UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA

Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de ingeniería social en el rubro empresarial

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

AUTORAS:

Alfaro Garbich, Vivian Elizabeth (orcid.org/0000-0002-4105-9450)

Perez Vasquez, Ana Claudia Nicole (orcid.org/0000-0001-6489-1250)

ASESOR:

Mg. Saboya Ríos, Nemias (orcid.org/0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de Servicio de Redes de Comunicación

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2023

DEDICATORIA

A mi hija Maïa que es mi impulso para salir adelante, a mi madre Elizabeth que me brindó su apoyo incondicional, a mi hermana Reyna, tía Aiza y a mi abuela Margo que siempre estuvieron dando fuerzas para que no me rindiera y a todas las personas que formaron parte del proceso.

Alfaro Garbich, Vivian Elizabeth

A mis padres, amigos y mentores, quienes han sido mi red de apoyo durante este desafiante pero enriquecedor viaje académico. Su amistad y sabios consejos han sido fundamentales. Esta tesis es un tributo a nuestra colaboración y amistad.

Perez Vasquez, Ana Claudia Nicole

AGRADECIMIENTO

Agradezco sinceramente a todos aquellos que contribuyeron a la realización de esta tesis. A nuestro asesor externo que nos orientó durante el proceso, ha sido invaluable. Este logro es también suyo. ¡Gracias por ser parte de este camino académico!

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, SABOYA RIOS NEMIAS, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial", cuyos autores son ALFARO GARBICH VIVIAN ELIZABETH, PEREZ VASQUEZ ANA CLAUDIA NICOLE, constato que la investigación tiene un índice de similitud de 19.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 18 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
SABOYA RIOS NEMIAS **DNI:** 42001721 **ORCID:** 0000-0002-7166-2197	Firmado electrónicamente por: NSABOYARI el 18-12-2023 11:25:18

Código documento Trilce: TRI - 0699736

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad de los Autores

Nosotros, ALFARO GARBICH VIVIAN ELIZABETH, PEREZ VASQUEZ ANA CLAUDIA NICOLE estudiantes de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaramos bajo juramento que todos los datos e información que acomp añan la Tesis titulada: "Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
ALFARO GARBICH VIVIAN ELIZABETH **DNI:** 71253484 **ORCID:** 0000-0002-4105-9450	Firmado electrónicamente por: VALFARO el 21-12-2023 00:38:21
PEREZ VASQUEZ ANA CLAUDIA NICOLE **DNI:** 75426493 **ORCID:** 0000-0001-6489-1250	Firmado electrónicamente por: CPEREZVA23 el 08-02-2024 11:33:02

Código documento Trilce: INV - 1475558

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

DEDICATORIA..... iii

AGRADECIMIENTO.....iv

Declaratoria de Autenticidad del Asesor.....v

Declaratoria de Originalidad del Autor / Autores.....v

ÍNDICE DE CONTENIDOS.....vii

ÍNDICE DE TABLAS..... vii

ÍNDICE DE FIGURAS.....viii

RESUMEN..... ix

ABSTRACT..... x

I. INTRODUCCIÓN..... 1

II. MARCO TEÓRICO..... 5

III. METODOLOGÍA.....24

3.1. Tipo y diseño de investigación.....24

3.2. Variables y operacionalización.....25

3.3. Población, muestra y muestreo.....26

3.4. Técnicas e instrumentos de recolección de datos.....28

3.5. Procedimientos.....29

3.6. Método de análisis de datos.....29

3.7. Aspectos éticos..... 30

IV. RESULTADOS.....31

V. DISCUSIÓN.....47

VI. CONCLUSIONES.....49

VII. RECOMENDACIONES..... 50

REFERENCIAS..... 51

ANEXOS..... 58

ÍNDICE DE TABLAS

Tabla 1. Técnicas de ataque de Ingeniería Social.....10
Tabla 2: Riesgos seleccionados para el desarrollo del producto de ingeniería.....19
Tabla 3: Lista de apartados del Anexo A.....20
Tabla 5 Limitación de la población.....26
Tabla 6. Especificación de la muestra.....27
Tabla 7 Validación por juicio de expertos.....28
Tabla 8. Estadísticos descriptivos de tasa de detección de sitios web.....31
Tabla 10. Estadísticos descriptivos de capacidad de detección temprana.....33
Tabla 11. Estadísticos descriptivos de capacidad de respuesta.....35
Tabla 12. Prueba de normalidad del indicador Tasa de Detección.....37
Tabla 13. Prueba de normalidad del indicador Capacidad de detección temprana.....38
Tabla 14 Prueba de normalidad del indicador Tiempo medio de Confirmación.....38
Tabla 15. Prueba T para dos grupos independientes de la Tasa de Detección.....40
Tabla 16. Estadístico para dos grupos independientes de la Tasa de Detección.....41
Tabla 17. Prueba T para dos grupos independientes de la Capacidad de Detección Temprana.....42
Tabla 18. Estadístico para dos grupos independientes de la Capacidad de Detección Temprana.....43
Tabla 19. Estadísticas de grupos para dos grupos independientes de Tiempo medio de confirmación.....45
Tabla 20. Estadístico de Prueba de U de Mann-Whitney del Tiempo medio de confirmación.....45
Tabla 21. Inventario de Activos.....66
Tabla 22. Valoración de activos.....67
Tabla 23. Valoración de activos según rangos.....68
Tabla 24. Probabilidad de riesgo.....69
Tabla 26. Nivel de riesgo.....70
Tabla 27. Lista de activos de información.....71
Tabla 28. Valoración de activos.....73
Tabla 29. Evaluación de riesgos.....75
Tabla 30. Riesgos seleccionados para el desarrollo del producto de ingeniería.....76
Anexo 8: Lista de controles del Anexo A de la norma ISO/IEC 27001:2013.....77
Tabla 31. Lista de controles del Anexo A de la norma ISO/IEC 27001:2013.....77
Tabla 32: Cronograma.....106

ÍNDICE DE FIGURAS

Figura 1 Modelo ontológico de los ataques de ingeniería social..... 8
Figura 2 Modelo conceptual de funcionamiento y efecto de los ataques de ingeniería social.....9
Figura 3. Circuito de ataque de Phishing para la obtención de información.....12
Figura 4 : Arquitectura de módulo de extensión de seguridad..... 14
Figura 5. Modelo de prevención de ataque de Ingeniería Social.....15
Figura 6. Modelo de prevención de ataque de Ingeniería Social.....18
Figura 7. Resultados descriptivos Tasa de detección de sitios web.....32
Figura 8. Resultados descriptivos de Capacidad de Detección Temprana.....34
Figura 9. Resultados descriptivos de Capacidad de Detección Temprana.....36

RESUMEN

El propósito principal del estudio fue implementar un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial. Para llevar a cabo la investigación, se optó por la metodología cascada y se utilizó el framework Vue.js. La evaluación se realizó en 3 indicadores: Tasa de detección, Capacidad de Respuesta y Tiempo medio de confirmación. Los resultados evidenciaron que el módulo de extensión cumplió los objetivos planteados para la detección y prevención de ataques de Ingeniería Social.

Se concluyó que el indicador tasa de detección tuvo un promedio de 91.73%, para el indicador capacidad de respuesta se obtuvo el promedio de 91,73% y por último para el indicador tiempo medio de confirmación obtuvo el promedio de 0,1320 ms, finalmente se visualizó que los indicadores obtuvieron resultados significativos y favorables gracias a la implementación del módulo de seguridad.

Palabras clave: Detección de sitios maliciosos, Capacidad de respuesta, Tiempo medio de confirmación, Ingeniería Social, Phishing,

ABSTRACT

The main purpose of the study was to implement a security extension module for the detection and prevention of Social Engineering attacks in the business sector. To carry out the research, the waterfall methodology was chosen and the Vue.js framework was used. The evaluation was carried out on 3 indicators: Detection rate, Response capacity and Average confirmation time. The results showed that the extension module met the objectives set for the detection and prevention of Social Engineering attacks.

It was concluded that the detection rate indicator had an average of 91.73%, for the response capacity indicator the average of 91.73% was obtained and finally for the average confirmation time indicator the average of 0.1320 ms was obtained. Finally, it was seen that the indicators obtained significant and favorable results thanks to the implementation of the security module.

Keywords: Detection of malicious sites, Responsiveness, Average confirmation time, Social engineering, Phishing,

I. INTRODUCCIÓN

En la actualidad, con el notable crecimiento de las redes de telecomunicación, las interacciones de los individuos con el ámbito digital han experimentado un incremento considerable. Este fenómeno posibilita que los usuarios se conecten desde cualquier ubicación a nivel global, facilitándoles el acceso a una amplia variedad de información.

Como consecuencia del uso atribuido y la voluminosa transmisión de información a través de internet, se ha observado un aumento significativo en los ataques de ingeniería social. Este fenómeno destaca la creciente vulnerabilidad que enfrenta la seguridad digital, demandando una atención especializada para mitigar los riesgos asociados. Si se habla de ingeniería social, se entiende como la persuasión a un usuario para obtener información y/o suplantar una identidad para beneficiarse de manera fraudulenta, para Fonte (2022), existen otros medios por donde suelen realizarlo como envíos de correos electrónicos no deseados con link y/o archivos adjuntos, que buscan extraer los datos de una persona como contraseñas, información personal o infectar tu equipo con un malware que luego es utilizado con el propósito de realizar extorsiones y posterior a ello liberar la información.

Es de conocimiento que los individuos involucrados en actividades ciber delictivas poseen las aptitudes necesarias para emplearlas en acciones ilícitas. La consideración de que el acceso a la información de sus víctimas puede ser utilizado en su beneficio, particularmente con propósitos de índole económica, destaca la importancia de abordar de manera rigurosa la protección de la información sensible(Pascual, 2018). Así como poseen habilidades considerablemente amplias en la identificación de vulnerabilidades con el propósito de descubrir fallos de seguridad a nivel de redes, computadoras, dispositivos móviles o servidores, estos individuos suelen perpetrar sus ataques manteniendo el anonimato, empleando técnicas de suplantación de identidad o a través de URLs maliciosas que escapan a la detección del usuario debido a la falta de conocimiento. Es por esta razón que se abordará el

estudio del ataque de phishing, el cual se fundamenta en la utilización de contenido fraudulento con la intención de inducir a la persona a caer en la trampa, posibilitando así la obtención de sus datos o cualquier tipo de información sensible. Se cuenta con diferentes tipos de phishing como el smishing que se basa en el envío de contenido por mensaje de texto, el vishing, que se realiza mediante un sistema de telefonía para obtener datos personales, el spear phishing el cual tiene como propósito vulnerar un conjunto de personas y, por último, el whaling que tiene como objetivo toda la organización y principalmente a ejecutivos (Fonte 2022).

Existen distintas herramientas para la detección de ataques de ingeniería social, como los antivirus, software que detecta y elimina virus informáticos en dispositivos infectados para contribuir en detener la propagación de contenido malicioso (Ahona Rudra 2022) , guías de estudio, test y/o simuladores, pero no todas las personas suelen utilizarlo, ya que algunos son sumamente costosos, no cuentan con una interfaz de usuario sencilla que genera dificultad para su uso o simplemente los usuarios no cuenta con el interés de aprender a cómo detectarlo por sí mismos

En el presente trabajo nos enfocamos en ayudar a la detección y prevención de ataques de ingeniería social, con una herramienta que facilite la detección temprana de contenido malicioso. Cabe mencionar que se tienen tecnologías que ayudan a la alta demanda de proceso comentado, pero son servicios que no están a disposición de todos por falta del recurso económico. A partir de lo mencionado se generan las siguientes interrogantes.

Como pregunta general: ¿Cómo contribuye la implementación de un módulo de extensión de seguridad contribuye a la detección y prevención de ataques de Ingeniería Social en el rubro empresarial? y como preguntas específicas ¿En qué medida la implementación de un módulo de extensión de seguridad favorece a la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial?, ¿De qué modo la implementación de un módulo de extensión de seguridad facilita el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial? y ¿De qué manera la implementación de un módulo de extensión de seguridad determina la

celeridad para alertar y notificar ataques web de Ingeniería Social en el rubro empresarial?

De igual modo, se presentan las justificaciones, para referir los motivos que impulsan esta investigación.

La justificación teórica se sustenta en la implementación de una extensión de seguridad para detectar ataques en el rubro empresarial con un valor teórico para prevenir el robo de datos personales y confidenciales de las empresas.

Como justificación metodológica, se optará por un enfoque que aproveche las cláusulas y controles que brinda la norma ISO/IEC 27001:2013 con respecto a los Sistemas de Gestión de la Seguridad de la Información (SGSI). Se selecciona este marco metodológico con el propósito de proteger la información que se puede adaptar a organizaciones de distintos tipos y tamaños, evaluando los tipos de riesgos que abordan la confidencialidad, integridad y disponibilidad de la información. (NQA 2015).

Para la justificación práctica se basa en la necesidad que existe de mejorar la seguridad de la información que es compartida o recibida por personas externas para prevenir el robo de información con el uso de una extensión de seguridad que mitiguen ataques.

Por otro lado, se formula el objetivo general junto con los objetivos específicos que estarán presentes durante el desarrollo del presente proyecto.

Como objetivo general: Implementar un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial. Y objetivos específicos para Determinar la eficacia de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial, Determinar la eficiencia de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial y Determinar la celeridad de un módulo de extensión de seguridad para alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

De igual manera, se evidencian las hipótesis que suponen lo que se busca en esta investigación:

En primer lugar tenemos la hipótesis general: El desarrollo de un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial. Seguidamente de las hipótesis específicas: El desarrollo de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial, El desarrollo de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial y El desarrollo de un módulo de extensión de seguridad para la celeridad de alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

II. MARCO TEÓRICO

En primera instancia tenemos a Jain y Gupta (2016) en su trabajo titulado, *A novel approach to protect against phishing attacks at client side using auto-updated whitelist* en donde proponen un enfoque novedoso contra los ataques de phishing utilizando una lista blanca actualizada automáticamente de sitios legítimos en los que un usuario suele visitar mediante algoritmos, para realizar la evaluación del desempeño del enfoque propuesto, se usaron un conjunto de datos de 1525 páginas web entre legítimas y que contiene phishing. Se aplicaron diversos experimentos para evaluar el rendimiento del sistema y compararon el propuesto con otros enfoques antiphishing populares. En esta investigación se encontró que la tasa general de verdaderos positivos del sistema fue del 86.02%, una tasa de falsos negativos del 1.48% y una exactitud del 89.38%. Concluyeron que el enfoque propuesto para protegerse en contra de ataques de phishing utilizando una lista blanca logró comprobar la legitimidad de una página web mediante las funciones de hipervínculos mostrando resultados eficaces para protegerse en contra de dichos ataques.

Seguidamente tenemos a Rao y Pais (2019), titulado *Jail-Phish: An improved search engine based phishing detection system*, que tiene como objetivo realizar el desarrollo de un sistema que detecte URL ilegítimas, dependiendo del idioma del contenido y la manera de transformar los datos para la correcta evaluación. Para realizar las pruebas y evaluar el rendimiento del sistema, utilizaron conjunto de datos reales de dos fuentes, PhishTank y Alexa, dividiéndolo en 5 conjuntos con cierta cantidad de sitios legítimos y de phishing. Utilizaron métricas de evaluación para evaluar los falsos positivos y los verdaderos positivos con respecto a los experimentos realizados. Dentro de los resultados, se evidenció que el TNR obtuvo un 99.36% según la evaluación de conjuntos legítimos populares y no populares, y un TPR del 97.77% evaluado en conjunto de phishing antiguos y nuevos. Concluyendo que al proponer una técnica heurística que utiliza resultados de motores de búsqueda y características basadas en similitudes, lograron desarrollar la técnica

propuesta para la aplicación que no solo detecta sitios phishing con registro maliciosos, sino que también detecta sitios de phishing alojados en sitios comprometidos o gratuitos.

Siguiendo el mismo contexto, tenemos a (Tan et al. 2016) con su trabajo de investigación titulado, Phish WHO: Phishing webpage detection via identity keywords extraction and target domain name finder, que tiene como objetivo realizar la identificación de características de phishing en páginas web basada en la diferencia entre la identidad objetivo y la identidad real. Se implementó un enfoque de tres fases utilizando un modelo N-gram, extracción de palabras clave y motores de búsqueda. Para realizar las pruebas experimentales, utilizaron alrededor de 10.000 páginas entre legítimas e infectadas de phishing en computadoras con especificaciones requeridas, como resultado según los tres experimentos realizados obtuvieron un valor MCC de más del 90% superando los métodos convencionales de detección de phishing. Concluyeron que la técnica de detección de páginas web con phishing logra diferenciarlos dos tipos de identidades al momento de clasificar una página.

Por otro lado, Heartfield y Loukas (2018) nos comparte su trabajo titulado, Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. El objetivo es permitir y alentar a los usuarios a detectar e informar activamente la ingeniería social. Para la evaluación experimental, utilizaron a 26 usuarios con distintos perfiles que ejecutan la herramienta dentro de un periodo de 45 días para demorar que los sensores humanos logran superar a los sistemas técnicos de seguridad, demostrando que la confiabilidad de la herramienta al obtener una tasa de detección fallida menos al 10% en comparación a los sistemas técnicos utilizados. Concluyeron que la construcción de defensas duraderas y prácticas contra ataques semánticos, es un desafío perpetuo que con ayuda del prototipo propuesto según el modelo para el diseño desarrollado en un sistema técnico HaaSS demostrando una evaluación exitosa de detección de ataques.

2.2. Bases teóricas

2.2.1. Ingeniería social

Se considera uno de los métodos más efectivos de personas malintencionadas para acceder a información utilizando psicológicamente a individuos.

Desde el punto de vista de IBM (2022) se trata de la manipulación de personas para compartir información confidencial, descargar softwares malintencionados, redirigir a webs o cometer errores que exponen sus activos personales o empresariales, además, de conocerse como la explotación de debilidades humanas llamadas “ataque informático humano”.

La ingeniería social es un ataque muy popular desde la década de 1970, que, a comparación a los ataques informáticos clásicos, como descifrado de contraseñas y la explotación de vulnerabilidades de software, los ataques de ingeniería social se centran en eludir o romper barreras de seguridad, sin la necesidad de combatir un firewall o software de antivirus (Wang, Zhu y Sun 2021).

Existe un modelo ontológico de los ataques de ingeniería social que fue propuesto por Mouton et al. (2014), para definir seis componentes que conforman un ataque.

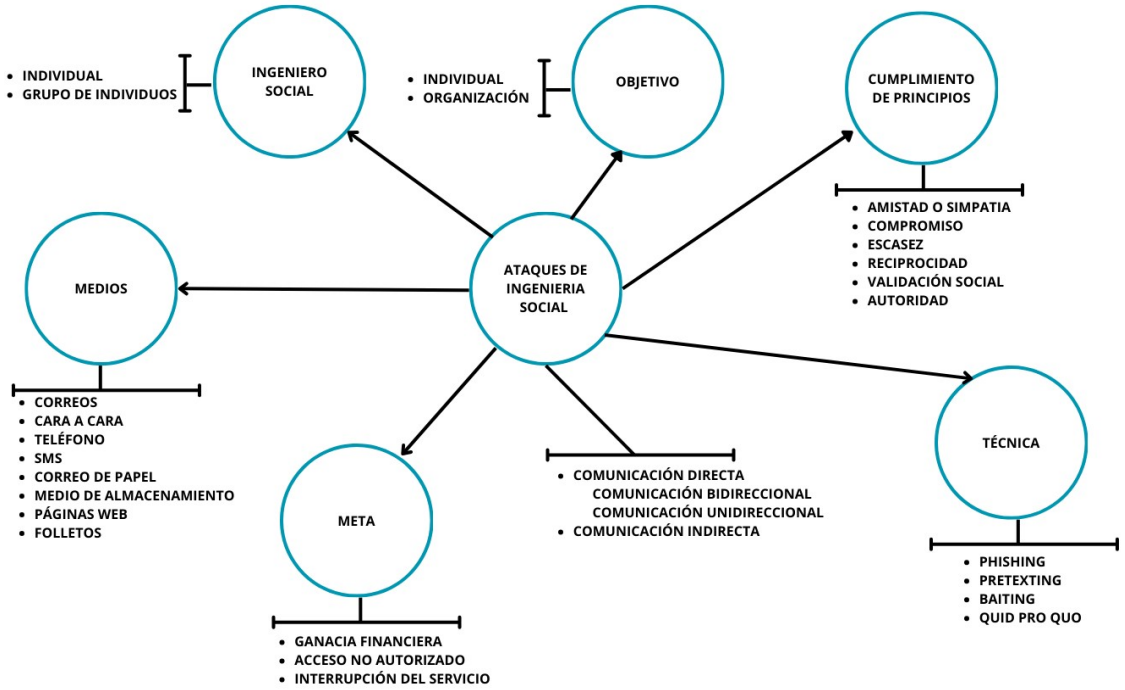


Figura 1 Modelo ontológico de los ataques de ingeniería social

Se observa en la figura 1, la relación entre los ataques de ingeniería social con los seis componentes que lo conforman; meta, se basa en las ganancias financieras, accesos no autorizados e interrupción de servicios; medios, enlaces entre el atacante y su víctima como los correos electrónicos, teléfonos, SMS, páginas web, entre otros; ingeniero social, persona que realiza el acto ya sea individual o en grupo; objetivo, es a donde va dirigido puede ser ataque personal o a nivel de organización; principio de cumplimiento, que son las maneras psicológicas utilizadas para cumplir con el objetivo y por último, las técnicas como phishing que son métodos para realizar un ataque.

Teniendo en cuenta lo planteado anteriormente, Wang, Zhu y Sun (2021) desarrollaron un modelo conceptual donde muestran tres perspectivas para comprender los ataques de ingeniería social.

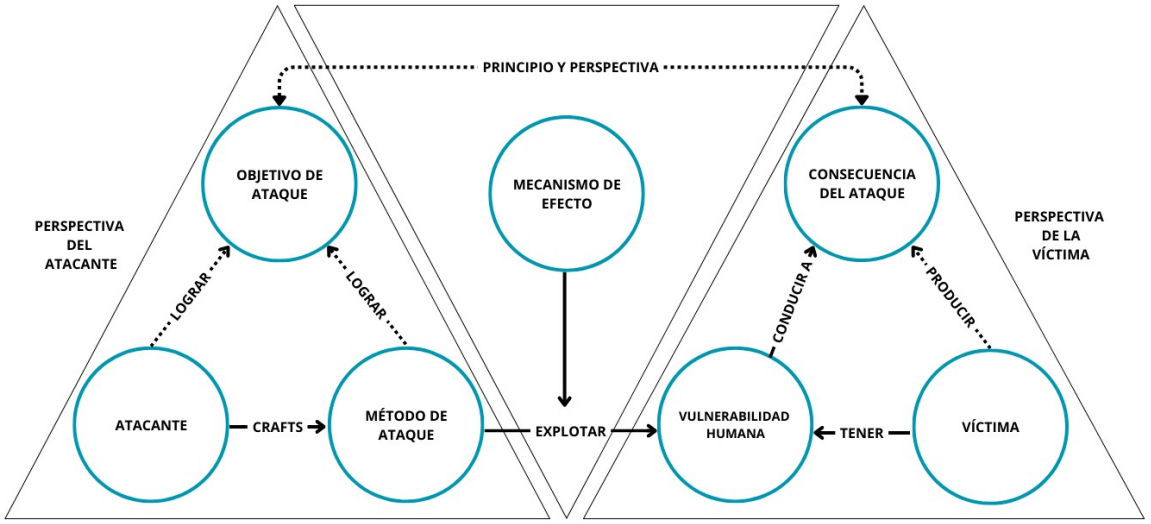


Figura 2 Modelo conceptual de funcionamiento y efecto de los ataques de ingeniería social.

- Perspectiva del atacante: es el método, modo o medio de ataques que causa directamente y afecta significativamente si este es exitoso.
- Perspectiva de la víctima: son las vulnerabilidades humanas que son la razón por la cual la víctima provoca las consecuencias del ataque.
- Perspectiva de principio y explicación: son los mecanismos de efecto que interpretan la manera en que los métodos de ataque van contra las vulnerabilidades humanas para que estas surtan efecto.

Técnicas de ataques de ingeniería social

Las técnicas de ingeniería social han evolucionado de distintas formas, con la que logran persuadir a las personas y/o empresas, por ello es sumamente importante reconocer los tipos de ataques en la ingeniería social. (HINOJOSA 2010). En la tabla 1, Zanello (2023) se describen diferentes técnicas de la Ingeniería Social.

Tabla 1. ***Técnicas de ataque de Ingeniería Social***

Técnica de ataque de Ingeniería Social	**Resumen**
Phishing	Suplantación de identidad.
Spear-phishing	Modalidad en donde los delincuentes logran convencer a las víctimas para brindar información.
Angler phishing	Basado en redes sociales, es decir, el delincuente crea un contacto falso para hacer creer a las víctimas que requieren de su ayuda.
Whaling	Se fijan en los clientes de empresas.
Tailgating	Violación de seguridad.
Baiting	Se trata de dar recompensas a la víctima para generar falsas expectativas.
Suplantación de DNS	Se trata de un envenenamiento en el caché DNS para alterar un dominio.
Pretexting	Converse a los usuarios por medio de mensajes de texto.
Correos de Spam	Se generan envíos de direcciones múltiples de correos electrónicos.
BEC	El acceso a correos electrónicos

	corporativos es uno de los métodos más peligrosos porque suplanta la identidad de un empleado.
Scareware	Técnica para asustar al usuario haciéndole creer que su dispositivo se encuentra infectado.
Tabnabbing/ Tabnabbing reverso	Se basan en ataques de páginas web, en donde el malware toma el control total del navegador
Pharming	Suele ser cuando una página web legítima la direccionan a un sitio falso para obtener credenciales.

Fuente: (Zanello 2023)

Estas técnicas se basan en un grupo de personas que mediante suplantación de páginas web, envío de correos electrónicos, llamadas telefónicas, mensajes de textos, entre otros logran obtener información confidencial de sus víctimas (Rodríguez Rincón 2018).

Técnica de Ingeniería Social: Phishing

Phishing depende de Ingeniería social y exploits técnicos que están diseñados para persuadir al usuario para que brinde información con el fin de obtener dinero. Uno de los ataques más utilizados es por medio de correos electrónicos falsos que suelen dirigirse a un URL malicioso.

Se clasifican según el servicio atacado como bancos, pasarelas de pago, juegos, ofertas, faltas de trabajo o productos. Y por modus operandi como softwares maliciosos, DNS, man in the miele phishing, entre otros (Benavides et al. 2020). En la figura 3 (Banco Central del Paraguay, 2022) nos muestra el flujo de la ejecución de un circuito de ataque con phishing.

Figura 3. ***Circuito de ataque de Phishing para la obtención de información.***

Módulo de extensión de seguridad web

Una extensión para navegadores se basa en una unidad de software que se complementa cuando se ejecuta código de alguna página, contiene filtros y controles que modifican la manera en que un usuario navega por una web o al visualizar información de un servicio web. Permiten la adaptación de funcionalidades a las necesidades o preferencias, cumplen con un solo propósito definido y fácil de comprender, además pueden eliminar características o denegar acceso a ciertos datos que pueden ser maliciosos o que el usuario puede excluir (Mozilla 2023).

Esto significa que puede potenciar cambios significativamente en una extensión de lo que puede con el código en una página web.

Estructura de una extensión

Según el MDN (2023) menciona como en el ámbito de la programación, una extensión de estructura de la siguiente manera:

- **Punto de entrada:** Tiene como un punto de entrada que es invocado por el software principal de carga. El cual permite que la extensión se registre e integre con el software existente.
- **Archivos de código:** Compone uno o varios archivos de código con las instrucciones y lógica necesaria para realizar una funcionalidad adicional.
- **Dependencias:** Para un funcionamiento adecuado, las extensiones pueden requerir otras bibliotecas, módulos o componentes. Estas dependencias generalmente se enumeran en un archivo de configuración o en los metadatos asociados para la extensión.
- **Interfaz:** Una extensión proporciona una interfaz que permite la interacción entre el software principal y sus funcionalidades adicionales. Esta interfaz puede incluir métodos, funciones, eventos, enlaces o cualquier otro mecanismo que permita al software principal interactuar y usar la extensión.

Además, consiste en un conjunto de archivos, empaquetados para una distribución e instalación correcta.

Arquitectura del módulo de extensión de seguridad propuesto.

En la figura 4 se observa el flujo que cumplirá el módulo para la detección de páginas web con phishing.

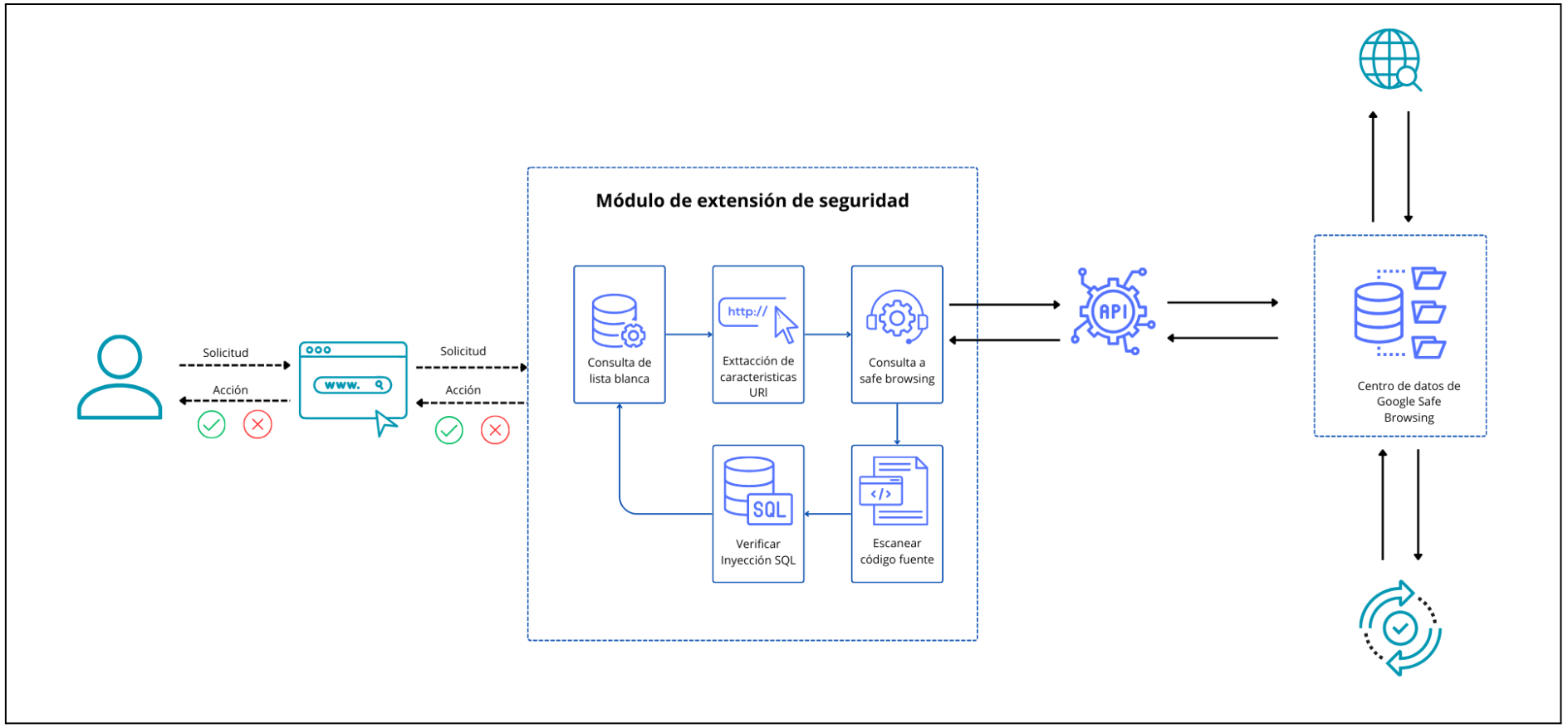


Figura 4 : Arquitectura de módulo de extensión de seguridad

Detección y Prevención de ataques de Ingeniería Social

Los ataques de Ingeniería Social son una amenaza constante, por ello para su detección se debe contar con una solución de seguridad sofisticada y configurada para evitar que caigan en algún tipo de engaño, para la prevención se recomendó la apertura enlaces o documentos de dudosa procedencia, añadirles doble autenticación a los usuarios de correos electrónicos entre otras aplicaciones (Lubeck, 2021).

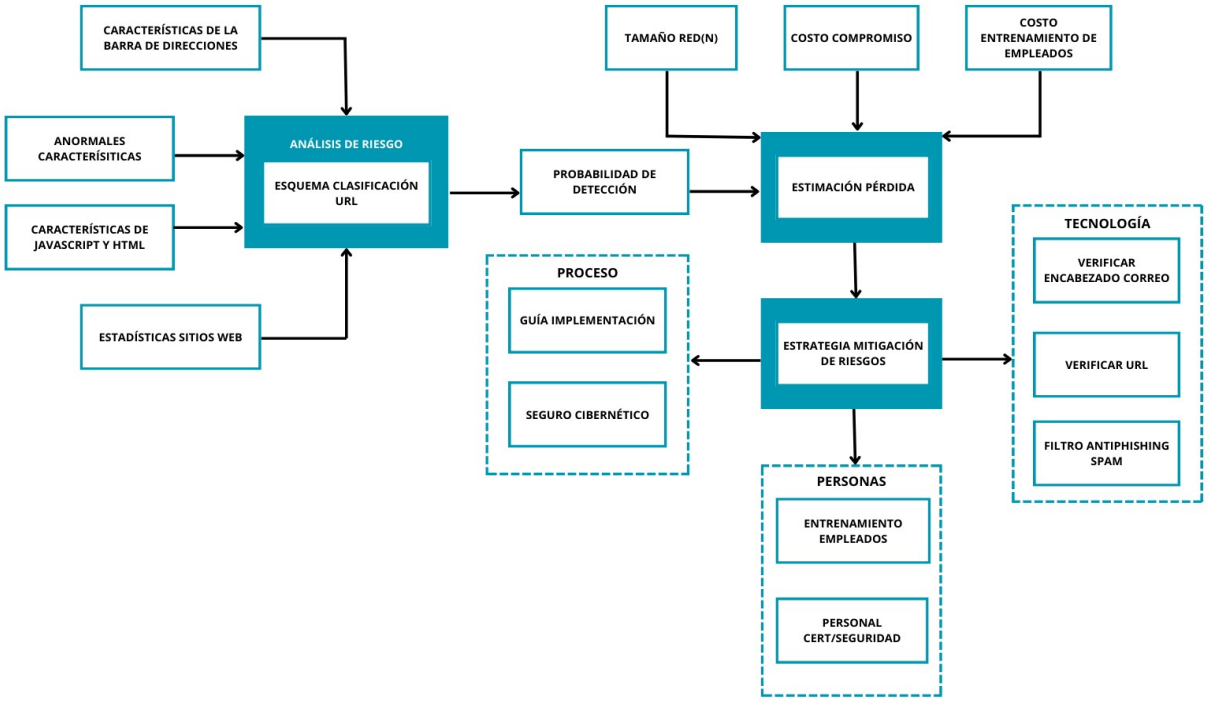


Figura 5. Modelo de prevención de ataque de Ingeniería Social

Métodos de detección y prevención

Para Sastoque (2015). La detección temprana puede utilizarse para la prevención de ataques de ingeniería social y evitar su propagación para que otras personas no sean víctimas de estafas.

La detección de ingeniería social se basa en similitud de páginas fraudulentas hacia una legítima.

Métodos no automáticos

Según López (2022**),** los métodos no automáticos incluyen diversas técnicas y enfoques, como la educación en ciberseguridad, el estudio de la ingeniería social y temas relacionados, así como el uso de modelos ontológicos para identificar estos tipos de ataques. Estos métodos comparten la característica común de la interacción del usuario para poder detectar los ataques de ingeniería social.

Métodos automáticos

Para Sawa et al. (2016),Son modelos que dependen de la interacción humana para evaluar el riesgo de un posible ataque de ingeniería social y definir el estado emocional para usar distintos métodos.

Un método conocido es el de Lansley et al. (2020) donde pretenden detectar la ingeniería social de manera automática con ayuda de lenguaje natural y redes neuronales, el cual consiste en tres pases:

- Procesamiento de datos.
- Extracción de características.
- Agregación de resultados.

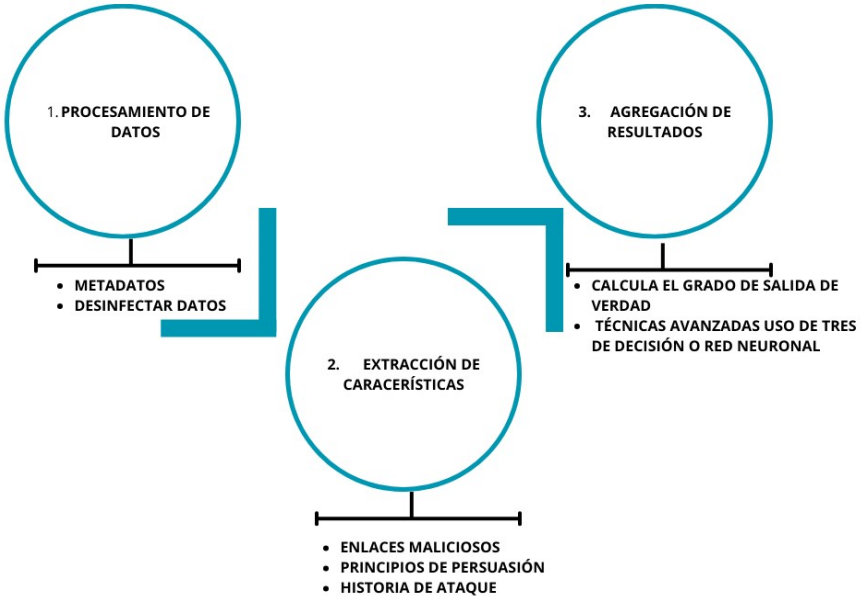


Figura 6. Modelo de prevención de ataque de Ingeniería Social.

Norma ISO/IEC 27001:2013

Es una pauta global establecida por la Organización Internacional de Normalización (ISO), que detalla las buenas prácticas para administrar la seguridad de la información dentro de una organización. La versión más reciente de esta norma fue lanzada en 2013 y se denomina ISO/IEC 27001:2013. Surgió de la integración con la norma BS7799-2. Tiene como finalidad el conseguir unos niveles de seguridad minicón y prescindibles para la gestión correspondiente. (Díaz 2010).

Estructura de la norma ISO/IEC 27001:2013

La norma ISO/IEC 27001:2013 está estructurada con cláusulas según el Ciclo Deming o PDCA, Planificar, Hacer, Comprobar y Actuar. **(Ver figura 7)**.

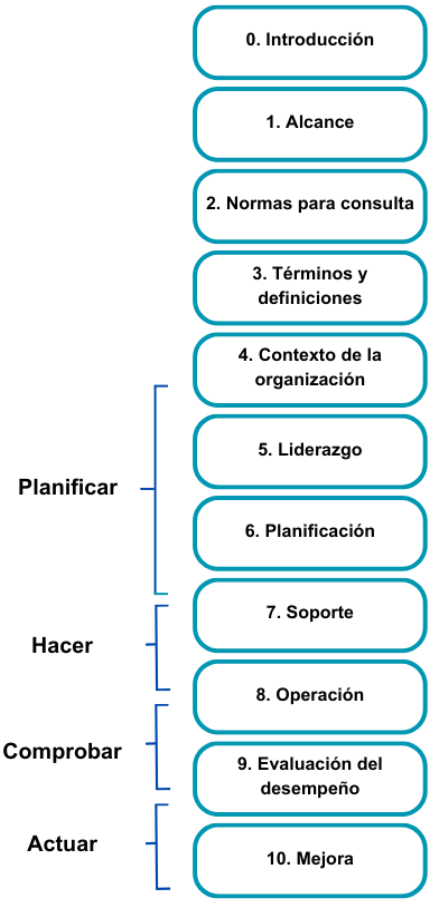


Figura 7. Modelo de prevención de ataque de Ingeniería Social

Según la NQA (2015), la norma cuenta con 10 cláusulas para su implementación, las cláusulas más importantes y obligatorias son a partir de la cuarta a la décima.

La cuarta cláusula se encarga del contexto de la organización donde se evalúan los factores internos y externos de la organización que permiten identificar los riesgos inherentes a la seguridad de los activos.

La quinta cláusula cuenta con la tarea de definir políticas de seguridad, roles y responsabilidades durante la implementación de un SGSI.

La sexta cláusula se encarga de la planificación para realizar la evaluación de riesgos y la selección de controles que son importantes al momento de la implementación.

La séptima cláusula da el soporte necesario sobre los recursos que se aplican ya sean capaces o competentes.

La octava cláusula tiene el control adecuado sobre la creación y entrega del producto o servicio según la planificación y evaluación de riesgos correspondientes.

La novena cláusula trata de la evaluación del desempeño, donde se da un seguimientos de la efectividad de los controles, se realizan auditorías internas.

Por último, la décima cláusula brinda la mejora del SGSI para evitar que ocurran eventos desafortunados de seguridad de la información.

Evaluación de riesgos

Para el desarrollo de la investigación y producto de ingeniería, nos basamos en ciertas cláusulas y controles que son parte de la norma ISO/IEC 27001:2013 que inició con la evaluación de riesgos presentados en la siguiente tabla # los cuales fueron analizados con una metodología de gestión de riesgos planteada por De la Sota Shicshie y Mechan Cristobal (2018) **(Ver anexo 2)**.

Tabla 2: ***Riesgos seleccionados para el desarrollo del producto de ingeniería***

ID	Activo	AMENAZA		OCURRENCIA		RIESGO	
		IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
SW-003	Lista de instalaciones de software	Alto	3	Probable	3	9	E
D-001	Lista de cuentas bancarias	Alto	3	Probable	3	9	E
D-002	Estados financieros	Alto	3	Probable	3	9	E
D-003	Informes contables	Alto	3	Probable	3	9	E
D-004	Proyecciones financieras	Medio	2	Probable	3	6	E
D-00	Contratos con	Alto	3	Probable	3	9	E

6	clientes y proveedores						
D-007	Lista de contraseñas	Alto	3	Probable	3	9	E

Fuente: Elaboración propia

Controles del Anexo A de la norma ISO/IEC 27001:2013

La norma cuenta con 114 controles que se encuentran agrupados en 14 apartados subdivididos en áreas de seguridad. (Escuela Europea 2023).

Tabla 3: ***Lista de apartados del Anexo A***

ID	Apartados
A.5	Políticas de Seguridad de la Información
A.6	Organización de la Gestión de SI
A.7	Recursos Humano
A.8	Gestión de Activos
A.9	Controles de Acceso
A.10	Criptografía
A.11	Seguridad Física y Ambiental
A.12	Seguridad de las Operaciones
A.13	Comunicaciones
A.14	Mantenimiento del sistema
A.15	Proveedores
A.16	Incidentes de Seguridad de la Información
A.17	Continuidad del Negocio
A.18	Cumplimiento

Fuente: Elaboración propia

Para el desarrollo de la investigación se evaluaron los 114 controles y fueron seleccionadas las siguientes **(Ver anexo 10)**.

Metodología Cascada

La metodología en cascada constituye un enfoque en la gestión de proyectos caracterizado por su proceso lineal y secuencial. Este método, ampliamente reconocido en la ingeniería de software y denominado como ciclo de vida de desarrollo de software (SDLC), ha extendido su aplicación al desarrollo de productos.(Pressman 2009)

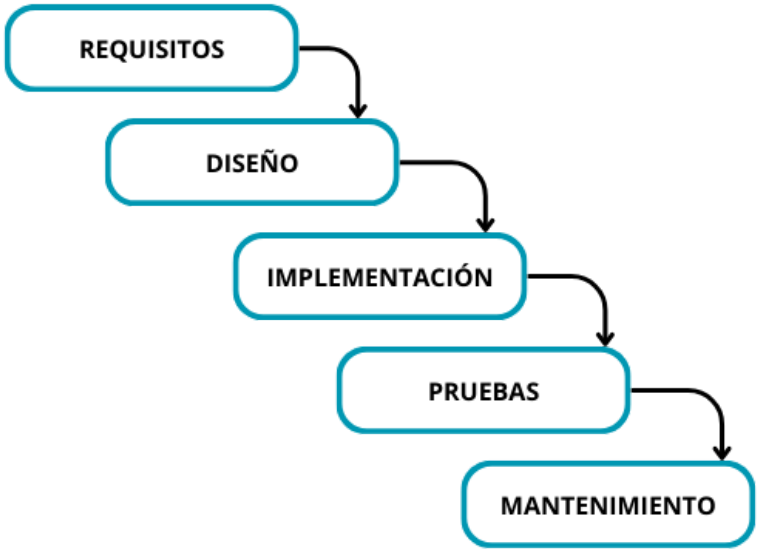


Figura 8. *Modelo del ciclo de vida en Waterfall*

2.3. Marco conceptual

Pyme

Las pymes, tanto a nivel local como global, han obtenido una importancia muy considerable en el sector económico actualmente en

numerosos países. Los cuales muestran un gran interés en reforzar y fortalecer a las empresas y sean más competitivas, siendo consideradas como impulsores fundamentales del desarrollo económico. Esta atención se refleja en un incremento significativo en los índices de empleo, producción y comercio, gracias al crecimiento y progreso de las pymes (Bolaños 2019).

Métricas de evaluación

Para evaluar el rendimiento del módulo de extensión, se aplica siente tradicionales métricas que estarán establecidas de acuerdo con cada dimensión planteada.

Según Rao y Pais (2019) las métricas se dividen de la siguiente manera.

- **Detection Rate** (DR) que viene a ser el porcentaje de sitios con phishing predichos correctamente entre el número total de sitios phishing (TP)

$$DR = \frac{TP}{TP+FN} * 100$$

Dónde:
TPR: Tasa de verdaderos positivos
TP: Verdaderos positivos
FN: Falsos negativos

- **Precisión** (pre) cálculo de predicción legítima y correcta de los sitios de phishing con el total de sitios web.

$$Pre = \frac{TP}{TP+FP}$$

Dónde:
TP: Verdaderos positivos
FN: Falsos negativos

Para la medición del indicador, alertar y notificar, se evaluará desde la capacidad de respuesta para lo cual, se utiliza la siguiente fórmula.

Según Atlassian (2020) es una métrica útil para dar seguimiento de la capacidad de respuesta que tiene un sistema, software o equipo. Se mide de la siguiente manera: La capacidad de respuesta es igual a la suma de los tiempos y la confirmación de recepción dividido por el número de eventos.

$$MTTA = \frac{Suma\ de\ los\ tiempos\ de\ respuesta}{Número\ total\ de\ eventos\ de\ respuesta}$$

Dónde:

MTTA: Tiempo medio de confirmación de recepción

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de Investigación

El proyecto de investigación es de tipo aplicada con enfoque cuantitativo ya que partimos de un objetivo que resolver para evidenciar la manera en que ayudaría el desarrollo de este para mejoras futuras. Para Risco (2020), una investigación aplicada está orientada a conseguir conocimientos nuevos que estén destinados a soluciones de problemas prácticos (p. 3).

Investigación Aplicada

Según Baena (2017), nos explica que una investigación aplicada tiene como objetivo llevar la teoría a la práctica para resolver un problema en corto tiempo y de manera concreta.

Enfoque Cuantitativo

Hernández, Fernández y Baptista (2014) nos dice que el enfoque cuantitativo se basa en la descripción, explicación, comprobación de teorías, que se recopilan para interpretar la información. Dicho enfoque se analiza utilizando herramientas de estadísticas, el objetivo principal es obtener los resultados y generalizables para la recopilación de datos.

3.1.2. Diseño de Investigación

En un diseño preexperimental, se seleccionan grupos de participantes que ya existen que están bajo observación considerando factores de causa y efecto. Por eso, Hernández, Fernández y Baptista (2014) nos aclara que los diseños preexperimentales consisten en realizar dos tipos de pruebas a un grupo designado para evaluar sus conocimientos antes y después del estímulo o experimento.

Se realizará un estudio de caso con una sola medición que para Hernández, Fernández y Baptista (2014) consiste en la administración del estímulo del grupo a trabajar y luego al momento de aplicar la medición según la variable.

En este caso se realizará el tercer diseño preexperimental que trata de la comparación con un grupo estático, para establecer el efecto de X. El diseño preexperimental de comparación con grupo estático es un enfoque de investigación utilizado en la psicología y otras disciplinas para evaluar el impacto de una intervención o tratamiento en un grupo de sujetos. (Campbell y Stanley 1995)

$$\begin{array}{ll} X & O_1 \\ \hline & O_2 \end{array}$$

Dónde:

x = Variable independiente

O1 y O2 = Mediciones de ambos grupos

3.2. Variables y operacionalización

Definición Conceptual

- **Variable independiente: Módulo de extensión de seguridad**

  Según Redacción (2023), son programas instalados dentro de un navegador web que agrega funciones y características para mejorar la experiencia de un usuario al navegar. Están diseñadas por lenguajes como HTML, css y JavaScript.

- **Variable dependiente: Detección y prevención de ataques de ingeniería social**

  Según Berenguer (2018) La identificación y prevención de ataques web de ingeniería social se enfoca en detectar y contrarrestar métodos empleados por los atacantes para psicológicamente influir en los usuarios y obtener datos confidenciales o llevarse a acciones dañinas. Estos ataques se sustentan en la explotación de la confianza, la persuasión y la manipulación emocional de las personas.

Definición Operacional

Variable independiente: Módulo de extensión de seguridad

Es la combinación de elementos lógicos necesarios para llevar a cabo una solución práctica a un problema específico, al mismo tiempo las extensiones proporcionan características que son ampliamente solicitadas por los usuarios en su vida diaria.

Variable dependiente: Detección y prevención de ataques de ingeniería social

La capacidad de la extensión para identificar y clasificar sitios web que contienen código malicioso o intentan engañar a los usuarios mediante técnicas de ingeniería social de acuerdo con el monitoreo constante durante la actividad del usuario y las alertas que se evidencian durante el uso.

3.3. Población, muestra y muestreo

Población

Según Luis (2004), la población se refiere a un conjunto de personas o a un grupo de individuos que comparten características que pueden ser objeto de estudio.

La población escogida en el presente estudio se ha determinado por la cantidad de registros realizados en las “Fichas de observación” y dicha cantidad no está definida. **(Ver tabla 5)**.

Tabla 5 *Limitación de la población*

VARIABLES	INDICADORES	POBLACIÓN
Detección y prevención de ataques web de Ingeniería Social	Tasa de detección de sitios web con phishing	Registro estimado de ataques de ingeniería social en un tiempo determinado de dos semanas o 15 días.
	Capacidad de detección temprana	
	Capacidad de respuesta	

Fuente: Elaboración propia

Muestra

Según Diaz (2018), nos manifiesta que la muestra se define como una porción o subgrupo de la población o universo en estudio, que representa y comparte las mismas características que la población en general. En el actual estudio, la muestra está delimitada por la cantidad de registros hechos en las "Fichas de observación" (Ver tabla 3)

***Tabla 6**. Especificación de la muestra*

VARIABLE	INDICADORES	TÉCNICA	INSTRUMENTO	MUESTRA
Detección y prevención de ataques web de Ingeniería Social	Tasa de detección de sitios web con phishing	Fichaje	Ficha de registro	Cantidad de registros que se evidencian
	Capacidad de detección temprana	Fichaje	Ficha de registro	
	Capacidad de respuesta	Fichaje	Ficha de registro	

Fuente: Elaboración propia

Muestreo

De acuerdo con Hernández y Mendoza (2018), la unidad de muestreo se refiere al tipo de caso seleccionado para el estudio, y es común que coincida con la unidad de análisis, que es la responsable de generar los datos o información que será analizada a través de métodos estadísticos.

En el presente informe se va a usar el muestreo no probabilístico, con el que se tomarán los resultados que se darán en el periodo de tiempo establecido. Además, se utilizará un muestreo intencional el cual consiste en seleccionar los elementos que son convenientes para la investigación, al ser uno de los más

sencillos, caracterizándose por el esfuerzo para obtener muestras representativas y por ser la más económica (Martínez 2017).

3.4. Técnicas e instrumentos de recolección de datos

Técnicas: Fichaje

Se denomina una técnica para investigaciones por su cierta serie de datos de las variables que no están referidos al tema lo que da valor propio. Permitiendo la recopilación de datos, facilitando la selección, el orden y la organización (Berrocal 2017).

Instrumento: Ficha de registro

Se utilizará una ficha de registro para la recolección de datos según el tiempo propuesto líneas que serán evidenciadas como un monitoreo presencial durante el uso de la extensión para medir la variable dependiente.

Validez

Según Medina y Verdejo (2020) la validez hace referencia al nivel en el que la teoría y la evidencia respaldan los estudios en base a los puntajes de un instrumento de medición o prueba para el uso de los propuestos.

Tabla 7 ***Validación por juicio de expertos***

EXPERTO	FICHAS DE REGISTRO		
	Tasa de detección de sitios web con phishing	**Capacidad de detección temprana**	**Capacidad de respuesta**
Mg. Nemias Saboya Ríos	98%	98%	98%

Fuente: Elaboración propia

3.5. Procedimientos

Luego de definir la metodología, variables y estudios similares de apoyo que sustenten lo diseñado, se continuó con los pasos a seguir de la investigación.

Se realizó el manejo de la herramienta elaborada con un grupo de participantes de distintas áreas de la empresa Consorcio Digital. Para ello se emitió una carta de presentación al gerente explicando el motivo de la investigación que posteriormente fué aprobada y sustentada con una carta de aceptación. Se realizaron las coordinaciones correspondientes en una reunión virtual con el gerente y los participantes para definir los deadlines y explicar las fases que se tomarán en cuenta para obtener la recolección de los datos en las fichas de observación definidas pasos atrás.

En un periodo de dos semanas, se monitoreo de manera presencial y virtual cada área comprometida para verificar el funcionamiento de la herramienta y así obtener un control de los datos que seguidamente fueron evaluados respectivamente. Cada documento presentado se encuentra en los anexos de esta investigación.

3.6. Método de análisis de datos

Para el análisis del proyecto se utilizó el descriptivo - comparativo, a través de gráficos como barras o líneas. Se hizo el uso de pruebas no paramétricas para las pruebas de hipótesis según el comportamiento que se obtenga de los datos. Según Ochoa y Yunkor (2019), nos explica que un estudio descriptivo es un tipo de investigación cuantitativa que se enfoca en una única variable de estudio, conocida como variable de interés. Dado que este estudio es univariado, es importante tener en cuenta los factores que influyen en su entorno. Estos factores suelen denominarse "factores de caracterización" ya que están relacionados con la variable de interés y se obtienen de la población en estudio.

Seguidamente tenemos a Tonon (2011) , que nos explica que el método comparativo es un procedimiento para revisar dos o más variables enunciadas en dos o más objetos, por un tiempo contemplado. De esta manera se relacionarán las unidades geopolíticas, instituciones, procesos, etc.

Por otro lado, Chesniuk (2021) menciona que las pruebas no paramétricas se basan en la clasificación o categorización de los datos, lo que puede resultar en una disminución de la precisión de la información al cambiar de datos sin procesar a una clasificación relativa.

Según el diseño preexperimental de comparación de un grupo estático, se utilizará la prueba de U de Mann-Whitney el cual se emplea para la comparación de dos muestras independientes con variables cuantitativas (Romero, 2013).

3.7. Aspectos éticos

Justificamos esta investigación con originalidad, discreción y autenticidad, cuidando el bienestar de los participantes que ayudaron con la obtención de datos para el desarrollo de los resultados presentados.

Cumple con el compromiso de seguir los lineamientos y reglamentos establecidos por la Universidad César Vallejo y la resolución del consejo universitario N°0340-2021-UCV y N°200-2018-UCV.

La información plasmada diferentes autores, investigadores y escritores que han sido citados en los puntos dentro de antecedentes, bases teóricas y conceptos que sustentaron para punto de la investigación, fueron recopilados de bibliotecas digitales reconocidas como Google scholar, Scopus, ScienceDirect, con una redacción de acuerdo con la normativa iso 690.

Por último, se confirmará la autenticidad con programas de verificación de plagio para evidenciar la ética profesional.

IV. RESULTADOS

4.1 Resultados descriptivos

4.1.1 Resultados descriptivos de tasa de detección de sitios web con phishing

De acuerdo con el primer indicador sobre la tasa de detección y el análisis exploratorio que realizamos con ambas herramientas en la tabla 8, la N es la cantidad de días de evaluación en dónde se evidenció una desviación estándar en la herramienta propuesta dónde obtuvo el 1,99 indicando la variabilidad en los datos y que se encuentran correctamente agrupadas alrededor de la media, en cambio con la herramienta externa alcanzó un 4,75, indicando así una mayor dispersión. Además, la herramienta propuesta logró un promedio de 91.73% demostrando que el módulo de seguridad cumple con el objetivo de detectar de manera eficiente en comparación con la herramienta externa que solo obtuvo el 62, 33% en la detección de sitios web con phishing.

Tabla 8. ***Estadísticos descriptivos de tasa de detección de sitios web***

Tasa de detección	Herramienta Propuesta	Herramienta Externa
N	15	15
Media	91,7353	62,4071
Mediana	91,5493	62,3377
Moda	87,65	55,00
Desv. Desviación	1,99651	4,75885
Mínimo	87,65	55,00
Máximo	95,35	72,00

Fuente: Elaboración propia

Asimismo, en la figura 9, que corresponde al indicador de la tasa de detección, se evidencian los datos obtenidos mediante la aplicación de ambas herramientas. Se presenta de color azul la herramienta propuesta y de color rojo

la herramienta externa, del mismo modo se añadieron marcadores para realizar hincapie en las fechas presentadas en el eje X. Es notable un aumento en el nivel de detección después de implementar la herramienta propuesta. Este hallazgo sugiere que la tasa de detección ha alcanzado el objetivo establecido, indicando así la eficacia de la herramienta propuesta. Este resultado respalda la efectividad de la solución implementada para mejorar la detección en comparación con la herramienta previamente utilizada.

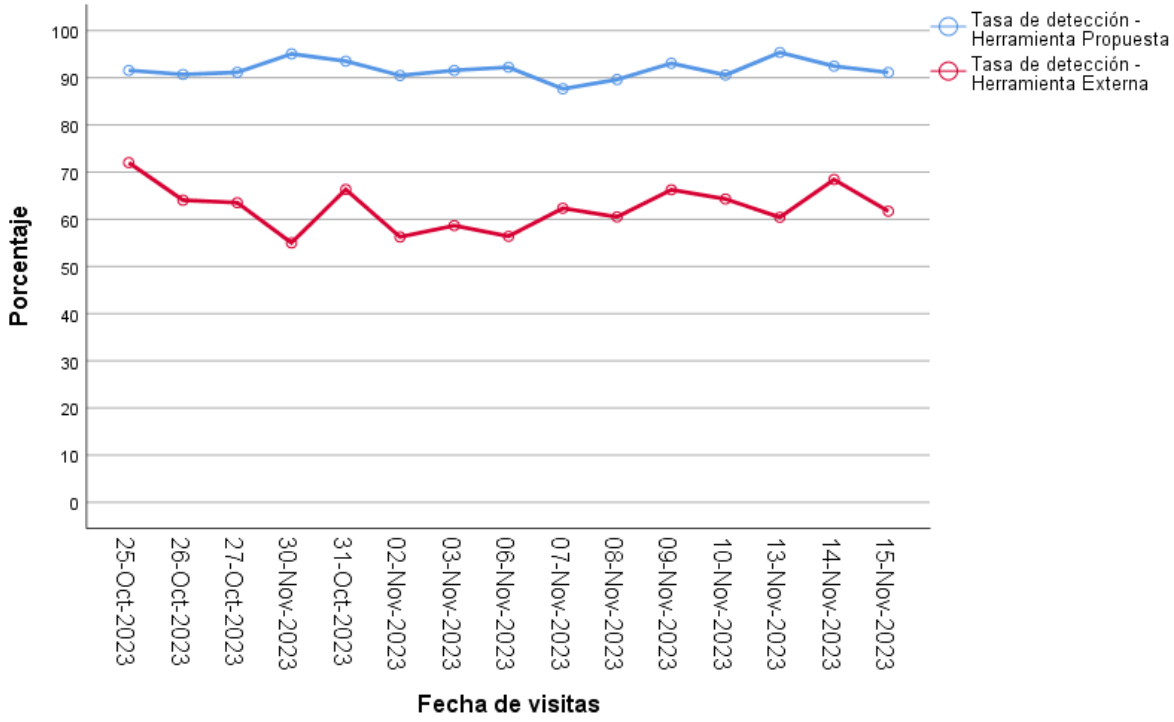


Figura 9. Resultados descriptivos Tasa de detección de sitios web

4.1.2 Resultados descriptivos de capacidad de detección temprana

Según el análisis exploratorio con ambas herramientas para el indicador de capacidad de detección temprana, en la tabla 10 la N es la cantidad de días de evaluación en dónde indica una desviación estándar en la herramienta propuesta dónde obtuvo el 1,99 indicando la variabilidad en los datos y que se encuentran correctamente agrupadas alrededor de la media, en cambio con la herramienta externa alcanzó un 4,75, indicando así una mayor dispersión. Además, la herramienta propuesta logró un

promedio de 91.73% demostrando que el módulo de seguridad cumple con el objetivo de detectar de manera eficiente en comparación con la herramienta externa que solo obtuvo el 62, 33% en el indicador mencionado.

Tabla 10. Estadísticos descriptivos de capacidad de detección temprana

Capacidad de detección temprana	Herramienta Propuesta	Herramienta Externa
N	15	15
Media	0,9462	0,3450
Mediana	91,5493	62,3377
Moda	87,65	55,00
Desv. Desviación	1,99651	4,75885
Mínimo	87,65	55,00
Máximo	95,35	72,00

Fuente: Elaboración propia

Asimismo, en la figura 10, correspondiente al indicador de capacidad de detección temprana, se presentan los datos recopilados mediante ambas herramientas. Se presenta de color azul la herramienta propuesta y de color rojo la herramienta externa, del mismo modo se añadieron marcadores para realizar hincapie en las fechas presentadas en el eje X. Se observa un aumento notable en la capacidad de detección temprana después de la implementación de la herramienta propuesta. Este incremento muestra que la herramienta ha logrado cumplir el objetivo planteado, mejorando significativamente la capacidad de detectar eventos en las primeras fases. Este hallazgo respalda la eficacia de la solución implementada y destaca su contribución positiva a la detección temprana en comparación con la herramienta anteriormente utilizada.

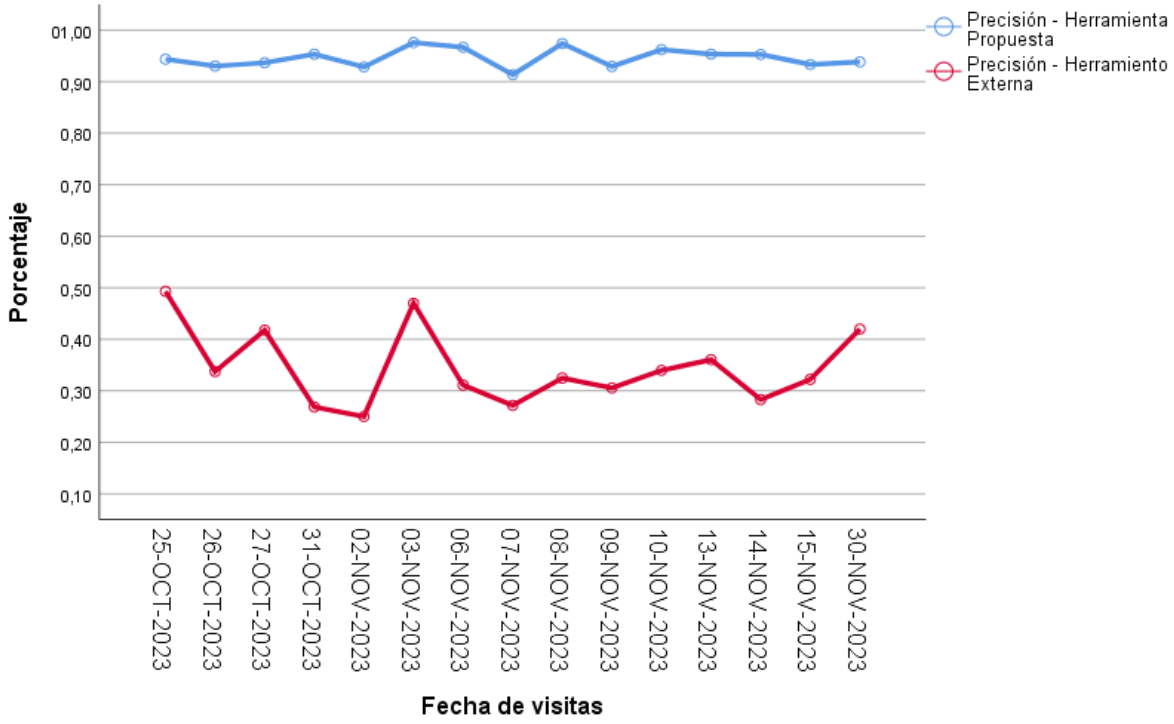


Figura 10. Resultados descriptivos de Capacidad de Detección Temprana

4.1.3 Resultados descriptivos de capacidad de respuesta

En base al análisis exploratorio con ambas herramientas para el indicador de capacidad de respuesta, en la tabla 11 la N es la cantidad de días de evaluación, en dónde muestra una desviación estándar en la herramienta propuesta dónde obtuvo el 0,1320 que está representado en milisegundos mostrando que el tiempo es más corto de alerta y notificación, en cambio la herramienta externa alcanzó un 0,4372 ms., indicando así una mayor tiempo estimado en la capacidad de respuesta al usuario. Por esta razón, la herramienta propuesta logró un promedio de 0,7971 ms. demostrando que el módulo de seguridad cumple con el objetivo de alertar y notificar al usuario de manera eficiente en comparación con la herramienta externa que solo obtuvo el 1,1137 en el indicador mencionado.

Tabla 11. ***Estadísticos descriptivos de capacidad de respuesta***

Capacidad de respuesta	Herramienta Propuesta	Herramienta Externa
N	15	15
Media	0,7971	1,1137
Mediana	0,7969	1,2398
Moda	0,53	0,49
Desv. Desviación	0,13204	0,43720
Mínimo	0,53	0,49
Máximo	0,93	1,52

Fuente: Elaboración propia

De igual manera, en la figura 11. correspondiente al indicador de capacidad de respuesta, se presentan los datos recopilados mediante ambas herramientas. Se presenta de color azul la herramienta propuesta y de color rojo la herramienta externa, del mismo modo se añadieron marcadores para realizar hincapie en las fechas de evaluación presentadas en el eje X. Se percibe que la herramienta propuesta se mantiene muy cerca entre 0.5s hasta los 0.9s el tiempo medio de confirmación de alerta y notificación al usuario, mientras que la otra herramienta va desde los 0.5s hasta el 1,50 min dando a destacar que la herramienta propuesta cumple con el objetivo establecido de alertar y notificar en el menor tiempo posible en comparación con la herramienta externa.

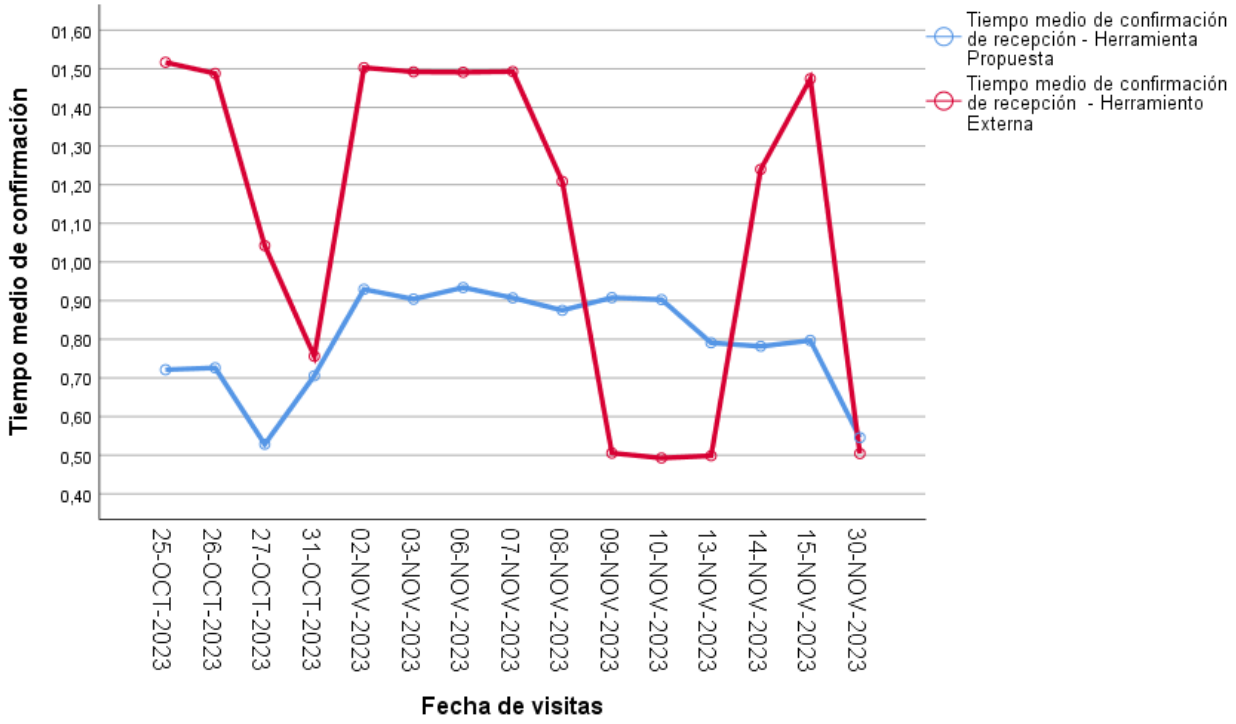


Figura 11. Resultados descriptivos de Capacidad de Detección Temprana

4.2 Resultados inferenciales

4.2.1. Planteamiento de la hipótesis de normalidad

Según (Kwak y Park 2019), una hipótesis estadística se refiere a la suposición de un parámetro poblacional, puede ser cierta o no. Las hipótesis suelen ser nulas y alternativas. Se utiliza para un experimento estadístico que pruebe la validez de la hipótesis.

Ho: La información presentada no refleja una distribución normal

Hα: La información presentada refleja una distribución normal

Análisis de normalidad de Shapiro-Wilk

Para la presente investigación se utilizó el desarrollo de las pruebas de normalidad de Shapiro-Wilk, debido a que las muestras empleadas eran menor a 30, por tal motivo se realizan los siguientes contrastes de hipótesis, validando que los datos cumplan o no, la distribución normal (Dietrichso 2019), para los indicadores de detección de sitios maliciosos, monitoreo y prevención en tiempo real y alertar y notificar, que cumplan con tener un valor menor al $\alpha = 0.05$, se usarán las pruebas no paramétricas de U de Mann-Whitney, correspondiente a los datos obtenidos con la población, por otro lado, si algún indicador presenta un valor mayor a $\alpha = 0.05$ se emplearán las pruebas paramétricas de T de Student para muestras independientes. Las pruebas mencionadas se realizaron con el programa SPSS 25, contando con un nivel de confiabilidad del 95% y la herramienta Microsoft Excel.

En la tabla 12, se evidencia los datos extraídos de la prueba de normalidad, con el indicador de Tasa de Detección de Sitios Maliciosos

Tabla 12. ***Prueba de normalidad del indicador Tasa de Detección***

Tasa de Detección de Sitios Maliciosos	**Kolmogorov-Smirnov**			**Shapiro-Wilk**		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Herramienta Propuesta	0,134	15	0,200	0,967	15	
Herramienta Externa	0,097	15	0,200	0,977	15	

Fuente: Elaboración propia

Debido a que los grupos muestran valores mayores (sig> 0.05), se procede a utilizar la prueba paramétrica de T de Student, para muestras independientes.

Asimismo, en la tabla 13, se visualizan los datos extraídos de la prueba de normalidad, con el indicador de Capacidad de detección temprana

Tabla 13. ***Prueba de normalidad del indicador Capacidad de detección temprana***

Capacidad de detección temprana	**Kolmogorov-Smirnov**			**Shapiro-Wilk**		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Herramienta Propuesta	0,133	15	0,200	0,959	15	0,671
Herramienta Externa	0,195	15	0,200	0,916	15	0,165

Fuente: Elaboración propia

Debido a que los grupos muestran valores mayores (sig> 0.05), se procede a utilizar la prueba paramétrica de T de Student, para muestras independientes.

De igual modo, en la tabla 14 se visualizan los datos extraídos de la prueba de normalidad, con el indicador de tiempo medio de confirmación

Tabla 14 ***Prueba de normalidad del indicador Tiempo medio de Confirmación***

Tiempo Medio de Confirmación	**Kolmogorov-Smirnov**			**Shapiro-Wilk**		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Herramienta Propuesta	0,189	15	0,155	0,865	15	0,028
Herramienta Externa	0,262	15	0,007	0,777	15	0,002

Fuente: Elaboración propia

Como se visualiza en la tabla 14, los grupos contiene valores diferentes (sig<0.05), en el cuál la herramienta propuesta obtuvo el resultado de 0,028; mientras que la herramienta externo tuvo un sig de 0.002, entonces se opta por utilizar la prueba no paramétrica de la U de Mann-Whitney

Contraste de Hipótesis de Detección de Sitios Maliciosos

Contraste de hipótesis de tasa de detección de sitios web con phishing

Ho: El desarrollo de un módulo de extensión de seguridad no es efectivo para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial

Ha: El desarrollo de un módulo de extensión de seguridad si es efectivo para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial

Nivel de confianza

La investigación considera un nivel de confianza del 95%, también debe contar con un nivel de significancia del α = 0.05

Regla de decisión

Se rechaza la H0, si el sig<0.05

Se acepta la Ho, si el sig>0.05

Prueba estadística:

La siguiente prueba estadística es empleada en la presente investigación, luego de realizar los análisis de los supuestos, dicha prueba es la prueba de T de Student, correspondiente a muestras independientes, de tal manera que la formulación se presentará de la siguiente manera.

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{(n_1-1)S_1^2+(n_2-1)S_2^2}{(n_1-1)+(n_2-1)}\left(\frac{1}{n_1}+\frac{1}{n_2}\right)}}$$

Resultados del estadístico de prueba usando el SPSS 25

El siguiente resultado estadístico se desarrolló la comparación entre ambos grupos de estudio que se visualizan en la tabla 15. Este resultado evidencia que el promedio de la herramienta externa antes de implementar el módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social mostró el siguiente valor ($\bar{x} = 61,783$), notando así un valor menor al análisis del uso del módulo de extensión seguridad con la herramienta propuesta ($\bar{x} = 90,817$). Estos resultados permiten evidenciar de manera favorable la detección de sitios maliciosos durante los 15 días de ejecución en la empresa.

Tabla 15. ***Prueba T para dos grupos independientes de la Tasa de Detección***

Indicador	Media	N	Desv. Desviación	Desv. Error promedio
Herramienta Propuesta	90,817	15	1,976	0,510
Herramienta Externa	61,783	15	4,711	1,216

Fuente: elaboración propia

Por otro lado, en la tabla 16, se muestran los resultados inferenciales que se obtuvieron tras realizar la prueba de T de Student para muestras relacionadas, en dónde el estadístico de la prueba sig = 0.000 < α = 0.05, resultado que evidencia que existen diferencias significativas entre la herramienta propuesta que obtuvo un promedio de 90,817 y la herramienta con un 61,783, dicho estudio es favorable hacia el investigador apoyando así la hipótesis plantado en el presente estudio.

Tabla 16. ***Estadístico para dos grupos independientes de la Tasa de Detección***

Indicador	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza				
				Inferior	Superior			
Herramienta Propuesta	90,817	1,976	0,510	89,723	91,912	177,955	14	0,000
Herramienta Externa	61,783	4,711	1,216	59,174	64,392	50,789	14	0,000

Fuente: elaboración propia

Por lo tanto, se procede a rechazar la hipótesis nula, a favor de la hipótesis alterna, asimismo validando las resultados de los grupos que demostraron que existen datos diferentes y así aceptando del desarrollo de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial

Contraste de Hipótesis de Monitoreo y prevención en tiempo real

Contraste de hipótesis de Capacidad de detección temprana

Ho: El desarrollo de un módulo de extensión de seguridad no es efectivo para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial

Ha: El desarrollo de un módulo de extensión de seguridad es efectivo para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial

Nivel de confianza

La investigación considera un nivel de confianza del 95%, también debe contar con un nivel de significancia del $\alpha = 0.05$

Regla de decisión

Se procede a rechazar la Ho si el valor de significancia es menor a 0.05

Por otro lado se acepta la Ho si el valor de significancia es mayor a 0.05

Prueba estadística:

La siguiente prueba estadística es empleada en la presente investigación, luego de realizar los análisis de los supuestos, dicha prueba es la prueba de T de Student, correspondiente a muestras independientes, de tal manera que la formulación se presentará de la siguiente manera.

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{(n_1-1)S_1^2+(n_2-1)S_2^2}{(n_1-1)+(n_2-1)}\left(\frac{1}{n_1}+\frac{1}{n_2}\right)}}$$

Resultados del estadístico de prueba usando el SPSS 25

El siguiente resultado descriptivo se desarrolló realizando la comparación entre ambos grupos de estudio que se visualizan en la tabla 17. Este resultado evidencia que el promedio de la Herramienta Externa antes de implementar el módulo de extensión de seguridad para monitorear y prevención en tiempo real de ataques de Ing Social mostró el siguiente valor ($\bar{x} = 0,344$), notando así un valor menor al análisis del uso del módulo de extensión seguridad con la herramienta propuesta ($\bar{x} = 0,946$). Estos resultados permiten evidenciar de manera favorable la capacidad de detección temprana durante los 15 días de ejecución en la empresa.

Tabla 17. *Prueba T para dos grupos independientes de la Capacidad de Detección Temprana*

Indicador	Media	N	Desv. Desviación	Desv. Error promedio
Herramienta Propuesta	0,946	15	0,018	0,004
Herramienta Externa	0,344	15	0,073	0,019

Fuente: elaboración propia

Por otro lado, en la tabla 18, se muestran los resultados inferenciales que se obtuvieron tras realizar la prueba de T de Student para muestras relacionadas, en dónde el estadístico de la prueba sig = 0.000 < α = 0.05, resultado que evidencia que existen diferencias significativas entre la herramienta propuesta que obtuvo un promedio de -93,669 y la herramienta con un -34,150, dicho estudio es favorable hacia el investigador apoyando así la hipótesis plantado en el presente estudio.

Tabla 18. *Estadístico para dos grupos independientes de la Capacidad de Detección Temprana*

Capacidad de Detección Temprana	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza				
				Inferior	Superior			
Herramienta Propuesta	-93,669	1,816	0,468	-94,675	-92,663	-199,751	14	0,000
Herramienta Externa	-34,150	7,314	1,888	-38,201	-30,099	-18,081	14	0,000

Fuente: elaboración propia

Por tal motivo, se procede a rechazar la hipótesis nula, a favor de la hipótesis alterna, asimismo validando las resultados de los grupos que demostraron que existen datos diferentes y así aceptando El desarrollo de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial.

Contraste de Hipótesis de Alertar y notificar

Contraste de hipótesis de Capacidad de respuesta

Ho: El desarrollo de un módulo de extensión de seguridad no es efectivo para la celeridad de alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

Ha: El desarrollo de un módulo de extensión de seguridad es efectivo para la celeridad de alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

Nivel de confianza

La investigación considera un nivel de confianza del 95%, también debe contar con un nivel de significancia del α = 0.05

Regla de decisión

Se procede a rechazar la Ho si el valor de significancia es menor a 0.05

Por otro lado se acepta la Ho si el valor de significancia es mayor a 0.05

Prueba estadística:

La siguiente prueba estadística es empleada en la presente investigación, luego de realizar los análisis de los supuestos, dicha prueba es la prueba de T de Student, correspondiente a muestras independientes, de tal manera que la formulación se presentará de la siguiente manera.

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{(n_1-1)S_1^2+(n_2-1)S_2^2}{(n_1-1)+(n_2-1)}\left(\frac{1}{n_1}+\frac{1}{n_2}\right)}}$$

Resultados del estadístico de prueba usando el SPSS 25

En el siguiente resultado descriptivo se realizó la comparación de ambos grupos de estudio que se visualizan en la tabla 19. El cual nos permitió evidenciar el promedio de los grupos entre la herramienta propuesta con un promedio de 223 puntos, en comparación de la herramienta externa que tuvo 262 puntos, el cual evidencia que el tiempo de respuesta es menor durante los 15 días de ejecución en la empresa.

Tabla 19. *Estadísticas de grupos para dos grupos independientes de Tiempo medio de confirmación*

Indicador		Nº	Rango promedio	Suma de rangos
Tiempo medio de Confirmación	Herramienta Propuesta	15	13.13	223
	Herramienta Externa	15	15.53	262
	Total	30		

Fuente: elaboración propia

Por otro lado, se visualiza la prueba estadística realizada en la tabla 20, el cual refleja una diferencia significativa entre los grupos de estudio (herramienta propuesta y herramienta externa), el resultado nos muestra el valor Z = -2,556 que es beneficioso para la alerta y notificación en la capacidad de respuesta, de tal manera evidencia el valor del sig=0.008 < α = 0.05, indicando así que los datos mostrados entre los grupos presentan distintos resultados, el cual es favorable para el presente estudio luego de la implementación del módulo de extensión de seguridad

Tabla 20. *Estadístico de Prueba de U de Mann-Whitney del Tiempo medio de confirmación*

Pruebas estadísticas	Capacidad de respuesta
U de Mann-Whitney	70
W de Wilcoxon	310,000
Z	-2,556
Sig. asintótica(bilateral)	0.008

Fuente: elaboración propia

En ende, se procede a rechazar la hipótesis nula, a favor de la hipótesis alterna, asimismo validando las resultados de los grupos que demostraron que existen datos diferentes y así aceptando el desarrollo de un módulo de extensión de seguridad para la celeridad de alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

V. DISCUSIÓN

Durante la ejecución de esta investigación, se tuvo como objetivo el implementar un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial y la relación con los indicadores planteados, obteniendo una sig<0,05 de acuerdo a las pruebas paramétricas y no paramétricas que se realizaron durante el análisis inferencial, demostrando que la herramienta propuesta cumple con cada uno de los indicadores con respecto a la detección y prevención de ataques web.

Estos resultados demuestran que es factible el correcto rechazo de la hipótesis nula y la aceptación de la alternativa cumpliendo, evidenciando la correcta funcionalidad de la herramienta durante un proceso de ataques web de ingeniería social.

Estos resultados son respaldados por los estudios relacionados a nuestra investigación. Donde Jain y Gupta (2016), realizaron un enfoque de detección de phishing en páginas web basado en una lista blanca actualizada que clasificaba sitios con phishing y sitios legítimos con la implementación de algoritmos y reglas heurísticas que identificaban ciertas características, esto ayudó a que puedan comprobar la legitimidad de los sitios visitados y protegerse de ataques. Dicha mejora, se relaciona con la capacidad de detectar sitios maliciosos.

Por otro lado, tenemos a Rao y Pais (2019) el cual planteó un sistema detector de URL ilegítimas basándose en la extracción de URL y código fuente del sitio web para realizar un análisis correcto del sitio y tomar la decisión de si es una página legítima o no con técnicas heurísticas que ayudaron a que la detección de manera efectiva se realice de manera temprana. Esto nos ayuda a verificar que cumplimos con la capacidad de detección planteada.

Además crearon una herramienta de detección basado en la extracción de palabras claves que ayudaron a la identificación de páginas ilegítimas en el cual realizaron pruebas exhaustivas en distintos experimentos donde la herramienta logra detectar y diferenciar las páginas de prueba.

VI. CONCLUSIONES

En el proceso de la investigación se ha concluido con lo siguiente:

1. Tras la implementación del módulo de seguridad se ha determinado la eficacia en la detección de sitios relacionados con ataques de Ingeniería Social en el rubro empresarial. Asimismo, los datos estadísticos que se recopilaron en el proceso de evaluación respaldan la afirmación, demostrando así la capacidad significativa para la identificación de amenazas en sitios web.
2. En el proceso de determinar la eficiencia del módulo en el monitoreo y la prevención en tiempo real se evidenció el desempeño de la recolección de datos, la capacidad de la extensión para identificar y contrarrestar ataques de Ingeniería Social de manera inmediata fue el factor clave para que se pueda fortalecer la seguridad en el rubro empresarial
3. Por consiguiente en el módulo de extensión para alertar y notificar ataques web de Ingeniera Social se validó con datos estadísticos para identificar la rapidez del sistema en detectar y comunicar amenazas. La capacidad de respuesta contribuye significativamente ante potenciales riesgos de seguridad.

Por último, la implementación del módulo de extensión de seguridad ha cumplido con éxito los objetivos propuestos en la investigación. Los resultados que se obtuvieron respaldan la eficacia, eficiencia y celeridad del sistema, consolidándose como una herramienta clave para fortalecer la seguridad web en el rubro empresarial frente a los ataques de Ingeniería Social.

VII. RECOMENDACIONES

Luego de los datos obtenidos en el proceso de la investigación sobre la implementación del módulo de extensión de seguridad para la detección y prevención de ataque de ingeniería Social en el rubro empresarial

Basándonos en la conclusión de la celeridad del módulo, se recomienda poder establecer un sistema de monitoreo proactivo, es decir, este enfoque nos permitirá anticipar posibles cambios en las tácticas de Ingeniería Social asegurando una respuesta aún más rápida y efectiva.

La mejora continua del módulo para establecer un proceso de optimización, correspondiente a la dinámica cambiante de las amenazas en los sitios web, realizar actualizaciones periódicamente para que se pueda adaptar a diferentes tácticas de Ingeniería Social y se pueda garantizar una protección efectiva y constante hacia amenazas emergentes.

Con respecto a las alertas y notificación ante sitios web maliciosos, considerar optimizar procesos en tiempo real y asegurar una respuesta rápida y eficaz

En línea con la eficacia del módulo, es recomendable mantener registros detallados de las actividades del sistema y realizar auditorías periódicas, esto no solo respaldará la validez de las alertas, si no que facilitará la identificación de patrones y la mencionada mejora continua.

Asimismo con el objetivo de mejorar la detección ante los sitios maliciosos, se sugiere realizar simulacros de manera periódica sobre ataques de Ingeniería Social, esta evaluación permitirá evaluar la respuesta del módulo e identificar áreas de mejora y ajuste.

REFERENCIAS

AHONA RUDRA, 2022. ¿Cómo protegerse de los ataques de ingeniería social? [en línea]. [consulta: 11 junio 2023]. Disponible en: https://powerdmarc.com/es/social-engineering-attacks-protection/.

ATLASSIAN, 2020. MTBF, MTTR, MTTF, MTTA: comprensión de las métricas de incidentes. *Atlassian* [en línea]. [consulta: 2 julio 2023]. Disponible en: https://www.atlassian.com/es/incident-management/kpis/common-metrics.

BAENA, 2017. *Metodologia de la Investigación* [en línea]. 3ra. S.l.: s.n. Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf.

BANCO CENTRAL DEL PARAGUAY [@BCP_PY], 2022. Alerta sobre fraudes ¡Conocé el circuito de un ataque de #Phishing, qué información roban y cuáles son los principales medios de propagación de sus mensajes! #SupervisiónBancaria https://t.co/QlgMa5uSHB. *Twitter* [en línea]. [consulta: 11 junio 2023]. Disponible en: https://twitter.com/BCP_PY/status/1534532454073131014.

BENAVIDES, E., FUERTES, W., SANCHEZ, S. y NUÑEZ-AGURTO, D., 2020. Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, vol. 13, no. 1, ISSN 1390-4043. DOI 10.18779/cyt. v13i1.357.

BERENGUER, D., 2018. Estudio de metodologías de ingeniería social. [en línea], Disponible en: https://openaccess.uoc.edu/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf.

BERROCAL, A., 2017. Técnicas del fichaje. [en línea]. [consulta: 21 junio 2023]. Disponible en: https://www.slideshare.net/AbrahamBerrocalPedre/tcnicas-del-fichaje.

BISWAS, B. y MUKHOPADHYAY, A., 2017. Detección de phishing y pérdida computacional modelo híbrido: Un enfoque de aprendizaje automático. *ISACA* [en línea]. [consulta: 11 junio 2023]. Disponible en:

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/phishing-detection-and-loss-computation-hybrid-model-a-machine-learning-approach.

BOLAÑOS, C.A.P., 2019. Actualidad de la gestión empresarial en las pymes. *Apuntes Contables*, no. 24, ISSN 2619-4899. DOI 10.18601/16577175.n24.03.

CAMPBELL, D. y STANLEY, J., 1995. *Diseños experimentales y cuasi experimentales en la investigación social*. Argentina: s.n. ISBN 950-518-042-X.

CHESNIUK, 2021. Pruebas no paramétricas. *MetroQuimica Net* [en línea]. [consulta: 25 junio 2023]. Disponible en: https://metroquimica.net/blogs/news/pruebas-no-parametricas.

DIAZ COBOS, J.G., 2016. *INGENIERÍA SOCIAL Y LOS DELITOS INFORMÁTICOS EN LA COMPAÑÍA INSTRUMENTAL Y ÓPTICA CÍA. LTDA*. Amabato, Ecuador: Universidad tecnologica indoamérica.

DIAZ, N., 2018. Población Y Muestra.,

FONTE, A., 2022. Técnicas de ingeniería social: así atacan al eslabón más débil de la ciberseguridad. [en línea]. [consulta: 10 junio 2023]. Disponible en: https://derechodelared.com/tecnicas-de-ingenieria-social/.

GOMEZCOELLO, R. y MISHELL, J., 2020. Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos.,

HERNÁNDEZ, R., FERNÁNDEZ, C. y BAPTISTA, M., 2014. *Metodologia de la Investigación* [en línea]. 6. Mexico: Punta Santa Fe. ISBN 978-1-4562-2396-0. Disponible en: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf.

HERNÁNDEZ, R. y MENDOZA, C., 2018. METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA. [en línea], ISSN 978-1-4562-6096-5. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/64591365/Metodolog%C3%ADa_de_la_investigaci%C3%B3n._Rutas_cuantitativa__cualitativa_y_mixta-libre.pdf?1601784484=&response-content-disposition=inline%3B+filename%3DMETODOLOGIA_DE_LA_INVESTIGACION_LAS_RUTA.pdf&Expires=1686980889&Signature=bGTgCkZ44rqTTelpoGhKth0r77NXAeovj870j0OpWCs0EG7RqZFIvixDZtucbobSlIciLLba4EvDmZ4TxUvNxTCzygZjC

9Lfoh~4pGcrj4zkja1a53rrXhz027fTVUcI1HoEUhqotXoR4TitHhwFzcvIka
FMsAWrAkDPekkdKW5cnxuDK2LT27Wxp75yndT1B814EKJf6B~KbttMH
2mza0xjpvG7X86Neiu20xags42XQ1CiOe1Dr1LTvcaq6L2fDnl3jcXdgLno
veRG-wHWDzqEIZVWjtBhE80az9oW3fknGmInYW6iFrczGo6~Jnnm4wh
YOV-Q6e-Ke8ZfaDLRYA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.

HINOJOSA, L., 2010. *ESTUDIO DEL GRADO DE INCIDENCIA DE LA INGENIERÍA SOCIAL EN LA PRIMERA FASE DE LOS ATAQUES INFORMÁTICOS QUE SE REALIZAN ACTUALMENTE EN LAS EMPRESAS PRIVADAS DEL ECUADOR* [en línea]. Quito, Ecuador: s.n. Disponible en: https://repositorio.uisek.edu.ec/bitstream/123456789/547/1/TESIS_GABRIELA_HINOJOSA.pdf.

IBM, 2022. ¿Qué es la ingeniería social? | IBM. [en línea]. [consulta: 11 junio 2023]. Disponible en: https://www.ibm.com/es-es/topics/social-engineering.

LANSLEY, M., MOUTON, F., KAPETANAKIS, S. y POLATIDIS, N., 2020. SEADer++: social engineering attack detection in online environments using machine learning. *Journal of Information and Telecommunication* [en línea], vol. 4, no. 3, [consulta: 11 junio 2023]. ISSN 2475-1839. DOI 10.1080/24751839.2020.1747001. Disponible en: https://doi.org/10.1080/24751839.2020.1747001.

LOPEZ, J., 2022. IMPLEMENTACIÓN DE MODELO COMPUTACIONAL PARA LA DETECCIÓN DE INGENIERIA SOCIAL BASADO EN APRENDIZAJE DE MAQUINA Y PROCESAMIENTO DE LENGUAJE.,

LUBECK, L., 2021. En 2020 se duplicaron las detecciones de ataques de ingeniería social. *WeLiveSecurity* [en línea]. [consulta: 11 junio 2023]. Disponible en: https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/.

LUIS, P., 2004. POBLACIÓN MUESTRA Y MUESTREO. *Punto Cero*, vol. 09, no. 08, ISSN 1815-0276.

MARTÍNEZ, D.V., 2017. MUESTREO PROBABILÍSTICO Y NO PROBABILÍSTICO.,

MAYO, C., 2022. *ANÁLISIS DE TÉCNICAS DE PREVENCIÓN, DETECCIÓN Y*

ATAQUES DE PHISHING. S.l.: s.n.

MDN, 2023. Anatomía de una extensión - Mozilla | MDN. [en línea]. [consulta: 11 junio 2023]. Disponible en: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Anatomy_of_a_WebExtension.

MEDINA, M. del R. y VERDEJO, A.L., 2020. Validez y confiabilidad en la evaluación del aprendizaje mediante las metodologías activas. *Alteridad. Revista de Educación*, vol. 15, no. 2,

DE LA SOTA SHICSHIE, K.C. y MECHAN CRISTOBAL, Y.J., 2018. *IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS DE LA ISO/IEC 27001:2013 PARA LA SEGURIDAD DE INFORMACIÓN EN UNA PYME CONSULTORA*. Lima Peru: Universidad San Martin de Porres.

DÍAZ, A., 2010. Sistema de Gestión de la Seguridad de la Información UNE-ISO/IEC 2700. ,

DIETRICHSO, A., 2019. *Métodos Cuantitativos* [en línea]. S.l.: s.n. [consulta: 10 diciembre 2023]. Disponible en: https://bookdown.org/dietrichson/metodos-cuantitativos/test-de-normalidad.html.

ESCUELA EUROPEA, 2023. Controles del Anexo A de ISO 27001: guía completa actualizada a la versión de 2022. *Escuela Europea de Excelencia* [en línea]. [consulta: 12 diciembre 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2023/03/controles-del-anexo-a-de-iso-27001-guia-completa-actualizada-a-la-version-de-2022/.

HEARTFIELD, R. y LOUKAS, G., 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security* [en línea], vol. 76, [consulta: 4 junio 2023]. ISSN 0167-4048. DOI 10.1016/j.cose.2018.02.020. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404818301780.

JAIN, A.K. y GUPTA, B.B., 2016. A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security* [en línea], vol. 2016, no. 1, [consulta: 20 noviembre 2023]. ISSN 1687-4161. DOI 10.1186/s13635-016-0034-3. Disponible

en: https://doi.org/10.1186/s13635-016-0034-3.

KWAK, S.G. y PARK, S.-H., 2019. Normality Test in Clinical Research. *Journal of Rheumatic Diseases* [en línea], vol. 26, no. 1, [consulta: 10 diciembre 2023]. DOI 10.4078/jrd.2019.26.1.5. Disponible en: https://www.jrd.or.kr/journal/view.html?doi=10.4078/jrd.2019.26.1.5.

NQA, 2015. *ISO 27001:2013 GUÍA DE IMPLEMENTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN* [en línea]. 2015. S.l.: s.n. Disponible en: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf.

PRESSMAN, R.S., 2009. Ingenieria del Software. Un Enfoque Practico. , vol. 7ma, ISSN 978-607-15-0314-5.

RAO, R.S. y PAIS, A.R., 2019. Jail-Phish: An improved search engine based phishing detection system. *Computers & Security* [en línea], vol. 83, [consulta: 16 junio 2023]. ISSN 0167-4048. DOI 10.1016/j.cose.2019.02.011. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404818304280.

TAN, C.L., CHIEW, K.L., WONG, K. y SZE, S.N., 2016. PhishWHO: Phishing webpage detection via identity keywords extraction and target domain name finder. *Decision Support Systems* [en línea], vol. 88, [consulta: 10 diciembre 2023]. ISSN 0167-9236. DOI 10.1016/j.dss.2016.05.005. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167923616300781.

MOUTON, F., LEENEN, L., MALAN, M.M. y VENTER, H.S., 2014. Towards an Ontological Model Defining the Social Engineering Domain. En: K. KIMPPA, D. WHITEHOUSE, T. KUUSELA y J. PHAHLAMOHLAKA (eds.), *ICT and Society*. Berlin, Heidelberg: Springer, pp. 266-279. IFIP Advances in Information and Communication Technology, ISBN 978-3-662-44208-1. DOI 10.1007/978-3-662-44208-1_22.

MOZILLA, M., 2023. ¿Qué son las extensiones? - Mozilla | MDN. [en línea]. [consulta: 11 junio 2023]. Disponible en: https://developer.mozilla.org/es/docs/Mozilla/Add-ons/WebExtensions/What_are_WebExtensions.

OCHOA, J. y YUNKOR, Y., 2019. El estudio descriptivo en la investigación científica. *ACTA JURÍDICA PERUANA* [en línea], vol. 2, no. 2, [consulta: 24 junio 2023]. ISSN 2663-7995. Disponible en: http://revistas.autonoma.edu.pe/index.php/AJP/article/view/224.

RAO, R.S. y PAIS, A.R., 2019. Jail-Phish: An improved search engine based phishing detection system. *Computers & Security* [en línea], vol. 83, [consulta: 16 junio 2023]. ISSN 0167-4048. DOI 10.1016/j.cose.2019.02.011. Disponible en: https://www.sciencedirect.com/science/article/pii/S0167404818304280.

REDACCIÓN, 2023. Extensiones para navegadores web: qué son y para qué sirven. *Marketing Insider Review* [en línea]. [consulta: 13 junio 2023]. Disponible en: https://www.marketinginsiderreview.com/que-son-extensiones-para-navegadores-web/.

RISCO, A.A., 2020. Clasificación de las Investigaciones.,

RODRIGUEZ, E., 2018. Metodologías de ingeniería social. [en línea], Disponible en: https://openaccess.uoc.edu/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf.

RODRÍGUEZ RINCÓN, Y., 2018. Metodologías de ingeniería social.,

ROMERO, M., 2013. *Contraste de Hipótesis Comparación de dos medias independientes mediante pruebas no paramétricas: Prueba U de Mann-Whitney*. 2013. S.l.: s.n.

SASTOQUE, D., 2015. *Técnicas de detección y control de phishing.* S.l.: s.n.

SAWA, Y., BHAKTA, R., HARRIS, I.G. y HADNAGY, C., 2016. Detection of Social Engineering Attacks Through Natural Language Processing of Conversations. *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)*. S.l.: s.n., pp. 262-265. DOI 10.1109/ICSC.2016.95.

TONON, [sin fecha]. LA UTILIZACION DEL METODO COMPARATIVO EN ESTUDIOS CUALITATIVOS EN CIENCIA POLITICA Y CIENCIAS SOCIALES: diseño y desarrollo de una tesis doctoral. *2011* [en línea], ISSN 1514-9331. Disponible en: http://www.revistakairos.org//Dialnet-LaUtilizacionDelMetodoComparativoEnEstudiosCualita-3702607%20(2).pdf.

Villegas Cubas, Juan Elías.pdf [en línea], [sin fecha]. S.l.: s.n. [consulta: 10 junio 2023]. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8897/Villegas%20Cubas%2c%20Juan%20El%c3%adas.pdf?sequence=1&isAllowed=y.

WANG, Z., ZHU, H. y SUN, L., 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* [en línea], vol. 9, [consulta: 2 junio 2023]. ISSN 2169-3536. DOI 10.1109/ACCESS.2021.3051633. Disponible en: https://ieeexplore.ieee.org/document/9323026/.

ZANELLO, C., 2023. 14 tipos de ataques que aplican la ingeniería social — Perallis Security. [en línea]. [consulta: 11 junio 2023]. Disponible en: https://www.perallis.com/noticias/14-tipos-de-ataques-que-aplican-la-ingenieria-social

ANEXOS

Anexo 1 Matriz de operacionalización

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ESCALA
Variable independiente: Módulo de extensión de seguridad	Según (Redacción 2023), son programas instalados dentro de un navegador web que agrega funciones y características para mejorar la experiencia de un usuario al navegar. Están diseñadas por lenguajes como HTML, CSS y JavaScript	Es la combinación de elementos lógicos necesarios para llevar a cabo una solución práctica a un problema específico, al mismo tiempo las extensiones proporcionan características que son ampliamente solicitadas por los usuarios en su vida diaria.			Ordinal
Variable Dependiente: Detección y prevención de ataques web de Ingeniería Social	Según (Berenguer 2018) La identificación y prevención de ataques web de ingeniería social se enfoca en detectar y contrarrestar métodos empleados por los atacantes para psicológicamente influir en los usuarios y obtener datos confidenciales o llevarse a acciones dañinas. Estos ataques se sustentan en la explotación de la confianza, la persuasión y la manipulación emocional de las personas.	La detección y prevención de ataques web de ingeniería social a nivel práctico se fundamenta en la aplicación de diversas acciones y metodologías con el propósito de identificar y disminuir de manera eficiente este tipo de ataques.	Detección de sitios maliciosos	**Tasa de detección de sitios web con phishing** $DR = \frac{TP}{TP+FN} * 100$	
			Monitoreo y prevención en tiempo real	**Capacidad de detección temprana** $Pre = \frac{TP}{TP+FN}$	
			Alertar y notificar	**Capacidad de respuesta**	

				$MTTA = \frac{Suma\ de\ los\ tiempos\ de\ respuesta}{Número\ total\ de\ eventos\ de\ respuesta}$	

Anexo 2 Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIÓN	INDICADOR	METODOLOGÍA
PG:¿Cómo contribuye la implementación de un módulo de extensión de seguridad contribuye a la detección y prevención de ataques de Ingeniería Social en el rubro empresarial?	**OG:** Implementar un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial	**HG:**El desarrollo de un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial.	**Variable independiente:** Módulo de extensión de seguridad			**Tipo de Investigación:** Aplicada con enfoque cuantitativo **Diseño de investigación:** Pre experimental **Población:** Registro estimado de ataques de ingeniería social en un tiempo determinado de dos semanas o 15 días. **Muestra:** Cantidad de registros que se evidencian **Muestreo:** No probabilístico **Técnica:** Fichaje **Instrumento:** Ficha de registro
PE1:¿En qué medida la implementación de un módulo de extensión de seguridad favorece a la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial?	**OE1:** Determinar la eficacia de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial	**HE1:** El desarrollo de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial				
PE2:¿De qué modo la implementación de un módulo de extensión de seguridad facilita el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial?	**OE2:** Determinar la eficiencia de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial	**HE2:** El desarrollo de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial	**Variable Dependiente:** Detección y prevención de ataques web de Ingeniería Social	Detección de sitios maliciosos	Tasa de detección de sitios web con phishing $DR = \frac{TP}{TP+FN} * 100$	
PE3:¿De qué manera la implementación de un módulo de extensión de seguridad determina la celeridad para alertar y notificar ataques web de Ingeniería Social en el rubro empresarial?	**OE3:** Determinar la celeridad de un módulo de extensión de seguridad para alertar y notificar ataques web de Ingeniería Social en el rubro empresarial	**HE3:** El desarrollo de un módulo de extensión de seguridad para la celeridad de alertar y notificar ataques web de Ingeniería Social en el rubro empresarial		Monitoreo y prevención en tiempo real	Capacidad de detección temprana $Pre = \frac{TP}{TP+FN}$	
				Alertar y notificar	Capacidad de respuesta	

					$MTTA = \frac{Suma\ de\ los\ tiempos\ de\ respuesta}{Número\ total\ de\ eventos\ de\ respuesta}$	

Anexo 2 Ficha de tasa de detección de sitios web con phishing

FICHA DE REGISTRO				
Investigador				
Descripción				
Empresa				
Dimensión	Detección de sitios maliciosos			
Indicador	**Técnica**	**Simbología de la fórmula**	**Fórmula**	**Medida**
Tasa de detección de sitios web con phishing	Fichaje	TP: True positive FN: False negative	$DR = \frac{TP}{TP+FN} * 100$	Porcentaje

Día	**Fecha**	**TP: Cantidad de páginas infectadas detectadas**	**FN: Cantidad de páginas infectadas no detectadas**	**DR: Tasa de detección de sitios web con con phishing**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Anexo 3 Ficha de capacidad de detección temprana

FICHA DE REGISTRO				
Investigador				
Descripción				
Empresa				
Dimensión	Monitoreo y prevención en tiempo real			
Indicador	**Técnica**	**Simbología de la fórmula**	**Fórmula**	**Medida**
Capacidad de detección temprana	Fichaje	TP: True positive FN: False negative	$Pre = \frac{TP}{TP+FN}$	Enteros

Día	**Fecha**	**TP: Cantidad de páginas infectadas detectadas**	**FN: Cantidad de páginas infectadas no detectadas**	**PRE: Capacidad de detección temprana**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Anexo 4 Ficha de capacidad de respuesta

FICHA DE REGISTRO				
Investigador				
Descripción				
Empresa				
Variable	Alertar y notificar			
Indicador	**Técnica**	**Simbología de la fórmula**	**Fórmula**	**Medida**
Capacidad de respuesta	Fichaje	STR: Suma de los tiempos de respuesta NTE: Número total de eventos de respuesta	$MTTA = \frac{Suma\ de\ los\ tiempos\ de\ respuesta}{Número\ total\ de\ eventos\ de\ respuesta}$	Enteros

Día	**Fecha**	**STR: Suma de los tiempos de respuesta**	**NTE: Número total de eventos**	**MTTA: Capacidad de respuesta**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Anexo 5: Carta de presentación

UNIVERSIDAD CÉSAR VALLEJO

Los Olivos, 08 de Julio del 2023

CARTA N°002-2023-UCV-VA-P18/CPP

Señor
VINIMAX SAC – CONSORCIO DIGITAL
Puquina 168, San Miguel - Lima
Presente,

De mi consideración:

Es grato saludarlo en nombre de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo - Lima Norte.

Recurro a usted, a fin de manifestarle que los alumnos:

ANA CLAUDIA NICOLE PÉREZ VÁSQUEZ con código 7002292840 y DNI 75426493

VIVIAN ELIZABETH ALFARO GARBICH con código 7002274773 y DNI 71253484

se encuentra matriculado en el IX ciclo de la EP de Ingeniería de Sistemas. Agradeceremos darles las facilidades para realizar su trabajo de investigación para el Desarrollo de su Tesis, en las instalaciones de la institución que usted dirige.

Con la seguridad de contar con su aceptación, le expreso de mi consideración y estima personal.

Atentamente,

UCV

DRA. YESENIA DEL ROSARIO VASQUEZ VALENCIA
Jefe de la EP de Ingeniería Sistemas
Campus - Lima Norte

Anexo 6: Carta de aceptación

Consultora de Transformación Digital
Consultoría digital * Desarrollo web * Aplicaciones web * Servicios para educación en línea
Servidores cloud * Hosting web * Videoconferencias * Producción AudioVisual * Fotografía Institucional

CONSORCIO DIGITAL

Señoritas:
Alfaro Garbich Vivian Elizabeth
Perez Vasquez Ana Claudia Nicole
Presente.

De mi mayor consideración

Sirva la presente para saludarles cordialmente y a la vez comunicarles que su solicitud de autorización para realizar su proyecto de investigación, titulado "Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial", ha sido aceptada por nuestra empresa.

Esperando que, con esta colaboración de nuestra representada a su personal, Ud. logre sus objetivos trazados y nuestra empresa también se va favoreciendo con los resultados de esta importante investigación que va desarrollar en nuestras instalaciones.

Es importante recordarle que deberá mantenerse la confidencialidad de la información, la cual es propiedad de "VINIMAX SAC - CONSORCIO DIGITAL". Esperamos que su investigación sea de gran aporte a nuestra institución como para la comunidad.

Sin otro particular, me despido.

Atentamente:

Lima, 8 de julio del 2023

OSCAR GONZALES
Gerente General
VINIMAX S.A.C.

OSCAR ANDRES GONZALES PORTILLA
GERENTE GENERAL

Anexo 7: Metodología de gestión de riesgos

1. Análisis de Riesgos

Para realizar el análisis de riesgos, se utilizó la metodología de gestión de riesgos de los autores, De la Sota Shicshie y Mechan Cristobal (2018) que nos brindan los pasos a seguir para tener un control de la información. Estos se dividen en los siguientes:

1.1. Inventario de Activos

Inicia con manejar un inventario de activos de información para los procesos a su alcance, para ello se realiza la categorización de los inventarios.

Tabla 21. *Inventario de Activos*

Grupo	Abreviatura	Descripción
Instalaciones	I	Las instalaciones que acogen equipos informáticos y de comunicaciones
Hardware	HW	Los equipos informáticos (hardware) que permiten hospedar datos, aplicaciones y servicios.
Software	SW	Las aplicaciones informáticas (software) que permiten manejar los datos.
Datos	D	Datos que materializan la información.
Redes de comunicación	COM	Datos que materializan la información.
Servicios	S	Servicios auxiliares que se necesiten para desarrollo de procesos y/o servicios

Equipamiento auxiliar	AUX	El equipamiento auxiliar que complementa el material informático
Media	M	Documentación, procedimientos, manuales de usuarios.

Fuente: elaboración propia

1.2. Valoración de activos

Para obtener una valoración adecuada, se forma una fórmula que está relacionada con el CID que es Confidencialidad, Integridad y Disponibilidad, tres campos importantes de la ISO 27001:2013.

$$Valor\ de\ activo\ = \frac{(confidencialidad+integridad+disponibilidad)}{3}$$

La valoración de empleada de la siguiente manera:

Tabla 22. *Valoración de activos*

Rango	**Valor**	**Confidencialidad**	**Integridad**	**Disponibilidad**
7-10	ALTO	La información asociada al activo es solo accedida por el Gerente o jefes responsables, pues su divulgación afectaría gravemente a la empresa.	El activo no puede tolerar pérdida o alteración de sus componentes 5% pues la alteración de su integridad afectaría gravemente a la empresa	Se requiere que el activo no esté disponible al menos una hora, pues su carencia afectaría gravemente a la empresa
4-6	MEDIO	La información asociada al activo es	La información asociada al activo es	Se considera que como máximo el

		confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la empresa	confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la empresa.	activo puede estar no disponible por un día, pues su carencia afectaría considerablemente a la empresa.
1-0	ALTO	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la empresa	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la empresa	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la empresa

Fuente: elaboración propia

Además, como parte del análisis, debemos medir el nivel de impacto para el activo que listamos. Se obtienen identificando el valor del activo según los rangos establecidos en la tabla 23

Tabla 23. *Valoración de activos según rangos*

ID	Rango	Valor		Criterio
3	7-10	Alto	A	Valor alto
2	4-6	Medio	M	Valor medio
1	1-3	Bajo	B	Valor bajo

Fuente: elaboración propia

Los criterios que pasen la fase de evaluación de riesgos con un nivel de impacto alto, serán los elegidos para el desarrollo del producto.

1.1. Evaluación de riesgos

Dentro de la evaluación de riesgos se consideran dos factores muy importante, probabilidad e impacto del riesgo. Ambos cuentan con puntajes que son multiplicados para obtener el riesgo total.

1.1.1. Probabilidad

El cálculo de la probabilidad se divide en 4 puntos con sus respectivas descripciones y frecuencias.

Tabla 24. *Probabilidad de riesgo*

ID	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
4	Casi seguro	Evento que probablemente ocurra en la mayoría de circunstancias presentadas	Más de una vez al año
3	Probable	Evento que probablemente ocurra en todas las circunstancias	Al menos una vez en los último 3 años
2	Improbable	Evento que probablemente ocurra en algún momento	Al Menos una vez en los últimos 5 años
1	Raro	Evento que probablemente ocurre en ciertas circunstancias	No se ha presentado en los últimos 5 años

Fuente: elaboración propia

1.1.2. Impacto

El cálculo de la probabilidad se divide en 3 puntos con sus respectivas descripciones y frecuencias.

Tabla 25. *Nivel de impacto*

ID	RANGO	DESCRIPCIÓN
3	Alto	1. Impacta negativamente la reputación, la misión y los intereses fundamentales de la entidad de manera significativa.

		2. Genera pérdidas económicas significativas, requiriendo un alto costo y esfuerzo para recuperar los activos y recursos de la organización. 3. Pone en riesgo la continuidad eficiente de los servicios ofrecidos por la organización.
2	Medio	1. Impacta negativamente en la reputación de la imagen, la misión y los intereses de la organización. 2. Genera pérdidas financieras que son recuperables en cierta medida para los activos o recursos de la organización. 3. Tiene un impacto moderado en la continuidad de los servicios ofrecidos por la organización.
1	Bajo	1. Causa un impacto insignificante en la reputación de la imagen, la misión y los intereses de la organización. 2. Genera pérdidas financieras mínimas en los activos o recursos de la organización. 3. No tiene repercusiones en la continuidad de los servicios ofrecidos por la organización.

Fuente: elaboración propia

Para conseguir el valor del riesgo, se calcula con la siguiente fórmula donde utilizamos tanto la probabilidad como el impacto que seguidamente es planteada en una tabla de zona de riesgos.

$$Nivel\ de\ riesgo\ =\ Nivel\ de\ impacto\ \ *\ \ probabilidad\ de\ ocurrencia\ del\ riesgo$$

Tabla 26. *Nivel de riesgo*

PROBABILIDAD		IMPACTO		
		Baje	Medio	Alto
		1	2	3
Raro	1	1	2	3
Improbable	2	2	4	6
Probable	3	3	6	9
Casi seguro	4	4	8	12

Fuente: elaboración propia

Tabla 27. *Lista de activos de información*

Ámbito	ID	Activo
Instalaciones	I-001	Oficinas
Hardware	HW-001	Laptops
	HW-002	Computadoras
	HW-003	Impresoras
	HW-004	Cámaras
	HW-005	Proyector
Software	SW-001	Antivirus
	SW-002	Licencias de Office 365
	SW-003	Lista de instalaciones de software
Datos	D-001	Lista de cuentas bancarias
	D-002	Estados financieros
	D-003	Informes contables
	D-004	Proyecciones financieras
	D-005	Información personal y financiera de clientes
	D-006	Contratos con clientes y proveedores
	D-007	Lista de contraseñas

Redes de comunicación	COM-001	Infraestructura tecnológica
	COM-002	Red de telefonía
	COM-003	Dispositivos de red
Servicios	S-001	Internet
	S-002	Correo electrónico
	S-003	Pagos de servicio a proveedores
Media	M-001	Documentación Administrativa
	M-002	Documentación técnica
	M-003	Documentación de políticas internas

Fuente: elaboración propia

Tabla 28. *Valoración de activos*

Ámbito	ID	Activo	Criterios			Total	Impacto
			C	I	D		
Instalaciones	I-001	Oficinas	2	5	4	4	M
Hardware	HW-001	Laptops	3	8	10	7	A
	HW-002	Computadoras	3	8	10	7	A
	HW-003	Impresoras	3	4	2	3	B
	HW-004	Cámaras	6	9	10	8	A
	HW-005	Proyector	3	3	3	3	B
Software	SW-001	Antivirus	5	10	10	8	A
	SW-002	Licencias de Office 365	3	5	3	4	M
	SW-003	Lista de instalaciones de software	6	10	10	9	A
Datos	D-001	Lista de cuentas bancarias	10	10	10	10	A
	D-002	Estados financieros	10	10	10	10	A
	D-003	Informes contables	7	7	8	7	A
	D-004	Proyecciones financieras	7	8	8	8	A
	D-005	Información personal y financiera de clientes	8	10	9	9	A
	D-006	Contratos con clientes y proveedores	7	8	8	8	A
	D-007	Lista de contraseñas	10	10	10	10	A
Redes de comunicación	COM-001	Infraestructura tecnológica	6	10	10	9	A
	COM-002	Red de telefonía	6	6	5	6	M
	COM-003	Dispositivos de red	6	9	9	8	A

Servicios	S-001	Internet	6	9	9	8	A
	S-002	Correo electrónico	3	8	8	6	M
	S-003	Pagos de servicio a proveedores	6	8	8	7	A
Media	M-001	Documentación Administrativa	3	6	8	6	M
	M-002	Documentación técnica	3	6	8	6	M
	M-003	Documentación de políticas internas	3	7	8	6	M

Fuente: elaboración propia

Tabla 29. *Evaluación de riesgos*

ID	Activo	AMENAZA		OCURRENCIA		RIESGO	
		IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
HW-001	Laptops	Bajo	1	Improbable	2	2	B
HW-002	Computadoras	Bajo	1	Improbable	2	2	B
HW-004	Cámaras	Alto	3	Probable	3	9	E
SW-001	Antivirus	Alto	3	Probable	3	9	E
SW-003	Lista de instalaciones de software	Alto	3	Probable	3	9	E
D-001	Lista de cuentas bancarias	Alto	3	Probable	3	9	E
D-002	Estados financieros	Alto	3	Probable	3	9	E
D-003	Informes contables	Alto	3	Probable	3	9	E
D-004	Proyecciones financieras	Medio	2	Probable	3	6	E
D-005	Información personal y financiera de clientes	Medio	2	Probable	3	6	A
D-006	Contratos con clientes y proveedores	Alto	3	Probable	3	9	E
D-007	Lista de contraseñas	Alto	3	Probable	3	9	E
COM-001	Infraestructura tecnológica	Medio	2	Raro	1	2	B
COM-003	Dispositivos de red	Medio	2	Raro	1	2	B
S-001	Internet	Medio	2	Raro	1	2	B
S-003	Pagos de servicio a proveedores	Medio	2	Raro	1	2	B

Fuente: elaboración propia

Tabla 30. *Riesgos seleccionados para el desarrollo del producto de ingeniería*

ID	Activo	AMENAZA		OCURRENCIA		RIESGO	
		IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
SW-003	Lista de instalaciones de software	Alto	3	Probable	3	9	E
D-001	Lista de cuentas bancarias	Alto	3	Probable	3	9	E
D-002	Estados financieros	Alto	3	Probable	3	9	E
D-003	Informes contables	Alto	3	Probable	3	9	E
D-004	Proyecciones financieras	Medio	2	Probable	3	6	E
D-006	Contratos con clientes y proveedores	Alto	3	Probable	3	9	E
D-007	Lista de contraseñas	Alto	3	Probable	3	9	E

Fuente: elaboración propia

Anexo 8: Lista de controles del Anexo A de la norma ISO/IEC 27001:2013

Tabla 31. *Lista de controles del Anexo A de la norma ISO/IEC 27001:2013*

ID	Controles según la norma ISO 27001	Aplicabilidad (SI/NO)	Descripción / Justificación
1	Objeto y campo de aplicación	No	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas	No	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones	No	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma	No	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	No	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información	No	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	No	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

A.6	Organización de la seguridad de la información		
A.6.1	Organización interna	No	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	No	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	No	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	No	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	No	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales Especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Si	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles	No	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

A.6.2.2	Teletrabajo	Si	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo	No	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección	No	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	No	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización encuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo	No	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	No	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la	No	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones

	seguridad de la información		regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	No	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo	No	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	No	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos	Si	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	No	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	No	Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	No	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	No	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se

			encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información	No	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	No	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	No	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	No	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles	No	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	No	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Si	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	Control de acceso		

A.9.1	Requisitos del negocio para control de acceso	No	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	No	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red	Si	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	Si	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	No	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	No	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	No	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Si	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de	No	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

	acceso de usuarios		
A.9.2.6	Retiro o ajuste de los derechos de acceso	No	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios	Si	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	Si	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones	Si	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información	No	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	Si	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	No	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Si	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de

			anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	No	Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía		
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	Si	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Si	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	No	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	No	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	No	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas	No	Control: Se debería diseñar y aplicar protección física contra

	externas y ambientales		desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	No	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	No	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos	No	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos	No	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	No	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	No	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	No	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	No	Control: Los equipos, información o software no se deberían retirar de

			su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	No	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	No	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	No	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	No	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades	No	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados	No	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	No	Control: Se deberían controlar los cambios en la organización, en los procesos de

			negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	No	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos	Si	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	Si	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo	No	Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información	No	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos	Si	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca

			de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Si	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	No	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes	No	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional	Si	Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	Si	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica	No	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	No	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

A.12.6.2	Restricciones sobre la instalación de software	No	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información	No	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas	No	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes	No	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes	No	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	No	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	No	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información	No	Objetivo: Mantener la seguridad de la información transferida dentro

			de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información	No	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	No	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	No	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	No	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	Requisitos de seguridad de los sistemas de información	Si	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Si	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Si	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Si	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte	No	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro	No	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	No	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	No	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios

			necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros	No	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	No	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	No	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	No	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	No	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba	No	Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba	No	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	Relación con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores	No	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	No	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	No	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	No	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores	No	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	No	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	No	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	No	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos	No	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	No	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	No	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	No	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	No	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	No	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7	Recolección de evidencia	No	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información	No	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	No	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	No	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias	No	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	No	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente

			para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento	No	
A.18.1	Cumplimiento de requisitos legales y contractuales	No	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	No	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	No	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	No	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	No	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	No	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

A.18.2	Revisiones de seguridad de la información	No	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información	No	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	No	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	No	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: elaboración propia

Anexo 9: Metodología cascada en el desarrollo del software

Tabla 32. *Lista de controles del Anexo A de la norma ISO/IEC 27001:2013*

ID	Controles según la norma ISO 27001	Aplicabilidad (SI/NO)	Descripción / Justificación
A.6.1.5	Seguridad de la información en la gestión de proyectos	Si	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2.2	Teletrabajo	Si	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.8.1	Responsabilidad por los activos	Si	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.3.3	Transferencia de medios físicos	Si	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.1.2	Política sobre el uso de los servicios de red	Si	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	Si	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

A.9.2.4	Gestión de información de autenticación secreta de usuarios	Si	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.3	Responsabilidades de los usuarios	Si	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	Si	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones	Si	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.2	Procedimiento de ingreso seguro	Si	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.4	Uso de programas utilitarios privilegiados	Si	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.10.1.1	Política sobre el uso de controles criptográficos	Si	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
A.10.1.2	Gestión de llaves	Si	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las

			llaves criptográficas durante todo su ciclo de vida.
A.12.2	Protección contra códigos maliciosos	Si	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	Si	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de concienciaapropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.4.1	Registro de eventos	Si	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Si	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.5	Control de software operacional	Si	Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	Si	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.14.1.1	Requisitos de seguridad de los sistemas de información	Si	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas

			de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Si	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Si	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Si	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Anexo 10: Controles utilizados para el desarrollo del módulo de extensión de seguridad

ID	**Controles según la norma ISO 27001**	**Aplicabilidad (SI/NO)**	**Descripción / Justificación**
A.6.1.5	Seguridad de la información en la gestión de proyectos	Si	Control: La seguridad de la información se debería tratar en la gestión de proyectos,

			independientemente del tipo de proyecto.
A.6.2.2	Teletrabajo	Si	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.8.1	Responsabilidad por los activos	Si	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.3.3	Transferencia de medios físicos	Si	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.1.2	Política sobre el uso de los servicios de red	Si	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	Si	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Si	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.3	Responsabilidades de los usuarios	Si	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	Si	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

A.9.4	Control de acceso a sistemas y aplicaciones	Si	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.2	Procedimiento de ingreso seguro	Si	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.4	Uso de programas utilitarios privilegiados	Si	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.10.1.1	Política sobre el uso de controles criptográficos	Si	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
A.10.1.2	Gestión de llaves	Si	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.12.2	Protección contra códigos maliciosos	Si	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	Si	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de concienciaapropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.4.1	Registro de eventos	Si	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

A.12.4.2	Protección de la información de registro	Si	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.5	Control de software operacional	Si	Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	Si	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.14.1.1	Requisitos de seguridad de los sistemas de información	Si	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Si	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Si	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Si	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Anexo 11: Metodología cascada en el desarrollo del software

Capítulo I: Marco de Trabajo

Introducción

Este documento detalla la adopción de la metodología Waterfall(cascada) para la implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial.
La ejecución del desarrollo, guiada por la metodología cascada, se llevó a cabo mediante la secuencial elaboración de fases, Cada una de estas fases requirió su completa finalización antes de proceder a la siguiente, lo que resultó una limitada flexibilidad para la introducción de modificaciones durante la ejecución del proyecto.
En el proceso de ejecución, se han considerado diversos aspectos para garantizar la efectividad y coherencia del proyecto.

Alcance

Considerando el objetivo principal y los específicos delineados para este proyecto, se establece el alcance del mismo mediante la definición de los objetivos prioritarios que deberán ser alcanzados durante su ejecución

- ➔ Implementar de un módulo de extensión de seguridad para la detección y prevención de ataques web de Ingeniería Social en el rubro empresarial
- ➔ Determinar la eficacia de un módulo de extensión de seguridad para la detección de sitios maliciosos de ataques de Ingeniería Social en el rubro empresarial
- ➔ Determinar la eficiencia de un módulo de extensión de seguridad para el monitoreo y prevención en tiempo real de ataques web de Ingeniería Social en el rubro empresarial
- ➔ Determinar la celeridad de un módulo de extensión de seguridad para alertar y notificar ataques web de Ingeniería Social en el rubro empresarial

Planteamiento del Producto

Para la elaboración del módulo de extensión de seguridad que se propuso tuvo como objetivo fundamental fortalecer las defensas cibernéticas que existen en el rubro empresarial, está específicamente focalizado en la detección y prevención de ataques de Ingeniería Social. Esta solución busca proporcionar una capa adicional de seguridad que te permita navegar de manera segura, así cómo también evitar que sean persuadidos por un sitio web falso

1. Fase de Análisis y requerimientos

1.1. Requerimientos funcionales

Se detallan todos los requerimientos que se tomarán en cuenta, durante el desarrollo del módulo de extensión de seguridad.

Tabla 33. Requerimientos Funcionales

ID	Requerimientos funcionales
1	La extensión debe detectar a tiempo real las páginas que contienen phishing.
2	La extensión debe poder detectar páginas con phishing
3	La extensión debe de poder alertar y notificar si una página está infectada
4	La extensión de poder alertar y notificar si una pagina es segura
5	Se debe tener una sección de configuración para que el usuario pueda activar o desactivar las notificaciones, monitoreo en tiempo real o desactivar la protección.
6	Se maneja tres tipos de alertas, segura, con phishing y sospechosa

1.2. Requerimientos no funcionales

Se detallan los requerimientos funcionales que son necesarios para el desarrollo pero no tan relevantes.

Tabla 34 Requerimientos no funcionales

ID	Requerimientos no funcionales
1	Desarrollado en Java y vue.js
2	Bajo rendimiento de
3	No invadir el navegación del usuario

2. Fase de Diseño

2.1. Arquitectura del módulo de extensión de seguridad

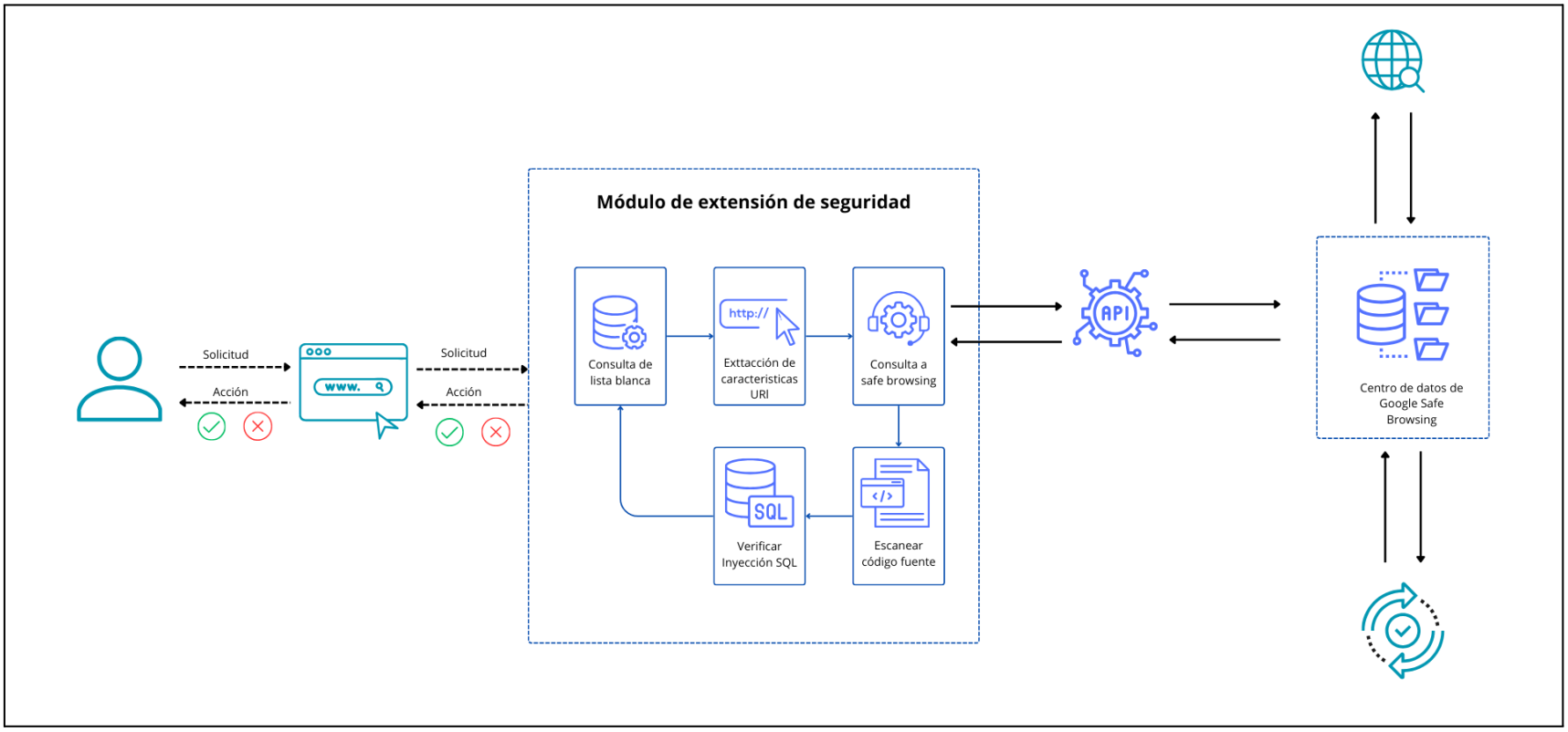


Figura 4 : Arquitectura de módulo de extensión de seguridad

El módulo de extensión de seguridad se divide en seis fases, que servirán como un filtro con ciertos requisitos que deberá cumplir un sitio web al ser estudiado durante el ingreso de tal sitio.

Fase 1: Lista Blanca

- Crea una base de datos local (por ejemplo, utilizando LocalStorage) para almacenar las URLs en la lista blanca.
- Cuando un usuario navegue a una página web, verifica si la URL está en la lista blanca.
- Si la URL está en la lista blanca, permite la navegación. Si no, pasa a la siguiente fase.

Fase 2: Verificación de URL

- Implementa funciones para extraer características distintivas de la URL, como la IP, la edad del dominio, la longitud de la URL, el número de puntos en el nombre del host y URL sospechosas.
- Verifica el certificado SSL de la página para asegurarte de que sea legítimo.
- Si se encuentran características de phishing o el certificado es sospechoso, muestra una alerta al usuario y bloquea la página. De lo contrario, pasa a la siguiente fase.

Fase 3: Consulta a Google Safe Browsing

- Utiliza la API de Google Safe Browsing para verificar la URL en busca de similitudes con sitios web maliciosos.
- Si se encuentra una similitud, muestra una advertencia al usuario y detiene el proceso de revisión. Si no se encuentra ninguna similitud, pasa a la siguiente fase.

Fase 4: Verificación de Contenido

- Descarga el código fuente de la página web y analízalo en busca de código malicioso.

- Busca enlaces y direcciones sospechosas, formularios de inicio de sesión falsos y contenido inusual.
- Si se encuentra alguna de estas características, muestra una alerta al usuario. De lo contrario, pasa a la siguiente fase.

Fase 5: Escaneo de Inyección SQL

- Implementa una solución para realizar el escaneo de inyección SQL en el código de la página.
- Si se encuentra una inyección SQL, muestra una alerta al usuario. Si no se encuentra ninguna inyección SQL, pasa a la última fase.

Fase 6: Confirmación y Lista Blanca

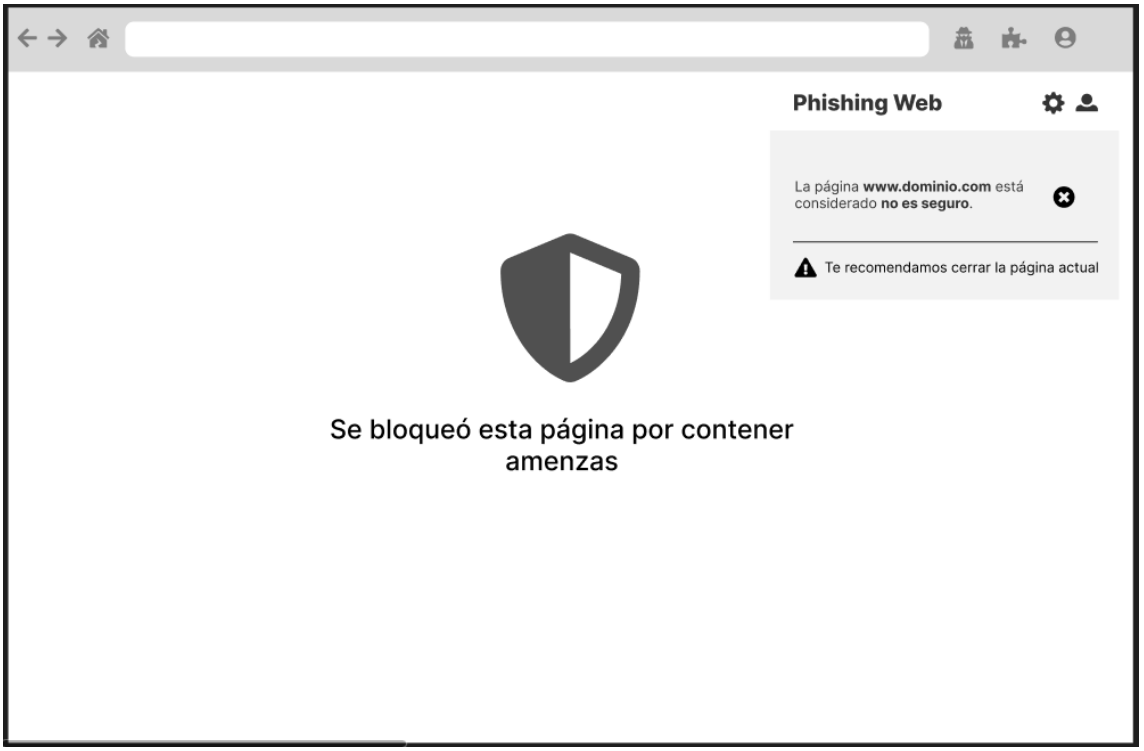
- Si la URL ha pasado por todas las fases sin generar una alerta, muestra un mensaje al usuario indicando que la página es segura.
- Agrega la URL a la lista blanca para evitar un bucle innecesario en futuras visitas.

2.2. Caso de Uso del Sistema

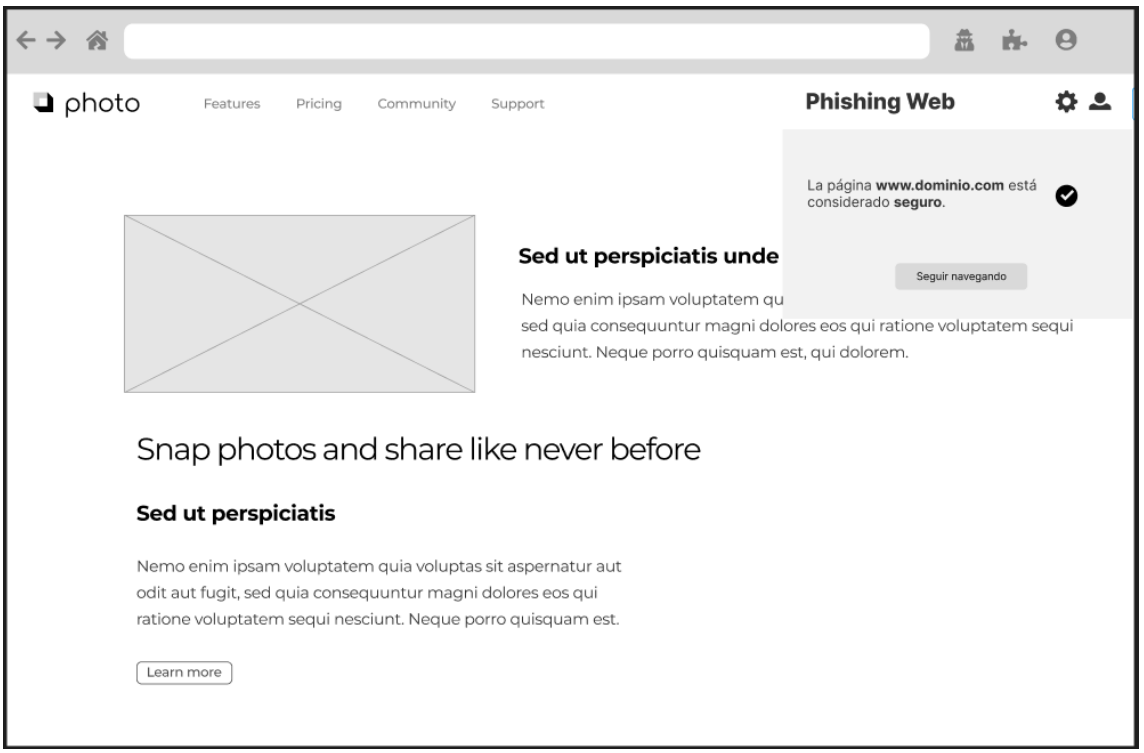
2.3. Prototipo

2.3.1. Vista de instalación de la extensión

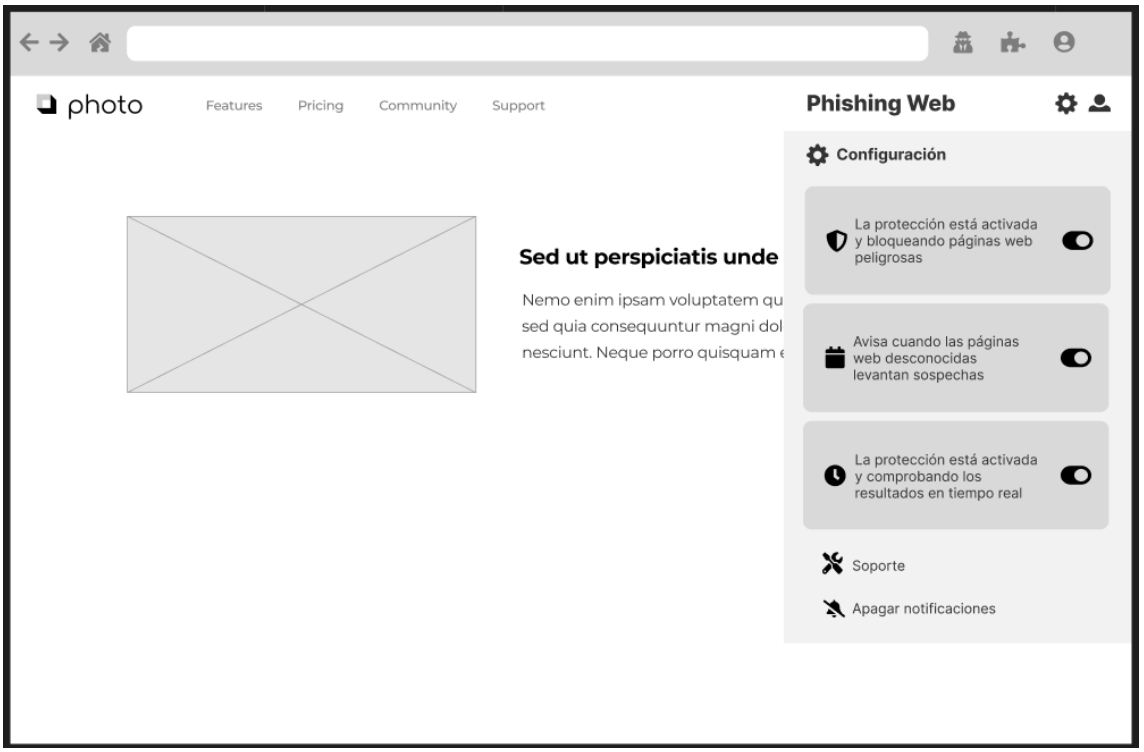
2.3.2. Vista de mensaje de detección



2.3.3. Vista de mensaje de página segura



2.3.4. Vista de configuración de la extensión



3. Fase de Implementación

Se realizó la implementación de la extensión según las seis fases definidas dentro de los requisitos y diseño propuesto.

- **Fase 1: Lista Blanca**

```
window.onload = () => {
    let url_initial = window.document.URL.split('//')
    url = url_initial[1]; url = url.split('/'); url = url[0];
    //FASE 01
    verificarEnListaBlanca(url, function (response) {
        if (!response)
        {
            console.log("Fase 1 desaprobada.")
            url = url_initial[0] + '//' + url + '/'
            validateFaseII(url)
        }
        else
        {
            console.log("Fase 1 aprobada.")
        }
    })
}

function verificarEnListaBlanca(url, callback) {
    let listaBlanca = localStorage.getItem('lista_blanca');
    listaBlanca = (listaBlanca != null && listaBlanca != '') ? JSON.parse(listaBlanca) : [];
    let flag_exists = listaBlanca.includes(url);
    flag_phishing = ((flag_exists) ? 0 : flag_phishing);
    callback(flag_exists);
}
```

- **Fase 2: Verificación de URL**

```
//* FASE 2 *//
async function validateFaseII(url) {
    try {
        const urlFeatures = await extraerCaracteristicasURL(url);
        const phishing = isPhishing(urlFeatures);

        if (phishing)
        {
            console.log(`La URL ${url} es phishing.`);
            showNotificationPhishing('fase 2');
        }
        else
        {
            console.log(`La URL ${url} no es phishing.`);
            validateFaseIII(url);
        }
    }
    catch (error) {
        console.error('Error al extraer características de la URL:', error);
        showNotificationPhishing('fase 2');
    }
}

async function extraerCaracteristicasURL(url) {
  return new Promise(async (resolve, reject) => {
  try {
    const features = {};
```

```
function isPhishing(features) {
// Reglas heurísticas
console.log(features)
return (
features.urlLength > 75 ||
features.domainLength < 3 ||
!features.useHttps ||
features.useIp ||
!features.validDomain ||
features.numForms > 0 ||
features.numDots > 3
);
}
```

- **Fase 3: Consulta a Google Safe Browsing**

```
//FASE 03
function validateFaseIII(url) {
    verificarURLSospechosa(url, function (response) {
        if (!response) {
            console.log("Fase 3 desaprobada.");
            showNotificationPhishing('fase 3');
        } else {
            console.log("Fase 3 aprobada.");
            validateFaseIV(url);
        }
    });
}


function verificarURLSospechosa(url, callback) {
    const apiKey = 'AIzaSyBdZh7oeCPq3UHApb5QqrnMlzOJJuRUOas';
    const apiUrl = 'https://safebrowsing.googleapis.com/v4/threatMatches:find';
    fetch(apiUrl + `?key=${apiKey}`, {
    method: 'POST',
    headers: {
        'Content-Type': 'application/json',
    },
    body: JSON.stringify({
        client: {
        clientId: 'YourAppName',
        clientVersion: '1.0.0',
        },
        threatInfo: {
        threatTypes: ['MALWARE', 'SOCIAL_ENGINEERING', 'UNWANTED_SOFTWARE'],
        platformTypes: ['ANY_PLATFORM'],
        threatEntryTypes: ['URL'],
        threatEntries: [{ url: url }],
        },
    }),
    })
```

- **Fase 4: Verificación de Contenido**

```
//FASE 04
function validateFaseIV(url) {
    console.log("Inicia la fase 4..");

    isSuspiciousURL(url, function (response) {
        if(!response)
        {
            console.log("Fase 4 desaprobada..");
            showNotificationPhishing('fase 4');
        }
        else
        {
            console.log("Fase 4 aprobada..");
            validateFaseV(url);
        }
    })
}

// Función para verificar si una URL es sospechosa
function isSuspiciousURL(url, callback) {
    let response = verificarContenidoSospechoso(url) && verificarArchivosPHPMaliciosos(url);
    callback(response);
}

// Función para verificar el contenido de una página web
async function verificarContenidoSospechoso(url) {
    let response = false
    // Realiza una solicitud para obtener el código fuente de la página web
    fetch(url)
    .then((response) => {
        if (!response.ok) {
            response = false;
        }
    })
    .then((html) => {
        response = contieneCaracteristicasSospechosas(html);
    })
```

- **Fase 5: Escaneo de Inyección SQL**

```
//* FASE 5 *//
function scanForSQLInjection(pageSource) {
    // Patrones SQL para detectar inyecciones
    const sqlInjectionPatterns = [
        /\b(?:SELECT|INSERT|UPDATE|DELETE|DROP|CREATE|ALTER)\b[\s\w\(\)]+\b(?:FROM|INTO|WHERE|SET|TABLE|DATABASE|VALUES|DESC)\b/i,
        /\bUNION\s+ALL\b/i,
        // Agrega más patrones según sea necesario
    ];
    // Verifica si se encuentra alguna coincidencia con los patrones
    const foundSQLInjection = sqlInjectionPatterns.some(pattern => pattern.test(pageSource));

    return foundSQLInjection;
};

function showNotificationPhishing(fase) {
    flag_phishing = 1
    alert('PHISHING! Esta página no es segura.')
    console.log('PHISHING! Esta página no es segura.' + ' - ' + fase)
}
```

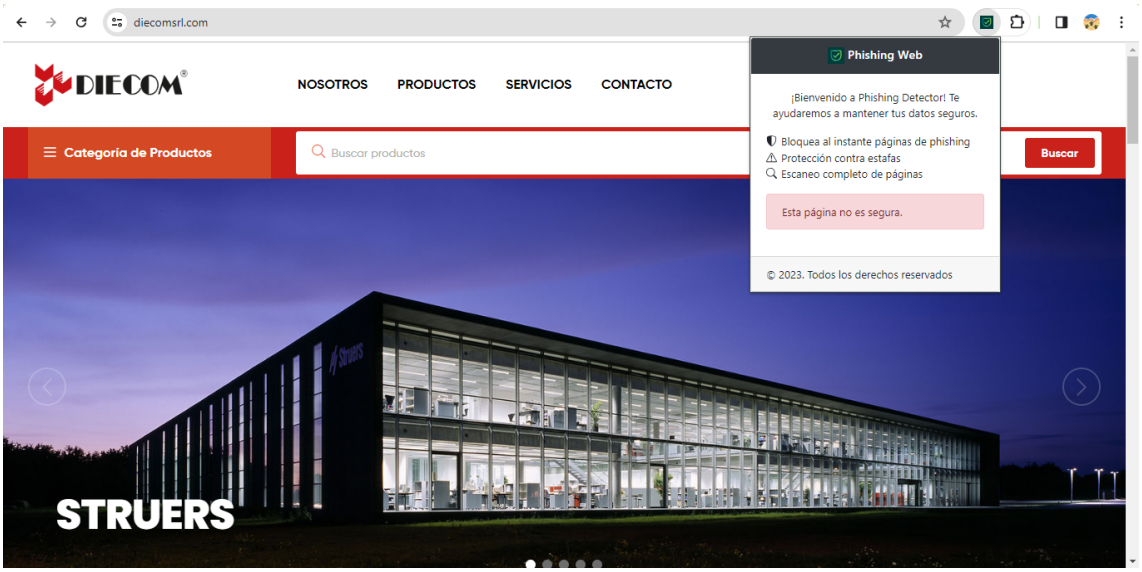
- **Fase 6: Confirmación y Lista Blanca**

```
function addToWhiteList(url) {
    if(!(parseFloat(flag_phishing) === 1))
    {
        let listaBlanca = JSON.parse(localStorage.getItem('lista_blanca'));
        listaBlanca = (listaBlanca != null && listaBlanca != '') ? listaBlanca : [];
        listaBlanca.push(url);
        localStorage.setItem('lista_blanca', JSON.stringify(listaBlanca));

        flag_phishing = 0
    }
}
```

4. Fase de Prueba

Dentro de la prueba, se generaron casos donde pusimos a prueba el producto de ingeniería con una lista de páginas infectadas para verificar el correcto funcionamiento de lo implementado.



5. Fase de Mantenimiento

Como parte de mantenimiento, se contará con soporte técnico en caso de fallas, mejora continua para llevar a un paso más el producto de ingeniería planteado.

Anexo 11. Cronograma de actividades

Tabla 32: *Cronograma*

ACTIVIDADES	INICIO	FIN	DURACIÓN
Implementación de un módulo de extensión de seguridad para la detección y prevención de ataques de Ingeniería Social en el rubro empresarial	3/09/2023	9/12/2023	97
Recopilación de requisitos	4/09/2023	9/09/2023	5
Entrevistas con los stakeholders para identificar y documentar sus requisitos de seguridad.	4/09/2023	5/09/2023	1
Análisis de documentación existente relacionada con los requisitos de seguridad.	5/09/2023	6/09/2023	1
Investigación de estándares y normativas de seguridad aplicables al proyecto.	6/09/2023	7/09/2023	1
Revisión de casos de uso y escenarios para comprender las necesidades del usuario.	7/09/2023	8/09/2023	1
Creación de un documento formal de requisitos de seguridad que sirva como base para el desarrollo del módulo de extensión.	8/09/2023	9/09/2023	1
Diseño del producto de ingeniería	11/09/2023	21/09/2023	10
Desarrollo de diagramas de arquitectura del sistema.	11/09/2023	15/09/2023	4
Creación de prototipos o mockups para visualizar la interfaz del usuario.	15/09/2023	18/09/2023	3
Identificación de tecnologías y herramientas específicas a utilizar en el diseño.	18/09/2023	19/09/2023	1
Revisión y refinamiento de los requisitos en colaboración con el equipo de desarrollo.	19/09/2023	20/09/2023	1

Documentación del diseño técnico del módulo de extensión de seguridad.	20/09/2023	21/09/2023	1
Implementación	26/09/2023	8/11/2023	43
RF01: La extensión deberá realizar una detección en tiempo real de las páginas web que posiblemente contengan amenazas de phishing.	26/09/2023	7/10/2023	11
RF02: La capacidad de la extensión para identificar de manera efectiva las páginas web con posibles intentos de phishing es esencial.	7/10/2023	19/10/2023	12
RF03: La extensión deberá contar con un sistema de alerta y notificación inmediata al usuario en caso de detectar una página web infectada.	20/10/2023	21/10/2023	1
RF04: La extensión debe ser capaz de alertar y notificar de manera clara y precisa cuando una página web es considerada segura para la navegación.	20/10/2023	21/10/2023	1
RF05: Se requiere la implementación de una sección de configuración que permita a los usuarios personalizar sus preferencias. Esta sección debe incluir opciones para activar o desactivar las notificaciones, habilitar o deshabilitar el monitoreo en tiempo real, y la capacidad de desactivar la protección en determinadas circunstancias.	23/10/2023	28/10/2023	5
RF06: La extensión deberá ofrecer tres tipos de alertas distintas: una para páginas seguras, otra para aquellas identificadas con phishing y, finalmente, una alerta para páginas sospechosas que podrían requerir atención adicional.	1/11/2023	8/11/2023	7
Despliegue	11/11/2023	15/11/2023	4
Configuración del Entorno de Producción: Preparación de los servidores y entornos necesarios para la implementación.	11/11/2023	12/11/2023	1
Pruebas de Despliegue: Realización de pruebas específicas de despliegue para asegurar que todos los componentes funcionen correctamente en el entorno de producción.	12/11/2023	13/11/2023	1
Despliegue Completo: Implementación completa del módulo en el entorno de producción.	13/11/2023	14/11/2023	1
Finalización del proyecto	17/11/2023	18/11/2023	1

Fuente: elaboración propia