocida por ser flexible, sistemática, así como reconocida en educación, tecnología y gestión del aprendizaje. La elaboración y ejecución del programa fueron desarrolladas en 5 etapas o fases, las cuales se describen a continuación:

Etapa 1: Compromiso y participación del área de accesos de la entidad financiera en el programa

La primera semana del mes de noviembre del 2024 se realizó la primera coordinación con el supervisor del área de helpdesk de la entidad financiera, mediante un test relacionado a conocimientos en ciberseguridad y ataques de ingeniería social, donde fue posible identificar las los puntos a reforzar, por lo cual, se establece un primer hito para analizar la mejor estrategia para lograr una mejora en la sensibilización, cultura y prevención de ataques de ingeniería social en seguridad de la información.

Etapa 2: Diseño del programa

En la segunda semana del mes de noviembre de 2024 se realizaron las coordinaciones con el área de helpdesk, revisando los temas del programa, de acuerdo a las falencias

encontradas en la etapa 1, y de esta manera reforzar los puntos débiles en el equipo de accesos.

En esta fase se tuvo en cuenta las falencias y amenazas más concurrentes presentadas en el día a día de los colaboradores, el programa se diseñó, bajo la revisión de la jefatura del área y para las pruebas simuladas de phishing, de tal manera que las pruebas tengan las características adecuadas a identificar, lo cual conllevó a diferenciar entre un correo legítimo y uno de phishing

Etapa 3: Construcción de material del programa

La elaboración del programa de seguridad informática (Anexo 2) fue construida en asesoría con un experto en seguridad informática perteneciente al equipo de seguridad de la entidad financiera.

La realización de los 2 cuestionarios se llevó a cabo en etapas distintas del programa la primera se hizo en base a otros artículos de seguridad de la información y el segundo cuestionario se realizó de la misma manera, pero incluyendo los conocimientos que necesitaban un mayor énfasis y se reforzaron mediante el programa de seguridad informática para el progreso de los colaboradores y finalmente, el programa se realizó tomando como base instrumentos obtenidos de trabajos de tesis de pregrado relacionados a seguridad de la información, con la finalidad de brindar los conocimientos necesarios a alcanzar, para lograr la relación entre la variable dependiente e independiente de la presente tesis. Así mismo, se tomó la decisión de no solicitar los datos personales del personal con el que se trabajó, con la finalidad de obtener respuestas sinceras.

En relación a la construcción de las pruebas phishing, se realizaron teniendo como base el día a día y las amenazas a las cuales se ven expuestos los trabajadores de área de helpdesk, los cuales representan un rol crítico en la entidad financiera ya que cuentan con la mayor cantidad de accesos a recursos y aplicaciones no solo en ambientes de desarrollo y certificación, sino también en ambientes productivos.

Etapa 4: Ejecución del programa y resultados obtenidos

En esta etapa se llevaron a cabo actividades específicas que se relacionan con la ejecución del programa, el cual comenzó con la notificación a los involucrados.

El programa contempló 3 módulos relacionados a conceptos y casos que puedan presentarse en el día a día de un colaborador. Lo cuales al finalizar cada módulo incluyen una serie de preguntas relacionadas a cada módulo, las cuales nos ayudan a retroalimentar los conocimientos brindados.

El programa estuvo compuesto por 3 módulos con información y contenido relacionado a seguridad informática, al finalizar cada módulo se incluía una ronda de preguntas a modo de examen que debían ser contestados, para seguir con el siguiente módulo. Los temas de programa fueron los siguientes:

- Peligros y amenazas de los ataques de ingeniería social en seguridad informática.
- Herramientas de IA generativa y ataques de phishing.
- Gestión de información confidencial.

Los colaboradores tuvieron la libertad de elegir el momento en el cual querían desarrollar el programa, el cual contaba con un diseño interactivo, pero sencillo. Se dio dos semanas como plazo para culminar el curso y resolver el test final. Debido a que la empresa cuenta con información crítica no fue posible plantear incidentes reales de ciberseguridad que acontecieron en la organización.

Etapa 5: Evaluación del Programa

Durante el desarrollo del programa, la evaluación de dividió en dos momentos: uno previo a impartirse el programa tomando una referencia acerca del nivel de conocimiento de los colaboradores y uno luego de la ejecución de programa con el fin de medir la eficiencia del programa para evaluar la preparación de los colaboradores ante las ciber amenazas de ingeniería social, al culminar el programa y al obtenerse los resultados de la evaluación, además se analizó la curva de tendencia de la evaluación luego de llevarse a cabo el programa de seguridad informática.

3.3 Materiales e instrumentos

De acuerdo con Marczyk et al. (2005), al operacionalizar múltiples variables en un diseño cuasi experimental, es posible verificar como distintos factores interactuan e influyen en el resultado. Esto te permite entender mejor las relaciones y controlar posibles factores adicionales, lo que hace que los hallazgos sean más precisos y relevantes.

La técnica de recolección de datos o instrumento utilizado fueron las pruebas estandarizadas de conocimientos, se realizaron dos pruebas estandarizadas de conocimientos, la primera prueba denominada como prueba pretest, la cual nos permitió medir los puntos altos y bajos de los colaboradores participantes, y así orientar el programa de seguridad informática para alcanzar mayores niveles de conocimiento. Posteriormente a la aplicación del programa se aplicó la prueba postest, la cual nos permitió comparar los resultados obtenidos y determinar la influencia que tuvo la variable independiente sobe la dependiente.

3.4 Población y muestra de estudio

Dada la naturaleza del diseño cuasi experimental con pruebas pretest y postest, se consideró un solo grupo de control y experimental para la población y muestra. La selección de la población no fue aleatoria, sino intencionada, ya que se buscaba centrarse en la división de tecnologías de información de la entidad bancaria, particularmente en el área de Helpdesk, lo cual era relevante para la investigación. Esta muestra, compuesta por 100 empleados, aunque no representó a toda la población de la división de TI, proporcionó hallazgos valiosos para entender el problema de investigación en ese contexto específico.

Al considerar un solo grupo como control y experimental, se pudo determinar la influencia del programa de seguridad informática. Arnau (1995), conceptualiza el diseño cuasi experimental como un plan de acción que tiene como fin investigar los efectos que tiene un tratamiento y/o los procesos de cambio en circunstancias en las que los sujetos o unidades de observación no han sido asignados de manera aleatoria, con la finalidad de explorar la influencia de dichos procesos, por lo que se recurre a grupos intactos o naturales.

3.5 Operacionalización de variables

Variable independiente: Programa de seguridad informática.

Variable dependiente: Ciberataques de ingeniería social.

En la tabla 1 de operacionalización de variables podemos observar cómo la variable dependiente e independiente y sus dimensiones respectivas, se alinean directamente con los objetivos, indicadores e hipótesis de nuestra matriz de consistencia (anexo 1), lo cual nos permite mantener una coherencia entre variables, instrumentos y objetivos del estudio.

Tabla 1

Operacionalización de variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala	Técnicas o métodos
VI. Programa de seguridad informática	Programa de capacitación en seguridad es un componente crucial para implementar una estrategia de seguridad completa en seguridad de la información, enfocada en educar a los usuarios sobre los riesgos y las mejores prácticas, su objetivo radica en formar una mayor conciencia del usuario como una línea de defensa fundamental. Stallings y Brown (2015)	Gestión de vulnerabilidades y riesgos	• Número de vulnerabilidades de alto riesgo • Número de incidentes de seguridad relacionados con vulnerabilidades. • Número de riesgos identificados • Precisión de la evaluación de riesgos.	Pretest y postest	Análisis Descriptivo y Análisis Inferencial
		Políticas y procedimientos	• Tasa de cumplimiento de las políticas • Número de reportes de incidentes por parte de los empleados	Pretest y postest	Análisis Descriptivo y Análisis Inferencial

Tabla 1 (continuación)

Variable	Definición Conceptual	Dimensiones	• Indicadores	Escala	Técnicas o métodos
VD. Ciberataques de ingeniería social.	Un ciberataque es un intento deliberado de causar daños a un sistema informático, una red, robar información de ellos u obtener acceso no autorizado a dichos sistemas o datos. Los ciberataques pueden adoptar muchas formas, desde el robo de información hasta actos de sabotaje, y tienen la capacidad de causar daños importantes tanto a la economía como a las operaciones. Schneier (2000)	Compromiso de datos	• Acceso a sitios web sospechosos. • Descarga de archivos sospechosos. • Interacción con mensajes sospechosos. • Ataques de Phishing. • Ataques de ransomware. • Daño a la reputación.	Pretest y postest	Análisis Descriptivo y Análisis Inferencial
		Medidas de seguridad	• Tasa de detección de vulnerabilidades. • Nivel de cumplimiento de las políticas de seguridad. • Número de usuarios que han completado la capacitación en seguridad.	Pretest y postest	Análisis Descriptivo y Análisis Inferencial

3.6 Procesamiento y análisis de datos

Una vez tabulados los datos y subsanadas las lagunas, se utilizó el software SPSS como explorador de los datos recopilados mediante instrumentos (véase anexo 3) (prueba estandarizada de conocimientos) (anexo 4) que habían sido sometidos a pruebas de fiabilidad y validez en el pasado. Se llevó a cabo el proceso de recopilación de datos.

Se realizó un análisis estadístico de los resultados para comprobar la hipótesis. Además, se realizaron otros análisis, que se presentarán en tablas con el fin de realizar su respectiva interpretación metodológica y temática.

Para realizar el análisis de datos , ya que la muestra es mayor a 50 usuarios, para probar el supuesto de normalidad se utilizó la prueba no paramétrica para muestras relacionadas de Kolmogorov – Smirnov. También se utilizó la prueba de rangos con signo de Wilcoxon para determinar los rangos positivos, negativos y empates en relación a los resultados obtenidos con el pretest y postest.

CAPÍTULO IV: RESULTADOS

4.1 Análisis de resultados

4.1.1 Resultados de la variable independiente: Programa de seguridad informática

4.1.1.1. Análisis general

La evaluación de la variable independiente programa de seguridad informática se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a los conocimientos relacionados a la variable independiente, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 96% rangos positivos, 4% empates y no hubo rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 4,11 a 7,72 puntos sobre un máximo de 10 puntos.

Este hallazgo se presenta en las tablas de resultados 2, 3 y 4, en las cuales se detalla el análisis general de la variable programa de seguridad informática, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 2.

Tabla 2

Prueba de Kolmogorov-Smirnov para la variable programa de seguridad informática

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Programa de seguridad informática	0,155	100	<0,001

Debido a que, luego de haberse realizado la prueba de normalidad de Kolmogorov – Smirnov, nuestro grado de significancia es menor al 5%, indicando que no hay una distribución normal, aplicamos la prueba no paramétrica para muestras relacionadas, donde obtenemos un cuadro de análisis de estadísticos descriptivos que se muestra en la tabla 3 y la prueba de rangos con signo de Wilcoxon que se muestra en la tabla 4.

Tabla 3

Análisis de estadísticos descriptivos de la variable programa de seguridad informática

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Programa de seguridad informática_Pre	100	4,11	1,230	2	7
Programa de seguridad informática_Post	100	7,72	1,164	4	10

Tabla 4

Prueba estadística de Wilcoxon para la variable programa de seguridad informática

	N	**Rango promedio**	**Suma de rangos**

Programa de seguridad informática_POST - Programa de seguridad informática_PRE	Rangos negativos	0[a]	0,00	0,00
	Rangos positivos	96[b]	48,50	4656,00
	Empates	4[c]		
	Total	100		

a. Programa de seguridad informática_POST < Programa de seguridad informática_PRE

b. Programa de seguridad informática_POST > Programa de seguridad informática_PRE

c. Programa de seguridad informática_POST = Programa de seguridad informática_PRE

4.1.2 Resultados de la variable dependiente: Ciberataques de ingeniería social

4.1.2.1 Análisis general

La evaluación de la variable dependiente ciberataques de ingeniería social se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a los conocimientos relacionados a la variable dependiente, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 90% rangos positivos, 8% empates y 2% rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 3,64 a 6,90 puntos sobre un máximo de 10 puntos.

Este hallazgo se presenta en las tablas de resultados 5, 6 y 7, en las cuales se detalla el análisis general de la variable ciberataques de ingeniería social, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 5.

Tabla 5

Prueba de Kolmogorov-Smirnov para la variable dependiente ciberataques de ingeniería social

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Ciberataques de ingeniería social	0,131	100	<0,001

Debido a que, luego de haberse realizado la prueba de normalidad de Kolmogorov – Smirnov, nuestro grado de significancia es menor al 5%, indicando que no hay una distribución normal, aplicamos la prueba no paramétrica para muestras relacionadas, donde obtenemos un cuadro de análisis de estadísticos descriptivos que se muestra en la tabla 6 y la prueba de rangos con signo de Wilcoxon que se muestra en la tabla 7.

Tabla 6

Análisis de estadísticos descriptivos para la variable dependiente ciberataques de ingeniería social

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Ciberataques de ingeniería social_PRE	100	3,64	1,812	1	9
Ciberataques de ingeniería social_POST	100	6,90	1,744	3	10

Tabla 7

Prueba estadística de Wilcoxon para la variable dependiente ciberataques de ingeniería social

		N	Rango promedio	Suma de rangos
Ciberataques de ingeniería social_POST - Ciberataques de ingeniería social_PRE	Rangos negativos	2[a]	8,00	16,00
	Rangos positivos	90[b]	47,36	4262,00
	Empates	8[c]		
	Total	100		

a. Ciberataques de ingeniería social_POST < Ciberataques de ingeniería social_PRE

b. Ciberataques de ingeniería social_POST > Ciberataques de ingeniería social_PRE

c. Ciberataques de ingeniería social_POST = Ciberataques de ingeniería social_PRE

4.2 Comprobación de la hipótesis

En primera instancia se ejecutó la prueba de normalidad de Kolgomorov-Smirnov ya que nuestra muestra contempla una población de más de 50 personas. Esta prueba se realiza con el fin de determinar cuál es la prueba estadística con mejor ajuste para determinar la relación entre las variables.

Se aplica la prueba de Kolgoromov-Smirnov, siendo el criterio:

Si el valor de significancia > 0,05: Existe normalidad estadística

Si el valor de significancia < 0,05: No existe normalidad estadística

En la Tabla 8, se detalla la prueba de normalidad de Kolgomorov-Smirnov, con sus respectivos estadísticos de la prueba de normalidad, los cuales se detallan a continuación:

Tabla 8

Prueba de normalidad Kolgomorov-Smirnov

	Estadístico	gl	Sig.
Diferencia_ general	0,119	100	0,001

De acuerdo a la prueba de normalidad Kolgoromov-Smirnov podemos validar que el valor de significancia es menor a 0,05, por lo tanto, se establece que no hay una distribución normal, por lo que se decidió aplicar la prueba de Wilcoxon, la cual es una prueba no paramétrica, empleada para establecer la relación y grado entre las variables.

4.2.1 Comprobación de la hipótesis general

Se formula:

H0: El programa de seguridad informática no influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

H1: El programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

Con el fin de determinar cómo influye el programa de seguridad informática sobre los empleados de una entidad bancaria ante los ataques de ingeniería social, se ejecuta la prueba de rangos con signo de Wilcoxon.

Entre nuestros resultados también se halló que en cuanto a lo propuesto en la hipótesis general, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 99% rangos positivos, 1% empates y no hubo rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 7,75 a 14,62 puntos sobre un máximo de 20 puntos.

Tabla 9

Análisis de estadísticos descriptivos de la *hipótesis general*

	N	Media	Desv. estándar	Mínimo	Máximo
Hipótesis General _pre	100	7,75	2,318	4	15
Hipótesis General _post	100	14,62	2,710	9	20

En la tabla 10 se detalla la prueba de normalidad de Kolgomorov-Smirnov, con sus respectivos estadísticos de la prueba de normalidad, los cuales se detallan a continuación:

Tabla 10

Prueba de normalidad Kolgomorov-Smirnov

	Estadístico	gl	Sig.
Post_programa-Pre_programa	0,129	100	0,001

De acuerdo a la prueba de normalidad Kolgoromov-Smirnov podemos validar que el valor de significancia es menor a 0,05, por lo tanto, se establece que no hay una distribución normal, por lo que se decidió aplicar la prueba de Wilcoxon, la cual es una prueba no paramétrica, empleada para establecer la relación y grado entre las variables.

Tabla 11

Prueba de rangos con signo de Wilcoxon para la hipótesis general.

		N	Rango promedio	Suma de rangos
Post_Programa - Pre_Programa	Rangos negativos	0[a]	0,00	0,00
	Rangos positivos	99[b]	50,00	4950,00
	Empates	1[c]		
	Total	100		

a. Post_programa < pre_programa

b. Post_programa > pre_programa

c. Post_programa = pre_programa

4.2.2 Comprobación de las hipótesis específicas

4.2.2.1 Comprobación de la hipótesis específica 1

Se formula:

H0: La gestión de vulnerabilidades y riesgos de un programa de seguridad informática no influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

H1: La gestión de vulnerabilidades y riesgos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

La evaluación de la hipótesis específica 1 se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a lo propuesto en la hipótesis específica 1, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 86% rangos positivos, 14% empates y no hubo rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 2,57 a 4,27 puntos sobre un máximo de 5 puntos.

Este hallazgo se presenta en las tablas de resultados 12, 13 y 14, en las cuales se detalla el análisis general de la variable programa de seguridad informática, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 12.

Tabla 12

Prueba de Kolmogorov-Smirnov para la hipótesis específica 1

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Gestión de riesgos y vulnerabilidades	0,184	100	<0,001

Tabla 13

Análisis de estadísticos descriptivos de la *hipótesis específica 1*

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Gestión de riesgos y vulnerabilidades_pre	100	2,57	0,807	0	5
Gestión de riesgos y vulnerabilidades_post	100	4,27	0,750	2	5

Tabla 14

Prueba estadística de Wilcoxon para hipótesis específica 1

		N	**Rango promedio**	**Suma de rangos**
Gestión de riesgos y vulnerabilidades_POST - Gestión de riesgos y vulnerabilidades_PRE	Rangos negativos	0[a]	0,00	0,00
	Rangos positivos	86[b]	43,50	3741,00
	Empates	14[c]		
	Total	100		

a. Gestión de riesgos y vulnerabilidades_POST < Gestión de riesgos y vulnerabilidades_PRE

b. Gestión de riesgos y vulnerabilidades_POST > Gestión de riesgos y vulnerabilidades_PRE

c. Gestión de riesgos y vulnerabilidades_POST = Gestión de riesgos y vulnerabilidades_PRE

4.2.2.2 Comprobación de la hipótesis específica 2

Se formula:

H0: Las políticas y procedimientos de un programa de seguridad informática no influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

H1: Las políticas y procedimientos de un programa de seguridad informática influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

La evaluación de la hipótesis específica 2 se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a lo propuesto en la hipótesis específica 2, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 84% rangos positivos, 12% empates y 4% rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 1,54 a 3,45 puntos sobre un máximo de 5 puntos.

Este hallazgo se presenta en las tablas de resultados 15, 16 y 17, en las cuales se detalla el análisis general de la variable programa de seguridad informática, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 15.

Tabla 15

Análisis de estadísticos descriptivos de la hipótesis específica 2

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Políticas y procedimientos	0,208	100	<0,001

Tabla 16

Prueba estadística de Wilcoxon de la hipótesis específica 2

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Políticas y procedimientos_PRE	100	1,54	0,758	0	4
Políticas y procedimientos_POST	100	3,45	1,019	1	5

Tabla 17

Prueba estadística de Wilcoxon de la hipótesis específica 2

		N	**Rango promedio**	**Suma de rangos**
Políticas y procedimientos_POST - Políticas y procedimientos_PRE	Rangos negativos	4[a]	10,50	42,00
	Rangos positivos	84[b]	46,12	3874,00
	Empates	12[c]		
	Total	100		

a. Políticas y procedimientos_POST < Políticas y procedimientos_PRE

b. Políticas y procedimientos_POST > Políticas y procedimientos_PRE

c. Políticas y procedimientos_POST = Políticas y procedimientos_PRE

4.2.2.3 Comprobación de la hipótesis específica 3

Se formula:

H0: El compromiso de datos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

H1: El compromiso de datos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

La evaluación de la hipótesis específica 3 se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a lo propuesto en la hipótesis específica 3, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 68% rangos positivos, 31% empates y 1% rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 2,17 a 3,27 puntos sobre un máximo de 5 puntos.

Este hallazgo se presenta en las tablas de resultados 18, 19 y 20, en las cuales se detalla el análisis general de la variable programa de seguridad informática, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 18.

Tabla 18

Prueba de Kolmogorov-Smirnov para la hipótesis específica 3.

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Compromiso de datos	0,200	100	<0,001

Tabla 19

Análisis de estadísticos descriptivos para la hipótesis específica 3

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Compromiso de datos_PRE	100	2,17	0,911	0	5
Compromiso de datos_POST	100	3,27	0,962	0	5

Tabla 20

Prueba estadística de Wilcoxon para la hipótesis específica 3

		N	**Rango promedio**	**Suma de rangos**
Compromiso de datos_POST - Compromiso de datos_PRE	Rangos negativos	1[a]	18,00	18,00
	Rangos positivos	68[b]	35,25	2397,00
	Empates	31[c]		
	Total	100		

a. Compromiso de datos_POST < Compromiso de datos_PRE

b. Compromiso de datos_POST > Compromiso de datos_PRE

c. Compromiso de datos_POST = Compromiso de datos_PRE

4.2.2.4 Comprobación de la hipótesis específica 4

Se formula:

H0: Las medidas de seguridad de un programa de seguridad informática no influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

H1: Las medidas de seguridad de un programa de seguridad informática influyen significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.

La evaluación de la hipótesis específica 4 se realizó a partir de la comparación de los resultados que se obtuvieron en los cuestionarios previos y posteriores a la aplicación del programa.

Los resultados en su mayoría fueron positivos, por lo tanto, podemos decir que, tras la comparación entre las evaluaciones realizadas a los colaboradores, antes y después de la ejecución del programa mostraron un resultado sumamente favorable.

Este resultado fue respaldado estadísticamente tras la aplicación de la prueba de Kolmogorov-Smirnov dando como resultado un grado de significancia menor al 5%, por lo tanto, quedó demostrado que se cumplió la hipótesis alterna, lo que nos permitió interpretar que hay una diferencia significativa en el promedio de los resultados obtenidos en las pruebas estandarizadas de conocimiento realizados a los colaboradores antes y después de la aplicación del programa de seguridad informática.

Entre nuestros resultados también se halló que en cuanto a lo propuesto en la hipótesis específica 4, tras la aplicación de la prueba estadística de rangos de Wilcoxon, para los resultados obtenidos entre el pretest y postest a los colaboradores sometidos a las pruebas estandarizadas de conocimiento, se reflejó un 86% rangos positivos, 10% empates y 4% rangos negativos, esta mejora se refuerza al obtener que en nuestra prueba de análisis de estadísticos descriptivos, se vio un aumento en el puntaje promedio de 1,47 a 3,63 puntos sobre un máximo de 5 puntos.

Este hallazgo se presenta en las tablas de resultados 21, 22 y 23, en las cuales se detalla el análisis general de la variable programa de seguridad informática, tales resultados son presentados a continuación:

Dado que nuestra muestra es mayor a los 50 usuarios se realiza la prueba de Kolmogorov – Smirnov para comprobar nuestro supuesto de normalidad, el cual se muestra en la tabla 21.

Tabla 21

Prueba de Kolmogorov-Smirnov para la hipótesis específica 4

	Kolmogorov-Smirnov[a]		
	Estadístico	**gl**	**Sig.**
Diferencia Medidas de seguridad	0,173	100	<0,001

Tabla 22

Análisis de estadísticos descriptivos para la hipótesis específica 4

	N	**Media**	**Desv. estándar**	**Mínimo**	**Máximo**
Medidas de seguridad_PRE	100	1,47	1,096	0	4
Medidas de seguridad_POST	100	3,63	1,107	1	5

Tabla 23

Prueba estadística de Wilcoxon para la hipótesis específica 4

		N	Rango promedio	Suma de rangos
Medidas de seguridad_POST - Medidas de seguridad_PRE	Rangos negativos	4[a]	9,50	38,00
	Rangos positivos	86[b]	47,17	4057,00
	Empates	10[c]		
	Total	100		

a. Medidas de seguridad_POST < Medidas de seguridad_PRE

b. Medidas de seguridad_POST > Medidas de seguridad_PRE

c. Medidas de seguridad_POST = Medidas de seguridad_PRE

CAPÍTULO V: DISCUSIÓN

La aplicación del programa logró incrementar significativamente la capacidad de los empleados de la entidad bancaria en la preparación y toma de decisiones ante ataques de ingeniería social, lo cual ayudará a evitar y reportar con mayor eficacia los ataques, por otro lado esta información puede ser utilizada por la jefatura encargada del área, para continuar con una capacitación que con estos antecedentes esté orientada a reforzar los puntos con mayor índice de mejora y abarcar temas relacionados a los ciberataques que no se abordaron en la presente investigación, con el fin de no caer en redundancias.

Los resultados obtenidos en este estudio tras la aplicación del programa de seguridad informática ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024, indican que tanto para variable independiente y la variable dependiente, tras una comparativa entre el pretest y el postest de las pruebas estandarizadas de conocimientos, nos muestra que la aplicación del programa de seguridad informática tuvo un efecto altamente influyente, ya que al realizarse la prueba de rangos con signo de Wilcoxon reflejó un total del 96% de rangos positivos, 4% de empates y no hubo rangos negativos para la variable independiente y un total de 90% rangos positivos, 8% empates y 2% rangos negativos para la variable dependiente.

Por otro lado, siguiendo con la congruencia de los resultados mostrados por nuestra hipótesis general y las hipótesis específicas, contrastamos que con la medición de la influencia, de la preparación y toma de decisiones ante ciberataques de ingeniería social informática sobre los empleados de una entidad bancaria, ya que los resultados mostraron ser en gran medida también positivos, lo cual nos ayudó a consolidar la influencia de nuestra investigación, dando un total del 90% de rangos positivos, 8% de empates y 2% de rangos negativos.

Estos resultados se ven vinculados con investigaciones previas, como la realizada a nivel nacional por Orihuela (2022), quien desarrolló la tesis titulada “Programa de seguridad de información ante ciberataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima”, llegando a la conclusión de que el piloto ha demostrado que existe una preocupación genuina por la seguridad de la información dentro de la organización, y que es de suma importancia cultivar en los trabajadores el conocimiento de la seguridad de la información para asegurar que se comporten y piensen de buena manera al interactuar con Internet. Esto guarda

relación con nuestra investigación ya que se toma en cuenta la importancia de la dimensión de gestión integral de la seguridad de la información.

Así mismo con respecto a la relación entre variables, Marchand (2020) desarrollo la tesis titulada “Cultura de seguridad de información en la protección de activos informáticos en la Universidad Nacional Agraria de la Selva, 2018-2020”, donde fue factible llegar a la conclusión de que existe una relación entre las variables de estudio que presenta un alto nivel de significación.

Estas revelaciones están relacionadas con investigaciones previas, como la realizada a nivel internacional por Serrano (2024), con su investigación “Plan de capacitación en ciberseguridad para la formación de personal en el centro de operaciones de seguridad soc de la empresa Datasec SAS”, en donde se concluye que la implementación del plan de capacitación garantiza que el Centro de Operaciones de Seguridad (SOC) cuente con personal formado y preparado para gestionar con éxito las nuevas amenazas cibernéticas. Como resultado, se protegen los activos digitales de la empresa y su capacidad para competir en el mercado. Esto se relaciona con los resultados de nuestra investigación, ya que se resalta la importancia de un programa de capacitación, tal como se suscito en la presente investigación donde se vió una mejora en el 99% de los casos.

Por otro lado, a nivel internacional Flores (2023), tras desarrollar la investigación titulada “Análisis de vulnerabilidades en el uso de las redes sociales en ciberataques de ingeniería social para fortalecer la seguridad de la información en la Facultad de Ciencias Humanas Y De La Educación, de la Universidad Técnica de Ambato”, se llegó a concluir que tan pronto como finalizó la charla informativa para alumnos y profesores, se pudo afirmar que el enfoque formativo y la técnica de evaluación utilizados eran adecuados. Esto se debió a que se obtuvieron buenos resultados en cuanto a los conocimientos adquiridos sobre seguridad de la información. Lo cual guarda relación con la hipótesis específica 1 del presente trabajo de investigación, donde se analiza como influye la gestión de riesgos y vulnerabilidades, obteniendo resultados altamente positivos.

Finalmente, en la investigación realizada por Villacís (2023), “Diseño de una campaña de ataques de ingeniería social”, como parte de este proyecto, se llevó a cabo con éxito una iniciativa que incluía ingeniería social, para determinar de que manera afecta en mayor grado a la información personal que se encuentra expuesta. Una de las formas en que se hizo posible fue aumentando la concienciación entre todas las cuentas de correo electrónico registradas entre los participantes. En cuanto a futuras

investigaciones, no solo recomendamos lanzar ataques de phishing, sino que también sugerimos evaluar diversas estrategias de ingeniería social para determinar cuáles son las más eficaces para engañar a las personas. Esto se relaciona con la investigación, ya que abarca temas relacionados a la dimensión políticas y procedimientos, la cual fue incluida dentro de los temas a reforzar en el programa de seguridad informática.

CONCLUSIONES

De acuerdo a los resultados obtenidos podemos concluir que hubo una influencia significativa en la preparación y toma de decisiones de los empleados ante ciberataques de ingeniería social, evidenciado por el incremento estadísticamente significativo en los puntajes obtenidos en las evaluaciones postest. Esta mejora permitió fortalecer la cultura organizacional en ciberseguridad, alineándose con los principios de mejora continua establecidos por la norma ISO/IEC 27001.

Se comprobó que la gestión integral de la seguridad informática y la mitigación de ciberataques de ingeniería social, como dimensiones del programa, influyeron de manera significativa en la preparación de los empleados ante amenazas de ingeniería social. Los resultados mostraron mejoras considerables en la identificación de riesgos, cumplimiento de normas internas y reducción de incidentes relacionados con errores humanos.

Se determinó que la mitigación de ataques de ingeniería social, mediante la capacitación orientada a la detección de técnicas como phishing y ransomware, mejoró sustancialmente la toma de decisiones por parte de los colaboradores frente a escenarios simulados. Este cambio fue observable tanto en los resultados cuantitativos como en el comportamiento seguro adoptado en las pruebas de simulación.

La investigación evidenció que una intervención educativa bien estructurada, con base en estándares internacionales y adaptada al entorno específico de la entidad financiera, puede reducir significativamente la vulnerabilidad humana ante ciberataques, contribuyendo así a una gestión integral de la seguridad de la información.

RECOMENDACIONES

A la gerencia de tecnología de la entidad bancaria, se recomienda institucionalizar el programa de seguridad informática desarrollado en esta investigación como un componente obligatorio de inducción y capacitación anual. Esta medida contribuirá a mantener un nivel elevado de preparación y conciencia del personal ante ciberataques de ingeniería social, reduciendo el riesgo organizacional asociado al factor humano.

Al equipo de seguridad de la información, se sugiere reforzar la gestión de vulnerabilidades mediante el uso de herramientas automáticas de escaneo y la revisión periódica de las políticas internas de ciberseguridad, integrando los aprendizajes derivados del programa. Esto garantizará una mejora continua en la detección y mitigación de amenazas antes de que puedan ser explotadas.

A los responsables de recursos humanos, se recomienda incorporar módulos formativos sobre amenazas emergentes (como inteligencia artificial usada en phishing o ingeniería social por deepfake) en futuras versiones del programa. Esta actualización permitirá anticiparse a nuevas modalidades de ataque que evolucionan con rapidez en el contexto digital actual.

A la alta dirección, se le insta a evaluar la posibilidad de replicar y adaptar este programa en otras áreas funcionales más allá del departamento de tecnología, como operaciones, atención al cliente y finanzas, debido al impacto positivo demostrado en la reducción del riesgo de ingeniería social.

A futuras investigaciones, se les recomienda profundizar en el análisis longitudinal del impacto del programa, midiendo la retención del conocimiento y el cambio de comportamiento de los colaboradores en el mediano y largo plazo, a fin de optimizar el diseño pedagógico y su efectividad real.

REFERENCIA BIBLIOGRAFICAS

Albladi, S., & Weir, G. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences. Obtenido de https://hcis-journal.springeropen.com/articles/10.1186/s13673-018-0128-7

Alfaro Garbich, V. E., & Perez Vasquez, A. C. (2023). Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería social en el rubro empresarial. Lima: Universidad Cesar Vallejo. Obtenido de https://repositorioslatinoamericanos.uchile.cl/handle/2250/9233460?show=full

Andress, J. (2011). The basics of information security. Waltham: British Library.

Arias, F. (2006). El Proyecto de Investigación: Introducción a la metodología científica 5ª Edición. Caracas: Episteme.

Arnau Gras, J. (1995). Diseños experimentales en psicología y educación. Barcelona: Trillas.

Campoverde Cabañarez, L. (2022). Implementación de técnicas en ingeniría social en un gobierno autónomo descentralizado de la provincia de Santa Elena. La Libertad: Universidad estatal Península de Santa Elena. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.upse.edu.ec/server/api/core/bitstreams/7829864c-257d-4942-8b3f-562b852af6d5/content

Chicano Tejada, E. (2014). Auditoría de seguridad informática. Málaga: IC Editorial.

CIBERTEC. (16 de Octubre de 2024). Tipos de seguridad informática. Obtenido de https://www.cibertec.edu.pe/: https://www.cibertec.edu.pe/noticias/tipos-seguridad-informatica/

De Vecchi, R., & Grossi, G. (2016). Metodología de la investigación herramientas prácticas para la investigación social. Roma: Carocci.

ESET. (2021). Manual de ingeniería social. Obtenido de www.eset.com

Flores López, S. (2023). Análisis de vulnerabilidades en el uso de las redes sociales en ciber ataques de ingeniería social para fortalecer la seguridad de la información en la Facultad de Ciencias Humanas Y De La Educación, de la Universidad Técnica de Ambato. Ambato, Ecuador: Universisad Tecnica de Ambato.

Fortinet. (2024). https://www.fortinet.com/. Obtenido de https://www.fortinet.com/lat/training/security-awareness-training

Gómez, A. (2006). Enciclopedia de la seguridad informática. Madrid: RA-MA.

Grupo Atico34. (2024). https://protecciondatos-lopd.com/. Obtenido de https://protecciondatos-lopd.com/empresas/politica-seguridad-informacion/

Harris, S., & Maymi, F. (2020). CISSP All-in-One Exam Guide.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación. Ciudad de México.

IBM. (2024). ibm.com. Obtenido de https://www.ibm.com/es-es/topics/social-engineering

IBM. (2024). X-Force Threat Intelligence Index 2024. New York, EEUU.

IBM. (2025). https://www.ibm.com/. Obtenido de https://www.ibm.com/mx-es/topics/it-security

IBM. (2014). IBM Security Services 2014 - Cyber Security Intelligence Index. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMS.

ICONTEC. (2017). Compendio seguridad de la información. ICONTEC.

INCIBE. (2015). Youtube. Obtenido de Comparativa de empresas sobre la concienciación: https://www.youtube.com/

International organization of standardization, & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022.

ISACA. (2022). The state of Cibersecurity. ISACA.

Kaspersky. (2023). https://latam.kaspersky.com/. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-security-awareness-training

Kissel, R. (2012). Glossary of Key Information Security Terms, National Institute of Standards and Technology. U.S: NIST.

Marchand Niño, W. (2020). Cultura de seguridad de información en la protección de activos informáticos en la Universidad Nacional Agraria de la Selva, 2020. Huancayo, Huancayo, Perú: Universidad nacional del centro del Perú.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). Essentials of Research Design and Methodology. New Jersey: John Wiley & Sons.

MetaCompliance. (2024). https://www.metacompliance.com/. Obtenido de https://www.metacompliance.com/es/blog/cyber-security-awareness/10-ways-to-improve-staff-cyber-security-awareness

Nieles, M., Dempsey, K., & Yan Pillietri, V. (Junio de 2017). An Introduction ro Information Security. NIST Special Publication 800-12. USA: U.S Departement Of Commerce.

Office, Information Comissioner's. (2023). https://ico.org.uk/. Obtenido de https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

Orihuela Quivaqui, A. I. (2022). Programa de seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima. Lima: Pontificia Universidad Católica del Perú.

OSTEC. (2024). https://ostec.blog. Obtenido de https://ostec.blog/es/seguridad-informacion/politicas-y-procedimientos-de-seguridad-de-la-informacion/

Palomino Cardenas, J., Cuneo Torres, A., & Gutierrez Arana, E. (2024). Modelo de desarrollo de reglas de correlación para la detección y alerta de. Lima: Universidad peruana de ciencias aplicadas. Obtenido de https://renati.sunedu.gob.pe/handle/renati/3272765/browse?type=title&sort_by=1&order=ASC&rpp=20&etal=-1&null=&offset=505

Pande, J. (2017). Introduction to Cyber Security. Uttarakhand Open University, Haldwani- 263139.

Paniagua Soza, R. (2022). Anatomía del Ransomware.

Pashentev, D., Zaloilo, M., Ivanyuk, O., & Alimova, D. (2019). Digital technologies and society directions of interaction,. https://www.revistaespacios.com/a19v40n42/19404202.html, 1-6.

Pavon Rosano, P., Romero Ternero, C., De Haro Olmo, F., & Varela Vaca, A. (2024). Incidentes de Ciberseguridad. Madrid.

Peñafiel Suárez, M. R. (2022). Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales. La Libertad, Ecuador: Universidad Estatal Península de Santa Elena. Obtenido de https://repositorio.upse.edu.ec/items/c5ccde94-9403-4c31-9133-ceb168f5e721

Pérez Márquez, F. (2019). Riesgo cibernético y ciberseguridad. Ciudad de México: Comisión nacional de seguros y finanzas.

Peterson, C. (2003). Bringing ADDIE to Life: Instructional Design at Its Best. Califonia: Universidad de Pennsylvania.

Raza Shirazi, S., Abbas Shah, S., & Anwar, A. (2024). COMPUTER SCIENCE AND INFORMATION TECHNOLOGY - ADVANCES AND APPLICATIONS. USA.

Rocohano Ramos, R., & Silva Ordoñez, L. (2021). Detección de vulnerabilidades en el comportamiento de las personas para evitar que sean víctimas de ataques de ingeniería social. Quito: Universidad de las fuerzas armadas de Ecuador.

Rodas Díaz, B., & Sánchez Zorrilla, J. (2024). La implementación de un protocolo de prevención contra ransomware para optimizar la seguridad del servidor en la empresa BBTI S.A.C entre el año 2022. Callao: Universidad Nacional del Callao.

Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D., Alava Cruzatty, J., Parrales Anzules, G., Alava Mero, C., . . . Castillo, M. M. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Manabí, Ecuador: ISBN: 978-84-949306-1-4.

Sandoval Castellano, E. (2011). Ingeniería Social: Corrompiendo la mente humana. Ciudad de México: UNAM.

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons.

Scientific Knowledge Publisher (SciKnowPub), USA. (01 de 01 de 2024). Computer science and information technology - advances and applications. USA, USA, USA: ISBN 978-1-960740-44-1.

Serra Ruiz, J., Navarro Arrivas, G., Castillo-Perez, S., Herrera, J., Robles Martinez, S., Castillo Perez, S., & García Alfaro, J. (2022). SEGURIDAD INFORMÁTICA. Programa de naciones unidas Colombia.

Serrano Tovar, F. (2024). Plan de capacitación en ciberseguridad para la formación de personal en el centro de operaciones de seguridad soc de la empresa Datasec SAS. Bogotá: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD .

Shadish, T., Cook, W., & Campbell, D. (2002). Diseños de investigación en psicología el enfoque cuasi-experimental. Fildadelfia: Temple University Press.

Stallings, W., & Brown, L. (2015). Computer Security Principles and Practice Third Edition. New Jersey.

UNIR. (2024). https://mexico.unir.net/. Obtenido de https://mexico.unir.net/noticias/ingenieria/politicas-seguridad-informatica/

Vega Briceño, E. (2021). Seguridad de la información. Alicante, España: Editorial Área de Innovación y desarrollo, S.I.

Villacís Miranda, S. (2023). Diseño de una campaña de ataques de ingeniería social. Quito: Pontificia Universidad Católica de Ecuador.

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security. USA.

ANEXOS

Anexo 1. Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLE	DIMENSIONES	METODOLOGÍA
Problema General ¿Como influye un Programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024? **Problemas específicos**	**Objetivo General** Identificar como influye un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024 **Objetivos específicos**	**Hipótesis General** El programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024. **Hipótesis específicas**	**Variable independiente:** Programa de seguridad informática.	• Gestión de vulnerabilidades y riesgos • Políticas y procedimientos	Tipo de investigación: Aplicada Nivel de investigación: Explicativo Diseño de investigación: Cuasi experimental, Longitudinal

¿Cómo influye la gestión de vulnerabilidades y riesgos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?	Conocer cómo influye la gestión de vulnerabilidades y riesgos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.	La gestión de vulnerabilidades y riesgos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.	**Variable dependiente:** Ciberataques de ingeniería social.	• Compromiso de datos • Medidas de seguridad
¿Cómo influyen las políticas y procedimientos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de	Conocer cómo influyen las políticas y procedimientos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de	Las políticas y procedimientos de un programa de seguridad informática influyen significativamente en la preparación y toma de decisiones ante los ciberataques de		

ingeniería social para empleados de una entidad bancaria en Lima, 2024?	ingeniería social para empleados de una entidad bancaria en Lima, 2024.	ingeniería social para empleados de una entidad bancaria en Lima, 2024.
¿Cómo influye el compromiso de datos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?	Conocer cómo influye el compromiso de datos de un programa de seguridad informática en la preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.	El compromiso de datos de un programa de seguridad informática influye significativamente en la preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.
¿Cómo influyen las medidas de seguridad de un programa de seguridad informática en la preparación y	Conocer cómo influyen las medidas de seguridad de un programa de seguridad informática en la	Las medidas de seguridad de un programa de seguridad informática influyen significativamente en la

toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024?	preparación y toma de decisiones ante ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.	preparación y toma de decisiones ante los ciberataques de ingeniería social para empleados de una entidad bancaria en Lima, 2024.	

Anexo 2. Programa de seguridad informática

Creado con iSpring Suite
Saber más

¿Qué piensas?
Si bien la mayoría de los malware se distribuyen mediante enlaces o archivos adjuntos en un correo electrónico, también se pueden propagar de otras formas.

¿Puedes adivinar algunas de esas otras formas? (Selecciona todas las que correspondan.)

- [ ] Mediante una vulnerabilidad de software conocida.
- [ ] Haciendo clic en un enlace de una publicación en redes sociales.
- [ ] Haciendo clic en un mensaje de texto.
- [ ] Conectando una unidad USB a tu dispositivo.
- [ ] Interactuando con una ventana emergente.

Su resultado: 0 de 10 Pregunta 1 de 1 Calificar

Creado con iSpring Suite
Saber más

¿Qué piensas?
Si bien la mayoría de los malware se distribuyen mediante enlaces o archivos adjuntos en un correo electrónico, también se pueden propagar de otras formas.

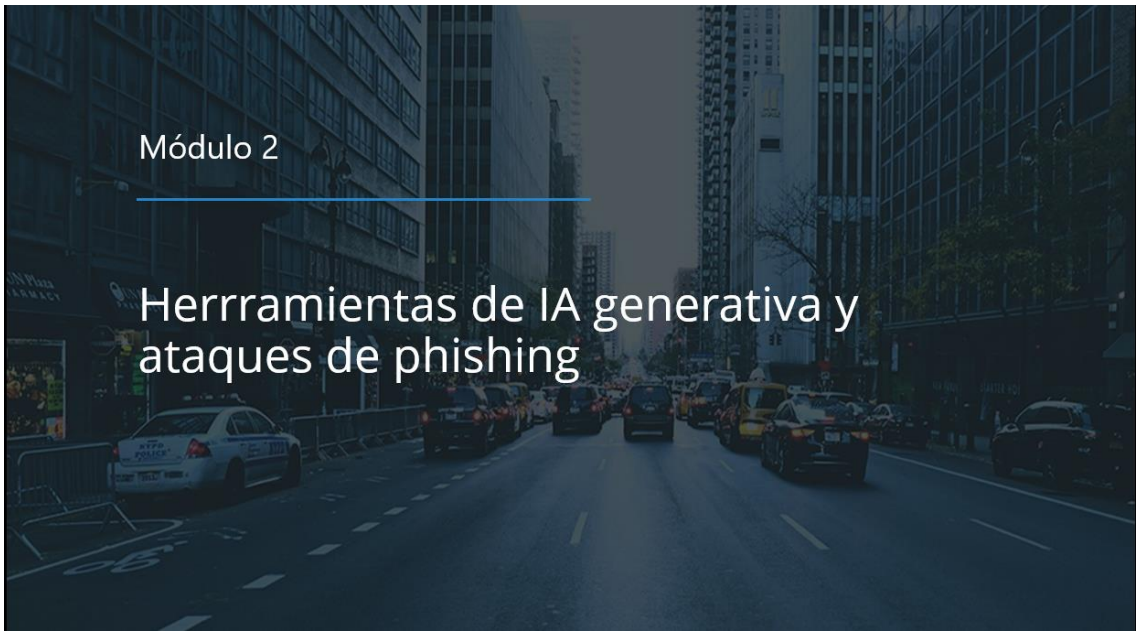
¿Puedes adivinar algunas de esas otras formas? (Selecciona todas las que correspondan.)

- [x] Mediante una vulnerabilidad de software conocida.
- [x] Haciendo clic en un enlace de una publicación en redes sociales.
- [x] Haciendo clic en un mensaje de texto.
- [x] Conectando una unidad USB a tu dispositivo
- [x] Interactu

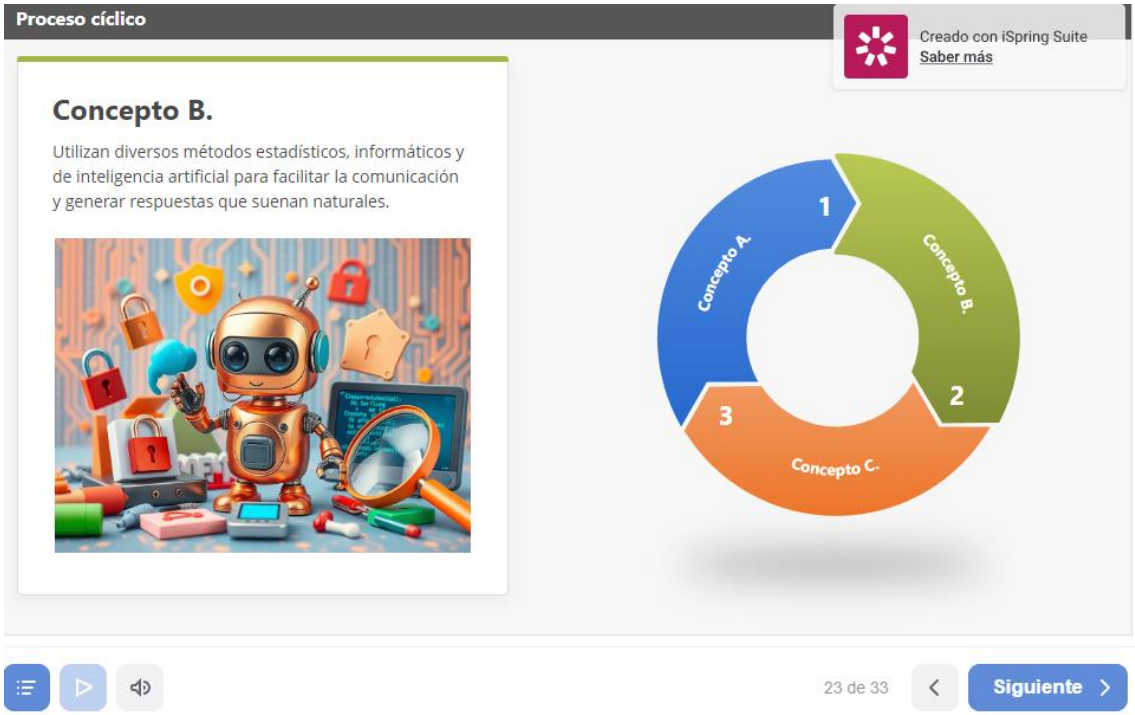
Correcto

¡Muy bien! Ha elegido la respuesta correcta.

Su resultado: 10 de 10 Pregunta 1 de 1 **Ver Resultados**




Proceso cíclico
Concepto A.
¿Qué son los chatbots de IA generativa?
La "IA generativa" también se conoce como "GenAI"
Creado con iSpring Suite
Saber más
Concepto B.
2
23 de 33
Siguiente


Proceso cíclico
Concepto B.
Utilizan diversos métodos estadísticos, informáticos y de inteligencia artificial para facilitar la comunicación y generar respuestas que suenan naturales.
Creado con iSpring Suite
Saber más
1
Concepto A.
Concepto B.
2
3
Concepto C.
23 de 33
Siguiente


Pestañas
Correos electrónicos
Traducción
Coincidencia de tono
Creado con iSpring Suite
Saber más
Cómo usan los chatbots para crear ataques de phishing
Las ventajas de los chatbots de IA generativa se pueden usar de forma malintencionada para crear estafas muy convincentes.
25 de 33
Siguiente


Pestañas
Correos electrónicos sin errores
Traducción
Coincidencia de tono y estilo
Creado con iSpring Suite
Saber más
Correos electrónicos sin errores
Los chatbots de IA generativa pueden + crear contenido sin errores ortográficos o gramaticales, que normalmente nos permiten identificar los ataques de phishing.
25 de 33
Siguiente

26 de 33 Siguiente

Creado con iSpring Suite
Saber más

Ten en cuenta esta situación
La experiencia de Juan con la IA

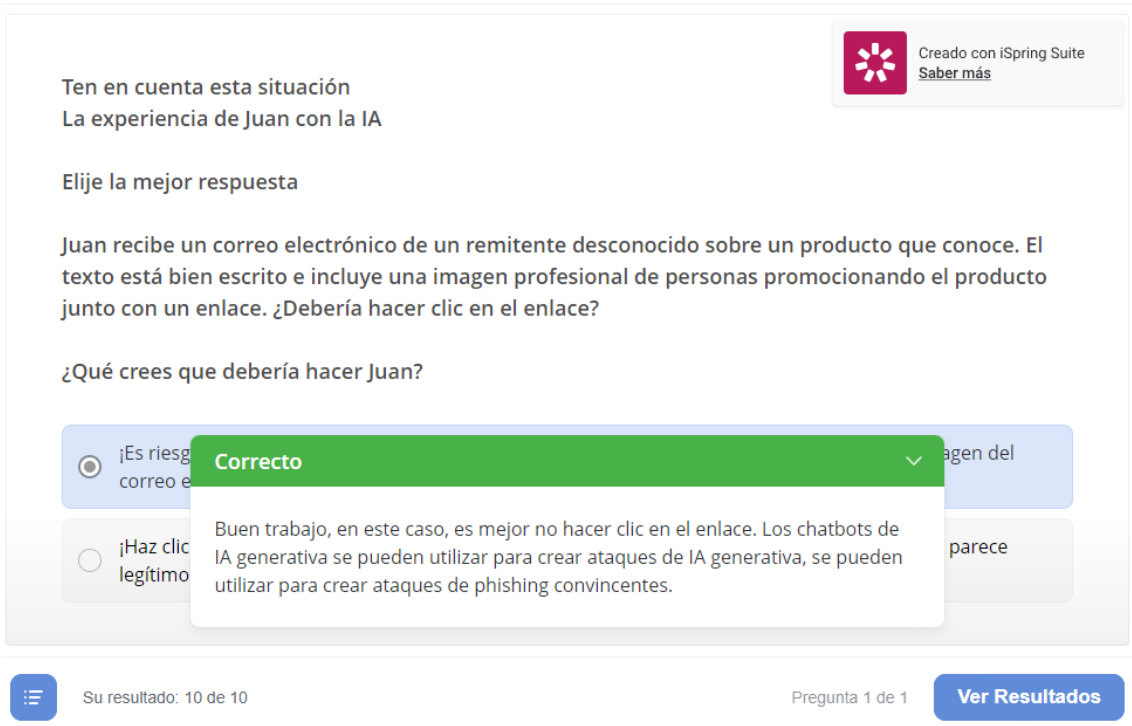
Elije la mejor respuesta

Juan recibe un correo electrónico de un remitente desconocido sobre un producto que conoce. El texto está bien escrito e incluye una imagen profesional de personas promocionando el producto junto con un enlace. ¿Debería hacer clic en el enlace?

¿Qué crees que debería hacer Juan?

- ¡Es riesgoso! No hagas clic en el enlace. Es posible que un atacante haya creado el texto y la imagen del correo electrónico utilizando un chatbot de IA generativa.
- ¡Haz clic! No puedes conocer todas las direcciones de correo electrónico, y el resto del mensaje parece legítimo.

Su resultado: 0 de 10 Pregunta 1 de 1 Calificar


Creado con iSpring Suite
Saber más
Ten en cuenta esta situación
La experiencia de Juan con la IA
Elije la mejor respuesta
Juan recibe un correo electrónico de un remitente desconocido sobre un producto que conoce. El texto está bien escrito e incluye una imagen profesional de personas promocionando el producto junto con un enlace. ¿Debería hacer clic en el enlace?
¿Qué crees que debería hacer Juan?
¡Es riesg
correo e
agen del
Correcto
Buen trabajo, en este caso, es mejor no hacer clic en el enlace. Los chatbots de IA generativa se pueden utilizar para crear ataques de IA generativa, se pueden utilizar para crear ataques de phishing convincentes.
¡Haz clic
legítimo
parece
Su resultado: 10 de 10
Pregunta 1 de 1
Ver Resultados


Línea de Tiempo
Creado con iSpring Suite
Saber más
Archivos adjuntos y enlaces inesperados
Trata todos los archivos adjuntos con precaución, especialmente si no los esperabas, no los habías solicitado o provienen de un remitente desconocido.
Y ten cuidado con los enlaces sospechosos. Pasa el mouse sobre ellos y comprueba a dónde llevan. En vez de hacer clic en un enlace, accede a la página web escribiendo la dirección directamente en el navegador o usando un marcador de confianza.
Señales de advertencia del phishing por IA
28 de 33
Siguiente

¿Qué son los datos confidenciales?

Creado con iSpring Suite
Saber más

Los datos confidenciales son aquellos datos privados o de naturaleza confidencial sobre las personas, las empresas o los proyectos (aplica tanto para individuos como para organizaciones).

Los detalles personales y financieros (sobre usted, sus colegas, sus clientes y sus socios de negocios) son valiosos para los defraudadores.

La información de propiedad intelectual y patentada del negocio es muy codiciada por los competidores y criminales.

Anterior Siguiente

1x

31 de 33

Siguiente

¿En dónde se alma… datos confidencial…?

Creado con iSpring Suite
Saber más

Los datos confidenciales están virtualmente en todas partes:

- Documentos impresos y archivos físicos.
- Medios de almacenamiento como CDs, DVDs, memorias USB, tarjetas de memoria, discos duros externos.
- Laptops, computadoras de escritorio, fotocopiadoras y servidores.
- Dispositivos móviles como teléfonos y tabletas.
- Cuentas en línea y servicios de almacenamiento en la nube.

Anterior Siguiente

1x

32 de 33

Siguiente

¿Por qué es import… manejar y eliminar los datos de manera segura?

Creado con iSpring Suite
Saber más

Si no protege los datos confidenciales a lo largo de su ciclo de vida podría haber serias consecuencias:

- Exponer sus propios datos y los de los demás a los criminales.
- Revelar información sobre clientes y secretos comerciales a la competencia.
- Arriesgarse a usted mismo y a su empleador a ser sujeto de multas y/o acciones legales.
- Dañar su reputación profesional y la marca de su empleador.

Anterior Siguiente

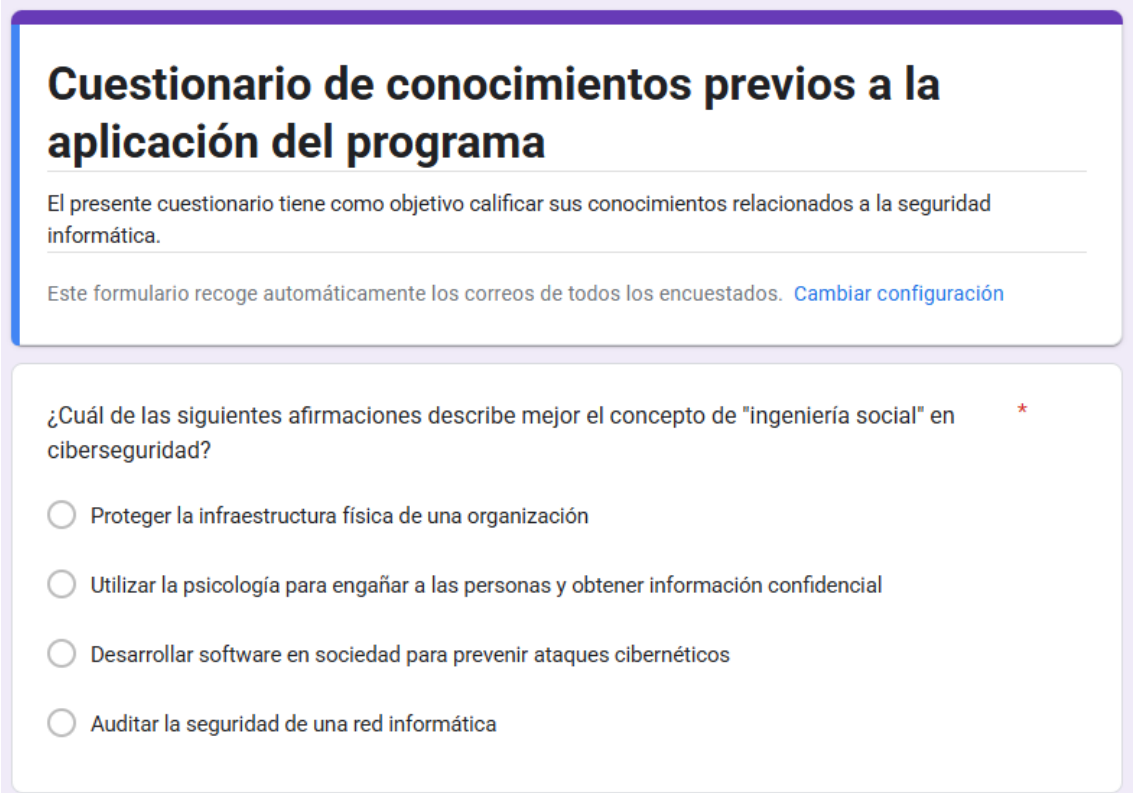
1x

33 de 33

Siguiente

Anexo 3. Instrumentos de investigación

Cuestionario pretest:



Cuestionario de conocimientos previos a la aplicación del programa

El presente cuestionario tiene como objetivo calificar sus conocimientos relacionados a la seguridad informática.

Este formulario recoge automáticamente los correos de todos los encuestados. Cambiar configuración

¿Cuál de las siguientes afirmaciones describe mejor el concepto de "ingeniería social" en ciberseguridad? *

- Proteger la infraestructura física de una organización
- Utilizar la psicología para engañar a las personas y obtener información confidencial
- Desarrollar software en sociedad para prevenir ataques cibernéticos
- Auditar la seguridad de una red informática

¿Qué es un ataque de phishing? *

- Intento de acceso no autorizado a un sistema
- Suplantación de identidad mediante correos electrónicos fraudulentos
- Virus que afecta a las computadoras
- Acceso indebido a través de una red inalámbrica

¿Cuál de los siguientes es un método común utilizado en ataques de ingeniería social? *

- Inyección de SQL
- Phishing
- Escaneo de puertos
- Malware

¿Qué herramienta de IA generativa puede ser utilizada para crear correos electrónicos de phishing más realistas? *

- Generadores de texto automáticos
- Herramientas de encriptación
- Analizadores de vulnerabilidades
- Sistemas de gestión de contraseñas
- Programas antivirus

¿De qué manera las herramientas de IA generativa pueden ayudar en la creación de ataques phishing? *

- Creando contraseñas seguras para los usuarios
- Generando mensajes de correo electrónico convincentes y personalizados
- Detectando automáticamente los correos de phishing
- Detecta como atacar, de acuerdo a las vulnerabilidades de cada usuario

A Juan le llega un correo electrónico de un remitente desconocido sobre un archivo que conoce. El texto está bien escrito y contiene una imagen profesional de una fuente que parece ser confiable. ¿Sería correcto hacer clic en el enlace? *

- Es riesgoso no debería hacer clic. Es probable que un atacante haya creado el texto y la imagen del corr...
- Haz clic, es imposible conocer todas las direcciones de correo electrónico seguras, además el resto del ...

¿Cuál de las siguientes prácticas es una forma adecuada de proteger la información confidencial en una organización? *

- Almacenar la información en un servidor público de acceso general
- Utilizar contraseñas simples para facilitar el acceso
- Cifrar la información y restringir el acceso solo a personal autorizado
- Dejar la información confidencial en documentos físicos accesibles para todos

Elige la mejor práctica: *

Mientras usted se encuentra en la oficina, su compañero de labores se levanta para ir al servicio, pero dejó su computadora desbloqueada y se puede acceder fácilmente a la información en el equipo.

¿Qué debería hacer usted?

- ○ No hacer nada. Ya que regresará en un tiempo breve.
- ○ Bloquear la computadora y recordarle que debe tener más cuidado.
- ○ Cerrar todos los programas abiertos y dejar la computadora como está.

Usted necesita enviar un archivo encriptado y la contraseña a un compañero. La información del archivo es altamente confidencial. *

- ○ Enviar el archivo y la contraseña en dos correos electrónicos por separado.
- ○ Enviar el archivo por correo electrónico y la contraseña en un mensaje de texto.
- ○ Enviar el archivo y la contraseña en un mismo correo electrónico. De tal manera que sea menos confuso.

¿Cuál de las siguientes es una técnica común utilizada en ataques de ingeniería social? *

- ○ Phishing
- ○ Firewalls
- ○ Antivirus
- ○ VPN

Los ataques de ransomware solo pueden infectar a un único dispositivo. No se propagan por toda la red. *

- ○ Verdadero
- ○ Falso

Los gusanos informáticos son más una molestia que una amenaza real *

- ○ Verdadero
- ○ Falso

¿Cuál de los siguientes tipos de datos es más susceptible a ser comprometido en un ataque de ingeniería social? *

- ○ Datos de configuración del servidor
- ○ Información personal identificable (PII)
- ○ Documentos de políticas de seguridad
- ○ Copias de seguridad de software

¿Cuál es una de las consecuencias más graves de un compromiso de datos? *

- ○ Mejora de la reputación de la empresa
- ○ Pérdida de confianza por parte de los clientes
- ○ Aumento de las ventas
- ○ Reducción de costos operativos

¿Por qué es más complicado detectar un ataque de phishing generado mediante IA? *

- ( ) Los correos son generados en su totalidad por una IA.
- ( ) Los textos generados mediante IA tienen menos probabilidad de contener errores ortográficos o gramati...
- ( ) No hay forma de detectar que el mensaje es generado por una IA.
- ( ) N.A

¿Cuál de las siguientes medidas es más efectiva para mitigar ataques de ingeniería social? *

- ( ) Actualizar el software regularmente
- ( ) Capacitar a los empleados sobre seguridad
- ( ) Instalar un firewall
- ( ) Realizar copias de seguridad

Habilitar una macro puede activar un malware *

- ( ) Verdadero
- ( ) Falso

¿Cuál de las siguientes es una forma en que un usuario puede reconocer un ataque de phishing generado por IA? * 1 punto

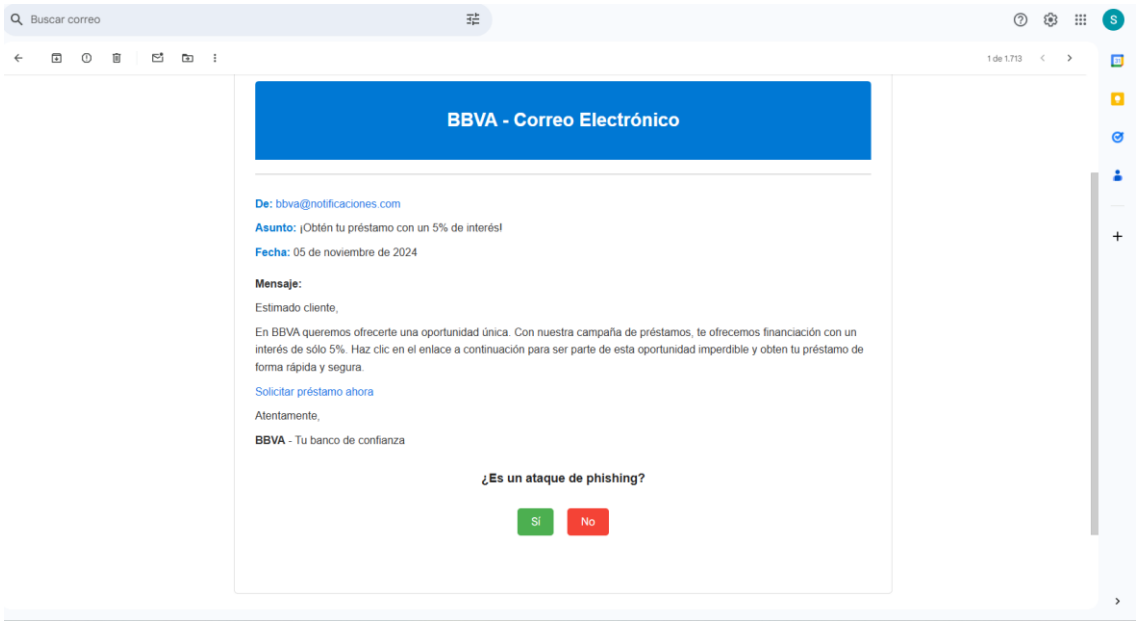
- ◯ Si el mensaje es enviado desde una dirección de correo oficial
- ◯ Si el mensaje contiene errores gramaticales o de estilo
- ◯ Si el mensaje está cifrado
- ◯ Si el mensaje contiene enlaces a sitios legítimos
- ◯ Si el mensaje proviene de una cuenta verificada

Si un dispositivo va a ser desechado de la empresa, es importante realizar un formateo y destrucción de los datos * 1 punto

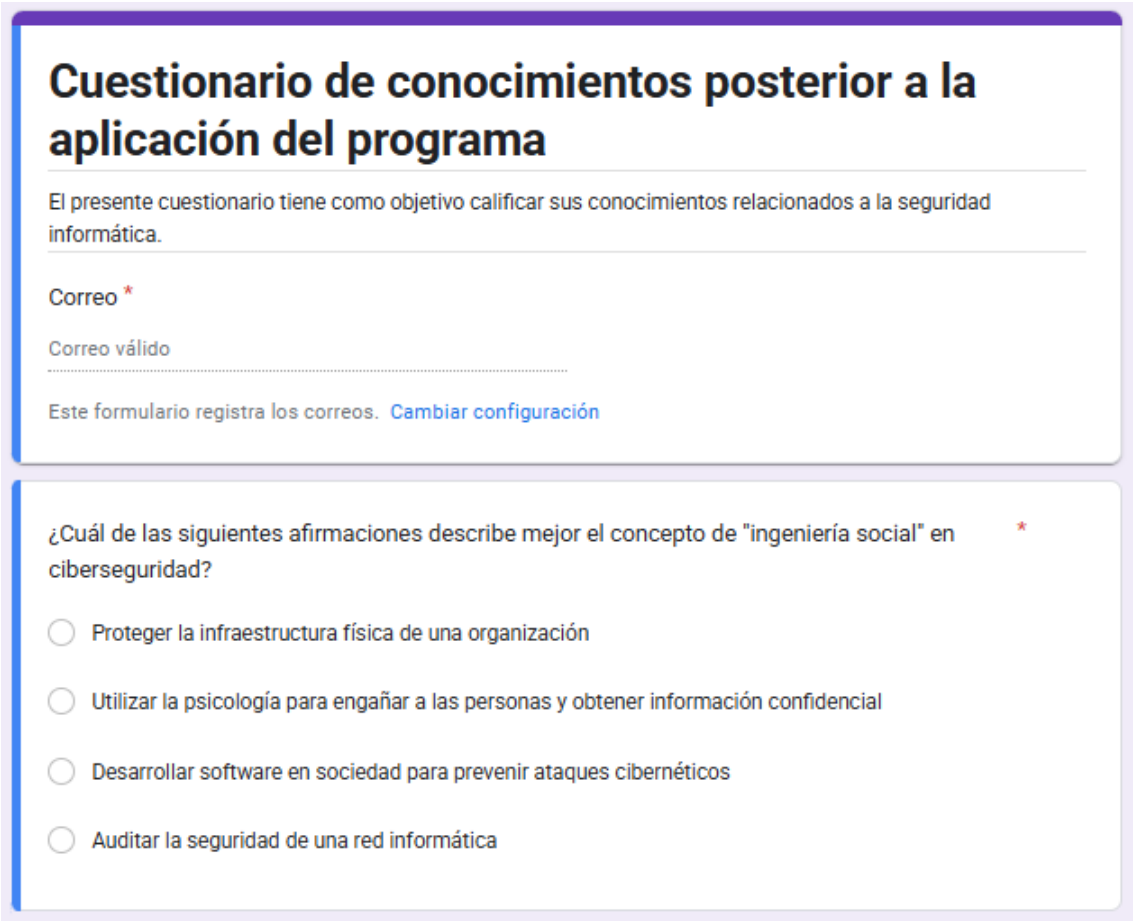
- ◯ Verdadero
- ◯ Falso

Se ha enviado un mail a su correo personal con el asunto "Campaña de prueba 1", de acuerdo a las características del correo, por favor indicar si se trataría de un correo verídico o se trataría de un ataque de phishing. * 1 punto

- ◯ No cuenta con las características de un ataque de phishing.
- ◯ Cuenta con las características de un ataque de phishing.


Buscar correo
1 de 1.713
BBVA - Correo Electrónico
De: bbva@notificaciones.com
Asunto: ¡Obtén tu préstamo con un 5% de interés!
Fecha: 05 de noviembre de 2024
Mensaje:
Estimado cliente,
En BBVA queremos ofrecerte una oportunidad única. Con nuestra campaña de préstamos, te ofrecemos financiación con un interés de sólo 5%. Haz clic en el enlace a continuación para ser parte de esta oportunidad imperdible y obten tu préstamo de forma rápida y segura.
Solicitar préstamo ahora
Atentamente,
BBVA - Tu banco de confianza
¿Es un ataque de phishing?
Sí
No

Cuestionario postest:



Cuestionario de conocimientos posterior a la aplicación del programa

El presente cuestionario tiene como objetivo calificar sus conocimientos relacionados a la seguridad informática.

Correo *

Correo válido

Este formulario registra los correos. Cambiar configuración

¿Cuál de las siguientes afirmaciones describe mejor el concepto de "ingeniería social" en ciberseguridad? *

- Proteger la infraestructura física de una organización
- Utilizar la psicología para engañar a las personas y obtener información confidencial
- Desarrollar software en sociedad para prevenir ataques cibernéticos
- Auditar la seguridad de una red informática

¿Qué es un ataque de phishing? *

- Intento de acceso no autorizado a un sistema
- Suplantación de identidad mediante correos electrónicos fraudulentos
- Virus que afecta a las computadoras
- Acceso indebido a través de una red inalámbrica

¿Cuál de los siguientes es un método común utilizado en ataques de ingeniería social? *

- Inyección de SQL
- Phishing
- Escaneo de puertos
- Malware

¿Qué herramienta de IA generativa puede ser utilizada para crear correos electrónicos de phishing más realistas? *

- Generadores de texto automáticos
- Herramientas de encriptación
- Analizadores de vulnerabilidades
- Sistemas de gestión de contraseñas
- Programas antivirus

¿De qué manera las herramientas de IA generativa pueden ayudar en la creación de ataques phishing? *

- Creando contraseñas seguras para los usuarios
- Generando mensajes de correo electrónico convincentes y personalizados
- Detectando automáticamente los correos de phishing
- Detecta como atacar, de acuerdo a las vulnerabilidades de cada usuario

A Juan le llega un correo electrónico de un remitente desconocido sobre un archivo que conoce. El texto está bien escrito y contiene una imagen profesional de una fuente que parece ser confiable. ¿Sería correcto hacer clic en el enlace? *

- Es riesgoso no debería hacer clic. Es probable que un atacante haya creado el texto y la imagen del corr...
- Haz clic, es imposible conocer todas las direcciones de correo electrónico seguras, además el resto del ...

¿Cuál de las siguientes prácticas es una forma adecuada de proteger la información confidencial en una organización? *

- Almacenar la información en un servidor público de acceso general
- Utilizar contraseñas simples para facilitar el acceso
- Cifrar la información y restringir el acceso solo a personal autorizado
- Dejar la información confidencial en documentos físicos accesibles para todos

Elige la mejor práctica: *

Mientras usted se encuentra en la oficina, su compañero de labores se levanta para ir al servicio, pero dejó su computadora desbloqueada y se puede acceder fácilmente a la información en el equipo.

¿Qué debería hacer usted?

- ○ No hacer nada. Ya que regresará en un tiempo breve.
- ○ Bloquear la computadora y recordarle que debe tener más cuidado.
- ○ Cerrar todos los programas abiertos y dejar la computadora como está.

Usted necesita enviar un archivo encriptado y la contraseña a un compañero. La información del archivo es altamente confidencial. *

- ○ Enviar el archivo y la contraseña en dos correos electrónicos por separado.
- ○ Enviar el archivo por correo electrónico y la contraseña en un mensaje de texto.
- ○ Enviar el archivo y la contraseña en un mismo correo electrónico. De tal manera que sea menos confuso.

¿Cuál de las siguientes es una técnica común utilizada en ataques de ingeniería social? *

- ○ Phishing
- ○ Firewalls
- ○ Antivirus
- ○ VPN

Los ataques de ransomware solo pueden infectar a un único dispositivo. No se propagan por toda la red. *

- Verdadero
- Falso

Los gusanos informáticos son más una molestia que una amenaza real *

- Verdadero
- Falso

¿Cuál de los siguientes tipos de datos es más susceptible a ser comprometido en un ataque de ingeniería social? *

- Datos de configuración del servidor
- Información personal identificable (PII)
- Documentos de políticas de seguridad
- Copias de seguridad de software

¿Cuál es una de las consecuencias más graves de un compromiso de datos? *

- Mejora de la reputación de la empresa
- Pérdida de confianza por parte de los clientes
- Aumento de las ventas
- Reducción de costos operativos

¿Por qué es más complicado detectar un ataque de phishing generado mediante IA? *

- Los correos son generados en su totalidad por una IA.
- Los textos generados mediante IA tienen menos probabilidad de contener errores ortográficos o gramati...
- No hay forma de detectar que el mensaje es generado por una IA.
- N.A

¿Cuál de las siguientes medidas es más efectiva para mitigar ataques de ingeniería social? *

- Actualizar el software regularmente
- Capacitar a los empleados sobre seguridad
- Instalar un firewall
- Realizar copias de seguridad

Habilitar una macro puede activar un malware *

- Verdadero
- Falso

¿Cuál de las siguientes es una forma en que un usuario puede reconocer un ataque de phishing generado por IA? * 1 punto

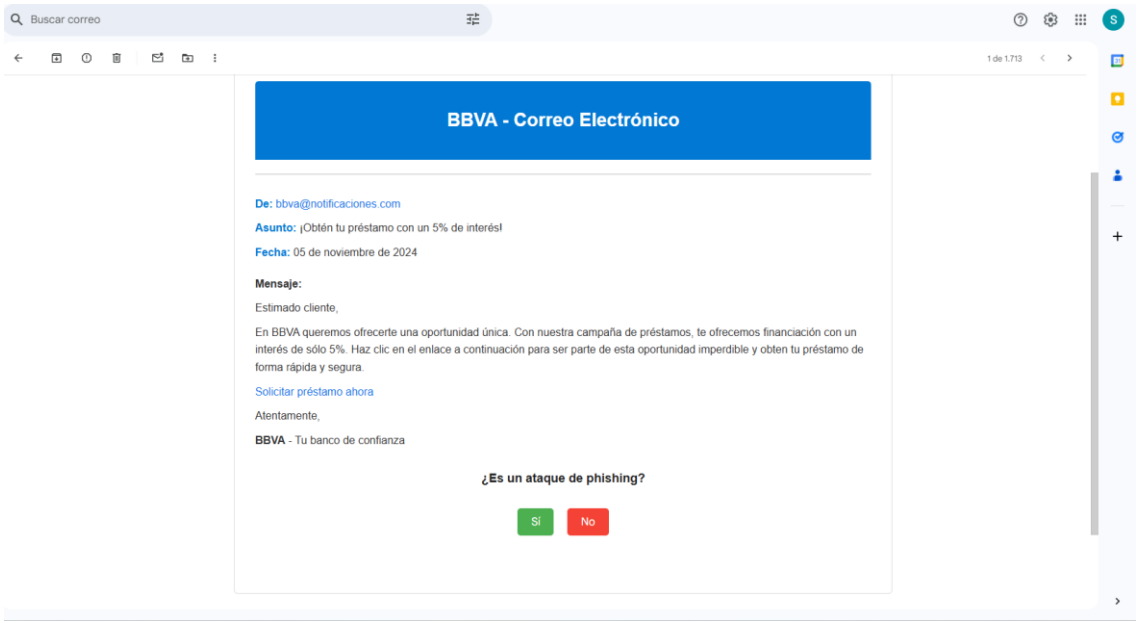
- ◯ Si el mensaje es enviado desde una dirección de correo oficial
- ◯ Si el mensaje contiene errores gramaticales o de estilo
- ◯ Si el mensaje está cifrado
- ◯ Si el mensaje contiene enlaces a sitios legítimos
- ◯ Si el mensaje proviene de una cuenta verificada

Si un dispositivo va a ser desechado de la empresa, es importante realizar un formateo y destrucción de los datos * 1 punto

- ◯ Verdadero
- ◯ Falso

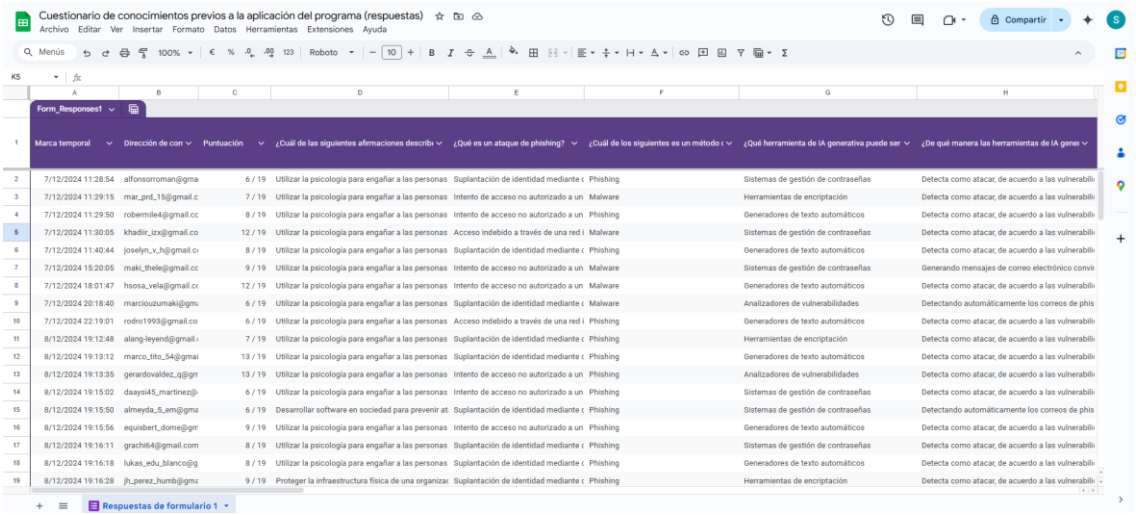
Se ha enviado un mail a su correo personal con el asunto "Campaña de prueba 1", de acuerdo a las características del correo, por favor indicar si se trataría de un correo verídico o se trataría de un ataque de phishing. * 1 punto

- ◯ No cuenta con las características de un ataque de phishing.
- ◯ Cuenta con las características de un ataque de phishing.


Buscar correo
1 de 1.713
BBVA - Correo Electrónico
De: bbva@notificaciones.com
Asunto: ¡Obtén tu préstamo con un 5% de interés!
Fecha: 05 de noviembre de 2024
Mensaje:
Estimado cliente,
En BBVA queremos ofrecerte una oportunidad única. Con nuestra campaña de préstamos, te ofrecemos financiación con un interés de sólo 5%. Haz clic en el enlace a continuación para ser parte de esta oportunidad imperdible y obten tu préstamo de forma rápida y segura.
Solicitar préstamo ahora
Atentamente,
BBVA - Tu banco de confianza
¿Es un ataque de phishing?
Sí
No

Anexo 4. Tabla de tabulación de datos de pruebas estandarizadas de conocimientos

Tabla de tabulación de datos pretest:


Cuestionario de conocimientos previos a la aplicación del programa (respuestas)

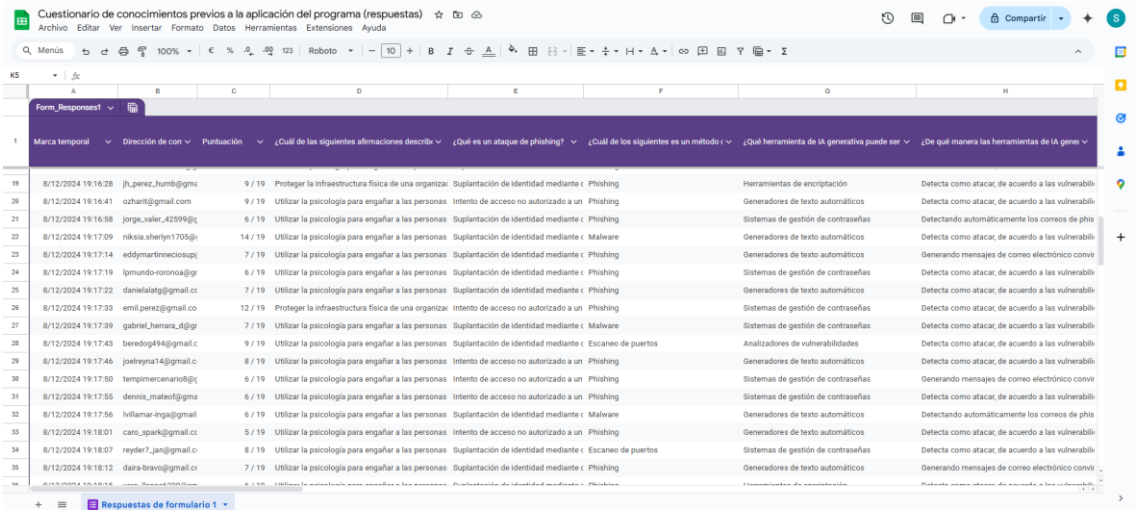
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

Compartir

Form_Responses1

Marca temporal	Dirección de con	Puntuación	¿Cuál de las siguientes afirmaciones describ	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método d	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas de IA gene
7/12/2024 11:28:54	alfonsorroman@gma	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 11:29:15	mar_prd_15@gmail.c	7 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 11:29:50	robermile4@gmail.cc	8 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 11:30:05	khadiir_izx@gmail.co	12 / 19	Utilizar la psicología para engañar a las personas	Acceso indebido a través de una red i	Malware	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 11:40:44	joselyn_v_h@gmail.c	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 15:20:05	maki_thele@gmail.cc	9 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Sistemas de gestión de contraseñas	Generando mensajes de correo electrónico convir
7/12/2024 18:01:47	hsosa_vela@gmail.cc	12 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
7/12/2024 20:18:40	marciouzumaki@gm	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Analizadores de vulnerabilidades	Detectando automáticamente los correos de phis
7/12/2024 22:19:01	rodro1993@gmail.co	6 / 19	Utilizar la psicología para engañar a las personas	Acceso indebido a través de una red i	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:12:48	alang-leyend@gmail.c	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:13:12	marco_tito_54@gmai	13 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:13:35	gerardovaldez_q@gm	13 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:15:02	daaysi45_martinez@	6 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:15:50	almeyda_5_em@gma	6 / 19	Desarrollar software en sociedad para prevenir at	Suplantación de identidad mediante	Phishing	Sistemas de gestión de contraseñas	Detectando automáticamente los correos de phis
8/12/2024 19:15:56	equisbert_dome@gm	9 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:16:11	grachi64@gmail.com	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:16:18	lukas_edu_blanco@g	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:16:28	jh_perez_humb@gma	9 / 19	Proteger la infraestructura física de una organizac	Suplantación de identidad mediante	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili

Respuestas de formulario 1


Cuestionario de conocimientos previos a la aplicación del programa (respuestas)

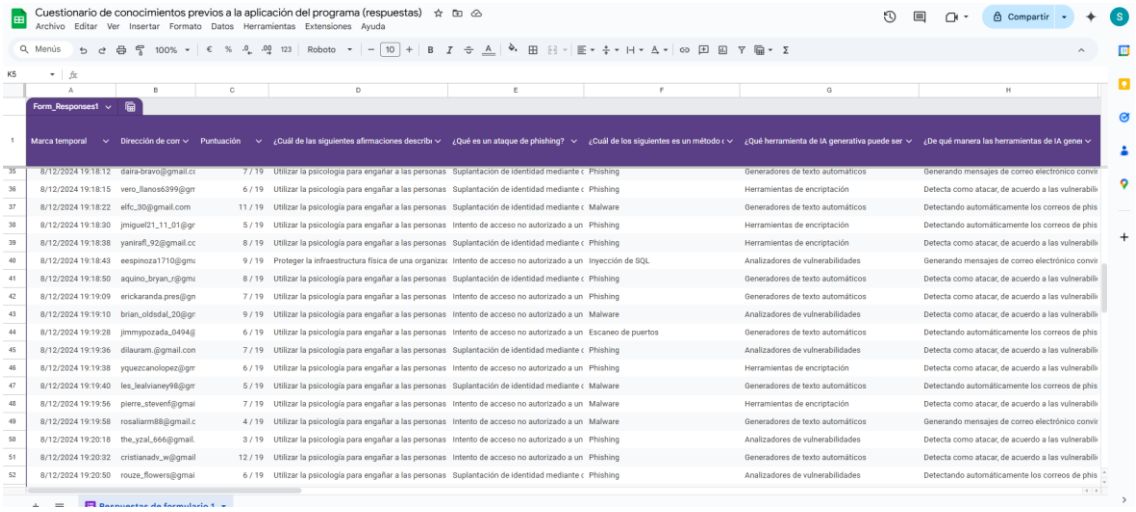
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

Compartir

Form_Responses1

Marca temporal	Dirección de con	Puntuación	¿Cuál de las siguientes afirmaciones describ	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método d	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas de IA gene
8/12/2024 19:16:28	jh_perez_humb@gma	9 / 19	Proteger la infraestructura física de una organizac	Suplantación de identidad mediante	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:16:41	ozharit@gmail.com	9 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:16:58	jorge_valer_42599@g	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Sistemas de gestión de contraseñas	Detectando automáticamente los correos de phis
8/12/2024 19:17:09	niksia.sherlyn1705@	14 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Malware	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:14	eddymartinneciosup(	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Generando mensajes de correo electrónico convir
8/12/2024 19:17:19	lpmundo-roronoa@gr	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:22	danielalatg@gmail.cc	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:33	emil.perez@gmail.co	12 / 19	Proteger la infraestructura física de una organizac	Intento de acceso no autorizado a un	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:39	gabriel_herrara_d@gr	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Malware	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:43	beredog494@gmail.c	9 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Escaneo de puertos	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:46	joelreyna14@gmail.c	8 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:50	tempimercenario8@g	6 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Sistemas de gestión de contraseñas	Generando mensajes de correo electrónico convir
8/12/2024 19:17:55	dennis_mateof@gma	6 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:17:56	lvillamar-inga@gmail	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Malware	Generadores de texto automáticos	Detectando automáticamente los correos de phis
8/12/2024 19:18:01	caro_spark@gmail.cc	5 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:18:07	reyder7_jan@gmail.c	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Escaneo de puertos	Sistemas de gestión de contraseñas	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:18:12	daira-bravo@gmail.cc	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Generando mensajes de correo electrónico convir

Respuestas de formulario 1

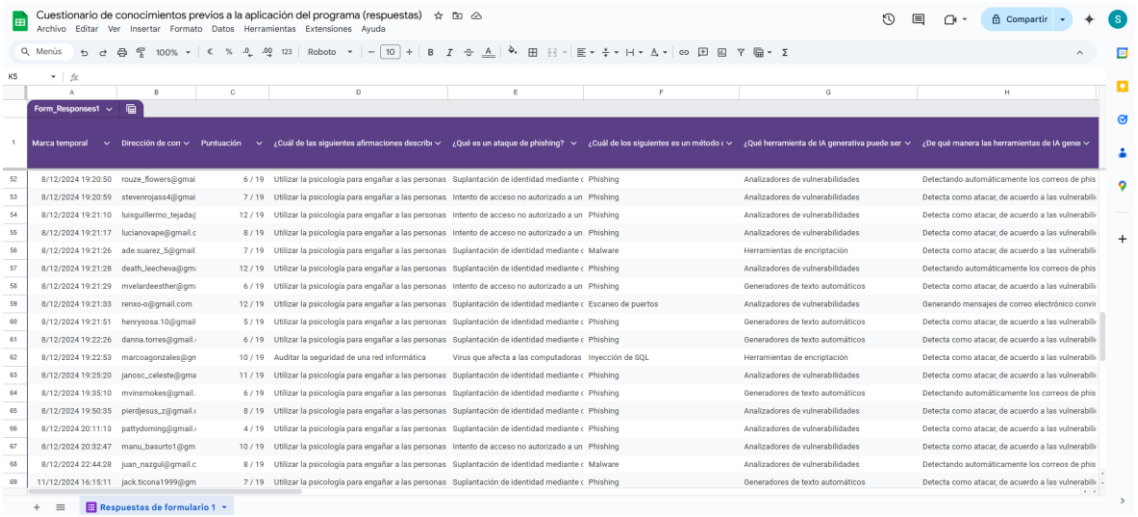

Cuestionario de conocimientos previos a la aplicación del programa (respuestas)

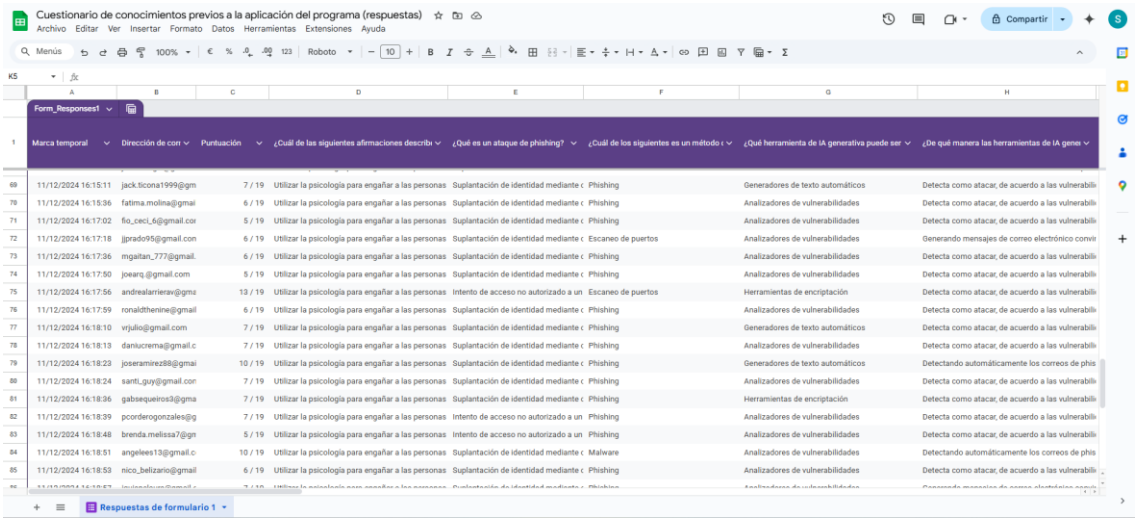
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

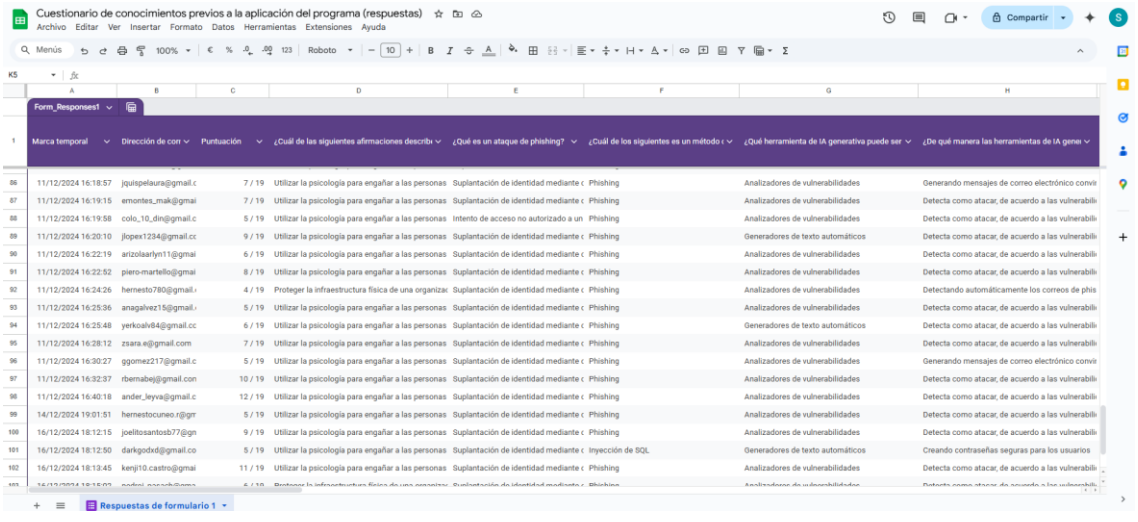
Compartir

Form_Responses1

Marca temporal	Dirección de con	Puntuación	¿Cuál de las siguientes afirmaciones describ	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método d	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas de IA gene
8/12/2024 19:18:12	daira-bravo@gmail.cc	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Generando mensajes de correo electrónico convir
8/12/2024 19:18:15	vero_llanos6399@gm	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:18:22	elfc_30@gmail.com	11 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Malware	Generadores de texto automáticos	Detectando automáticamente los correos de phis
8/12/2024 19:18:30	jmiguel21_11_01@gr	5 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Herramientas de encriptación	Detectando automáticamente los correos de phis
8/12/2024 19:18:38	yanirafl_92@gmail.cc	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:18:43	eespinoza1710@gmu	9 / 19	Proteger la infraestructura física de una organizac	Intento de acceso no autorizado a un	Inyección de SQL	Analizadores de vulnerabilidades	Generando mensajes de correo electrónico convir
8/12/2024 19:18:50	aquino_bryan_r@gmu	8 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:09	erickaranda.pres@gn	7 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:10	brian_oldsdal_20@gr	9 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:28	jimmypozada_0494@	6 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Escaneo de puertos	Generadores de texto automáticos	Detectando automáticamente los correos de phis
8/12/2024 19:19:36	dilauram.@gmail.con	7 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:38	yquezcanolopez@gm	6 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:40	les_lealvianey98@gm	5 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Malware	Generadores de texto automáticos	Detectando automáticamente los correos de phis
8/12/2024 19:19:56	pierre_stevenf@gmai	7 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Herramientas de encriptación	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:19:58	rosaliarm88@gmail.c	4 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Malware	Generadores de texto automáticos	Generando mensajes de correo electrónico convir
8/12/2024 19:20:18	the_yzal_666@gmail.	3 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:20:32	cristianadv_w@gmail	12 / 19	Utilizar la psicología para engañar a las personas	Intento de acceso no autorizado a un	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:20:50	rouze_flowers@gmai	6 / 19	Utilizar la psicología para engañar a las personas	Suplantación de identidad mediante	Phishing	Analizadores de vulnerabilidades	Detectando automáticamente los correos de phis


Cuestionario de conocimientos previos a la aplicación del programa (respuestas)
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda
Compartir
Form_Responses1
Marca temporal | Dirección de corr | Puntuación | ¿Cuál de las siguientes afirmaciones describ | ¿Qué es un ataque de phishing? | ¿Cuál de los siguientes es un método c | ¿Qué herramienta de IA generativa puede ser | ¿De qué manera las herramientas de IA gene
8/12/2024 19:20:50 | rouze_flowers@gmai | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detectando automáticamente los correos de phis
8/12/2024 19:20:59 | stevenrojass4@gmai | 7 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:21:10 | luisguillermo_tejada@ | 12 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:21:17 | lucianovape@gmail.c | 8 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:21:26 | ade.suarez_5@gmail. | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Malware | Herramientas de encriptación | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:21:28 | death_leecheva@gm | 12 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detectando automáticamente los correos de phis
8/12/2024 19:21:29 | mvelardeesther@gm | 6 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:21:33 | renxo-o@gmail.com | 12 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Escaneo de puertos | Analizadores de vulnerabilidades | Generando mensajes de correo electrónico convir
8/12/2024 19:21:51 | henrysosa.10@gmail | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:22:26 | danna.torres@gmail.c | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:22:53 | marcoagonzales@gn | 10 / 19 | Auditar la seguridad de una red informática | Virus que afecta a las computadoras | Inyección de SQL | Herramientas de encriptación | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:25:20 | janosc_celeste@gma | 11 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 19:35:10 | mvinsmokes@gmail. | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detectando automáticamente los correos de phis
8/12/2024 19:50:35 | pierdjesus_z@gmail.c | 8 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 20:11:13 | pattydoming@gmail.c | 4 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 20:32:47 | manu_basurto1@gm | 10 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
8/12/2024 22:44:28 | juan_nazgul@gmail.c | 8 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Malware | Analizadores de vulnerabilidades | Detectando automáticamente los correos de phis
11/12/2024 16:15:11 | jack.ticona1999@gm | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
Respuestas de formulario 1


Cuestionario de conocimientos previos a la aplicación del programa (respuestas)
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda
Compartir
Form_Responses1
Marca temporal | Dirección de corr | Puntuación | ¿Cuál de las siguientes afirmaciones describ | ¿Qué es un ataque de phishing? | ¿Cuál de los siguientes es un método c | ¿Qué herramienta de IA generativa puede ser | ¿De qué manera las herramientas de IA gene
11/12/2024 16:15:11 | jack.ticona1999@gm | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:15:36 | fatima.molina@gmail | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:17:02 | fio_ceci_6@gmail.cor | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:17:18 | jjprado95@gmail.con | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Escaneo de puertos | Analizadores de vulnerabilidades | Generando mensajes de correo electrónico convir
11/12/2024 16:17:36 | mgaitan_777@gmail. | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:17:50 | joearq.@gmail.com | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:17:56 | andrealarrierav@gma | 13 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Escaneo de puertos | Herramientas de encriptación | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:17:59 | ronaldthenine@gmail | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:10 | vrjulio@gmail.com | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:13 | daniucrema@gmail.c | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:23 | joseramirez88@gmai | 10 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detectando automáticamente los correos de phis
11/12/2024 16:18:24 | santi_guy@gmail.con | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:36 | gabsequeiros3@gma | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Herramientas de encriptación | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:39 | pcorderogonzales@g | 7 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:48 | brenda.melissa7@gn | 5 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:18:51 | angeles13@gmail.c | 10 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Malware | Analizadores de vulnerabilidades | Detectando automáticamente los correos de phis
11/12/2024 16:18:53 | nico_belizario@gmail | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
Respuestas de formulario 1


Cuestionario de conocimientos previos a la aplicación del programa (respuestas)
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda
Compartir
Form_Responses1
Marca temporal | Dirección de corr | Puntuación | ¿Cuál de las siguientes afirmaciones describ | ¿Qué es un ataque de phishing? | ¿Cuál de los siguientes es un método c | ¿Qué herramienta de IA generativa puede ser | ¿De qué manera las herramientas de IA gene
11/12/2024 16:18:57 | jquispelaura@gmail.c | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Generando mensajes de correo electrónico convir
11/12/2024 16:19:15 | emontes_mak@gmai | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:19:58 | colo_10_din@gmail.c | 5 / 19 | Utilizar la psicología para engañar a las personas | Intento de acceso no autorizado a un | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:20:10 | jlopex1234@gmail.cc | 9 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:22:19 | arizolaarlyn11@gmai | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:22:52 | piero-martello@gmai | 8 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:24:26 | hernesto780@gmail.c | 4 / 19 | Proteger la infraestructura física de una organizac | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detectando automáticamente los correos de phis
11/12/2024 16:25:36 | anagalvez15@gmail.c | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:25:48 | yerkoalv84@gmail.cc | 6 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Generadores de texto automáticos | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:28:12 | zsara.e@gmail.com | 7 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:30:27 | ggomez217@gmail.c | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Generando mensajes de correo electrónico convir
11/12/2024 16:32:37 | rbernabej@gmail.con | 10 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
11/12/2024 16:40:18 | ander_leyva@gmail.c | 12 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
14/12/2024 19:01:51 | hernestocuneo.r@gr | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
16/12/2024 18:12:15 | joelitosantosb77@gn | 9 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
16/12/2024 18:12:50 | darkgodxd@gmail.co | 5 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Inyección de SQL | Generadores de texto automáticos | Creando contraseñas seguras para los usuarios
16/12/2024 18:13:45 | kenji10.castro@gmai | 11 / 19 | Utilizar la psicología para engañar a las personas | Suplantación de identidad mediante c | Phishing | Analizadores de vulnerabilidades | Detecta como atacar, de acuerdo a las vulnerabili
Respuestas de formulario 1

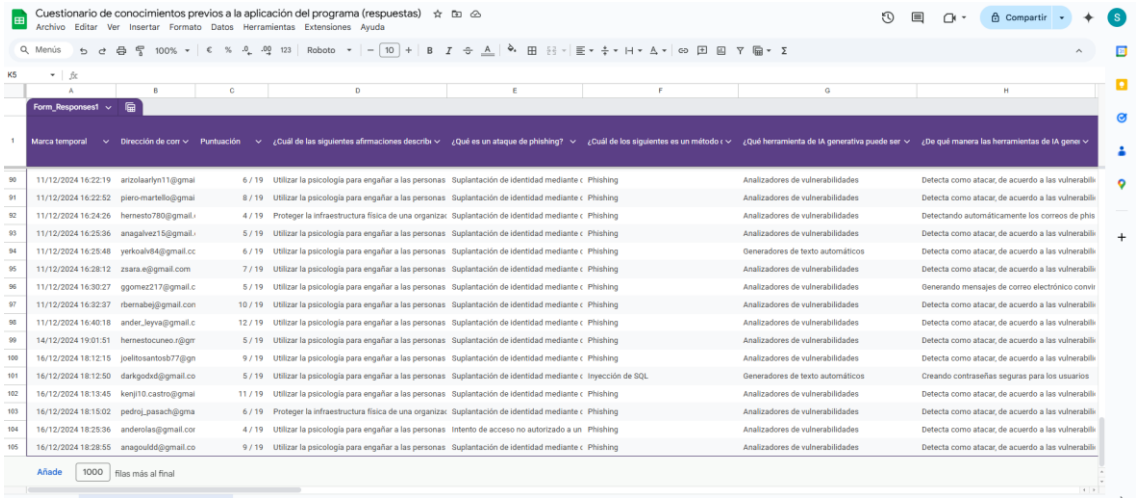
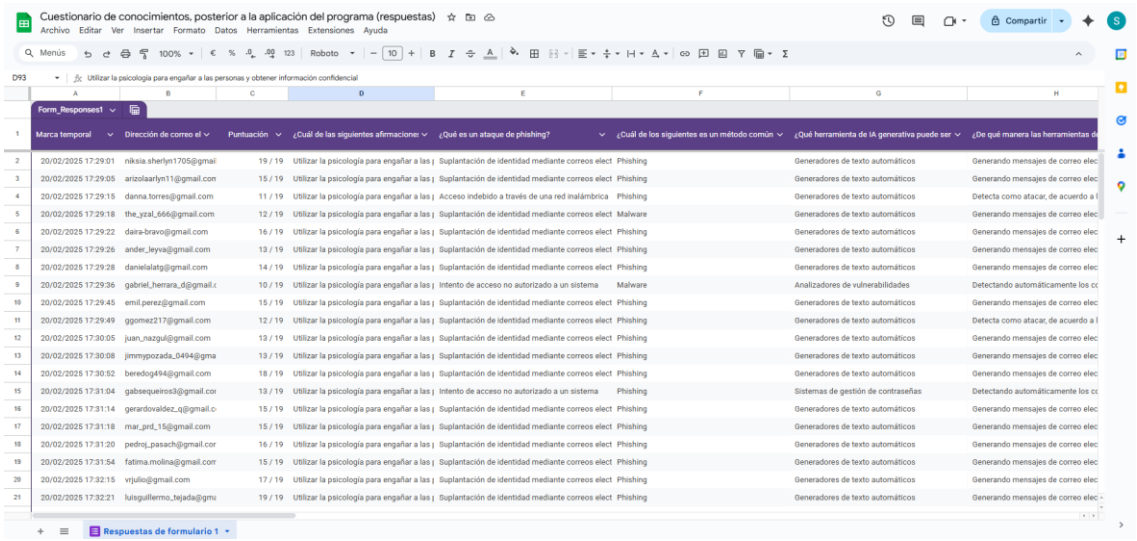
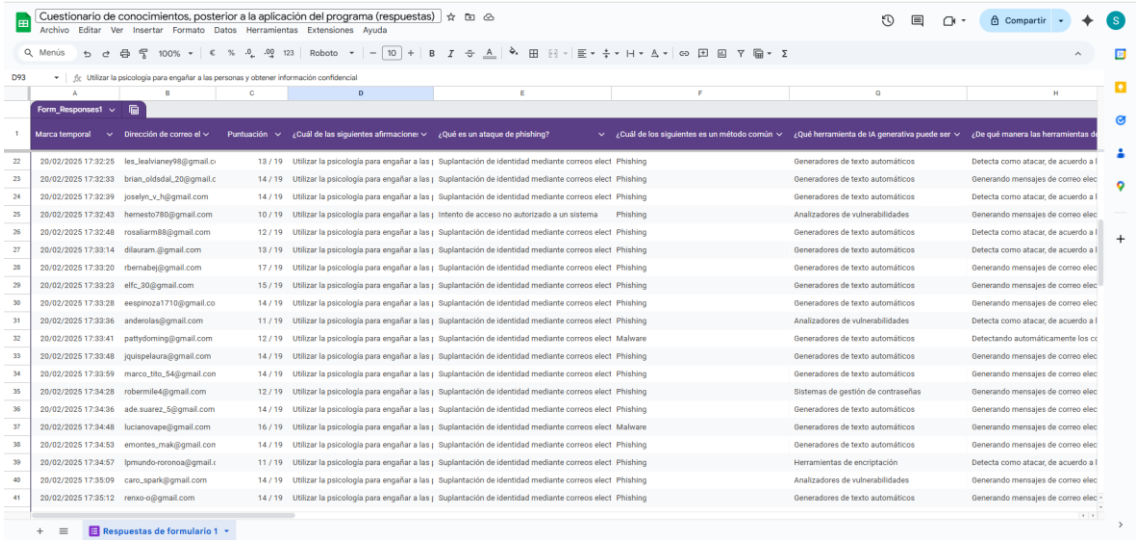
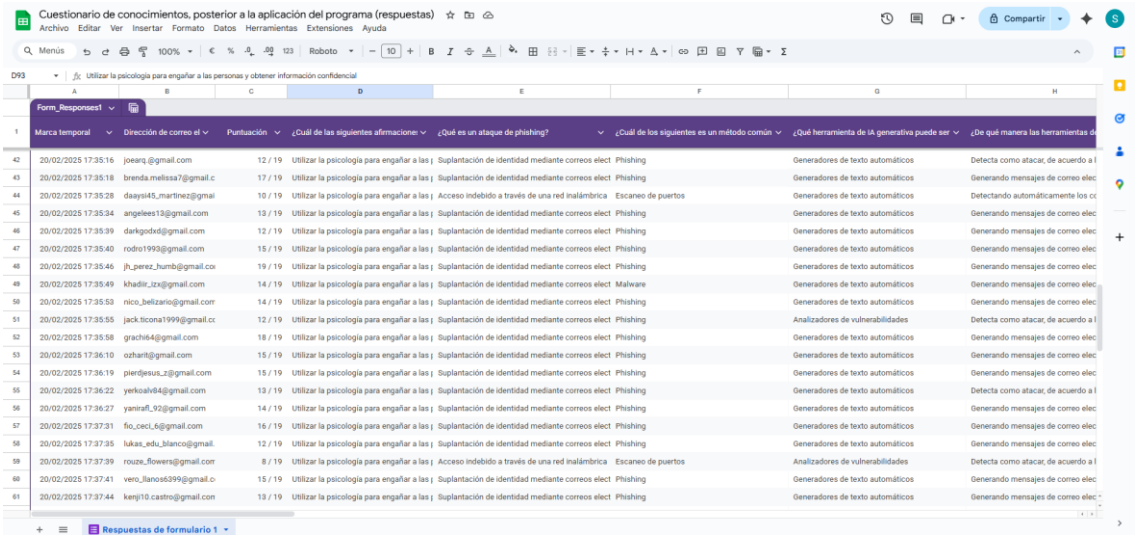


Tabla de tabulación de datos postest:







Cuestionario de conocimientos, posterior a la aplicación del programa (respuestas)

Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

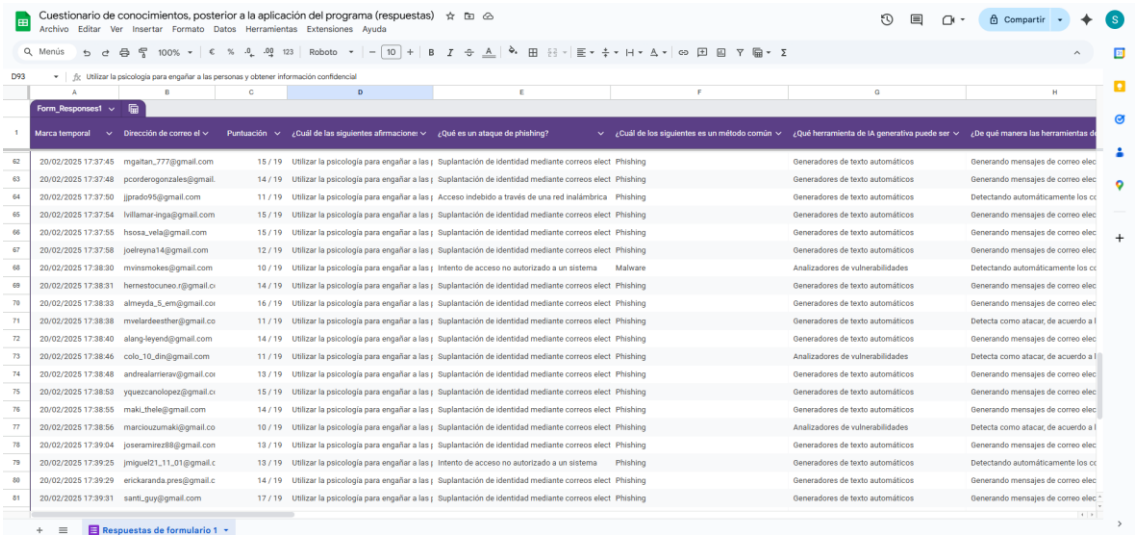
Compartir

D93 | Utilizar la psicología para engañar a las personas y obtener información confidencial

Form_Responses1

Marca temporal	Dirección de correo el	Puntuación	¿Cuál de las siguientes afirmaciones	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método común	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas
20/02/2025 17:35:16	joearq_@gmail.com	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a l
20/02/2025 17:35:18	brenda.melissa7@gmail.c	17 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:28	daaysi45_martinez@gmai	10 / 19	Utilizar la psicología para engañar a las	Acceso indebido a través de una red inalámbrica	Escaneo de puertos	Generadores de texto automáticos	Detectando automáticamente los cc
20/02/2025 17:35:34	angelees13@gmail.com	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:39	darkgodxd@gmail.com	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:40	rodro1993@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:46	jh_perez_humb@gmail.co	19 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:49	khadiir_izx@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Malware	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:53	nico_belizario@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:35:55	jack.ticona1999@gmail.cc	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:35:58	grachi64@gmail.com	18 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:36:10	ozharit@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:36:19	pierdjesus_z@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:36:22	yerkoalv84@gmail.com	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a l
20/02/2025 17:36:27	yanirafl_92@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:31	fio_ceci_6@gmail.com	16 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:35	lukas_edu_blanco@gmail.	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:39	rouze_flowers@gmail.com	8 / 19	Utilizar la psicología para engañar a las	Acceso indebido a través de una red inalámbrica	Escaneo de puertos	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:37:41	vero_llanos6399@gmail.c	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:44	kenji10.castro@gmail.com	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec

Respuestas de formulario 1



Cuestionario de conocimientos, posterior a la aplicación del programa (respuestas)

Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

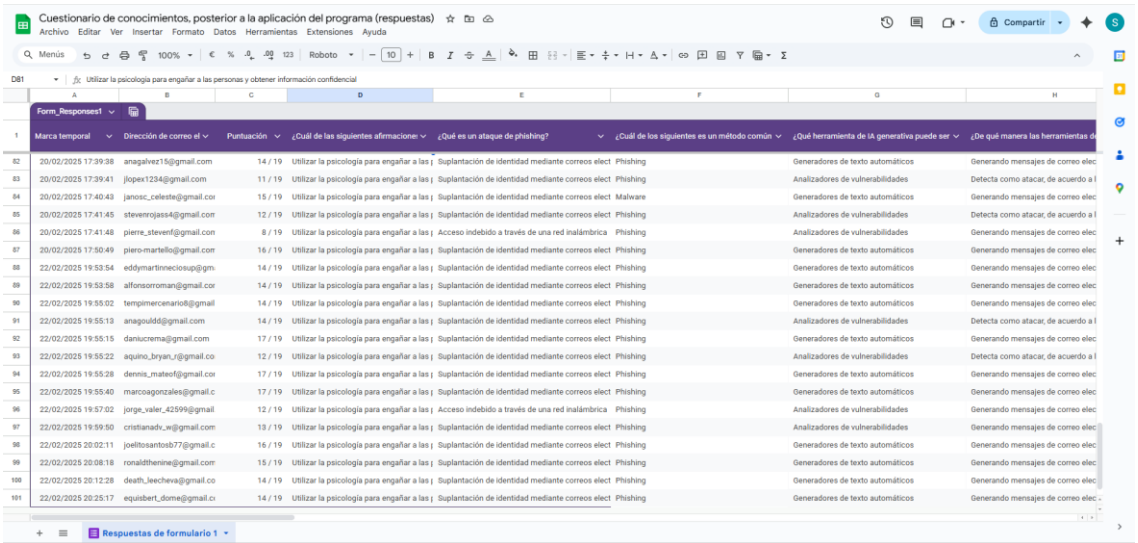
Compartir

D93 | Utilizar la psicología para engañar a las personas y obtener información confidencial

Form_Responses1

Marca temporal	Dirección de correo el	Puntuación	¿Cuál de las siguientes afirmaciones	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método común	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas
20/02/2025 17:37:45	mgaitan_777@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:48	pcorderogonzales@gmail.	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:50	jjprado95@gmail.com	11 / 19	Utilizar la psicología para engañar a las	Acceso indebido a través de una red inalámbrica	Phishing	Generadores de texto automáticos	Detectando automáticamente los cc
20/02/2025 17:37:54	lvillamar-inga@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:55	hsosa_vela@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:37:58	joelreyna14@gmail.com	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:30	mvinsmokes@gmail.com	10 / 19	Utilizar la psicología para engañar a las	Intento de acceso no autorizado a un sistema	Malware	Analizadores de vulnerabilidades	Detectando automáticamente los cc
20/02/2025 17:38:31	hernestocuneo.r@gmail.c	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:33	almeyda_5_em@gmail.co	16 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:38	mvelardeesther@gmail.co	11 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Detecta como atacar, de acuerdo a l
20/02/2025 17:38:40	alang-leyend@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:46	colo_10_din@gmail.com	11 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:38:48	andrealarrierav@gmail.co	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:53	yquezcanolopez@gmail.c	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:55	maki_thele@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:38:56	marciouzumaki@gmail.co	10 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:39:04	joseramirezll8@gmail.com	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:39:25	jmiguel21_11_01@gmail.c	13 / 19	Utilizar la psicología para engañar a las	Intento de acceso no autorizado a un sistema	Phishing	Generadores de texto automáticos	Detectando automáticamente los cc
20/02/2025 17:39:29	erickaranda.pres@gmail.c	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:39:31	santi_guy@gmail.com	17 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec

Respuestas de formulario 1



Cuestionario de conocimientos, posterior a la aplicación del programa (respuestas)

Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

Compartir

D81 | Utilizar la psicología para engañar a las personas y obtener información confidencial

Form_Responses1

Marca temporal	Dirección de correo el	Puntuación	¿Cuál de las siguientes afirmaciones	¿Qué es un ataque de phishing?	¿Cuál de los siguientes es un método común	¿Qué herramienta de IA generativa puede ser	¿De qué manera las herramientas
20/02/2025 17:39:38	anagalvez15@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:39:41	jlopex1234@gmail.com	11 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:40:43	janosc_celeste@gmail.co	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Malware	Generadores de texto automáticos	Generando mensajes de correo elec
20/02/2025 17:41:45	stevenrojass4@gmail.com	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:41:48	pierre_stevenf@gmail.com	8 / 19	Utilizar la psicología para engañar a las	Acceso indebido a través de una red inalámbrica	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
20/02/2025 17:50:49	piero-martello@gmail.com	16 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:53:54	eddymartinneciosup@gm	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:53:58	alfonsorroman@gmail.cor	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:55:02	tempimercenario8@gmail	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:55:13	anagouldd@gmail.com	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
22/02/2025 19:55:15	daniucrema@gmail.com	17 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:55:22	aquino_bryan_r@gmail.co	12 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Detecta como atacar, de acuerdo a l
22/02/2025 19:55:28	dennis_mateof@gmail.cor	17 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:55:40	marcoagonzales@gmail.c	17 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 19:57:02	jorge_valer_42599@gmail	12 / 19	Utilizar la psicología para engañar a las	Acceso indebido a través de una red inalámbrica	Phishing	Analizadores de vulnerabilidades	Generando mensajes de correo elec
22/02/2025 19:59:50	cristianadv_w@gmail.com	13 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Analizadores de vulnerabilidades	Generando mensajes de correo elec
22/02/2025 20:02:11	joelitosantosb77@gmail.c	16 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 20:08:18	ronaldthenine@gmail.com	15 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 20:12:28	death_leecheva@gmail.co	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec
22/02/2025 20:25:17	equisbert_dome@gmail.c	14 / 19	Utilizar la psicología para engañar a las	Suplantación de identidad mediante correos elect	Phishing	Generadores de texto automáticos	Generando mensajes de correo elec

Respuestas de formulario 1

Anexo 5. Validación de expertos

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. Datos generales

Ítem	Descripción	Información
1.1	Nombres y apellidos del experto	
1.2	Grado académico	
1.3	Profesión	
1.4	Institución donde labora	
1.5	Cargo que desempeña	
1.6	Denominación del instrumento	
1.7	Autor del instrumento	

II. Validación

Indicadores de evaluación del instrumento	Criterios sobre los ítems del instrumento	Muy malo (1)	Malo (2)	Regular (3)	Bueno (4)	Muy bueno (5)
1. Claridad	Están formulados con lenguaje apropiado que facilita su comprensión					
2. Objetividad	Están expresados en términos observables o medibles					
3. Consistencia	Existe una organización lógica en los contenidos y relación con la teoría					
4. Coherencia	Existe relación de los contenidos con los indicadores de la variable					
5. Pertinencia	Las categorías de respuestas y sus valores son apropiados					
6. Suficiencia	Son suficientes la cantidad y calidad de ítems presentados en el instrumento					

Sumatoria parcial: _____

Sumatoria total: _____

III. Resultados de la validación

3.1. Valoración total cuantitativa: _____

3.2. Opinión (marque con X):

Evaluación	Selección
No favorable (≤ 15 puntos)	
Debe mejorar (15 – 17 puntos)	
Favorable (≥ 18 puntos)	

IV. Mejoras recomendadas

Preguntas que el experto considera que pudieran mejorarse:

Ítem	**Descripción**
N° de la(s) pregunta(s)	
Motivos por los que se considera que pudiera mejorar	
Propuestas de mejora (modificación, sustitución o supresión)	

Lugar y fecha: _____

Firma del experto:

_____

Nombre del experto: _____

DNI: _____