UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C – LIMA; 2023

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

NEYRA HIDALGO, ANTONY WILLIAM

ORCID: 0009-0005-1186-823X

ASESORA

DRA. SUXE RAMÍREZ, MARÍA ALICIA

ORCID: 0000-0002-1358-4290

Chimbote – Perú

2023

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ACTA N° 0062-108-2023 DE SUSTENTACIÓN DEL INFORME DE TESIS

En la Ciudad de **Chimbote** Siendo las **09:28** horas del día **21** de **Agosto** del **2023** y estando lo dispuesto en el Reglamento de Investigación (Versión Vigente) ULADECH-CATÓLICA en su Artículo 34º, los miembros del Jurado de Investigación de tesis de la Escuela Profesional de **INGENIERÍA DE SISTEMAS**, conformado por:

OCAÑA VELASQUEZ JESUS DANIEL Presidente
TORRES CECLEN CARMEN CECILIA Miembro
ANCAJIMA MIÑAN VICTOR ANGEL Miembro
Dr(a). SUXE RAMIREZ MARIA ALICIA Asesor

Se reunieron para evaluar la sustentación del informe de tesis: **IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C – LIMA; 2023**

Presentada Por :
(2709070013) **NEYRA HIDALGO ANTONY WILLIAM**

Luego de la presentación del autor(a) y las deliberaciones, el Jurado de Investigación acordó: **APROBAR** por **UNANIMIDAD**, la tesis, con el calificativo de **14**, quedando expedito/a el/la Bachiller para optar el TITULO PROFESIONAL de **Ingeniero de Sistemas.**

Los miembros del Jurado de Investigación firman a continuación dando fe de las conclusiones del acta:

OCAÑA VELASQUEZ JESUS DANIEL
Presidente

TORRES CECLEN CARMEN CECILIA
Miembro

ANCAJIMA MIÑAN VICTOR ANGEL
Miembro

Dr(a). SUXE RAMIREZ MARIA ALICIA
Asesor

CONSTANCIA DE EVALUACIÓN DE ORIGINALIDAD

La responsable de la Unidad de Integridad Científica, ha monitorizado la evaluación de la originalidad de la tesis titulada: IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C – LIMA; 2023 Del (de la) estudiante NEYRA HIDALGO ANTONY WILLIAM, asesorado por SUXE RAMIREZ MARIA ALICIA se ha revisado y constató que la investigación tiene un índice de similitud de 11% según el reporte de originalidad del programa Turnitin.

Por lo tanto, dichas coincidencias detectadas no constituyen plagio y la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Católica Los Ángeles de Chimbote.

Cabe resaltar que el turnitin brinda información referencial sobre el porcentaje de similitud, más no es objeto oficial para determinar copia o plagio, si sucediera toda la responsabilidad recaerá en el estudiante.

Chimbote,12 de Setiembre del 2023

Mg. Roxana Torres Guzmán
Responsable de Integridad Científica

Dedicatoria

A mi familia, esposa e hijo por su apoyo, comprensión, dedicación y tiempo tomado que será recompensado, para poder seguir adelante, y así ser cada día mejor persona y un buen profesional. A mis padres que confiaron en mi desde el primer momento que elegí estudiar esta carrera y que gracias a ellos y sus enseñanzas y consejos me orientaron a seguir la por el buen camino, y, por último, pero no me nos importante a mis hermanos que hoy en día me representan como un modelo a seguir para sus hijos.

Antony William Neyra Hidalgo

Agradecimiento

Mi especial agradecimiento a la empresa “SOAINT” por haberme permitido la elaboración de la tesis y así optar el título profesional de Ingeniero de Sistemas, con su ayuda y aporte ayudaron a culminar el proyecto de investigación con éxito y a mi asesora, la Dra. María Alicia Suxe Ramírez por su valioso asesoramiento, paciencia y entendimiento para la culminación de mi investigación.

Antony William Neyra Hidalgo

Índice de Contenido

Lista De Tablas

Lista De Figuras

Resumen

La presente tesis se desarrolló en base a la línea de investigación de sistemas de información y comunicaciones de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote, la problemática fue tomada gracias a los antecedentes de ataques a aplicaciones web que exponen información sensible, por lo que es recomendable realizar una evaluación de vulnerabilidades, teniendo como objetivo general implementar un modelo de análisis de vulnerabilidades y riesgos a la aplicación web, para protegerla de posibles amenazas y ataques, el alcance de esta investigación beneficio a las gerencias y áreas que en su totalidad que utilizan constantemente la aplicación web, la metodología fue de un enfoque cuantitativo, de nivel descriptivo, de diseño no experimental y de corte transversal, como técnica se utilizó la encuesta y como instrumento el cuestionario, en cuanto a la población y muestra, se obtuvo en la primera dimensión los resultados donde el 80.00% de empleados de expresaron que están satisfechos con la aplicación web y la protección de sus datos; en la segunda dimensión el 71.25% de empleados de expresaron que están de acuerdo con la propuesta de implementación de un modelo de análisis de vulnerabilidades y riesgos, se concluyó que si es necesaria la propuesta de implementación de un modelo de análisis de vulnerabilidades y riesgos para proteger de posibles amenazas y ataques a la aplicación web de SOAINT S.A.C – Lima; 2023.

Palabras claves: Amenazas, aplicación web, ataques. vulnerabilidades

Abstracts

This thesis was developed based on the information and communications systems research line of the Professional School of Systems Engineering of the Los Angeles de Chimbote Catholic University, the problem was taken thanks to the history of attacks on web applications that expose sensitive information, so it is advisable to carry out a vulnerability assessment, with the general objective of implementing a vulnerability and risk analysis model for the web application, to protect it from possible threats and attacks. The scope of this investigation benefits management and areas that in their entirety constantly use the web application, the methodology was a quantitative approach, descriptive level, non-experimental and cross-sectional design, the survey was used as a technique and the questionnaire as an instrument, in terms of the population and sample, the results were obtained in the first dimension where 80.00% of employees expressed that they are satisfied with the web application and the protection of their data; In the second dimension, 71.25% of employees expressed that they agree with the proposal for the implementation of a vulnerability and risk analysis model, it was concluded that the proposal for the implementation of a vulnerability and risk analysis model is necessary for protect the web application of SOAINT S.A.C – Lima from possible threats and attacks; 2023.

Keywords: Attacks, threats, Vulnerabilities, web application

I. PLANTEAMIENTO DEL PROBLEMA

1.1. Planteamiento del Problema

1.1.1. Planteamiento del problema internacional

Según Ortega (2020) actualmente, las nuevas tecnologías son un orquestador fundamental en la sociedad de la información, lo cual incluye a las personas y los nuevos tipos de relaciones que se establecen entre ellas. Esta dependencia se halla presente en múltiples escenarios y contextos, desde actividades comerciales y sociales hasta el ámbito militar o la gestión de las infraestructuras críticas nacionales. Ello ha provocado la necesidad creciente de que la tecnología se comporte como se espera, esto es de acuerdo con sus especificaciones, y de que implemente los mecanismos de seguridad apropiados desde el punto de vista de la confidencialidad, privacidad y seguridad de los datos.

Además Ortega (2020) indica que, a pesar de ello, se ha demostrado ampliamente que la tecnología actual no ha alcanzado el grado de madurez y seguridad requerido, pues es vulnerable a una gran cantidad de amenazas. Según estudios realizados, cerca del 90 % de los incidentes de seguridad del software están causados por atacantes que han explotado fallos conocidos en él. Además, en un análisis de 45 aplicaciones de negocio electrónico, se mostró que el 70 % de los fallos del software estaban relacionados con el diseño. De media, un ingeniero de software experimentado y capacitado introduce un fallo por cada nueve líneas de código. Aproximadamente, un millón de líneas de código podrían tener de mil a cinco mil fallos, los cuales podrían ser el origen de alrededor de cien vulnerabilidades en producción. Además, se ha demostrado que el software se degrada con el tiempo. y lo que vale en un momento en concreto puede no valer al cabo de seis meses.

1.1.2. Planteamiento del problema nacional

De acuerdo a la columna de opinión de Linares (2022) indica que en el 2021 hubo intentos de ciberataques en Latinoamérica y que tuvieron un incremento de un 600% comparado al 2020, en el caso de Perú, presentó 11,5 millones de intentos aproximadamente, estando por debajo de Brasil con 88,5 millones y su contraparte México con 156 millones de intentos. De acuerdo al informe de ENSC, los otros

países de la región como Colombia, Chile, Brasil y Argentina, tienen implementado estrategias de seguridad digital, en cambio Perú tiene una fase de desarrollo con nivel de madurez formativo, por lo cual aún mantienen vulnerables. según la reseña del sector público peruano, se confirman este tipo de escenarios por los ciberataques realizados. En 2011 los sitios web del Congreso de la República, Ministerio de Economía y Finanzas, Policía Nacional del Perú, Servicios al Ciudadano, Oficina Nacional de Gobierno Electrónico e Informática y Empresas reportaron ataques de varias horas ocasionados por el grupo internacional de hackers conocido como Anonymous de la sección peruana.

En su investigación Linares (2022) indago que el 2015 Anonymous nuevamente atacó sitios web de los gobiernos municipales y también al parque de las leyendas de Lima, ocasionando el bloqueo de sus accesos y colocando imágenes como medida de protesta siendo parte de un ataque masivo denominado "#OpIndependencia", en septiembre de ese mismo año, 12 sitios web del Gobierno Regional de Cajamarca presentaron ciberataques parecidos a los reportados por Anonymous esto como muestra de apoyo a Máxima Acuña una defensora ambiental. En el 2018, denunciaron un error informático en la web de la ONPE que había filtrado por varios meses datos personales de ciudadanos peruanos y que esta información se volvió accesible y descargable. En mayo del 2020 expertos de ciberseguridad reportaron que 500 hackers robaron casi un millón de soles del sistema web del Registro Nacional de Identificación y Estado Civil – RENIEC, que fue destinado a un beneficio otorgado por el gobierno nacional llamado "Bono Universal" y que se obtuvieron los datos personales de los ciudadanos beneficiarios y que fueron suplantaron. Finalmente, en noviembre del 2020, nuevamente Anonymous hackeo las páginas del Poder Judicial, Congreso Peruano, la Policía Nacional, y otras instituciones realizando su inactivación temporal, como parte del apoyo a las protestas en contra del gobierno transitorio del presidente de la república Manuel Merino. Este tipo de eventos demuestran que no es necesario iniciar enfrentamientos internacionales para vulnerar la ciberseguridad de una nación, sino que surgen de grupos individuales o colectivos.

a. Caracterización del problema

SOAINT dispone de una aplicación de información basado en la web, que contiene módulos de información y solicitudes para empleados, siendo esta web un espacio de apoyo y autogestión para sus trabajadores, al desplegar en producción esta aplicación web, se consideró adecuada la función para la cual había sido creada, pero por los antecedentes ocurridos en diversas empresas que utilizan este tipo de aplicaciones web donde en muchos caso se expone información sensible, es recomendable un analizar, identificar y gestionar las posibles brechas o debilidades en la web, con el fin de proteger los activos relevantes en el alcance propuesto y considerar su aseguramiento.

b. Enunciado del problema

¿De qué manera la implementación un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT ayudará a proteger de posibles amenazas y ataques?

1.2. Objetivos de la investigación

1.2.1. Objetivo general

Implementar un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT que permita protegerlo de posibles amenazas y ataques.

1.2.2. Objetivos específicos

1. Ejecutar pruebas de Pentesting con el fin de descubrir las vulnerabilidades presentes en la aplicación web de SOAINT.
2. Identificar las vulnerabilidades presentes en la aplicación web de SOAINT de acuerdo con las directrices del OWASP TOP 10 - 2021.
3. Evaluar la gravedad de los riesgos detectados en la aplicación web de SOAINT utilizando la metodología de riesgos de OWASP.

1.3. Justificación de la investigación

1.3.1. Justificación académica

Se aplicó los conocimientos adquiridos durante mi formación académica en la Universidad Católica los Ángeles de Chimbote, esto unido a la experiencia laboral adquirida en las funciones que desempeño, sirvió de base para solucionar los requerimientos de información de organización de estudio.

1.3.2. Justificación operativa

Se implementó el modelo de análisis de vulnerabilidades y riesgos que permitió identificar y proteger a la aplicación web de posibles amenazas y ataques que perjudiquen a la organización.

1.3.3. Justificación económica

La organización obtuvo una infraestructura y aplicación web más segura y minimizó los riegos asociados a la perdida, fuga o uso no autorizado de la información contenida en la aplicación web, así evitó gastos en nuevas tecnologías y costos operacionales.

1.3.4. Justificación tecnológica

Permitió asegurar la infraestructura tecnológica donde esta alojada la aplicación web relacionada con las TIC, benefició a la organización y solucionó la las brechas de seguridad para minimizar las posibles amenazas o ataques cibernéticos.

1.3.5. Justificación Institucional

Se implementó un modelo de análisis de vulnerabilidades y riesgos con el fin de asegurar a la aplicación web y en consecuencia ayudó al análisis continuo de seguridad en nuevos desarrollos webs o implementaciones hacia la web investigada.

1.3.6. Alcance de la Investigación

El trabajo de investigación tuvo el alcance únicamente de la aplicación web SIGO (Sistema Integrado para la Gestión y la Operación) y los componentes que la integran, la organización cuenta gerencias y áreas que en su totalidad utilizan

constantemente la aplicación web, para el presente estudio se levantó información para analizar la aplicación web y sus componentes, implementando un modelo de vulnerabilidades y riesgos, utilizando herramientas tecnológicas relacionadas a las TIC y las buenas prácticas y marcos metodológicos en seguridad, y ayudar a la organización a protegerse de posibles agentes de amenazas o ataques hechos por ciberdelincuentes, además la implementar el proyecto de investigación sirvió para implementarse en otras organizaciones que pretenden asegurar o robustecer sus aplicaciones web, infraestructura y componentes involucrados, y más aún cuando su solución se encuentra expuesto a Internet.

II. MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

La de tesis de López & Gamboa (2021), indica que las aplicaciones web en la Universidad Técnica de Ambato muestran información de vital importancia, en muchas ocasiones ésta información es estática y en otras dinámica; en muchos casos, un portal web ofrece es una ventana abierta para los ciberdelincuentes que logran utilizarlo como un medio para realizar sus ataques, por eso resulta importante, realizar un análisis de vulnerabilidades de software de las plataformas que brindan soporte en la Universidad Técnica de Ambato; para cumplir este objetivo se aplica la metodología de proyecto de seguridad de aplicaciones web (OWASP), que aporta diferentes enfoques para el análisis de vulnerabilidades utilizando herramientas que ayudan a realizar pruebas de penetración en aplicaciones web, además, aplica métodos para resolución y mitigación de dichas vulnerabilidades. Este trabajo se realiza a una determinada aplicación web de la institución, durante el segundo semestre del año académico 2020, para demostrar el cumplimiento de los objetivos se utiliza diferentes guías de prueba de ataques a sitios web usando herramientas de código abierto; con lo que se espera, que éste aporte de solución a la seguridad informática en la aplicación web de la Institución, genera una obtención de un conjunto de buenas prácticas en cuanto a la seguridad en aplicaciones web se refiere. La metodología OWASP aporta diferentes enfoques para el análisis de vulnerabilidades en aplicaciones web.

La tesis de Tasan & Morocho (2020) indica que la seguridad es importante en el desarrollo de websites y más aun tratándose del voto electrónico, así pues, el propósito de esta investigación fue sistematizar el proceso de votaciones para la elección de la Asociación de Estudiantes de la carrera de Tecnología de la Información de la Universidad Nacional de Chimborazo. Se desarrolló dos websites, un website aplicando la metodología OWASP y otro desarrollado vertiginosamente, cumpliendo los siguientes requerimientos: registro de partidos políticos con sus candidatos, sufragio, entrega del certificado, contabilización de votos, y finalmente, la emisión de resultados. Posteriormente, se realizó pentesting a los dos websites utilizando Kali Linux evaluando: disponibilidad, confidencialidad, integridad y autenticidad, al analizar los resultados obtenidos se evidenció un 19.15% de seguridad en el website desarrollado vertiginosamente, a diferencia del website desarrollado con la metodología OWASP que alcanzo un 91.75% de seguridad, de esta manera se demostró que la metodología planteada permite desarrollar un website con menos vulnerabilidades. Finalmente, se realizaron las votaciones participando 65 estudiantes de la carrera de TI, una vez terminado dicho proceso, el website con la metodología OWASP contabilizó 65 votos, correspondientes al total de votantes, a diferencia del website desarrollado de forma vertiginosa que contabilizó 78 votos, pues, algunos sufragantes pudieron votar más de una vez, por lo tanto se concluye que la metodología OWASP permitió mejorar la seguridad en el desarrollo de un website para el proceso de votación electrónica.

En la tesis de Días & Marulanda (2018), se indicó que el objetivo de analizar los riesgos de seguridad de la información en el sistema e-commerce siembraviva.com, era establecer los niveles de seguridad implementados en la actualidad, donde aplicó pruebas de caja negra, logrando así tomar acciones correctivas evitando posibles fallos y perdida de información en base a las vulnerabilidades encontradas en el sistema analizado. Para la recopilación de información utilizó herramientas de reconocimiento pasivo de acceso público como motores de búsqueda, enviando peticiones HTTP simples, forzar a la aplicación para que envíe al exterior mensajes de error. La ejecución de la metodología la dividió en dos fases, basadas en OWASP, pasiva y activa; en la primera explora las

funcionalidades de la aplicación web identificando los formularios y páginas a las que se puede acceder; en la segunda, la aplicación es sometida a pruebas mediante herramientas de rastreo entrada y salida de resultados, sniffers, mapeo de software y debilidades de parches, plugin, themes y validaciones de datos. Todo esto permitió identificar las vulnerabilidades de la aplicación web, para luego aplicar una metodología de mitigación de vulnerabilidades encontradas.

2.1.2. Antecedentes a nivel nacional

En la tesis de Pérez (2022), indico que el objetivo de este estudio fue analizar si una evaluación cuantitativa de riesgos tecnológicos de ciberseguridad ayudó en la toma de decisiones para la gestión del riesgo y de la ciberseguridad en una entidad financiera peruana. Se enfocaron en el riesgo de "Actividades maliciosas por un usuario privilegiado" en su aplicación de transferencias digitales para clientes. Se utilizaron reuniones y entrevistas con los principales stakeholders de la entidad para recopilar información y se aplicó la metodología FAIR para realizar la evaluación cuantitativa, utilizando el simulador web FAIR-U basado en el modelo matemático de Monte Carlo. Los resultados mostraron que la evaluación cuantitativa proporciona información más probabilística y permite una gestión más eficiente de los riesgos de ciberseguridad y los controles tecnológicos en comparación con una evaluación cualitativa. También se demostró de manera visual y gráfica la exposición monetaria de la entidad financiera, lo que permite a los usuarios finales tomar decisiones a corto, mediano y largo plazo para cerrar las brechas de seguridad.

En la tesis de Catillo (2021), indica que el trabajo de investigación se centra en evaluar metodologías de hacking ético para el diagnóstico de vulnerabilidades en la seguridad informática de una empresa de servicios logísticos. Se destaca la importancia de la ciberseguridad en las organizaciones peruanas y se menciona que las aplicaciones web son el principal objetivo de los ciberataques. El estudio se basó en pruebas realizadas a la empresa cliente, como pruebas a puertos abiertos, servidores web y FTP, así como ataques de fuerza bruta. Se implementaron metodologías de hacking ético utilizando herramientas como Nessus y Burp Suite.

El trabajo concluyó con la medición de los resultados obtenidos a través del hacking ético.

En la tesis de Rojas & Muedas (2019), indica que la creciente competitividad del mercado ha llevado a las organizaciones a priorizar criterios económicos, tiempo, costo, calidad y alcance en sus proyectos, lo que ha resultado en la falta de controles de seguridad y brechas en la compañía. En particular, se descuidan los procedimientos de seguridad como el testeo de aplicaciones web, las cuales pueden contener vulnerabilidades que permiten a usuarios maliciosos acceder a información privada o recursos de la empresa. Se pronostica que la industria de la salud será el objetivo principal de los ataques cibernéticos debido al alto valor de los registros de salud electrónicos, que representan una fuente de ganancias atractiva para los cibercriminales en comparación con la información de tarjetas o cuentas bancarias.

2.1.3. Antecedentes a nivel regional

En la tesis de Calvo (2022) realizó una introducción a la seguridad informática, con el fin de identificar las posibles vulnerabilidades, aplicando las fases de un pentesting, teniendo como objetivo principal el determinar la relación entre la aplicación de un pentesting y la seguridad informática para los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo. Se utilizó OWASP Top 10 para lograr identificar vulnerabilidades, dando como resultado hallazgos de riesgos altos en servidores de aplicación y en el código fuente de desarrollo.

En la tesis de Terrones (2022) indica que existe el peligro de ser vulnerado por ataques cibernéticos que aprovechan las vulnerabilidades o brechas de seguridad para apropiarse de la información de la empresa; por lo que tuvo como objetivo, realizar una propuesta para implementar de un honeypot de seguridad informática en la agropecuaria Wilian & Roque; aplicando en una investigación de tipo cuantitativo y de nivel descriptivo, que fue desarrollada con diseño no experimental de corte transversal, tomando de muestra una población de 20 personas, entre ellas empleados y clientes y utilizó el cuestionario como instrumento de recolección de datos y la encuesta como la técnica, los resultados

indicaron consideran importante la seguridad informática y necesitaban implementar un honeypot para controlar los ataques cibernéticos; su alcance de investigación es controlar los ataques cibernéticos y conocer las técnicas que utiliza el ciberdelincuente con el fin de vulnerar los sistemas de información y afectar a la empresa, empleados y clientes.

En la tesis de Llerena (2018), indica que el objetivo principal de esta investigación es evaluar la seguridad informática en el área de sistemas de la municipalidad distrital de Nuevo Chimbote, identificando vulnerabilidades y proponiendo medidas preventivas para su mejora. Este estudio se basa en una metodología documental-descriptiva y no experimental. Se recopilaron datos utilizando técnicas como observación, análisis, encuestas, entrevistas y revisión de documentos. Para evaluar la seguridad informática, se utilizó el marco de trabajo Cobit 5, que se centra en la integridad, confidencialidad y disponibilidad de la información, así como en el cumplimiento de normas y estándares internacionales. El objetivo final es garantizar la continuidad de los servicios y mejorar el control de procesos para gestionar los riesgos de manera efectiva.

2.2. Bases teóricas

2.2.1. El rubro de la empresa

SOAINT una compañía global con presencia en 10 países y cerca de 800 personas, que analiza su impacto estratégico y aporta la visión necesaria para evaluar, planificar, adecuar y desplegar tecnologías emergentes, así como de productos y soluciones asociados con equipos o metodologías agile.

Ofrecemos soluciones tecnológicas avanzadas como:

- Customer Experience (CX)
- Automatización de Procesos (BPM /RPA)
- Interoperabilidad (SOA /MSA)
- Gestión de Contenido Empresarial (ECM)
- API Governance

- Modernización de Aplicaciones
- Gestión de Fraude e Identidades

En servicios de implementación, somos especialistas en cada una de las tecnologías señaladas, bajo los productos de IBM, Red Hat, Automation Anywhere, Amazon y Oracle.

Nuestro know-how (Conocimientos) técnico y aplicación metodológica han sido validados y ejecutados en sectores como administración pública, retail, sanidad, banca, seguros y telecomunicaciones. (SOAINT, Linkedin - SOAINT, 2023)

2.2.2. La empresa investigada

- **Información general**

DENOMINACIÓN DE LA ORGANIZACIÓN

Nombre : Soaint Perú S.A.C.

Sigla : SOAINT

Ubicación : Calle 21 N° 713 Int. 206 Urb. Corpac – San Isidro, Lima - Perú

Categorización : Consultores Prog. y Sumin. Informatic.

DATOS GEOGRÁFICOS

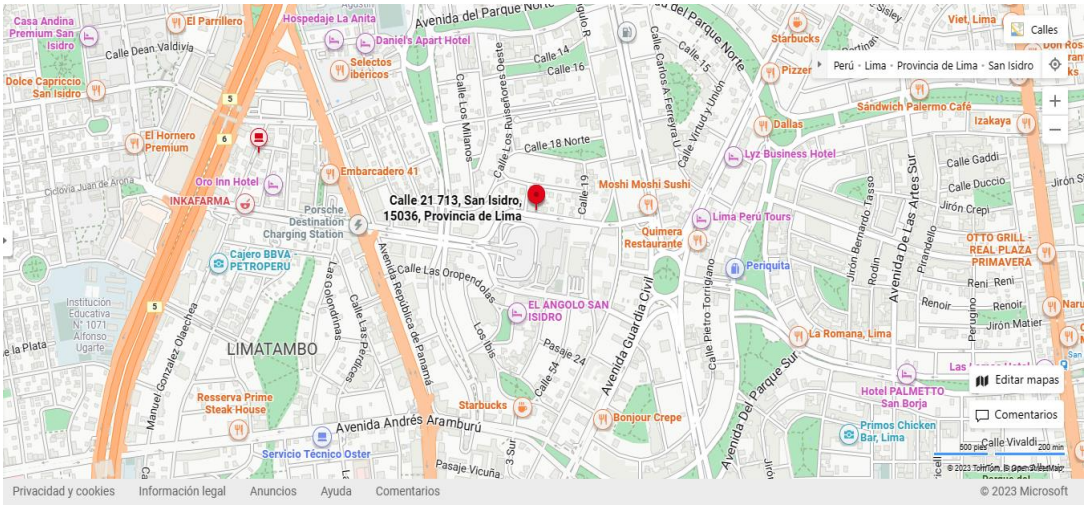
Localización : Soaint se encuentra en ubicado en Urbanización Corpac, frente al ministerio del interior del Perú (MININTER), del Distrito San Isidro en la Provincia del Lima, Perú.

Superficie : Tiene un área física conformada y saneada de aproximadamente de 200 m2.

Altitud : Se encuentra a una altitud de 109 msnm

Figura 1

Ubicación Geográfica de Soaint



Nota. Imagen de Ubicación (Google, 2023)

- **Historia**

  Fundada en 1996, SOAINT ha crecido hasta convertirse en una de las principales empresas de tecnología en América Latina. Cuenta con oficinas en varios países de la región, incluyendo Perú, Chile, Colombia, México y Argentina, lo que le permite brindar servicios a clientes en toda la región. Comenzaron con una pequeña oficina en Madrid y un reducido equipo, pero con mucho esfuerzo para conseguir internacionalizarse y que la marca tenga presencia, no solo en España, sino en prácticamente toda Latino América. (SOAINT, Quiénes Somos, 2022)

- **Objetivos organizacionales**

  Misión

  Desde un enfoque creativo e innovador, conectamos con nuestros clientes brindando las mejores personas para las mejores soluciones

  “Para dar lo mejor, hay que ser lo mejor”

  Buscamos la mejor versión de nuestros talentos y nos enfocamos en formar equipos diversos, sólidos y comprometidos, preparados para entender las necesidades particulares de nuestros clientes y brindar soluciones desde un enfoque creativo e innovador. (SOAINT, 2022)

Visión

Transformar el mundo con soluciones tecnológicas inspirando el progreso de nuestras comunidades

A través de la tecnología buscamos inspirar a nuestras comunidades y contribuir con la prosperidad sostenible de las mismas. Queremos transformar el mundo desde nuestras soluciones tecnológicas y nuestros servicios, fomentar el desarrollo de nuestros clientes y el crecimiento de nuestros colaboradores como personas y miembros de nuestra comunidad. (SOAINT, 2022)

Valores institucionales

- Responsabilidad
- Compromiso
- Identificación
- Dedicación

Principios institucionales

Aún no brindan la información (En coordinación con la empresa)

- **Funciones**

a. Identificar objetivos estratégicos relacionados con el plan de TI,

b. Incorporar elementos de arquitectura empresarial que permitan ordenar el camino.

c. Incorporar interesados de todas las áreas responsables para organizar iniciativas compartidas.

d. Identificar y mapear las capacidades de negocio que se quieren apoyar con una optimización.

e. Identificar las capacidades técnicas, y en general, el compromiso de las partes interesadas (Stakeholders), entre otros.

- **Organigrama**

Nueva Filosofía de Liderazgo; Más que una metodología, es una filosofía de liderazgo que nos permitirá ser ágiles y dinámicos para afrontar nuestros desafíos, cumplir nuestros objetivos y acercarnos cada vez más a nuestro propósito de ayudar a transformar el mundo a través de la tecnología

Figura 2

Organigrama por anillos - Presidencia

Nota. Presidencia (SOAINT, Nueva Filosofía de Liderazgo, 2023)

Figura 3

Organigrama por anillos – Dirección regional

Nota. Dirección regional (SOAINT, Nueva Filosofía de Liderazgo, 2023)

Figura 4

Organigrama por anillos – Centro regional de apoyo

Nota. Centro regional de apoyo (SOAINT, Nueva Filosofía de Liderazgo, 2023)

Figura 5

Organigrama por anillos – Comité de Gerencia

Nota. Comité de gerencia (SOAINT, Nueva Filosofía de Liderazgo, 2023)

Infraestructura tecnológica existente

No se brindó la información

Una tabla para aplicaciones propias de la empresa

Aún no brindan la información (En coordinación con la empresa)

2.2.3. Las tecnologías de la información y comunicaciones

- **Definición**

  Las tecnologías de la información y comunicación se encuentran en todos los ámbitos de la vida actual, reflejándose en diversos instrumentos técnicos de manera interactiva como dispositivos y sistemas que nos ayudan a que las acciones del día sean mucho más fáciles, como computadoras, teléfonos inteligentes, televisores o tablets y los sistemas que se encuentran dentro de ellas que permiten su funcionamiento Las Tecnologías de la Información y la Comunicación (TIC) son el conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas. (Meneses, 2007)

  Las TIC han transformado la forma en que nos relacionamos, desplazando los espacios de socialización presenciales por los virtuales. Esta incorporación ha tenido un impacto social significativo, ya que el Internet, los teléfonos inteligentes, los videojuegos y las redes sociales han pasado de ser simples herramientas de comunicación interpersonal a plataformas complejas que afectan tanto la esfera privada como la pública. Aunque su uso genera diferentes sensaciones relacionadas con la independencia, el estatus social, la seguridad, el control y el ocio, el abuso y exceso de estas tecnologías pueden conducir a alteraciones conductuales y representar un riesgo real si no se tiene conciencia de su uso y sus consecuencias. (Hernández-Pérez, 2019)

- **TIC es la abreviatura de Tecnologías de la Información y la Comunicación.**

  Las TIC han transformado los parámetros de obtención de información por medio de las tecnologías de la comunicación (diario, radio y televisión), a través del desarrollo de Internet y de los nuevos dispositivos tecnológicos como la computadora, la tableta y el smartphone, así como las plataformas y softwares disponibles.

Actualmente el papel de las TIC en la sociedad es muy importante porque ofrecen muchos servicios como: correo electrónico, búsqueda de información, banca online, descarga de música y cine, comercio electrónico, etc. Por esta razón las TIC han incursionado fácilmente en diversos ámbitos de la vida, entre ellos, el de la educación.

- **Historia**

Las TIC surgen de manera aproximativa a raíz de la invención del telégrafo (1833) y el posterior despliegue de redes telegráficas por la geografía nacional, que en España se desarrolla entre los años 1850 y 1900. Actualmente, estamos acostumbrados a coexistir con todo tipo de servicios que nos facilitan la comunicación entre personas, pero la experiencia con estos sistemas es relativamente reciente (Alex, 2011).

El uso de nuevos tipos de señales y el desarrollo de nuevos medios de transmisión, adaptados a las crecientes necesidades de comunicación, han sido fenómenos paralelos al desarrollo de la historia. Otros hitos y hechos importantes que han marcado la evolución de las telecomunicaciones y, por tanto, el devenir de las tecnologías de la información y comunicaciones.

Las Tecnologías de Información y Comunicación (TIC) ocupan un lugar primordial en la sociedad de la información, con una tendencia creciente. El concepto de TIC surge como tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones, la agrupación de estas tres tecnologías da lugar a una concepción del avance progresivo de la información, en el que las comunicaciones otorgan nuevos horizontes y paradigmas (Alex, 2011).

Este progreso histórico de las TIC, desde la década 70 constituye el punto de partida para la creciente Era Digital, los avances científicos en el campo de la electrónica tuvieron dos consecuencias inmediatas, la caída vertiginosa de los precios de las materias primas y el predominio de las Tecnologías de la Información, que combinan esencialmente la electrónica y el software (Alex, 2011).

Las investigaciones desarrolladas a inicios de los años 80 han permitido la convergencia de la electrónica, la informática y las telecomunicaciones lo que posibilita la conexión entre redes, de esta manera las TIC son un sector estratégico para la "Nueva Economía", por lo que los criterios de éxito en una

organización o institución dependen cada vez de su capacidad para adaptarse a las nuevas innovaciones tecnológicas y saber explotarlas en su propio beneficio (Sutori, 2019).

- **Las TIC más utilizadas en la empresa investigada**

  Soaint, como organización cuenta con una aplicación web, contiene módulos para solicitudes de sus empleados, esta web un espacio para gestionar solicitudes de sus trabajadores, cuenta con controles de seguridad intuitos para el resguardo de su información.

2.2.4. Tecnología de la investigación

2.2.4.1. Aplicaciones Web

Las aplicaciones web son sistemas que se ejecutan a través de Internet utilizando un navegador web. La información que se visualiza en estas aplicaciones es almacenada y procesada en un entorno web. En general, el desarrollo de aplicaciones web es utilizado porque su desarrollo requiere menos recursos en comparación con las aplicaciones de escritorio. Además, se puede acceder a ellas en cualquier momento a través de dispositivos como teléfonos móviles, tablets y laptops, siempre y cuando se disponga de conexión a Internet. La comunicación entre las páginas web se lleva a cabo mediante protocolos, siendo los más comunes HTTP, HTTPS, SMTP y FTP, los cuales facilitan la interacción entre diferentes procesos.

2.2.4.2. Lenguajes de Programación del Servidor Web

Los lenguajes de programación se utilizan para crear aplicaciones web y permiten a los desarrolladores escribir instrucciones, realizar cálculos y ejecutar operaciones con el objetivo de alcanzar un objetivo o solución. A continuación, se mencionan algunos de los lenguajes de programación más comúnmente utilizados en el desarrollo de aplicaciones web:

JAVA: Es ampliamente utilizado por organizaciones y es un lenguaje de programación orientado a objetos que puede ser ejecutado en diversos dispositivos. Tiene una amplia gama de bibliotecas y frameworks, lo que le permite ser utilizado tanto para aplicaciones de escritorio como para aplicaciones web.

PHP: Este lenguaje de programación es ampliamente reconocido y cuenta con una licencia de código abierto. Fue especialmente creado para el desarrollo de sitios web y ofrece la capacidad de integrar código HTML en su estructura, lo que simplifica la creación de contenido dinámico en páginas web.

PYTHON: Es un lenguaje de programación de alto nivel, orientado a objetos y de fácil interpretación, con una sintaxis legible. Es especialmente adecuado para prototipos y tareas ad hoc. tiene una amplia gama de aplicaciones, desde la computación científica hasta el desarrollo web y la automatización. Como un lenguaje popular tanto para principiantes como para desarrolladores experimentados, Python es ampliamente respaldado por la comunidad científica y de desarrollo de aplicaciones en todo el mundo.

2.2.4.3.Lenguajes de Base del Servidor Web

Los sistemas son responsables de administrar datos almacenados en una base de datos, con el propósito principal de manipular, utilizar y describir dichos datos. A continuación, a continuación, se definen los sistemas de gestión de bases de datos (DBMS):

SQL SERVER: Base de datos ampliamente utilizada en organizaciones de diversos tamaños que ofrece compatibilidad con sistemas Windows. Además, puede integrarse con numerosas herramientas de Microsoft, lo que facilita su adopción.

MYSQL: Es una base de datos relacional muy popular que se ha desarrollado bajo una licencia de código abierto. Su uso está extendido y es apreciado por su eficiencia y versatilidad en diferentes aplicaciones.

MongoDB: Es una base de datos que está ganando popularidad debido a su capacidad para trabajar con datos estructurados y no estructurados. Destaca por su excelente rendimiento y escalabilidad, lo que la hace una opción atractiva para proyectos que requieren un manejo eficiente de grandes volúmenes de datos.

2.2.4.4.OWASP (Open Web Application Security Project)

OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera. (Wikipedia, 2022)

2.2.4.5.OWASP TOP 10 – 2021

OWASP Top 10 es un proyecto sin ánimo de lucro que establece cuáles son los 10 ciberataques más comunes en el mundo de las aplicaciones web. Su última actualización fue realizada en 2021 y vale la pena utilizar esta lista como una guía para tus auditorías de ciberseguridad. No es posible automatizar un escaneo de todo este tipo de ciberataques en una app web. Por eso, debe hacerse de forma manual.

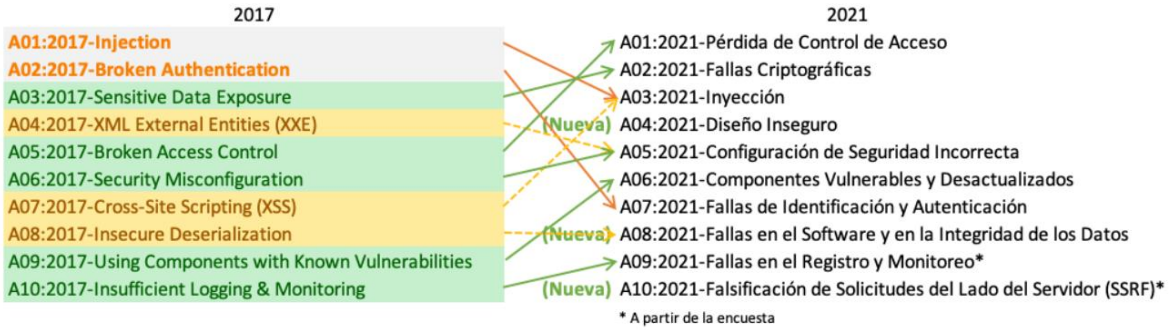
OWASP (Open Web Application Security Project) es una organización sin ánimo de lucro que se fundó el 2 de diciembre de 2001 en Maryland, Estados Unidos. Surgió con el fin de crear conciencia sobre la seguridad de aplicaciones web. En este momento, que existe una enorme cantidad de páginas web, los riesgos de seguridad son más altos que nunca y, por eso, su proyecto de OWASP Top 10 ha cobrado mayor vigencia que nunca. (KeepCoding, 2023)

2.2.4.6.OWASP TOP 10 – 2017 vs 2021

Hay tres nuevas categorías, cuatro categorías con cambios de nombre y alcance, y alguna consolidación en el Top 10 de 2021. Hemos cambiado los nombres cuando ha sido necesario para centrarnos en la causa principal en lugar del síntoma.

Figura 6

Owasp Top 10 – 2017 vs 2021

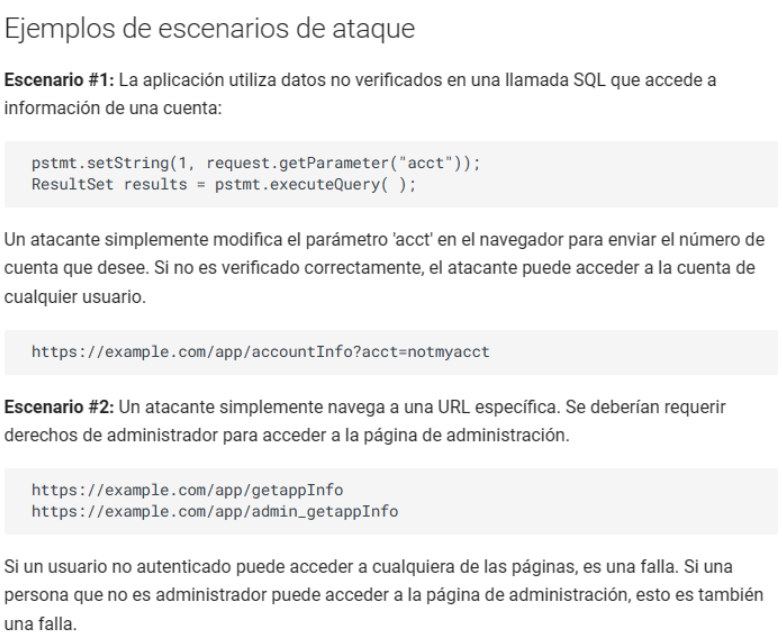


Nota. Owasp Top 10 – 2017 vs. 2021 (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

a. A01:2021 – Pérdida de Control de Acceso

Figura 7

Pérdida de Control de Acceso



Ejemplos de escenarios de ataque

Escenario #1: La aplicación utiliza datos no verificados en una llamada SQL que accede a información de una cuenta:

```
pstmt.setString(1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery( );
```

Un atacante simplemente modifica el parámetro 'acct' en el navegador para enviar el número de cuenta que desee. Si no es verificado correctamente, el atacante puede acceder a la cuenta de cualquier usuario.

```
https://example.com/app/accountInfo?acct=notmyacct
```

Escenario #2: Un atacante simplemente navega a una URL específica. Se deberían requerir derechos de administrador para acceder a la página de administración.

```
https://example.com/app/getappInfo
https://example.com/app/admin_getappInfo
```

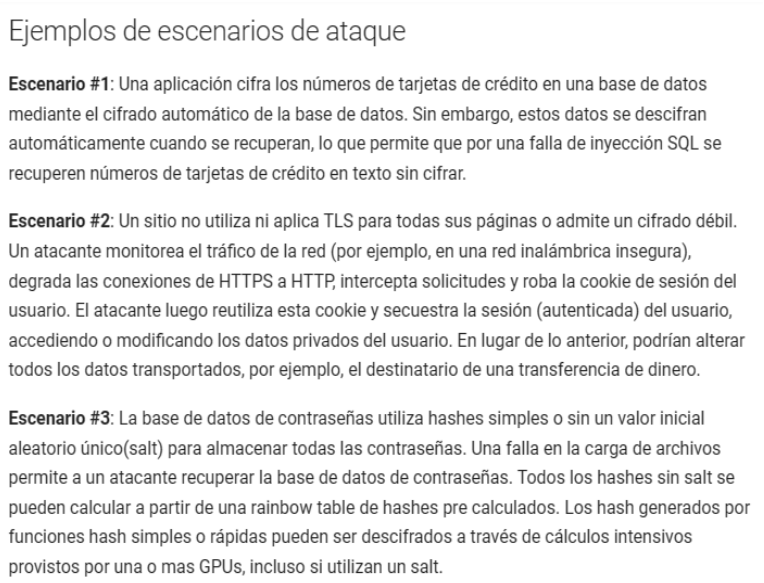
Si un usuario no autenticado puede acceder a cualquiera de las páginas, es una falla. Si una persona que no es administrador puede acceder a la página de administración, esto es también una falla.

Nota. Ejemplos de pérdida de control de acceso (Owasp, OWASP Top 10:2021, 2021)

b. A02:2021 – Fallas Criptográficas

Figura 8

Fallas Criptográficas



Nota. Ejemplos de fallas criptográficas (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

c. A03:2021 – Inyección

Figura 9

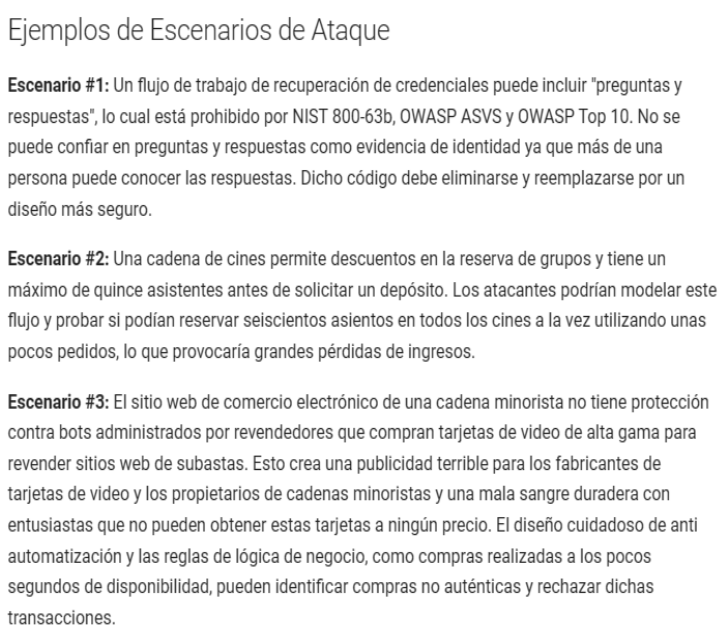
Inyección

Nota. Ejemplos de inyección (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

d. A04:2021 – Diseño Inseguro

Figura 10

Diseño Inseguro



Ejemplos de Escenarios de Ataque

Escenario #1: Un flujo de trabajo de recuperación de credenciales puede incluir "preguntas y respuestas", lo cual está prohibido por NIST 800-63b, OWASP ASVS y OWASP Top 10. No se puede confiar en preguntas y respuestas como evidencia de identidad ya que más de una persona puede conocer las respuestas. Dicho código debe eliminarse y reemplazarse por un diseño más seguro.

Escenario #2: Una cadena de cines permite descuentos en la reserva de grupos y tiene un máximo de quince asistentes antes de solicitar un depósito. Los atacantes podrían modelar este flujo y probar si podían reservar seiscientos asientos en todos los cines a la vez utilizando unas pocos pedidos, lo que provocaría grandes pérdidas de ingresos.

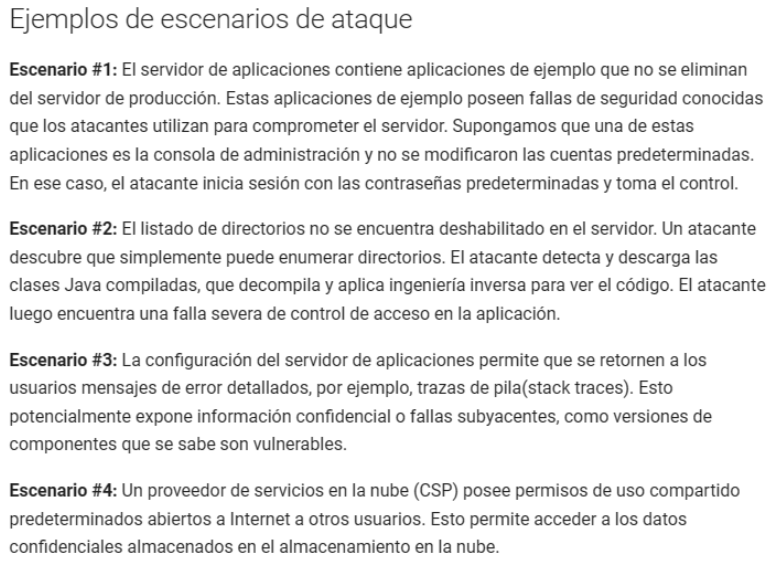
Escenario #3: El sitio web de comercio electrónico de una cadena minorista no tiene protección contra bots administrados por revendedores que compran tarjetas de video de alta gama para revender sitios web de subastas. Esto crea una publicidad terrible para los fabricantes de tarjetas de video y los propietarios de cadenas minoristas y una mala sangre duradera con entusiastas que no pueden obtener estas tarjetas a ningún precio. El diseño cuidadoso de anti automatización y las reglas de lógica de negocio, como compras realizadas a los pocos segundos de disponibilidad, pueden identificar compras no auténticas y rechazar dichas transacciones.

Nota. Ejemplos de diseño inseguro (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

e. A05:2021 – Configuración de Seguridad Incorrecta

Figura 11

Configuración de Seguridad Incorrecta



Ejemplos de escenarios de ataque

Escenario #1: El servidor de aplicaciones contiene aplicaciones de ejemplo que no se eliminan del servidor de producción. Estas aplicaciones de ejemplo poseen fallas de seguridad conocidas que los atacantes utilizan para comprometer el servidor. Supongamos que una de estas aplicaciones es la consola de administración y no se modificaron las cuentas predeterminadas. En ese caso, el atacante inicia sesión con las contraseñas predeterminadas y toma el control.

Escenario #2: El listado de directorios no se encuentra deshabilitado en el servidor. Un atacante descubre que simplemente puede enumerar directorios. El atacante detecta y descarga las clases Java compiladas, que decompila y aplica ingeniería inversa para ver el código. El atacante luego encuentra una falla severa de control de acceso en la aplicación.

Escenario #3: La configuración del servidor de aplicaciones permite que se retornen a los usuarios mensajes de error detallados, por ejemplo, trazas de pila(stack traces). Esto potencialmente expone información confidencial o fallas subyacentes, como versiones de componentes que se sabe son vulnerables.

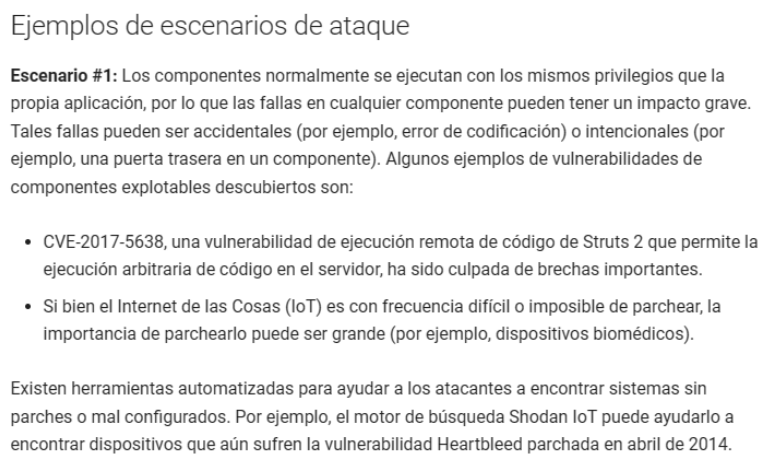
Escenario #4: Un proveedor de servicios en la nube (CSP) posee permisos de uso compartido predeterminados abiertos a Internet a otros usuarios. Esto permite acceder a los datos confidenciales almacenados en el almacenamiento en la nube.

Nota. Ejemplos de configuración de seguridad incorrecta (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

f. A06:2021 – Componentes Vulnerables y Desactualizados

Figura 12

Componentes Vulnerables y Desactualizados



Ejemplos de escenarios de ataque

Escenario #1: Los componentes normalmente se ejecutan con los mismos privilegios que la propia aplicación, por lo que las fallas en cualquier componente pueden tener un impacto grave. Tales fallas pueden ser accidentales (por ejemplo, error de codificación) o intencionales (por ejemplo, una puerta trasera en un componente). Algunos ejemplos de vulnerabilidades de componentes explotables descubiertos son:

- CVE-2017-5638, una vulnerabilidad de ejecución remota de código de Struts 2 que permite la ejecución arbitraria de código en el servidor, ha sido culpada de brechas importantes.
- Si bien el Internet de las Cosas (IoT) es con frecuencia difícil o imposible de parchear, la importancia de parchearlo puede ser grande (por ejemplo, dispositivos biomédicos).

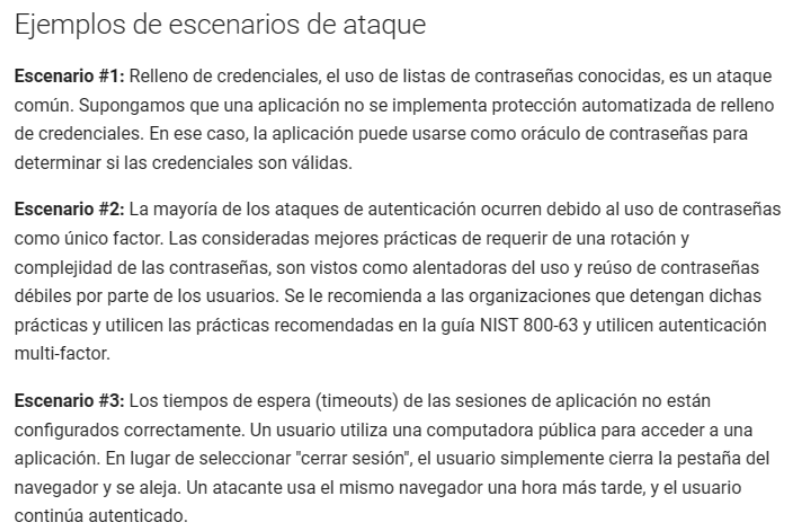
Existen herramientas automatizadas para ayudar a los atacantes a encontrar sistemas sin parches o mal configurados. Por ejemplo, el motor de búsqueda Shodan IoT puede ayudarlo a encontrar dispositivos que aún sufren la vulnerabilidad Heartbleed parchada en abril de 2014.

Nota. Ejemplos de componentes vulnerables y desactualizados (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

g. A07:2021 – Fallas de Identificación y Autenticación

Figura 13

Fallas de Identificación y Autenticación



Ejemplos de escenarios de ataque

Escenario #1: Relleno de credenciales, el uso de listas de contraseñas conocidas, es un ataque común. Supongamos que una aplicación no se implementa protección automatizada de relleno de credenciales. En ese caso, la aplicación puede usarse como oráculo de contraseñas para determinar si las credenciales son válidas.

Escenario #2: La mayoría de los ataques de autenticación ocurren debido al uso de contraseñas como único factor. Las consideradas mejores prácticas de requerir de una rotación y complejidad de las contraseñas, son vistos como alentadoras del uso y reúso de contraseñas débiles por parte de los usuarios. Se le recomienda a las organizaciones que detengan dichas prácticas y utilicen las prácticas recomendadas en la guía NIST 800-63 y utilicen autenticación multi-factor.

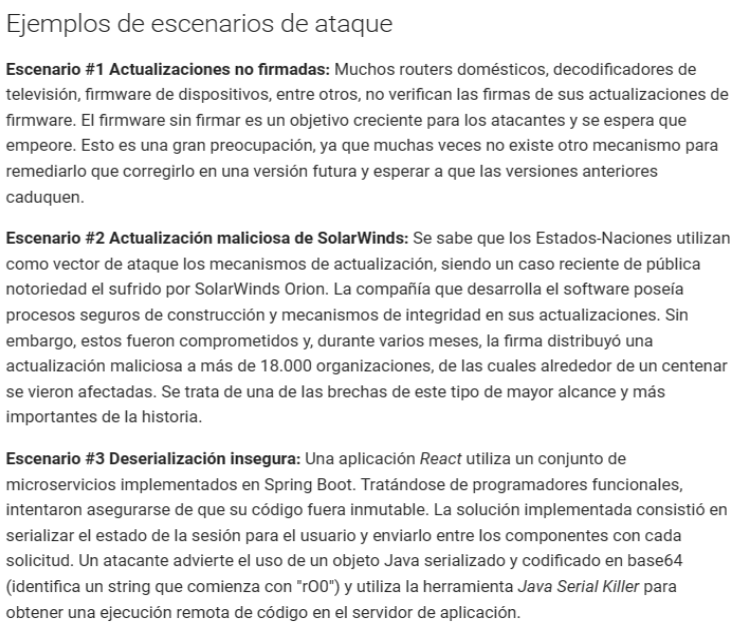
Escenario #3: Los tiempos de espera (timeouts) de las sesiones de aplicación no están configurados correctamente. Un usuario utiliza una computadora pública para acceder a una aplicación. En lugar de seleccionar "cerrar sesión", el usuario simplemente cierra la pestaña del navegador y se aleja. Un atacante usa el mismo navegador una hora más tarde, y el usuario continúa autenticado.

Nota. Ejemplos de fallas de identificación y autenticación (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

h. A08:2021 – Fallas en el Software y en la Integridad de los datos

Figura 14

Fallas en el Software y en la Integridad de los Datos



Ejemplos de escenarios de ataque

Escenario #1 Actualizaciones no firmadas: Muchos routers domésticos, decodificadores de televisión, firmware de dispositivos, entre otros, no verifican las firmas de sus actualizaciones de firmware. El firmware sin firmar es un objetivo creciente para los atacantes y se espera que empeore. Esto es una gran preocupación, ya que muchas veces no existe otro mecanismo para remediarlo que corregirlo en una versión futura y esperar a que las versiones anteriores caduquen.

Escenario #2 Actualización maliciosa de SolarWinds: Se sabe que los Estados-Naciones utilizan como vector de ataque los mecanismos de actualización, siendo un caso reciente de pública notoriedad el sufrido por SolarWinds Orion. La compañía que desarrolla el software poseía procesos seguros de construcción y mecanismos de integridad en sus actualizaciones. Sin embargo, estos fueron comprometidos y, durante varios meses, la firma distribuyó una actualización maliciosa a más de 18.000 organizaciones, de las cuales alrededor de un centenar se vieron afectadas. Se trata de una de las brechas de este tipo de mayor alcance y más importantes de la historia.

Escenario #3 Deserialización insegura: Una aplicación *React* utiliza un conjunto de microservicios implementados en Spring Boot. Tratándose de programadores funcionales, intentaron asegurarse de que su código fuera inmutable. La solución implementada consistió en serializar el estado de la sesión para el usuario y enviarlo entre los componentes con cada solicitud. Un atacante advierte el uso de un objeto Java serializado y codificado en base64 (identifica un string que comienza con "rO0") y utiliza la herramienta *Java Serial Killer* para obtener una ejecución remota de código en el servidor de aplicación.

Nota. Ejemplos de fallas en el software y en la integridad de los datos (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

i. A09:2021 – Fallas en el Registro y Monitoreo

Figura 15

Fallas en el Registro y Monitoreo

Ejemplos de escenarios de ataque

Escenario #1: El sitio web de un prestador de salud que provee un plan para niños no pudo detectar una brecha debido a la falta de monitoreo y registro. Alguien externo informó al prestador que un atacante había accedido y modificados registros médicos sensibles de más de 3,5 millones de niños. Una revisión post incidente detectó que los desarrolladores del sitio web no habían encontrado vulnerabilidades significativas. Como no hubo ni registro ni monitores del sistema, la brecha de datos pudo haber estado en proceso desde el 2013, por un período de más de 7 años.

Escenario #2: Una gran aerolínea India tuvo una brecha de seguridad que involucró a la pérdida de datos personales de millones de pasajeros por más de 10 años, incluyendo pasaportes y tarjetas de crédito. La brecha se produjo por un proveedor de servicios de almacenamiento en la nube, quien notificó a la aerolínea después de un tiempo.

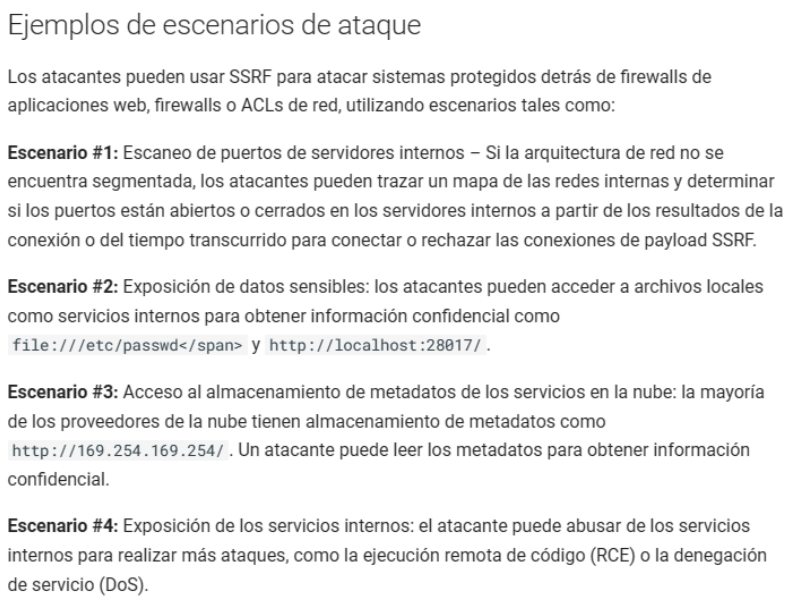
Escenario #3: Una gran aerolínea Europea sufrió un incumplimiento de la GRPD que debe reportar. La causa de la brecha se debió a que un atacante explotó una vulnerabilidad en una aplicación de pago, obteniendo más de 400,000 registros de pagos de usuarios. La aerolínea fue multada con 20 millones de libras como resultado del regulador de privacidad.

Nota. Ejemplos de fallas en el registro y monitoreo (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

j. A10:2021 – Falsificación de Solicitudes del Lado del Servidor (SSRF)

Figura 16

Falsificación de Solicitudes del Lado del Servidor (SSRF)



Ejemplos de escenarios de ataque

Los atacantes pueden usar SSRF para atacar sistemas protegidos detrás de firewalls de aplicaciones web, firewalls o ACLs de red, utilizando escenarios tales como:

Escenario #1: Escaneo de puertos de servidores internos – Si la arquitectura de red no se encuentra segmentada, los atacantes pueden trazar un mapa de las redes internas y determinar si los puertos están abiertos o cerrados en los servidores internos a partir de los resultados de la conexión o del tiempo transcurrido para conectar o rechazar las conexiones de payload SSRF.

Escenario #2: Exposición de datos sensibles: los atacantes pueden acceder a archivos locales como servicios internos para obtener información confidencial como `file:///etc/passwd</span>` y `http://localhost:28017/`.

Escenario #3: Acceso al almacenamiento de metadatos de los servicios en la nube: la mayoría de los proveedores de la nube tienen almacenamiento de metadatos como `http://169.254.169.254/`. Un atacante puede leer los metadatos para obtener información confidencial.

Escenario #4: Exposición de los servicios internos: el atacante puede abusar de los servicios internos para realizar más ataques, como la ejecución remota de código (RCE) o la denegación de servicio (DoS).

Nota. Ejemplos de SSRF (Owasp, Bienvenido al OWASP Top 10 - 2021, 2021)

2.2.4.7. OWASP Risk Rating Methodology

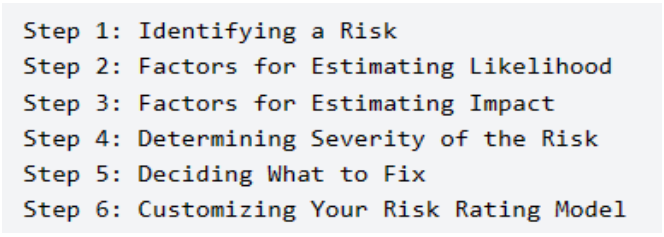
Al principio del ciclo de vida, se puede tener una identificación de brechas de seguridad en la arquitectura o en el diseño, bajo un modelo de amenazas. luego, podemos encontrar brechas de seguridad mediante el análisis de código o pentesting. Las brechas pueden no ser descubiertas en el momento del desarrollo y pruebas, pero cuando la aplicación se encuentra en un ambiente productivo surgen los hallazgos y se compromete la aplicación.

Siguiendo esta metodología, es factible evaluar la gravedad de cada uno de estos riesgos para poder tomar decisiones informadas sobre cómo abordarlos. Contar con un sistema establecido para clasificar los riesgos permitirá ahorrar tiempo y evitar debates sobre cuáles riesgos son prioritarios. Este sistema garantizará que el negocio no se distraiga con

riesgos de menor importancia y, en cambio, se enfoque en los riesgos más graves que requieren una atención adecuada.

Figura 17

Pasos a seguir para OWASP Risk Rating Methodology



Nota. Pasos a seguir para OWASP Risk Rating Methodology (Owasp, 2023)

a. Paso 1: Identificar un riesgo

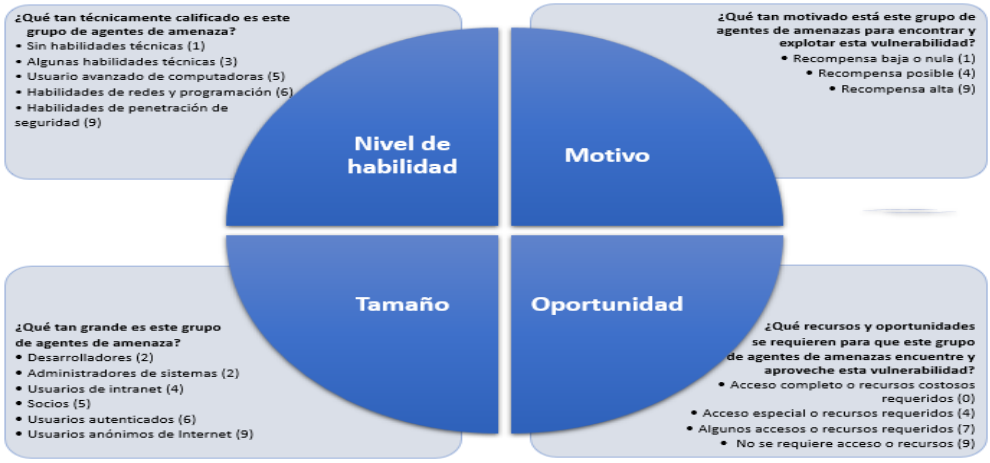
El primer paso es identificar un riesgo de seguridad que necesita ser calificado. El probador necesita reunir Información sobre el agente de amenaza involucrado, el ataque que se utilizará, la vulnerabilidad involucrados, y el impacto de un exploit exitoso en el negocio. Puede haber múltiples posibilidades grupos de atacantes, o incluso múltiples posibles impactos en el negocio. En general, es mejor errar en el lado de la precaución al usar la opción del peor de los casos, ya que eso resultará en el mayor riesgo general. (Owasp, OWASP_Risk_Rating_Methodology, 2023)

b. Paso 2: Factores para estimar la probabilidad

- **Factores del agente de amenazas**

Figura 18

Factores del agente de amenazas

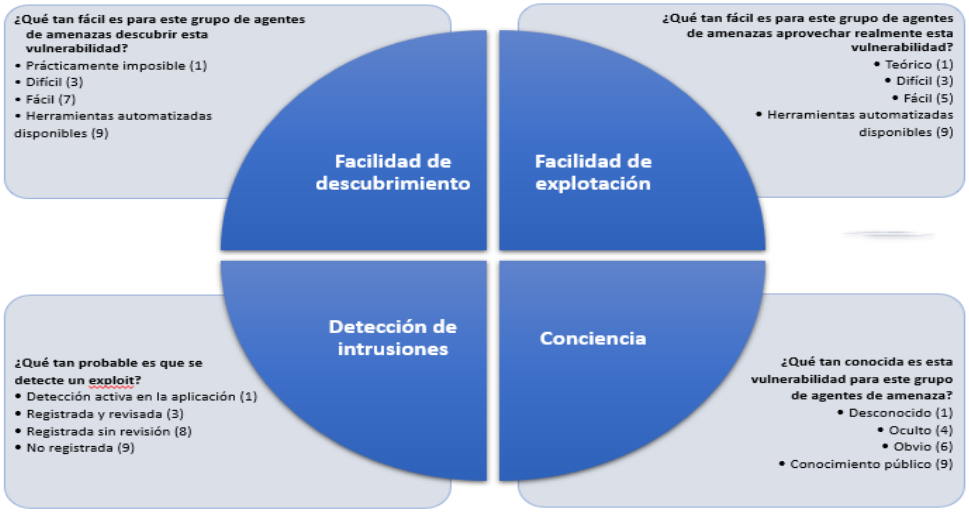


Nota. Factores del agente de amenazas (Owasp, OWASP_Risk_Rating_Methodology, 2023)

- **Factores de vulnerabilidad**

Figura 19

Factores de vulnerabilidad



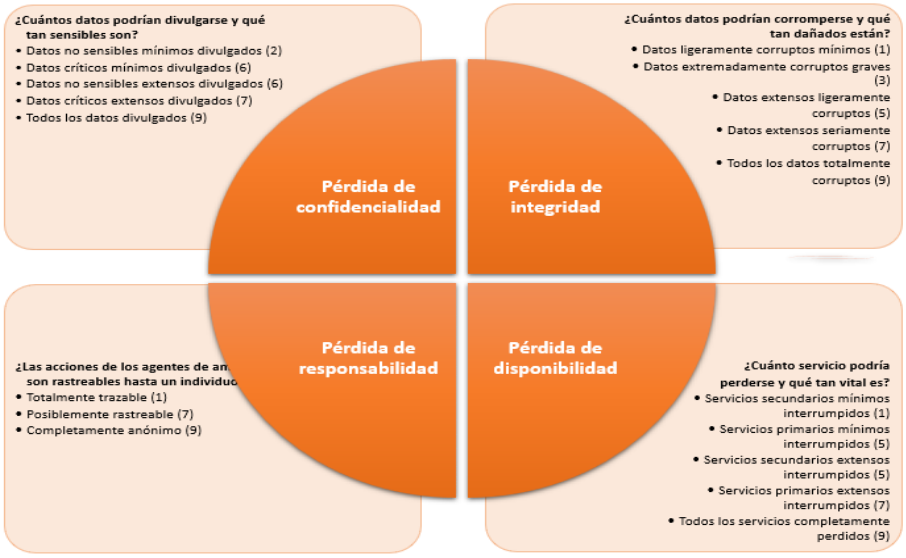
Nota. Factores de vulnerabilidad (Owasp, OWASP_Risk_Rating_Methodology, 2023)

c. Paso 3: Factores para estimar el impacto

- **Factores de impacto técnico**

Figura 20

Factores de impacto técnico

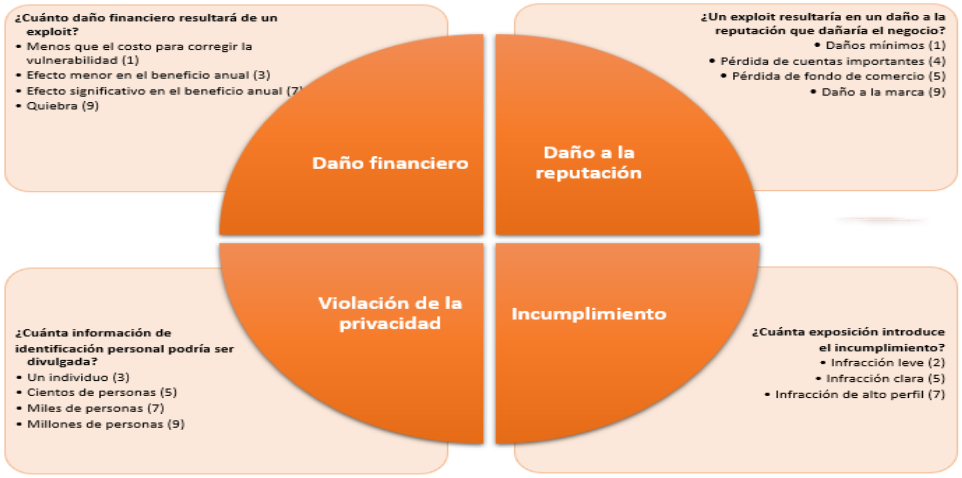


Nota. Factores de impacto técnico (Owasp, OWASP_Risk_Rating_Methodology, 2023)

- **Factores de impacto en el negocio**

Figura 21

Factores de impacto en el negocio

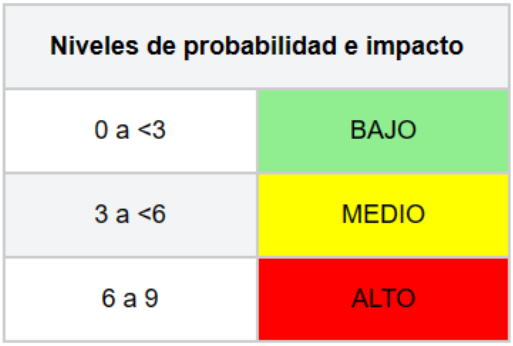


Nota. Factores de impacto en el negocio (Owasp, OWASP_Risk_Rating_Methodology, 2023)

d. Paso 4: Determinar la gravedad del riesgo

Figura 22

Niveles de probabilidad e impacto



Niveles de probabilidad e impacto	
0 a <3	BAJO
3 a <6	MEDIO
6 a 9	ALTO

Nota. Niveles de probabilidad e impacto (Owasp, OWASP_Risk_Rating_Methodology, 2023)

e. Paso 5: Decidir qué arreglar

Después de que se hayan clasificado los riesgos para la aplicación, habrá una lista priorizada de qué arreglar. Como regla general, los riesgos más graves deben fijarse primero. Simplemente no ayuda a la Perfil de riesgo para corregir riesgos menos importantes, incluso si son fáciles o baratos de solucionar. (Owasp, OWASP_Risk_Rating_Methodology, 2023)

f. Paso 6: Personalización del modelo de calificación de riesgo

Tener un marco de clasificación de riesgos que sea personalizable para una empresa es fundamental para la adopción. A medida es mucho más probable que el modelo produzca resultados que coincidan con las percepciones de las personas sobre lo que es un riesgo grave. Se puede perder mucho tiempo discutiendo sobre las calificaciones de riesgo si no están respaldadas por un modelo como este. Hay varias maneras de adaptar este modelo para la organización. (Owasp, OWASP_Risk_Rating_Methodology, 2023)

2.2.4.8.Hacking ético

La tarea de un hacker ético en una empresa específica implica llevar a cabo un análisis metódico y bien planificado de sus sistemas informáticos, redes y otros activos, previa autorización de la organización. Esto posibilita detectar, comprender y solucionar las vulnerabilidades que podrían ser explotadas por hackers malintencionados o incluso grupos delictivos para acceder de manera ilícita a los sistemas de la empresa. (Deloitte, 2021)

2.2.4.9. Tipos de Hacking ético

Los tipos de hacker ético se pueden enmarcar en dos grandes tipos, dependiendo de las acciones que realizan.

a. Hacking ético externo

Se aplica a los dispositivos conectados a la red de Internet. Por esta razón, implica la inclusión de lugares críticos como el enrutador, el firewall y los servidores. (Deloitte, 2021)

b. Hacking ético interno

Se aplica desde la infraestructura interna del cliente, en el mismo ámbito de trabajo, incluso podría ser alguien cercano, como un empleado de confianza, llevando a cabo acciones maliciosas contra sus propios dispositivos o sistemas. (Deloitte, 2021)

2.2.4.10. Fases pentesting

Fase 1: Recopilación de información / Enumeración

Esta fase es la principal del pentest, el objetivo es obtener toda la información posible sobre el objetivo en cuestión, haciendo uso de diversas técnicas tales como:

- Escaneo de dominios/IPs/puertos/versiones/servicios
- Dorking
- Uso de herramientas automatizadas para obtener información de nuestro objetivo
- Obtención de metadatos

(bidaidea, 2022)

Fase 2: Análisis de vulnerabilidades

Esta fase consiste en realizar todas las posibles acciones que nos permitan comprometer a nuestro objetivo, usuarios y/o su información. (bidaidea, 2022)

Fase 3: Explotación

Esta fase se encarga de aprovechar ("explotar") las vulnerabilidades encontradas de la fase anterior, es decir: ejecutamos exploits contra las vulnerabilidades identificadas o simplemente hacemos uso de credenciales obtenidas en la fase anterior para obtener acceso a los sistemas u objetivos. (bidaidea, 2022)

Fase 4: Post – Explotación

Esta fase de post explotación no siempre es aplicable, por que consiste en, una vez logrado entrar al sistema mediante las anteriores fases, lograr credenciales o permisos de administrador, o incluso vulnerar otros sistemas de mayor importancia dentro de la organización objetivo mediante técnicas de pivoting o similares. Es decir; el objetivo de esta fase es escalar privilegios con la finalidad de obtener una cuenta con todos los privilegios habilitados sobre el sistema. (bidaidea, 2022)

Fase 5: Reporte

Es la fase final donde se genera el reporte definitivo de vulnerabilidades, o llamado "informe de vulnerabilidades".

Aquí describimos todo lo realizado en nuestro test de intrusión (las vulnerabilidades encontradas, los recursos desactualizados, etc).

También es recomendable definir las contramedidas adecuadas para solucionar las brechas de seguridad encontrados anteriormente, de forma que ayuden a nuestro cliente o a la empresa afectado a solucionar la vulnerabilidad (o conjunto de vulnerabilidades). (bidaidea, 2022)

2.2.4.11. Tipos pentesting

Dependiendo de la cantidad de información y alcance sobre los sistemas informáticos que se van a testar, podemos clasificar el Pentesting en tres tipos:

a. Caja negra

También conocido como Black Box Pentesting, en esta prueba el testeador realiza sus análisis completamente a ciegas, es decir, sin contar con información de ningún tipo sobre el sistema a evaluar. Por tanto, el ataque lo realizará como si lo hiciera alguien totalmente ajeno a la empresa. (school nuclio, 2022)

b. Caja blanca

También conocido como White Box Pentesting, en este tipo de prueba el testeador conoce todos los datos del sistema a evaluar (las contraseñas, firewalls o IPs del sistema informático, entre otros). Por tanto, el ataque se simula como si fuese realizado por alguien de dentro, es decir, alguien que forma parte de la empresa. (school nuclio, 2022)

c. Caja gris

También conocido como Grey Box Pentesting, esta prueba **es un intermedio o** mezcla de las dos anteriores. En este caso el testeador contará con algo de información a la hora de realizar el test, aunque sigue siendo un buen simulacro de ataque ajeno al sistema. (school nuclio, 2022)

2.3. Hipótesis

2.3.1. Hipótesis general

La propuesta de la implementación de un modelo de análisis de vulnerabilidades y riesgos para la aplicación web de SOAINT - Lima; 2023, proporciona una visión clara de las debilidades de seguridad, además de ayudar a tomar medidas proactivas para proteger la aplicación de posibles amenazas y ataques.

2.3.2. Hipótesis específicas

1. La ejecución de pruebas de Pentesting, descubre un conjunto significativo de posibles vulnerabilidades presentes en la aplicación web de SOAINT.

2. La identificación de vulnerabilidades de acuerdo con las directrices de OWASP TOP 10 – 2021 permite subsanarlas en la aplicación web de SOAINT.
3. La evaluación de la gravedad de los riesgos detectados en la aplicación web de SOAINT mitiga y genera planes de acción, donde utiliza la metodología de riesgos de OWASP.

III. METODOLOGÍA

3.1. Nivel, Tipo y Diseño de Investigación

3.1.1. Nivel de investigación

La investigación fue de nivel cuantitativo, en el objetivo se describió las situaciones, eventos siguiendo procedimientos para detallar como son y cómo se manifiestan siendo sometidos a un análisis, es decir que midió o recogió información de manera independiente. (Tamayo y Tamayo, 2003).

3.1.2. Tipo de Investigación

La investigación fue de tipo descriptiva, que consistió en afinar y estructurar más formalmente la investigación, y que desarrollo cinco elementos de la investigación: objetivos, preguntas, justificación, viabilidad y evaluación de las deficiencias. En la investigación cuantitativa los cinco elementos fueron capaces de conducir una investigación concreta y una prueba empírica. (Hernandez, Fernandez, & Baptista, Metodologia de la Investigacion, 2014).

3.1.3. Diseño de investigación

La investigación fue de diseño no experimental, que se basó en la observación, no se modificó la realidad ni se manipuló las variables, solo se observan los fenómenos a analizar (Hernandez, Fernandez, & Baptista, Metodologia de la Investigacion, 2014); y además fue corte transversal que se centró en la recolección de datos, también describió variables y analizó su incidencia e interrelación en un momento dado, se recopilaron los datos a través de las encuestas y entrevistas que tuvieron análisis distinto, que permitió medir un determinado grupo de individuos con ciertas características en un punto específico de tiempo (Hernandez, Fernandez, & Baptista, Metodologia de la Investigacion, 2014) .

El esquema del diseño de la investigación tuvo la siguiente estructura:

Dónde:

M = Muestra

O = Observación

¿Qué es el diseño no experimental?

Es aquel que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para después analizarlos. (Dzul, 2013)

¿En qué se basa?

Se basa en categorías, conceptos, variables, sucesos, comunidades o contextos que ya ocurrieron o se dieron sin la intervención directa del investigador. Es por esto que también se le conoce como investigación «ex post facto» (hechos y variables que ya ocurrieron), al observar variables y relaciones entre estas en su contexto. (Dzul, 2013)

3.2. Población y Muestra

3.2.1. Población

Para el caso de esta investigación la población se delimito a 0 trabajadores de las unidades operativas involucradas en la elaboración, consolidación y toma de decisiones de SOAINT que son: trabajadores de la Oficina principal de Perú (10).

La población: es la totalidad de elementos o individuos los cuales tendrán características comunes y que van a ser sujetas de estudio, este conjunto de elementos puede ser finito o infinito y de esta se extrae la información que se requiere y por eso se selecciona una muestra (Hernandez, Fernandez, & Baptista, Metodologia de la Investigacion, 2014).

3.2.2. Muestra

A efectos de seleccionar la muestra sujeta a estudio se seleccionará mediante el muestreo no probabilístico por conveniencia a los 10 trabajadores, por

ser integrantes de las unidades operativas involucradas en la elaboración, consolidación y toma de decisiones, selección de personal y de la parte operativa de la organización inmersos en el proceso en estudio.

La muestra: Es un subconjunto del universo considerado para la investigación, es de importancia para el análisis de datos a realizar en todo proyecto de investigación, con características semejantes y que están sometidos al estudio (Hernandez, Fernandez, & Baptista, 2014).

Tabla 1

Muestra de trabajadores

Unidades Operativas/funcionales	**Población/Muestra**
Empleados Soaint Perú	10
Total	**10**

Nota. Elaboración propia

3.3.Variable. Definición y operacionalización

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala medición
Modelo de análisis de vulnerabilidades y riesgos	Es una estructura conceptual diseñada para identificar y evaluar los posibles puntos débiles y amenazas asociadas a una aplicación web. Su objetivo principal es identificar las vulnerabilidades de seguridad y los riesgos inherentes a la aplicación, a fin de implementar medidas de mitigación adecuadas y reducir la probabilidad de que se produzcan incidentes de seguridad. El modelo se basa en un enfoque sistemático y metódico para analizar la aplicación web en busca de	- Si - No	Nivel de satisfacción de la aplicación web y la protección de sus datos	- Navegación web intuitiva y dinámica - Protección de información adecuada - Módulos u opciones acotados al alcance - Visualización y descarga de documentos efectiva - Ingreso de solicitudes eficiente - Inicio de sesión a la aplicación web adecuado - Gestión de accesos adecuado	Nominal

	vulnerabilidades y riesgos potenciales. Esto implica una combinación de técnicas de evaluación manual y herramientas automatizadas para descubrir posibles problemas de seguridad, como brechas en la autenticación, autorización deficiente, inyecciones de código, exposición de datos sensibles, entre otros.			- Oportunidad de mejoras en procesos e interfaz	
			Necesidad de proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos	- Importancia de implementar un modelo de análisis de vulnerabilidades y riesgos - Incidentes de seguridad o problemas en la aplicación - Amenazas y vulnerabilidades generan perdida de información - Proteger mejor los activos	

				- Inversión de un modelo de análisis de vulnerabilidades y riesgos - Conocimiento de estándares y marcos de seguridad - Tener una visión más clara de sus infraestructura y componentes - Posible reestructuración de la aplicación web	

Nota. Elaboración propia

3.4. Técnicas e instrumentos de recolección de información

3.4.1. Descripción de técnicas

Se utilizará la técnica de la encuesta

Encuesta: Conjunto de interrogantes que se hace a un cierto grupo de personas para recopilar datos para dar un análisis detallado de un tema determinado.

3.4.2. Descripción de instrumentos

Se utilizará como instrumento el cuestionario

Cuestionario: Conjunto de preguntas que deben ser contestadas en una encuesta.

3.5. Método de análisis de datos

Después de recolectar la información utilizando los métodos y procedimientos mencionados previamente, se procederá a crear una base de datos temporal en MS Excel 2021 y llevar a cabo la tabulación de los datos recopilados. Para el análisis de los datos, se utilizarán las preguntas del cuestionario, lo que permitirá resumir la información en tablas y gráficos que mostrarán el impacto porcentual de cada pregunta.

Con el objetivo de obtener la información adecuada, se realizará una cuidadosa selección de las personas apropiadas para aplicar los cuestionarios, coordinando con los diferentes líderes de la organización según su área o jefatura, para entregar los cuestionarios a las personas seleccionadas y resolver cualquier duda relacionada con las preguntas planteadas.

Para la tabulación de las respuestas de cada cuestionario, se creará un archivo en formato MS Excel 2021 que organizará las respuestas según cada dimensión de estudio. Esto permitirá obtener los resultados de manera rápida y se podrá llegar a conclusiones para cada una de las dimensiones.

3.6. Aspectos Éticos

Durante el desarrollo de la presente investigación denominada, implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023. Se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación:

El principal objetivo de cualquier investigación es garantizar el bienestar y la seguridad de las personas involucradas. Para lograr esto, es fundamental proteger su dignidad, identidad, diversidad socio-cultural, confidencialidad, privacidad, creencias y religión. Además, es necesario asegurarse de que las personas que participan en la investigación lo hagan de manera voluntaria y con información completa, y también se deben salvaguardar sus derechos fundamentales si se encuentran en una posición de vulnerabilidad.

Aquellas personas que participan en actividades de investigación tienen el derecho de recibir una adecuada información sobre los propósitos y objetivos de la investigación en la que están involucrados, y tienen la libertad de decidir si desean participar de manera voluntaria.

En toda investigación, se requiere obtener el consentimiento claro, informado, libre y específico de las personas involucradas, ya sea como sujetos de investigación o como titulares de datos, para poder utilizar la información con fines específicos establecidos en el proyecto.

Es esencial que toda investigación cuente con un equilibrio positivo y justificado entre los riesgos y beneficios, con el fin de garantizar el cuidado de la vida y el bienestar de los participantes. En este sentido, los investigadores deben seguir ciertas reglas generales, como evitar causar daño, reducir los posibles efectos adversos y maximizar los beneficios.

Los investigadores deben anteponer la justicia y el bien común por encima de sus propios intereses personales. Además, deben ejercer un juicio razonable y asegurarse de que las limitaciones de su conocimiento, capacidades o sesgos no conduzcan a prácticas injustas. Es responsabilidad del investigador tratar de manera equitativa a aquellos que participan en los procesos, procedimientos y servicios relacionados con la investigación, y garantizar su acceso a los resultados.

Es fundamental que los investigadores, ya sean estudiantes, egresados, docentes o no docentes, eviten cualquier forma de engaño en todos los aspectos de la investigación. También deben evaluar y declarar los posibles daños, riesgos y beneficios que puedan afectar a quienes participan en la investigación. Asimismo,

deben llevar a cabo su labor con rigor científico, asegurándose de la validez de sus métodos, fuentes y datos utilizados. (ULADECH, 2022)

IV. RESULTADOS

4.1. Resultados de la encuesta

4.1.1. Dimensión 1: Nivel de satisfacción de la aplicación web y la protección de sus datos

Tabla 2

Navegación web es intuitiva y dinámica

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Nota. Se observa que el 100.00% de los empleados encuestados manifestaron que están satisfechos con la Navegación web por ser intuitiva y dinámica.

Tabla 3

Información en aplicación web está segura

Alternativas	n	%
Si	7	70.00
No	3	30.00
Total	10	100.00

Nota. Se observa que el 70.00% de los empleados encuestados manifestaron que la información en aplicación web es segura, mientras un 30.00% dicen lo contrario.

Tabla 4

Vínculos externos a páginas referentes a Soaint

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Nota. Se observa que el 80.00% de los empleados encuestados manifestaron que deben existir vínculos externos a páginas referentes a Soaint, mientras un 20.00% dicen lo contrario.

Tabla 5

Calidad y disponibilidad de documentos o reportes

Alternativas	n	%
Si	9	90.00
No	1	10.00
Total	10	100.00

Nota. Se observa que el 90.00% de los empleados encuestados manifestaron que están satisfechos con la calidad y disponibilidad de documentos o reportes, mientras un 10.00% dicen lo contrario.

Tabla 6

Considera eficientes los tiempos de respuesta

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Nota. Se observa que el 100.00% de los empleados encuestados manifestaron que los tiempos de respuesta en la aplicación web son eficientes.

Tabla 7

Factores de autenticación adicionales a usuario y contraseña

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Nota. Se observa que el 80.00% de los empleados encuestados manifestaron que debe existir factores de autenticación adicionales a usuario y contraseña, mientras un 20.00% dicen lo contrario.

Tabla 8

Autogestión de credenciales

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Nota. Se observa que el 60.00% de los empleados encuestados manifestaron que debe existir una autogestión de sus credenciales, mientras un 40.00% dicen lo contrario.

Tabla 9

Directorio de contactos general

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Nota. Se observa que el 60.00% de los empleados encuestados manifestaron que debe existir un directorio de contactos general, mientras un 40.00% dicen lo contrario.

4.1.2. Dimensión 2: Implementación de un modelo de análisis de vulnerabilidades y riesgos

Tabla 10

Vulnerabilidades y riesgos en aplicación

Alternativas	n	%
Si	1	10.00
No	9	90.00
Total	10	100.00

Nota. Se observa que el 10.00% de los empleados encuestados manifestaron que existen vulnerabilidades y riesgos en aplicación, mientras un 90.00% dicen lo contrario.

Tabla 11

Incidentes de seguridad en aplicación web

Alternativas	n	%
Si	4	40.00
No	6	60.00
Total	10	100.00

Nota. Se observa que el 40.00% de los empleados encuestados manifestaron han identificado incidentes de seguridad en aplicación web, mientras un 60.00% dicen lo contrario.

Tabla 12

Amenazas y vulnerabilidades afectan la disponibilidad y pérdida de información

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Nota. Se observa que el 80.00% de los empleados encuestados manifestaron que las amenazas y vulnerabilidades afectan la disponibilidad y pérdida de información, mientras un 20.00% dicen lo contrario.

Tabla 13

Integrar AD para inicio de sesión

Alternativas	N	%
Si	10	100.00
No	-	-
Total	10	100.00

Nota. Se observa que el 100.00% de los empleados encuestados manifestaron que se debe integrar Active Directory (AD) para la autentificación inicio de sesión en la aplicación web.

Tabla 14

Modelo de análisis de vulnerabilidades y riesgos mejorará la seguridad y la reducción de riesgos

Alternativas	N	%
Si	10	100.00
No	-	-
Total	10	100.00

Nota. Se observa que el 100.00% de los empleados encuestados manifestaron que aplicar un modelo de análisis de vulnerabilidades y riesgos mejorará la seguridad y la reducción de riesgos en la aplicación web.

Tabla 15

Conocimientos de estándares y marcos de seguridad

Alternativas	N	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Nota. Se observa que el 60.00% de los empleados encuestados manifestaron que tienen conocimientos de estándares y marcos de seguridad, mientras un 40.00% dicen lo contrario.

Tabla 16

El Análisis de vulnerabilidades y riesgos ayudará a identificar componentes de red expuestos

Alternativas	n	%
Si	9	90.00
No	1	10.00
Total	10	100.00

Nota. Se observa que el 90.00% de los empleados encuestados manifestaron que el Análisis de vulnerabilidades y riesgos ayudará a identificar componentes de red expuestos en Internet, mientras un 10.00% dicen lo contrario.

Tabla 17

Reestructurar la interfaz luego del análisis de vulnerabilidades y riesgos

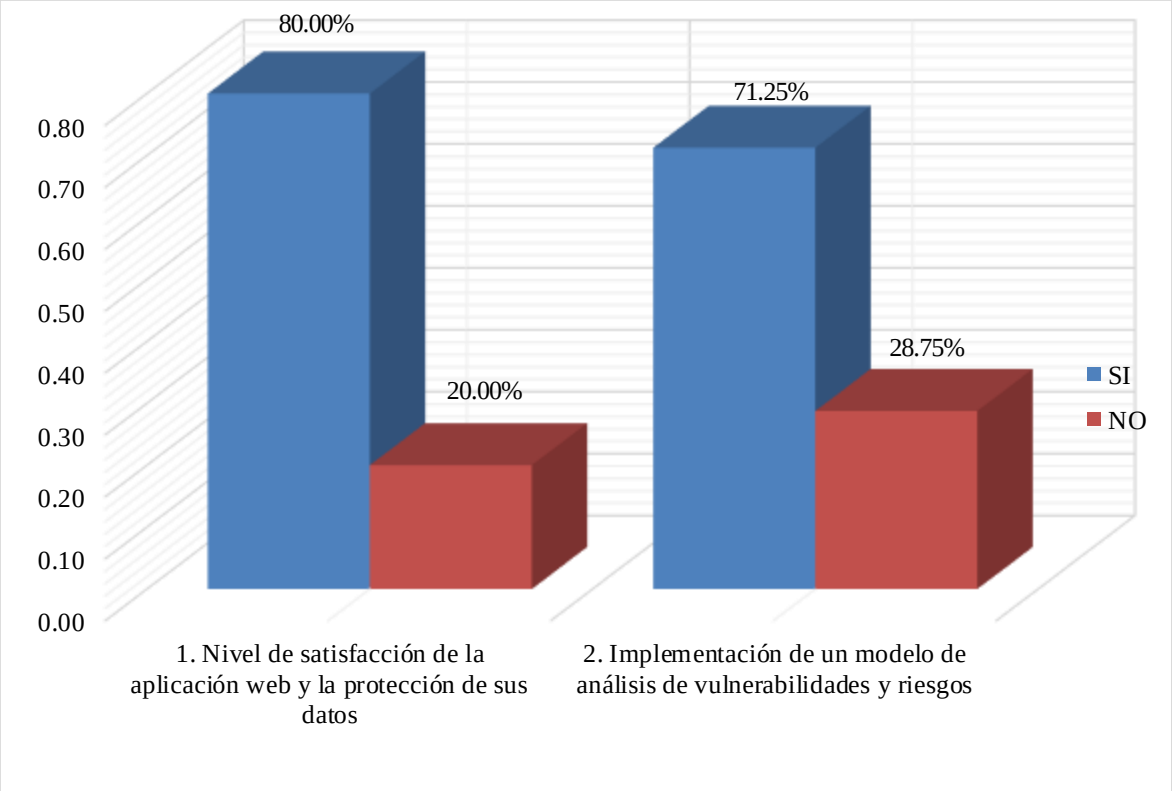
Alternativas	N	%
Si	9	90.00
No	1	10.00
Total	10	100.00

Nota. Se observa que el 90.00% de los empleados encuestados manifestaron que luego del análisis de vulnerabilidades y riesgos se puede reestructurar la interfaz de la aplicación web, mientras un 10.00% dicen lo contrario.

4.1.3. Resultados de dimensiones

Figura 23

Resumen de encuestas sobre las dimensiones



Nota. Diagrama resumen de encuestas sobre las dos dimensiones aplicadas en el informe.

4.2. Discusión

La presente investigación tuvo como objetivo general realizar la implementación de un modelo de análisis de vulnerabilidades y riesgos de la

aplicación web de SOAINT S.A.C – Lima; 2023, en el cual se ha realizado dos dimensiones que son de satisfacción y protección de datos para la aplicación web actual y la necesidad de implementar un modelado de vulnerabilidades y riesgos. Por lo tanto, una vez interpretado los resultados se proceden a analizarlo detenidamente en los párrafos:

Respecto a la dimensión 01: Nivel de satisfacción de la aplicación web y la protección de sus datos en el que se puede observar que el 80.00% de empleados de SOAINT expresaron que están SI están satisfechos, mientras que el 20.00% indicó que NO se encuentran satisfechos. Estos resultados tienen semejanza con lo definido por (Tasan & Morocho, 2020) quienes en su tesis de investigación "Metodología OWASP en el desarrollo de un website para voto electrónico. caso práctico: sistema de elecciones asociación de estudiantes TI-UNACH" se define que los estudiantes de la carrera de TI, tenían la necesidad de sintetizar el proceso de votaciones para la elección de Asociación de Estudiantes de la carrera de TI, por lo cual se consideran que sus websites eran satisfactorias, pero necesitaban la aplicabilidad de metodologías OWASP para mitigar las vulnerabilidades, esto coincide con el autor (Sutori, 2019) quien cree que los criterios de éxito en la organización dependen de la capacidad de adaptación a las nuevas tecnologías y el aprovecharlo para su beneficio, estos resultados fueron obtenidos por que las organizaciones o instituciones cuentan con aplicaciones web que ayudan a automatizar y agilizar los procesos que necesitan por demanda, pero a su vez, se requiere realizar una revisión constante con el fin de incorporar las nuevas prácticas de desarrollo y seguridad, ya que poco a poco la exposición de las aplicaciones web hacia la nube o Internet, generan que sean blanco de amenazas y vulnerabilidades hacia el activo más importante de las organizaciones, que es la información.

Respecto a la dimensión 02: Implementación de un modelo de análisis de vulnerabilidades y riesgos en él, se puede observar que el 71.25% de empleados de SOAINT expresaron que están SI están de acuerdo con la propuesta, mientras que el 28.75% indicó que NO se requieren la propuesta, estos resultados tienen similitud a lo que indica (Llerena, 2018) quien en su tesis de investigación "Evaluación de la seguridad informática en el área de sistemas", propone el uso de medidas preventivas de seguridad para la identificación de vulnerabilidades y así

garantizar la continuidad de los servicios y dar mejora al control de procesos para gestionar los riesgos, esto coincide con el autor (Hernández-Pérez, 2019) quien menciona que las TIC nos relaciona y socializa en entornos virtuales pero a su vez se debe controlarse ya que puede traer consecuencias contractuales o convertirse en un riesgo, estos resultados fueron obtenidos por que las organizaciones o instituciones requieren que sus aplicaciones web cuenten con una evaluación de vulnerabilidades y la identificación de los riesgos, por lo que las revisiones en los activos de información, deben ser constantes y aplicar los controles necesarios para su aseguramiento.

4.3. Propuesta de mejora

Con los resultados y análisis obtenidos de la investigación, se procedió con la implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023, en donde se plantea como propuesta de mejora lo siguiente: Implementar un modelo de análisis de vulnerabilidades y riesgos utilizando la metodología PMBOK para gestionar el proyecto además de OWASP Risk Rating Methodology para la identificar y evaluar las vulnerabilidades y riesgos, adicionando herramientas y técnicas para identificar, detecta, evaluar y prevenir las vulnerabilidades y riesgos de la aplicación web.

4.3.1. Propuesta de técnica

4.3.1.1. Fundamentación de la metodología

En la investigación se empleó la metodología la metodología PMBOK para gestionar el proyecto y OWASP Risk Rating Methodology para la identificar y evaluar las vulnerabilidades y riesgos, además de herramientas y técnicas para prevenir las vulnerabilidades y riesgos de la aplicación web, para la implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023, cuyo objetivo es protegerlo de posibles amenazas y ataques.

Las principales razones de utilizar las metodologías y herramientas mencionadas son para:

- Ejecuta pruebas de Pentesting con el fin de descubrir las vulnerabilidades presentes en la aplicación web.

- Identifica las vulnerabilidades presentes en la aplicación web de acuerdo con las directrices del OWASP TOP 10 - 2021.

- Evalúa la gravedad de los riesgos detectados en la aplicación web, utilizando la metodología de riesgos de OWASP.

4.3.1.2. Desarrollo de la metodología

Se eligió la metodología PMBOK para gestionar el proyecto, por que cumple con los procesos para el seguimiento eficaz de un proyecto y OWASP Risk Rating Methodology para la identificar y evaluar las vulnerabilidades y riesgos, siendo este una metodología muy utilizada para la gestión de vulnerabilidades y riesgos en aplicaciones web.

Tabla 18

Entregables de Metodologías

METODOLOGIA	**ETAPA**	**ENTREGABLE**	
PMBOK	INICIO	Caso del Negocio	
		Red Organizacional	
		Documento de acuerdo de confidencialidad	
	PLANIFICACIÓN	Gestión del alcance	
	CIERRE	Gestión del tiempo	
		Gestión de costo	
		Documento de acta de conformidad.	
PENTESTING	ETAPA I: PLANIFICACIÓN DE LA AUDITORIA	Elaboración de la Carta de Permiso	Documento Carta de Permiso de la Empresa
		Descripción del Entorno a Auditar	Cuadro de Características

			de la aplicación Web
			Diagrama de Infraestructura de la Red
	ETAPA II: EJECUCIÓN DE PRUEBAS DE PENTESTING	Fase 1: Recopilación de información / Enumeración	Resumen de Reconocimiento Pasivo
			Resumen de Reconocimiento Activo
		Fase 2: Análisis de vulnerabilidades	Reconocimiento del Escaneo de Vulnerabilidades Basadas en OWASP Top 10 – 2021
		Fase 3: Explotación	Resultados de las Pruebas de Explotación de Vulnerabilidades Basadas en OWASP Top 10 – 2021
		Fase 4: Post – Explotación	Resultados de las Pruebas de Post-Explotación de Vulnerabilidades
		Fase 5: Reporte	Carpeta del Proyecto

			Documento Técnico de Análisis de Vulnerabilidades
OWASP RISK RATING METHODOLOGY	ETAPA III: EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS	Paso 1: Identificar un riesgo	
		Paso 2: Factores para estimar la probabilidad	
		Paso 3: Factores para estimar el impacto	
		Paso 4: Determinar la gravedad del riesgo	
		Paso 5: Decidir qué arreglar	
		Paso 6: Personalización del modelo de calificación de riesgo	
OWASP Top 10 – 2021	ETAPA IV: PLAN DE PREVENCIÓN DE RIESGOS ENCONTRADOS.	Desarrollo del plan de Prevención	Plan de Prevención de Riesgos

Nota. Elaboración Propia

A. INICIO:

Caso del negocio

La empresa Soaint es una consultora internacional especializada en brindar servicios de consultoría TI, soporte a áreas tecnológicas u operativas, a grandes empresas públicas y privadas de diversos rubros, buscan desarrollarse como una empresa líder en consultoría de proyectos aplicando un modelo de empresa orientado cada vez más hacia las personas y las relaciones.

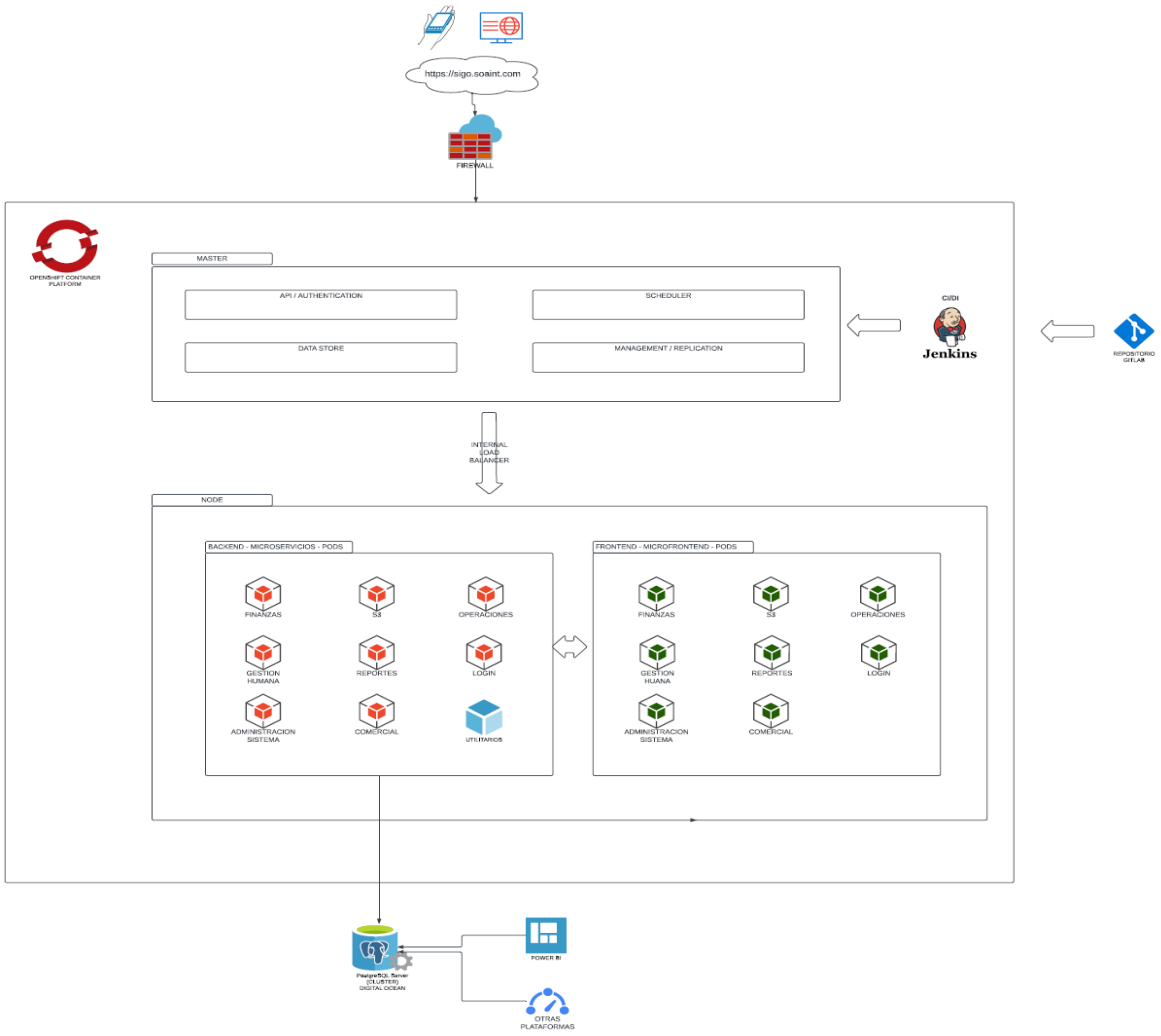
Red Organizacional

SOAINT cuenta con más 180 equipos tecnológicos (Laptops, PCs, Smartphones, etc.), que se conectan a la aplicación web SIGO de la organización, tal como se visulaiza en la figura 24, el objetivo del acceso de los usuarios es gestionar solicitudes propias de empleados como vacaciones, entrega de documentos, registro

de horas, reporte de planillas y noticias acerca de la organización, es por ello que se debe aplicar un análisis o monitoreo para validar que los componentes no cuenten con vulnerabilidades que pongan en riesgo la información de la organización.

Figura 24

Diagrama de red SIGO



Nota. Fuente de Soaint 2023

Acuerdo de confidencialidad

A continuación, se presenta el documento modelo de Acuerdo de Confidencialidad de nuestro proyecto, para llevar a cabo el acuerdo necesario con la empresa y realizar el trabajo de manera legal.

Figura 25

Acuerdo de Confidencialidad

Acuerdo de Confidencialidad

Chimbote, ...de……. de 20…..

Mediante la presente, RAZON SOCIAL EMPRESA con RUC: RUC y dirección en DIRECCIÓN DE LA EMPRESA representada por NOMBRE DEL PRESENTANTE actuando en nombre y representación de esta entidad en virtud de su condición de CARGO DE LA EMPRESA.

De otra parte, ALUMNO con DNI: DNI y representado por NOMBRE DE LA UNIVERSIDAD actuando en nombre y representación de esta entidad en virtud de su condición de ALUMNO

Ambas partes acuerdan mutuamente, la capacidad legal necesaria para la suscripción del presente acuerdo y el cumplimiento y a dar cumplimiento a las siguientes obligaciones:

I. Que EMPRESA es una organización dedicada a ACTIVIDAD A LA QUE SE DEDICA EMPRESA y por tanto es responsable de la información generada y gestionada en su actividad.
II. Que ALUMNO es un estudiante dedicado a SE DEDICA EL ALUMNO SERVICIOS QUE PRESTA A EMPRESA ACTIVIDAD A LA QUE proporciona servicios de la EMPRESA.
III. Que ALUMNO durante la prestación de sus servicios a EMPRESA puede recibir información confidencial de EMPRESA o disponer del acceso o de potencial acceso la misma. en este sentido se considera por información (confidencial, toda la información relativa a sus procesos, infraestructura, usuarios know-how. métodos análisis funcionales, código fuente, estadísticas, datos financieros, y toda aquella información que EMPRESA no haya autorizado de modo explícito a ALUMNO su libre uso o difusión.
IV. El ALUMNO solo hará uso de la información facilitada por la EMPRESA en el ámbito de los servicios prestados por el ALUMNO descritos en el apartado II. En este sentido el ALUMNO se compromete a guardar el deber de secreto y mantener

Nota. Elaboración Propia, en la figura 25, visualizamos una parte del documento del acuerdo de confidencialidad, el cual será aplicado para el cumplimiento del desarrollo del proyecto.

B. PLANIFICACIÓN

Gestión del alcance

El alcance del proyecto aplica desde la Etapa I Planificación de la Auditoria y termina en la etapa IV Plan de prevención de riesgos encontrados. Con este alcance, el proyecto está enfocado en un modelo de análisis de vulnerabilidades y riesgos

para la aplicación web de SOAINT, inicia desde el proceso de detección hasta identificar las vulnerabilidades más críticas de acuerdo a OWASP Top 10 2021, además de aplicar pruebas de Pentesting, y de definir su severidad a los riesgos encontrados basado en su metodología para evaluarlos en OWASP Risk Rating Methodology.

Enunciado

A continuación, se muestra el enunciado sobre el alcance de nuestro proyecto:

ALCANCE
El alcance de proyecto aplica desde la Etapa I Planificación de la Auditoria y termina en la etapa IV Plan de prevención de riesgos encontrados. Con este alcance, el proyecto está enfocado en un modelo de análisis de vulnerabilidades y riesgos para la aplicación web de SOAINT, inicia desde el proceso de detección hasta identificar las vulnerabilidades más críticas de acuerdo a OWASP Top 10 2021, además de aplicar pruebas de Pentesting, y de definir su severidad a los riesgos encontrados basado en su metodología para evaluarlos en OWASP Risk Rating Methodology.
OBJETIVOS
- Ejecutar pruebas de Pentesting con el fin de descubrir las vulnerabilidades presentes en la aplicación web de SOAINT. - Identificar las vulnerabilidades presentes en la aplicación web de SOAINT de acuerdo con las directrices del OWASP TOP 10 - 2021. - Evaluar la gravedad de los riesgos detectados en la aplicación web de SOAINT utilizando la metodología de riesgos de OWASP.
REQUERIMIENTOS DEL PROYECTO
- Contar con un equipo o laptop con las características mínimas: Procesador Core i7, memoria RAM de 12GB o 16GB, Disco duro sólido de 256GB. - Uso de máquinas virtuales como Box y sistema operativo Kali Linux para la auditoria de seguridad.

- En las fases de pentesting se deberá garantizar el uso de herramientas de penetración y análisis además de motores de búsqueda.

REQUERIMIENTOS DEL PRODUCTO

- Reconocimiento del objetivo pasivo y activo de la fase de recolección de información.
- Escaneo de vulnerabilidades del OWASP TOP 10 – 2021.
- Carpeta del proyecto, donde se muestren las imágenes y documentos de la auditoria
- Estimación de la probabilidad y el impacto, de los componentes:
    - Factores de amenazas
    - Factores de vulnerabilidad
    - Factores técnicos de impacto
    - Factores de impacto en el negocio
- Gravedad del riesgo de los componentes: Niveles de probabilidad e impacto.

ENTREGABLES DEL PROYECTO

- Gestión del proyecto: Abarca lo siguiente
    - Acuerdo de confidencialidad
    - Enunciado del alcance
    - Diagrama de desglose del Trabajo EDT
    - Cronograma de actividades
    - Análisis del presupuesto
    - Estimación del proyecto
- Etapa I: Planificación de la Auditoria, los entregables son:
    - Elaboración de la Carta de Permiso
    - Descripción del Entorno a Auditar

- Etapa II: Ejecución de Pentesting: los entregables son:
    - Fase 1: Recopilación de información / Enumeración
    - Fase 2: Análisis de vulnerabilidades
    - Fase 3: Explotación
    - Fase 4: Post – Explotación
    - Fase 5: Reporte
- Etapa III: Calificación de los Riesgos: los entregables son:
    - Paso 1: Identificar un riesgo
    - Paso 2: Factores para estimar la probabilidad
    - Paso 3: Factores para estimar el impacto
    - Paso 4: Determinar la gravedad del riesgo
    - Paso 5: Decidir qué arreglar
    - Paso 6: Personalización del modelo de calificación de riesgo
- Etapa IV: Plan de Prevención: el entregable es: el Plan de Prevención de Riesgos.

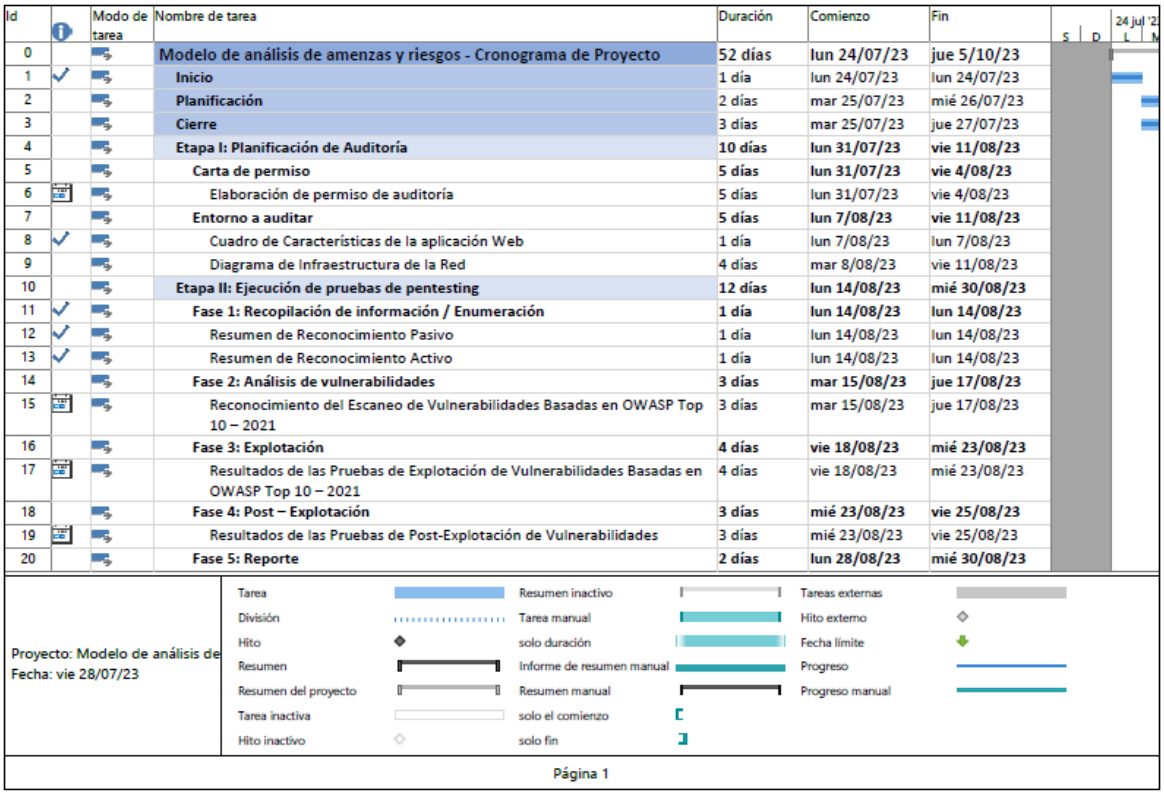
Fuente: Elaboración Propia

4.3.2. Diagrama de Gantt

A continuación, se muestra el cronograma de actividades, para desarrollar la implementación de un modelo de análisis de vulnerabilidades y riesgos a SOAINT.

Figura 26

Diagrama de Gantt - 1

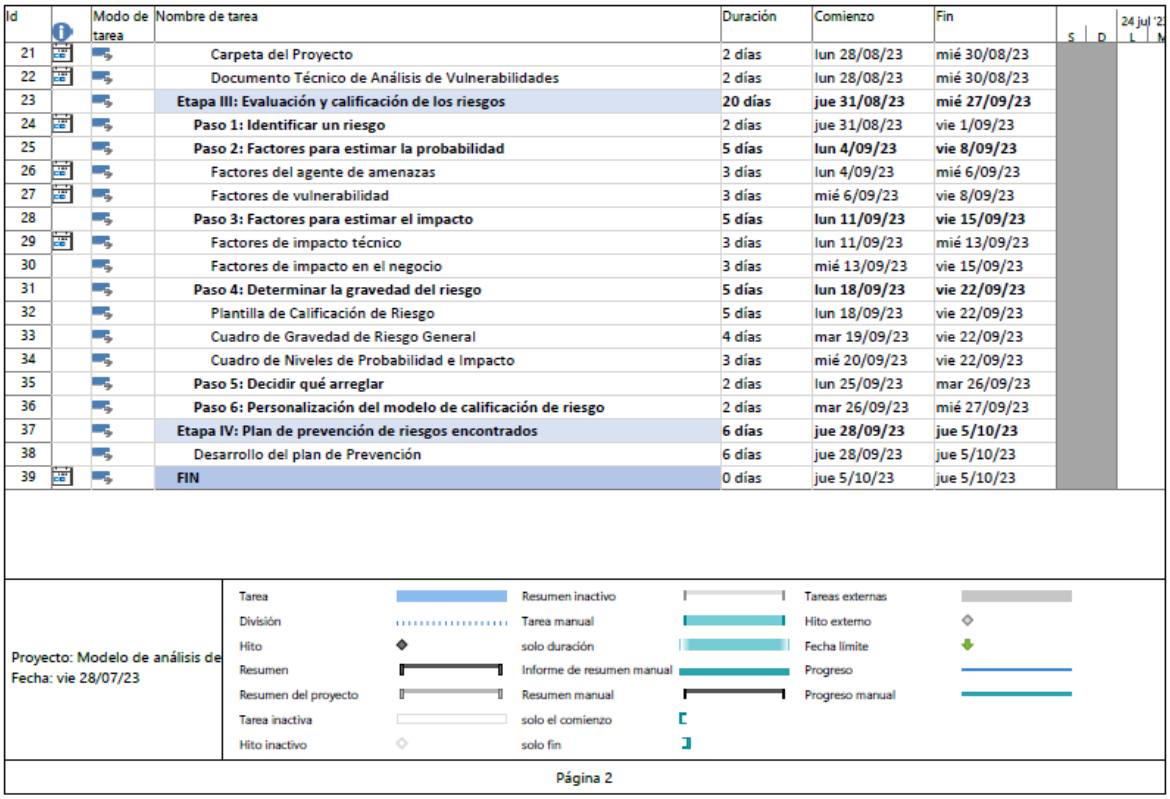


Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
0		**Modelo de análisis de amenzas y riesgos - Cronograma de Proyecto**	**52 días**	**lun 24/07/23**	**jue 5/10/23**
1		**Inicio**	1 día	lun 24/07/23	lun 24/07/23
2		**Planificación**	2 días	mar 25/07/23	mié 26/07/23
3		**Cierre**	3 días	mar 25/07/23	jue 27/07/23
4		**Etapa I: Planificación de Auditoría**	**10 días**	**lun 31/07/23**	**vie 11/08/23**
5		**Carta de permiso**	**5 días**	**lun 31/07/23**	**vie 4/08/23**
6		Elaboración de permiso de auditoría	5 días	lun 31/07/23	vie 4/08/23
7		**Entorno a auditar**	**5 días**	**lun 7/08/23**	**vie 11/08/23**
8		Cuadro de Características de la aplicación Web	1 día	lun 7/08/23	lun 7/08/23
9		Diagrama de Infraestructura de la Red	4 días	mar 8/08/23	vie 11/08/23
10		**Etapa II: Ejecución de pruebas de pentesting**	**12 días**	**lun 14/08/23**	**mié 30/08/23**
11		**Fase 1: Recopilación de información / Enumeración**	**1 día**	**lun 14/08/23**	**lun 14/08/23**
12		Resumen de Reconocimiento Pasivo	1 día	lun 14/08/23	lun 14/08/23
13		Resumen de Reconocimiento Activo	1 día	lun 14/08/23	lun 14/08/23
14		**Fase 2: Análisis de vulnerabilidades**	**3 días**	**mar 15/08/23**	**jue 17/08/23**
15		Reconocimiento del Escaneo de Vulnerabilidades Basadas en OWASP Top 10 – 2021	3 días	mar 15/08/23	jue 17/08/23
16		**Fase 3: Explotación**	**4 días**	**vie 18/08/23**	**mié 23/08/23**
17		Resultados de las Pruebas de Explotación de Vulnerabilidades Basadas en OWASP Top 10 – 2021	4 días	vie 18/08/23	mié 23/08/23
18		**Fase 4: Post – Explotación**	**3 días**	**mié 23/08/23**	**vie 25/08/23**
19		Resultados de las Pruebas de Post-Explotación de Vulnerabilidades	3 días	mié 23/08/23	vie 25/08/23
20		**Fase 5: Reporte**	**2 días**	**lun 28/08/23**	**mié 30/08/23**

Nota. Elaboración Propia

Figura 27

Diagrama de Gantt - 2

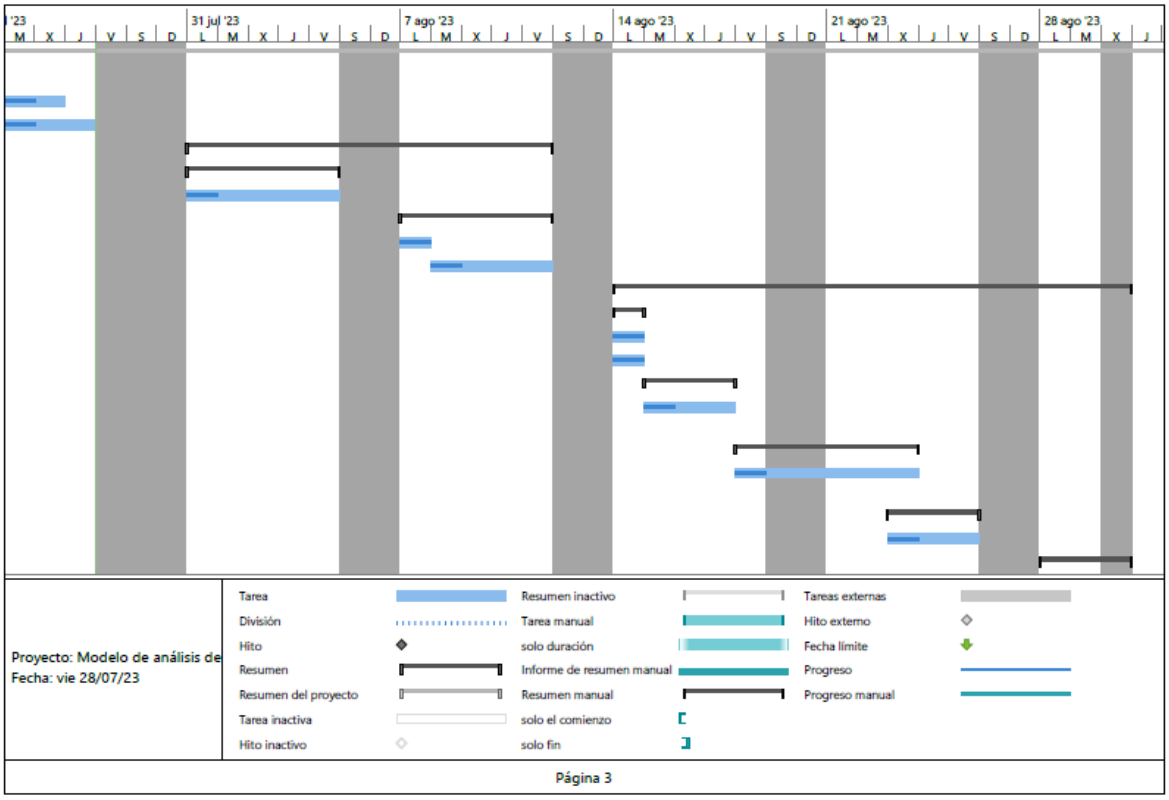


Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
21		Carpeta del Proyecto	2 días	lun 28/08/23	mié 30/08/23
22		Documento Técnico de Análisis de Vulnerabilidades	2 días	lun 28/08/23	mié 30/08/23
23		**Etapa III: Evaluación y calificación de los riesgos**	**20 días**	**jue 31/08/23**	**mié 27/09/23**
24		**Paso 1: Identificar un riesgo**	2 días	jue 31/08/23	vie 1/09/23
25		**Paso 2: Factores para estimar la probabilidad**	**5 días**	**lun 4/09/23**	**vie 8/09/23**
26		Factores del agente de amenazas	3 días	lun 4/09/23	mié 6/09/23
27		Factores de vulnerabilidad	3 días	mié 6/09/23	vie 8/09/23
28		**Paso 3: Factores para estimar el impacto**	**5 días**	**lun 11/09/23**	**vie 15/09/23**
29		Factores de impacto técnico	3 días	lun 11/09/23	mié 13/09/23
30		Factores de impacto en el negocio	3 días	mié 13/09/23	vie 15/09/23
31		**Paso 4: Determinar la gravedad del riesgo**	**5 días**	**lun 18/09/23**	**vie 22/09/23**
32		Plantilla de Calificación de Riesgo	5 días	lun 18/09/23	vie 22/09/23
33		Cuadro de Gravedad de Riesgo General	4 días	mar 19/09/23	vie 22/09/23
34		Cuadro de Niveles de Probabilidad e Impacto	3 días	mié 20/09/23	vie 22/09/23
35		**Paso 5: Decidir qué arreglar**	2 días	lun 25/09/23	mar 26/09/23
36		**Paso 6: Personalización del modelo de calificación de riesgo**	2 días	mar 26/09/23	mié 27/09/23
37		**Etapa IV: Plan de prevención de riesgos encontrados**	**6 días**	**jue 28/09/23**	**jue 5/10/23**
38		Desarrollo del plan de Prevención	6 días	jue 28/09/23	jue 5/10/23
39		**FIN**	0 días	jue 5/10/23	jue 5/10/23

Nota. Elaboración Propia

Figura 28

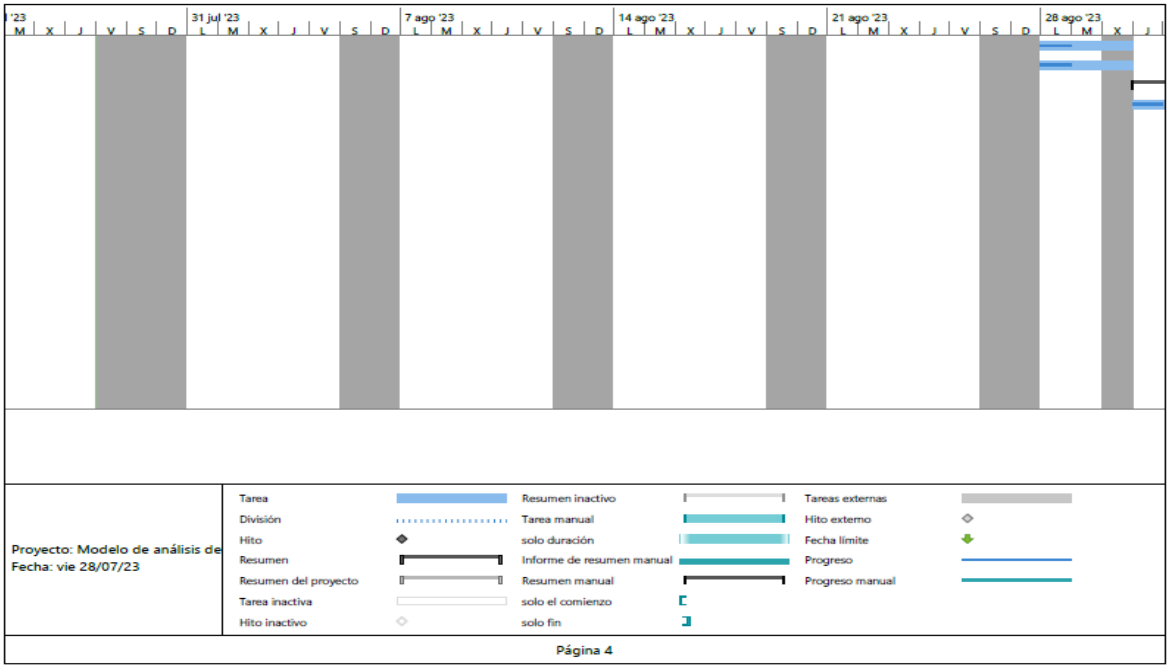
Diagrama de Gantt - 3



Nota. Elaboración Propia

Figura 29

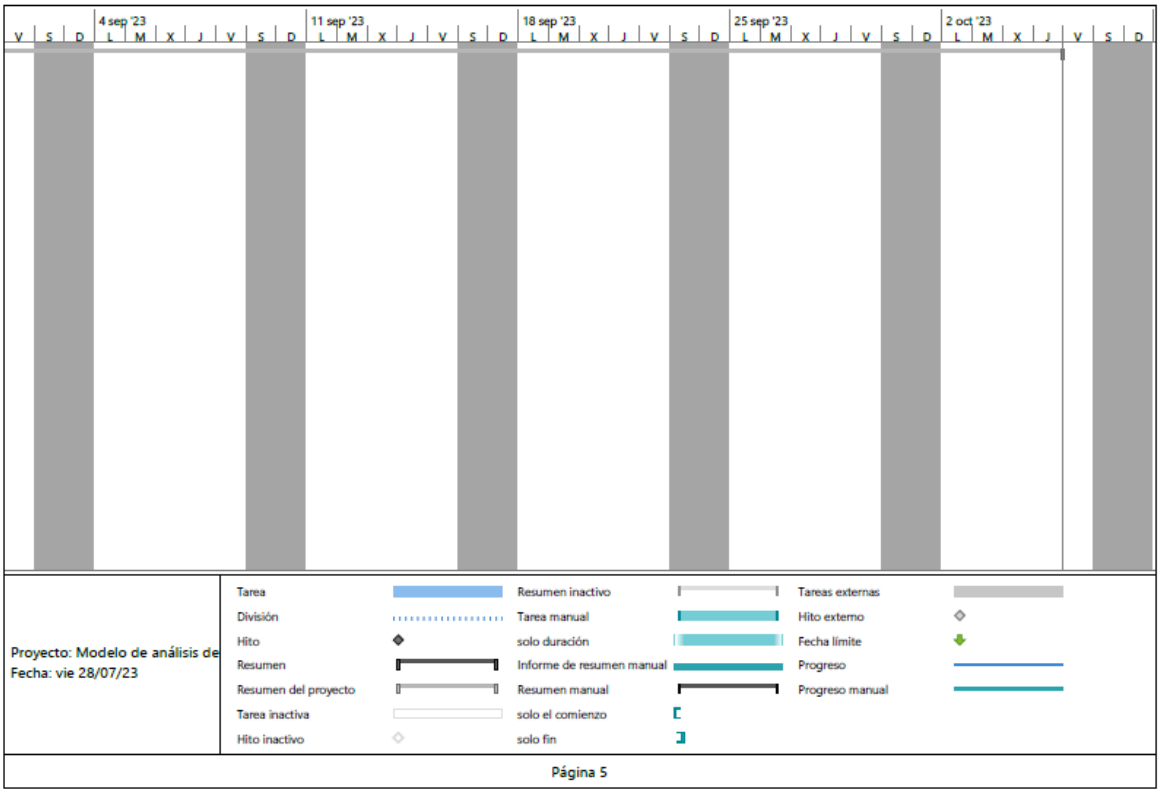
Diagrama de Gantt - 4



Nota. Elaboración Propia

Figura 30

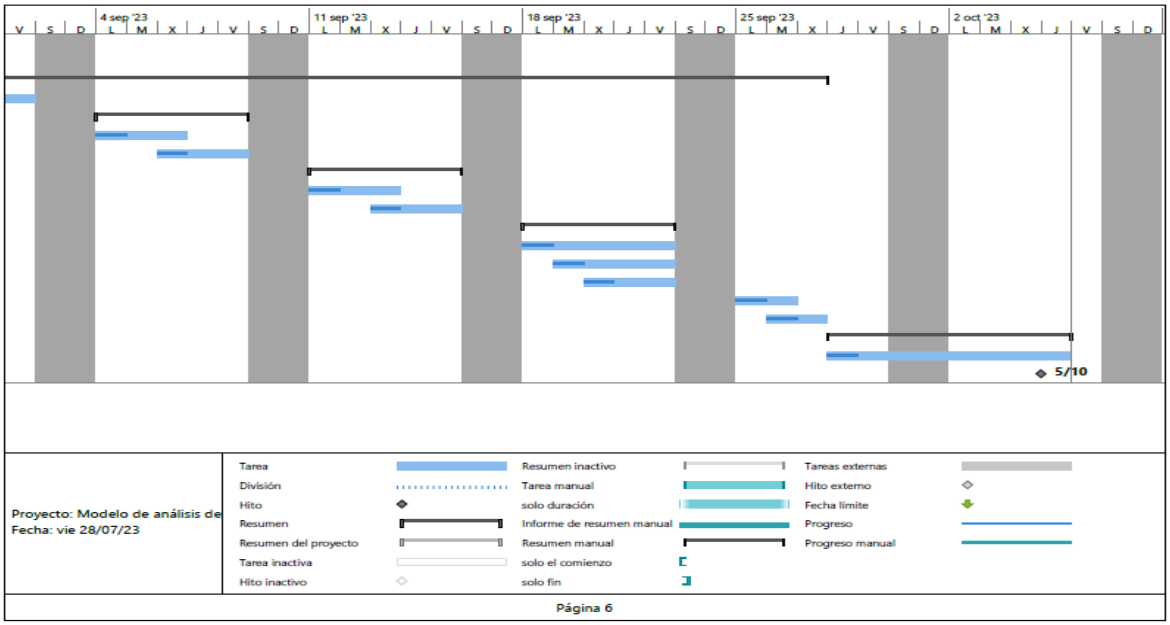
Diagrama de Gantt - 5



Nota. Elaboración Propia

Figura 31

Diagrama de Gantt - 6



Nota. Elaboración Propia

4.3.3. Propuesta económica

A continuación, se muestra la propuesta económica, para la implementación de un modelo de análisis de vulnerabilidades y riesgos para SOAINT.

Figura 32

Propuesta Económica

PROPUESTA ECONÓMICA DEL PROYECTO	MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS

DURACIÓN DEL PROYECTO	
FECHA DE INICIO	FECHA FIN
24/07/2023	5/10/2023

TIPO DE CAMBIO (Dolar $)	3.58

RECURSOS HUMANOS						
RECURSO	CANTIDAD	FECHA INGRESO	FECHA DE SALIDA	SUELDO BRUTO	COSTO MENSUAL	COSTO TOTAL
JEFE DE PROYECTO DE SEGURIDAD TI	1	24/07/2023	5/10/2023	S/ 5,000.00	S/ 7,350.00	S/ 17,885.00
ANALISTA CIBERSEGURIDAD PENTESTING	1	14/08/2023	5/10/2023	S/ 2,800.00	S/ 4,116.00	S/ 10,015.60
					SUBTOTAL	S/ 27,900.60
						$7,793.46

EQUIPOS/IMPLEMENTOS						
RECURSO	CANTIDAD			PRECIO/TARIFA		COSTO TOTAL
NoteBook Lenovo ThinkPad T14 2da Gen - Black (Intel) Procesador Intel® Core™ i7-1185G7 vPro® de 11ª generación (3,00 GHz hasta 4,80 GHz) 16 GB DDR4-3200MHz (Soldado) 512 GB SSD M.2 2280 PCIe TLC Opal	2			$1,142.46		$2,284.92
Cooler para laptop Teraware 15.6", 2 puertos usb, 5 ventiladores	2			$22.35		$44.69
Monitor plano 19.5" AOC E2070SWHN Panel TN, 1600 x 900, 60Hz, 5ms, negro	2			$111.73		$223.46
Teclado alámbrico Logitech K120, conexión usb, teclado numérico, negro	2			$16.76		$33.52
Mouse inalámbrico Teraware 4W019, receptor usb, 1600 dpi, 4 botones, usa pilas, negro	2			$11.17		$22.35
					SUBTOTAL	S/ 9,340.00
						$2,608.94

OTROS GASTOS						
RECURSO	CANTIDAD			PRECIO/TARIFA		COSTO TOTAL
SERVICIO DE INTERNET	2			S/ 90.00		S/ 180.00
SERVICIO DE LUZ	2			S/ 50.00		S/ 100.00
					SUBTOTAL	S/ 280.00
						$78.21

COSTO TOTAL DEL SERVICIO (Sin IGV)	S/ 37,520.60
	$10,480.61

TOTAL A FACTURAR DEL SERVICIO (Con IGV)	S/ 44,274.31
	$12,367.13

Nota. Elaboración Propia

V. CONCLUSIONES

De acuerdo a los resultados obtenidos, se concluyó que si es necesaria la propuesta de implementación de un modelo de análisis de vulnerabilidades y riesgos para proteger de posibles amenazas y ataques a la aplicación web de SOAINT S.A.C – Lima; 2023, en tal sentido se afirma la hipótesis general, como aporte el investigador mejoró la seguridad del perímetro, componentes red y codificación de la aplicación web y como valor agregado, al usuario final que labora y utiliza la aplicación de web de SOAINT se le realizó una capacitación de concientización, sobre la importancia de la ciberseguridad y los riesgos asociados al manejo de la información.

Por consiguiente, teniendo en cuenta los objetivos específicos llegamos a las siguientes conclusiones:

1. Se ejecutaron las pruebas de Pentesting y se descubrieron las vulnerabilidades en los componentes de red de la aplicación, se establecieron planes de acción para la remediación o subsanación de vulnerabilidades, como aporte se recomendó ejecutar el proceso pentesting a la aplicación de manera semestral como mínimo, con la finalidad de identificar posibles vulnerabilidades en la aplicación web y evitar riesgos a futuro y como valor agregado se programará una capacitación técnica de pentesting al personal de TI y operaciones de la empresa, que se coordinará con un proveedor de Ethical Hacking y pentesting con la finalidad de aplicar este tipo de procesos necesarios para la seguridad de la empresa.

2. Se identificaron vulnerabilidades presentes en la aplicación web de acuerdo a los 10 riesgos más críticos del apartado de las directrices del OWASP TOP 10 – 2021, y se establecieron planes de acción para la remediación o subsanación de vulnerabilidades con el objetivo de asegurar que no existan vulnerabilidades que expongan los datos sensibles o backdoors que un atacante pueda aprovechar, como aporte se recomendó utilizar buenas prácticas de desarrollo seguro aplicando las directrices de OWASP y que antes de realizar cambios en el código fuente de la aplicación, antes de un pase a producción, pasen por un proceso de Ethical Hacking propio o subcontratado con el fin de remediar las observaciones sobre vulnerabilidades criticas o altas antes de la puesta en

producción y como valor agregado se programará una capacitación técnica del uso de herramientas para identificar las vulnerabilidades más críticas de acuerdo al TOP 10 – 2021 de OWASP, con la finalidad de que el personal de TI y operaciones de SOAINT, pueda aplicar las técnicas de ethical hacking en beneficio de la empresa.

3. Se evaluó la gravedad de los riesgos detectados en la aplicación web utilizando la metodología de riesgos de OWASP, aplicando las etapas de la metodología para evaluar y calificar los riesgos identificados en el proceso de

   pentesting y aplicación de OWASP Top-10. y se establecieron planes de acción para la remediación de vulnerabilidades, las cuales serán ejecutadas por el personal técnico encargado de la aplicación web, como aporte se recomendó establecer un equipo de trabajo aplicando metodologías agiles como SCRUM o Kanban para la implementación de mejoras en la aplicación web u otro tipo de iniciativas que tenga la empresa, con el fin de establecer modelos de trabajo agiles, además de contar con un equipo multidisciplinario experto para llevar un desarrollo ordenado y controlado y como valor agregado se realizará una capacitación acerca de la metodología ágil SCRUM y sus herramientas para el manejo de iniciativas, que ayudarán a llevar un mejor desarrollo y trabajo en equipo.

VI. RECOMENDACIONES

1. Se sugiere contar con un perfil de analista de ciberseguridad para que apoye a la revisión y gestión de los nuevos desarrollos o implementaciones que realice la empresa.

2. Se sugiere contar con un rol Scrum Master para implementar los modelos de metodologías agiles para llevar un mejor control en los desarrollos o iniciativas TI de la organización, este rol ayudará a seleccionar roles evocados a la gestión de proyectos y desarrollos agiles.

3. Se recomienda, establecer normas, políticas y procedimientos para la seguridad de la información y el desarrollo seguro que alcance a la organización en general y

más aún a su equipo de desarrollo, con el fin de contar con lineamientos que ayuden a mejorar los procesos de manejo de información y el desarrollo seguro.

4. Se recomienda generar planes de capacitaciones orientadas al desarrollo seguro, y promover al personal a realizar cursos y certificaciones de ciberseguridad.
5. Se recomienda aplicar prácticas de desarrollo de software DevSecOps con el fin de hacer más eficiente el desarrollo del ciclo de vida del software.

REFERENCIAS BIBLIOGRÁFICAS

Alex, F. (2011). Recuperado el 10 de 10 de 2019, de http://alejandrofitz.blogspot.com/: http://alejandrofitz.blogspot.com/2011/10/el-origen-y-la-evolucion-de-las-tic.html

bidaidea. (21 de Marzo de 2022). *¿Cuál son la 5 Fases del Pentesting?* Obtenido de https://ciberseguridadbidaidea.com/fases-del-pentesting/

Calvo, L. (2022). *Aplicación de pentesting y la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo, 2022.* Huaraz.

Castillo, O. (2021). *Evaluación de metodologías de hacking ético para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa de servicios logísticos.* Pimentel.

Deloitte. (07 de Julio de 2021). *Hacking ético: qué es y cómo aprenderlo*. Obtenido de https://www2.deloitte.com/es/es/blog/cyber-pills/2021/hacking-etico-que-es-y-como-aprenderlo.html

Días, j., & Marulanda, M. (2018). *Aplicacion de la metodologia de pruebas OWASP para el mejoramiento de la seguridad en el sistema e-commerce siembraviva.com*. Antioquia.

Dzul, M. (13 de 12 de 2013). *Unidad 3. Aplicación básica de los métodos cientificos "Diseño No-Experimental"*. Obtenido de https://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES38.pdf

Google. (2023). *Imagen de Ubicación*. Obtenido de Imagen de Ubicación: https://www.google.es/maps

Hernandez, R., Fernandez, C., & Baptista, P. (2014). *Metodologia de la Investigacion* (Sexta Edicion ed.). (M. Rocha Martinez, Ed.) Mexico: McGRAW-HILL /INTERAMERICANA EDITORES,S.A. DE C.V.

Hernandez, R., Fernandez, C., & Baptista, P. (2014). *Metodologia de la Investigacion* (Sexta Edicion ed.). (M. Rocha Martinez, Ed.) Mexico: McGraw-Hill /Interamericana Editores,S.A. DE C.V.

Hernández-Pérez, F. (2019). Los riesgos de las tecnologías de la información y la comunicación. *Revista Conamed - https://www.medigraphic.com/pdfs/conamed/con-2019/con194d.pdf*, 184.

KeepCoding. (27 de Enero de 2023). *KeepCoding Tech School*. Obtenido de https://keepcoding.io/blog/que-es-owasp-top-10/#:~:text=OWASP%20Top%2010%20es%20un%20proyecto%20sin%20%C3%A1nimo,como%20una%20gu%C3%ADa%20para%20tus%20auditor%C3%ADas%20de%20ciberseguridad.

Linares, F. (28 de Marzo de 2022). *Vulnerabilidad en el sector público y la urgencia de pensar en ciberseguridad.* Obtenido de https://ciup.up.edu.pe/analisis/vulnerabilidad-en-sector-publico-la-urgencia-de-pensar-ciberseguridad/

Llerena, R. (2018). *Evaluación de la seguridad informática en el área de sistemas.* Chimbote.

López, G., & Gamboa, D. (2021). *Vulnerabilidades en aplicaciones web utilizando la metodología de "proyecto abierto de seguridad de aplicaciones web".* Ambato.

Meneses, G. (2007). *NTIC, Interacción y Aprendizaje en la Universidad. Universitat Rovira i Virgili.*

Ortega, J. (2020). *Desarrollo seguro en ingeniería del software.* Bogotá: Alpha Editorial.

Owasp. (2021). *Bienvenido al OWASP Top 10 - 2021*. Obtenido de https://owasp.org/Top10/es/

Owasp. (2021). *OWASP Top 10:2021*. Obtenido de https://owasp.org/Top10/es/

Owasp. (2023). *OWASP_Risk_Rating_Methodology*. Obtenido de https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Pérez, M. (2022). *Evaluación cuantitativa de riesgos tecnológicos de ciberseguridad en una aplicación de transferencias digitales en una entidad financiera peruana, periodo 2021-2022.* Lima.

Rojas, R., & Muedas, A. (2019). *Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2.* Lima.

school nuclio. (28 de Noviembre de 2022). *¿Qué es el Pentesting?* Obtenido de https://nuclio.school/que-es-el-pentesting/

SOAINT. (2022). *Quiénes Somos*. Obtenido de https://soaint.com/quienes-somos/

SOAINT. (2022). *SOBRE SOAINT*. Obtenido de https://soaint.com/grupo/#

SOAINT. (2023). *Linkedin - SOAINT*. Obtenido de https://pa.linkedin.com/company/soaint

SOAINT. (2023). *Nueva Filosofía de Liderazgo*. Obtenido de https://soaint.com/threeone/?utm_campaign=GLO%20-%20Filosof%C3%ADa%20anillos&utm_medium=email&_hsmi=248683281&_hsenc=p2ANqtz-_Sibyursw6K-nsbbqEcMnLd3dSdCJoHcj4QI1cUNt-B4tstr6ZsEUsaXVzhusqX_inPytKJMibNV2OG1vKiEUCDN2eIg&utm_content=248683281&utm_source=hs_e

Sutori. (s.f.). Recuperado el 10 de 10 de 2019, de Tecnología Educativa, Origen, evolución y Aportes a la educación: https://www.sutori.com/story/tecnologia-educativa-origen-evolucion-y-aportes-a-la-educacion--dz9uk6gtnPnhYwYcibQgDa5K

Tamayo y Tamayo, M. (2003). *El Proceso de la Investigacion Cientifica* (Cuarta Edicion ed.). (G. N. Editores, Ed.) Mexico: LIMUSA S.A. DE C.V.

Tasan, F., & Morocho, M. (2020). *Metodología OWASP en el desarrollo de un Website para voto electrónico. Caso práctico: Sistema de elecciones asociación de estudiantes TI-UNACH*. Riobamba.

Terrones, V. (2022). *Propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021*. Chimbote.

ULADECH. (2022). *Código de ética para la investigación.* Chimbote.

Wikipedia. (18 de 01 de 2022). *Wikipedia - La enciclopedia libre*. Obtenido de https://es.wikipedia.org/wiki/Open_Web_Application_Security_Project

ANEXOS

Anexo 01. Matriz de Consistencia

Problema	**Objetivo general**	**Hipótesis general**	**Variables**	**Metodología**
¿De qué manera la implementación un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de	Implementar un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT para protegerlo de posibles amenazas y ataques.	La propuesta de la implementación de un modelo de análisis de vulnerabilidades y riesgos para la aplicación web de SOAINT - Lima; 2023, proporciona una visión clara de las debilidades de seguridad, además de ayudar a tomar medidas proactivas para proteger la aplicación de posibles amenazas y ataques.	Modelo de análisis de vulnerabilidades y riesgos	Nivel: Cuantitativo Tipo: Descriptiva

SOAINT ayudará a proteger de posibles amenazas y ataques?	Objetivos específicos 1. Ejecutar pruebas de Pentesting con el fin de descubrir las vulnerabilidades presentes en la aplicación web de SOAINT. 2. Identificar las vulnerabilidades presentes en la aplicación web de SOAINT de acuerdo con las directrices del OWASP TOP 10 - 2021. 3. Evaluar la gravedad de los riesgos detectados en la aplicación web de SOAINT utilizando la metodología de riesgos de OWASP.	Hipótesis específicas 1. La ejecución de pruebas de Pentesting, descubre un conjunto significativo de posibles vulnerabilidades presentes en la aplicación web de SOAINT. 2. La identificación de vulnerabilidades de acuerdo con las directrices de OWASP TOP 10 – 2021 permite subsanarlas en la aplicación web de SOAINT. 3. La evaluación de la gravedad de los riesgos detectados en la aplicación web de SOAINT mitiga y genera planes de acción, donde utiliza la metodología de riesgos de OWASP.		Diseño: No Experimental de Corte Transversal.

Fuente: Elaboración propia

Anexo 02. Instrumento de recolección de información

TITULO: Implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023

TESISTA: Antony William Neyra Hidalgo

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; y se le invita a participar respondiendo a cada pregunta de forma objetiva y precisa. La información que proporcione se tratará de manera confidencial y se mantendrá en reserva. Los resultados obtenidos se utilizarán exclusivamente con fines académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere su alternativa

DIMENSIÓN 1: NIVEL DE SATISFACCIÓN DE LA APLICACIÓN WEB Y LA PROTECCIÓN DE SUS DATOS			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?		
2	¿Considera que la información disponible en la aplicación web está segura, sabiendo que se puede acceder desde cualquier dispositivo con acceso a Internet?		
3	¿Considera que la aplicación web debe tener vínculos externos hacia páginas informativas referentes a Soaint?		

4	¿Los documentos o reportes que se generan y almacenan en la aplicación web cumplen con la calidad y disponibilidad?		
5	Los procesos de solicitudes como, por ejemplo: vacaciones, ¿Considera que son eficientes y cumplen con el tiempo de respuesta?		
6	¿Considera que la página de inicio de sesión de la aplicación web, debería contar con otros factores de autenticación adicionales a usuario y contraseña?		
7	¿La gestión de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable o por el mismo trabajador?		
8	¿Considera que es importante contar con un directorio de contactos, general, dentro de la aplicación web?		

DIMENSIÓN 2: NECESIDAD DE PROPONER LA IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Ha identificado alguna vulnerabilidad o riesgos en la aplicación?		
2	¿Ha experimentado incidentes de seguridad o problemas como caídas en la aplicación web que han generado indisponibilidad?		

3	¿Considera que las posibles amenazas y vulnerabilidades pueden afectar la disponibilidad y posible pérdida de información de la aplicación web?		
4	¿Considerar que integrar el directorio activo (AD) para autentificación e inicio de sesión en la aplicación web, sería más seguro y eficientes?		
5	¿Considera que la inversión en un modelo de análisis de vulnerabilidades y riesgos sería justificada en términos de la mejora de la seguridad y la reducción de riesgos?		
6	¿Conoce estándares y marcos de seguridad existentes que respaldan la implementación de un modelo de análisis de vulnerabilidades y riesgos?		
7	¿Cree que un modelo de análisis de vulnerabilidades y riesgos proporcionaría una visión más clara de la infraestructura y sus componentes de red expuestos?		
8	¿Ha considerado que la evaluación de análisis de vulnerabilidades y riesgos ayudará a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?		

Elaboración Propia

Anexo 03. Validez del instrumento

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

3.1. Apellidos y nombres del informante (Experto): Tello Pacheco Benghir Eliel

3.2. Grado Académico: Mg (c) Ciencia de Datos

3.3. Profesión: Ingeniero de Telecomunicaciones

3.4. Institución donde labora: Clínica Internacional

3.5. Cargo que desempeña: Arquitecto de Seguridad de la Información

3.6. Denominación del instrumento: Cuestionario

3.7. Autor del instrumento: Antony Neyra Hidalgo

3.8. Carrera: Ingeniería de Telecomunicaciones

II. VALIDACIÓN:

N° de Ítem	Validez de contenido		Validez de constructo		Validez de criterio		Observaciones
	El ítem corresponde a alguna dimensión de la variable		El ítem contribuye a medir el indicador planteado		El ítem permite clasificar a los sujetos en las categorías establecidas		
	SI	NO	SI	NO	SI	NO	
Dimensión 1: Nivel de satisfacción de la aplicación web y la protección de sus datos							
¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?		X		X		X	La operabilidad de la página no contribuye a la validación de la hipótesis sobre la variable.
¿Considera que la información disponible en la aplicación web está segura, considerando que se puede acceder desde	X			X		X	Debido a que es una opinión, puede usarse como una dimensión cualitativa, pero no cuantitativa. Podría contribuir con ayudar a la definición del modelo, más que con la

103

cualquier dispositivo con acceso a Internet?							determinación del mismo.
¿Esta satisfecho con los módulos u opciones de la aplicación web que cumplen con sus necesidades como usuario?		X		X		X	La operabilidad de la pagina no contribuye a la validación de la hipótesis sobre la variable.
¿La presentación de los documentos que generan y almacenan en la aplicación web es satisfactorio en cuanto a calidad y disponibilidad?		X		X		X	La operabilidad de la pagina no contribuye a la validación de la hipótesis sobre la variable.
¿Los procesos de solicitudes como vacaciones, considera que son eficientes y cumplen con el tiempo requerido?		X		X		X	La operabilidad de la pagina no contribuye a la validación de la hipótesis sobre la variable.
¿Considera que la pagina de inicio de sesión de la aplicación	X		X		X		El doble factor corresponde a un control que se mide dicotómicamente (se tiene o no se tiene). Por tanto, si

104

web requerirá la implementación de otros factores de autenticación?							contribuye al modelo de determinación de vulnerabilidades.
¿La gestión de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable ?	X		X		X		Debe ser autogestionable, pero no buscando la facilidad de los usuarios, sino para aprovechar el estado de arte de las arquitecturas de seguridad que dan una capa extra de seguridad más allá de la contraseña (Ej: Autenticación basado en OAuth, SAML, JWT, etc)
¿Considera que deben existir otros módulo u opciones?		X		X		X	La pregunta es muy general. No aporta valor y no se puede cuantificar.

105

Dimensión 2: Necesidad de proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos							
¿Considera que es importante implementar un modelo de análisis de vulnerabilidades y riesgos en su organización?	X			X		X	El tener una opinión de la importancia puede contribuir a la concienciación. No obstante, no contribuye a la medición de un indicador para medir la efectividad, pero ayuda a dar un primer vistazo del status inicial del proceso.
¿Ha experimentado incidentes de seguridad o problemas en la aplicación que han generado indisponibilidad de la aplicación web?	X		X		X		La pregunta permite la entrada hacia la variable. Asimismo, se pued e cuantificar en una métrica y ayudar a la segmentación.
¿Considera que las posibles amenazas y vulnerabilidades pueden afectar lo disponibilidad y posible pérdida de información de la aplicación web?	X		X		X		Esta pregunta si genera conciencia. Genera una respuesta basada en mayéutica, por lo que permite el fin de la concienciación.

100

¿Cree que la implementación de un modelo de análisis de vulnerabilidades y riesgos ayudaría a proteger mejor los activos y la información de su organización?	X		X		X		Esta pregunta sí genera conciencia. Genera una respuesta basada en mayéutica, por lo que permite el fin de la concienciación. La determinación de las vulnerabilidades permite la priorización y, por tanto, la implementación efectiva de controles que mitiguen la explotación de vulnerabilidades.
¿Considera que la inversión en un modelo de análisis de vulnerabilidades y riesgos sería justificada en términos de la mejora de la seguridad y la reducción de riesgos?	X		X		X		Esta pregunta sí genera conciencia. Genera una respuesta basada en mayéutica, por lo que permite el fin de la concienciación. La inversión en Seguridad tiene un retorno directo en la mitigación de riesgos. En adición, se puede utilizar dicha inversión para tener una mayor visibilidad de red, así como brindar insights a la organización gracias al enfoque estratégico de riesgos.
¿Conoce estándares y marcos de seguridad	X		X		X		El principal marco de Seguridad es la ISO27001, el cual incluye la dimensión de análisis de

existentes que respaldan la implementación de un modelo de analisis de vulnerabilidades y riesgos?							vulnerabilidades y riesgos.
¿Cree que un modelo de analisis de vulnerabilidades y riesgos proporcionaria una visión mas clara de la infraestructura y sus componentes?	X		X		X		Asi es. Como explique anteriormente, se puede utilizar la inversión en identificación de activos y vulnerabilidades para tener una mayor visibilidad de red, asi como brindar insights a la organizacion gracias al enfoque estrategico de riesgos.
¿Ha considerado que la evaluación de analisis de vulnerabilidades y riesgos ayudara a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?	X		X		X		Esta es una pregunta que permite dar valor a un proceso de Seguridad. La gestión de vulnerabilidades permitiria poder redefinir la forma de pensar de las opciones UI/UX, las cuales pueden ayudar a mejorar la experiencia de usuario y generar retorno en nuevos leads o una mejor percepción del servicio por parte de los usuarios.

102

Firma del experto

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

3.9. **Apellidos y nombres del informante (Experto):** Gary Navarro Rojas

3.10. **Grado Académico:** Universitario titulado

3.11. **Profesión:** Ingeniero de Sistemas

3.12. **Institución donde labora:** MiBanco

3.13. **Cargo que desempeña:** Especialista de Seguridad Informatica

3.14. **Denominación del instrumento:** Cuestionario

3.15. **Autor del instrumento:** Antony Noyra Hidalgo

3.16. **Carrera:** Ingenieria de Sistemas

II. VALIDACIÓN:

Nº de Ítem	Validez de contenido		Validez de constructo		Validez de Criterio		Observaciones
	El ítem corresponde a alguna dimensión de la variable		El ítem contribuye a medir el indicador planteado		El ítem permite clasificar a los sujetos en las categorías Establecidas		
	SI	NO	SI	NO	SI	NO	
Dimensión 1: Nivel de satisfacción de la aplicación web y la protección de sus datos							
¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?	X		X		X		

103

¿Considera que la información disponible en la aplicación web está segura, considerando que se puede acceder desde cualquier dispositivo con acceso a Internet?	X		X		X		
¿Está satisfecho con los modulos u opciones de la aplicación web que cumplen con sus necesidades como usuario?	X		X		X		
¿La presentación de los documentos que generan y almacenan en la aplicación web es satisfactorio en cuanto a calidad y disponibilidad?	X		X		X		
¿Los procesos de solicitudes como vacaciones, considera que	X		X		X		

104

son eficientes y cumplen con el tiempo requerido?							
¿Considera que la pagina de inicio de sesión de la aplicación web requerirta la implementación de otros factores de autenticación?	X		X		X		
¿La gestión de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable ?	X		X		X		
¿Considera que deben existir otros módulo u opciones?	X		X		X		

105

Dimensión 2: Necesidad de proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos							
¿Considera que es importante implementar un modelo de análisis de vulnerabilidades y riesgos en su organización?	X		X		X		
¿Ha experimentado incidentes de seguridad o problemas en la aplicación que han generado indisponibilidad de la aplicación web?	X		X		X		
¿Considera que las posibles amenazas y vulnerabilidades pueden afectar lo disponibilidad y posible pérdida de información de la aplicación web?	X		X		X		

100

¿Cree que la implementación de un modelo de analisis de vulnerabilidades y riesgos ayudaria a proteger mejor los activos y la información de su organización?	X		X		X		
¿Considera que la inversión en un modelo de analisis de vulnerabilidades y riesgos seria justificada en términos de la mejora de la seguridad y la reducción de riesgos?	X		X		X		
¿Conoce estándares y marcos de seguridad existentes que respaldan la implementación de un modelo de analisis de vulnerabilidades	X		X		X		

101

y riesgos?							
¿Cree que un modelo de análisis de vulnerabilidades y riesgos proporcionaría una visión más clara de la infraestructura y sus componentes?	X		X		X		
¿Ha considerado que la evaluación de análisis de vulnerabilidades y riesgos ayudará a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?	X		X		X		

Navarro Rojas Gary

Firma del experto

102

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

3.17. **Apellidos y nombres del informante (Experto):** Jhon Romero Lovera

3.18. **Grado Académico:** Magister

3.19. **Profesión:** Ingeniero de Sistemas

3.20. **Institución donde labora:** MiBanco

3.21. **Cargo que desempeña:** Especialista de Seguridad de la Información

3.22. **Denominación del instrumento:** Cuestionario

3.23. **Autor del instrumento:** Antony Neyra Hidalgo

3.24. **Carrera:** Ingeniería de Sistemas

II. VALIDACIÓN:

Nº de Ítem	Validez de contenido		Validez de constructo		Validez de criterio		Observaciones
	El ítem corresponde a alguna dimensión de la variable		El ítem contribuye a medir el indicador planteado		El ítem permite clasificar a los sujetos en las categorías establecidas		
	SI	NO	SI	NO	SI	NO	
Dimensión 1: Nivel de satisfacción de la aplicación web y la protección de sus datos							
¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?	X		X		X		
¿Considera que la información disponible en la aplicación web está segura, considerando que se puede acceder desde	X		X		X		

103

cualquier dispositivo con acceso a Internet?							
¿Está satisfecho con los modulos u opciones de la aplicación web que cumplen con sus necesidades como usuario?	X		X		X		
¿La presentación de los documentos que generan y almacenan en la aplicación web es satisfactorio en cuanto a calidad y disponibilidad?	X		X		X		
¿Los procesos de solicitudes como vacaciones, considera que son eficientes y cumplen con el tiempo requerido?	X		X			X	Puede generar una confusión, porque dice "un proceso, o hablas en general, pero si es en general por lo general siempre piensan en el proceso más lento, se recomienda colocar el proceso de solicitudes de vacaciones que sea a ese u otro.
¿Considera que la pagina de inicio de sesión de la aplicación	X		X			X	Si es para gente de sistemas si lo entienden, pero si no debes hablar menos técnicamente sore otros factores de autentificación

104

web requerirta la implementación de otros factores de autenticación?							Podria ser algo asi, "Crees que la seguridad a inicio de sesión……"
¿La gestion de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable ?	X		X			X	Por el mismo cliente/trabajador te falta colocar a quien lo autogestionara
¿Considera que deben existir otros módulo u opciones?	X		X		X		Siempre debes colocar donde… considera que deben existir otros modulo u opciones en la aplicación, en todas las preguntas colocarle a donde está dirigido.

105

Dimensión 2: Necesidad de proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos							
¿Considera que es importante implementar un modelo de análisis de vulnerabilidades y riesgos en su organización?	X		X		X		
¿Ha experimentado incidentes de seguridad o problemas en la aplicación que han generado indisponibilidad de la aplicación web?	X		X		X		
¿Considera que las posibles amenazas y vulnerabilidades pueden afectar lo disponibilidad y posible pérdida de información de la aplicación web?		X	X		X		la
¿Cree que la implementación de un modelo de análisis de vulnerabilidades	X		X	106		X	Si es para sistemas si se entiende pero si no debe cambiar esta palabra.....recursos de la organización

y riesgos ayudaría a proteger mejor los activos y la información de su organización?							
¿Considera que la inversión en un modelo de análisis de vulnerabilidades y riesgos sería justificada en términos de la mejora de la seguridad y la reducción de riesgos?	X		X		X		
¿Conoce estándares y marcos de seguridad existentes que respaldan la implementación de un modelo de análisis de vulnerabilidades y riesgos?	X		X		X		
¿Cree que un modelo de análisis de vulnerabilidades y riesgos	X		X		X		

107

proporcionaría una visión más clara de la infraestructura y sus componentes?							
¿Ha considerado que la evaluación de análisis de vulnerabilidades y riesgos ayudará a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?	X		X		X		

Romero Lovera Jhon

Firma del experto

INFORME DE OPINIÓN DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

3.1. Apellidos y nombres del informante (Experto): Pérez Castro Manuel

3.2. Grado Académico: Universitario titulado

3.3. Profesión: Ingeniero de Sistemas

3.4. Institución donde labora: MiBanco

3.5. Cargo que desempeña: Experto de Ciberseguridad

3.6. Denominación del instrumento: Formularios

3.7. Autor del instrumento: Antony Neyra Hidalgo

3.8. Carrera: Ingeniería de Sistemas

II. VALIDACIÓN:

Nº de Ítem	Validez de contenido		Validez de constructo		Validez de criterio		Observaciones
	El ítem corresponde a alguna dimensión de la variable		El ítem contribuye a medir el indicador planteado		El ítem permite clasificar a los sujetos en las categorías establecidas		
	SI	NO	SI	NO	SI	NO	
Dimensión 1: Nivel de satisfacción de la aplicación web y la protección de sus datos							
¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?	X			X		X	Se recomienda implementar un Threat Modeling como Trike para identificar vulnerabilidades entre interfaces.
¿Considera que la información disponible en la aplicación web está segura, considerando que se puede acceder desde	X		X		X		Se recomienda ejecutar un Ethical Hacking para validar vulnerabilidades, así como, validar los diagramas de arquitectura.

100

cualquier dispositivo con acceso a Internet?							
¿Esta satisfecho con los módulos u opciones de la aplicación web que cumplen con sus necesidades como usuario?	X			X		X	Suma para el negocio, pero no necesariamente para seguridad de la información.
¿La presentación de los documentos que generan y almacenan en la aplicación web es satisfactorio en cuanto a calidad y disponibilidad?	X			X		X	Se recomienda implementar una clasificación de la información y comunicarlo al interno de la organización, en base a esta clasificación, se tendra que colocar los controles correspondientes.
¿Los procesos de solicitudes como vacaciones, considera que son eficientes y cumplen con el tiempo requerido?	X			X		X	Suma para el negocio, pero no necesariamente para seguridad de la información.
¿Considera que la pagina de inicio de sesión de la aplicación	X		X		X		Si la pagina esta expuesta en internet si se deberia tener un MFA robusto.

101

web requerirá la implementación de otros factores de autenticación?							
¿La gestión de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable?	X		X		X		Si debería ser auto gestionable, a esto sumarle el MFA para el reinicio de la contraseña y la comunicación de estas acciones a los equipos especializados en los casos de usuarios con altos privilegios (gerentes, administradores, etc).
¿Considera que deben existir otros módulo u opciones?	X			X		X	Suma para el negocio, pero no necesariamente para seguridad de la información.

Dimensión 2: Necesidad de proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos							
¿Considera que es importante implementar un modelo de análisis de vulnerabilidades y riesgos en su organización?	X		X		X		Si se considera una buena práctica de seguridad.
¿Ha experimentado incidentes de seguridad o problemas en la aplicación que han generado indisponibilidad de la aplicación web?	X		X		X		Se recomienda definir el procedimiento de SLAs de atención de los incidentes, así como los responsables, también se recomienda integrar los logs de salud a un SIEM para darle seguimiento por parte del equipo especializado de soporte (SOC)
¿Considera que las posibles amenazas y vulnerabilidades pueden afectar la disponibilidad y posible pérdida de información de la aplicación web?	X		X		X		Se recomienda tener un gobierno de riesgos así como una matriz de riesgos.

100

¿Cree que la implementación de un modelo de analisis de vulnerabilidades y riesgos ayudaria a proteger mejor los activos y la información de su organización?	X		X		X		La pregunta es muy parecida a la primera realizada, se recomienda consolidarla en una sola.
¿Considera que la inversión en un modelo de analisis de vulnerabilidades y riesgos seria justificada en términos de la mejora de la seguridad y la reducción de riesgos?	X		X		X		Este modelo deberia estar considerado desde el inception del desarrollo de la aplicación, asi como en los skills de los stakeholders técnicos responsables del proyecto.
¿Conoce estándares y marcos de seguridad existentes que respaldan la implementación de un modelo de analisis de vulnerabilidades	X		X		X		Se recomienda aplicar NIST, ISO 27001, OWASP, entre otros.

101

y riesgos?							
¿Cree que un modelo de analisis de vulnerabilidades y riesgos proporcionaria una visión mas clara de la infraestructura y sus componentes?	X		X		X		Si se considera una buena practica de seguridad.
¿Ha considerado que la evaluación de analisis de vulnerabilidades y riesgos ayudara a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?	X		X		X		Si se considera una buena practica de seguridad.

Perez Castro Manuel

Firma del experto

Anexo 04. Confiabilidad del instrumento

CARTA DE PRESENTACIÓN

Magister/Doctor: Benghir Ellel Tello Pacheco

Presente. -

Tema: PROCESO DE VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTOS

Ante todo, saludarlo cordialmente y agradecerle la comunicación con su persona para hacer de su conocimiento que yo ANTONY WILLIAM NEYRA HIDALGO estudiante / egresado del programa académico de Ingeniería de Sistemas de la Universidad Católica Los Ángeles de Chimbote, debo realizar el proceso de validación de mi instrumento de recolección de información, motivo por el cual acudo a Ud. para su participación en el Juicio de Expertos.

Mi proyecto se titula: IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C y envió a Ud. el expediente de validación que contiene:

- Ficha de Identificación de experto para proceso de validación
- Carta de presentación
- Matriz de operacionalización de variables
- Matriz de consistencia
- Ficha de validación

Agradezco anticipadamente su atención y participación, me despido de usted.

Atentamente.

---------- DNI: 45905574

Firma de Estudiante

CARTA DE PRESENTACIÓN

Magister/Doctor: GARY JOEL NAVARRO ROJAS .....

Presente. -

Tema: PROCESO DE VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTOS

Ante todo, saludarlo cordialmente y agradecerle la comunicación con su persona para hacer de su conocimiento que yo ANTONY WILLIAM NEYRA HIDALGO estudiante / egresado del programa académico de Ingeniería de Sistemas de la Universidad Católica Los Ángeles de Chimbote, debo realizar el proceso de validación de mi instrumento de recolección de información, motivo por el cual acudo a Ud. para su participación en el Juicio de Expertos.

Mi proyecto se titula: IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C y envió a Ud. el expediente de validación que contiene:

- Ficha de Identificación de experto para proceso de validación
- Carta de presentación
- Matriz de operacionalización de variables
- Matriz de consistencia
- Ficha de validación

Agradezco anticipadamente su atención y participación, me despido de usted.

Atentamente.

---------- DNI: 45905574

Firma de Estudiante

CARTA DE PRESENTACIÓN

Magister/Doctor: JHON ALEX ROMERO LOVERA

Presente. -

Tema: PROCESO DE VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTOS

Ante todo, saludarlo cordialmente y agradecerle la comunicación con su persona para hacer de su conocimiento que yo ANTONY WILLIAM NEYRA HIDALGO estudiante / egresado del programa académico de Ingeniería de Sistemas de la Universidad Católica Los Ángeles de Chimbote, debo realizar el proceso de validación de mi instrumento de recolección de información, motivo por el cual acudo a Ud. para su participación en el Juicio de Expertos.

Mi proyecto se titula: IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C y envió a Ud. el expediente de validación que contiene:

- Ficha de Identificación de experto para proceso de validación
- Carta de presentación
- Matriz de operacionalización de variables
- Matriz de consistencia
- Ficha de validación

Agradezco anticipadamente su atención y participación, me despido de usted.

Atentamente.

---------- DNI: 45905574

Firma de Estudiante

CARTA DE PRESENTACIÓN

Magister/Doctor: Manuel Martin Perez Castro

Presente. -

Tema: PROCESO DE VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTOS

Ante todo, saludarlo cordialmente y agradecerle la comunicación con su persona para hacer de su conocimiento que yo ANTONY WILLIAM NEYRA HIDALGO estudiante / egresado del programa académico de Ingeniería de Sistemas de la Universidad Católica Los Ángeles de Chimbote, debo realizar el proceso de validación de mi instrumento de recolección de información, motivo por el cual acudo a Ud. para su participación en el Juicio de Expertos.

Mi proyecto se titula: IMPLEMENTACIÓN DE UN MODELO DE ANALISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C y envío a Ud. el expediente de validación que contiene:

- Ficha de Identificación de experto para proceso de validación
- Carta de presentación
- Matriz de operacionalización de variables
- Matriz de consistencia
- Ficha de validación

Agradezco anticipadamente su atención y participación, me despido de usted.

Atentamente.

---------- DNI: 45905574

Firma de Estudiante

Anexo 05. Formato de Consentimiento Informado

Investigador principal del proyecto: Neyra Hidalgo Antony William

Consentimiento informado

Estimado participante,

El presente estudio tiene como objetivo: Implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023, para proteger la aplicación web de posibles amenazas y ataques.

La presente investigación informa que la Empresa SOAINT S.A.C, genera, almacena y comparte información a sus empleados a través de módulos y opciones que se encuentren en una aplicación web llamada SIGO, y se busca asegurar la aplicación web.

Toda la información que se obtenga del análisis de esta investigación, será confidencial y sólo los investigadores y el comité de ética podrán tener acceso a esta información. Será guardada en una base de datos protegidas con contraseñas. Tu nombre no será utilizado en ningún informe. Si decides no participar, no se te tratará de forma distinta ni habrá prejuicio alguno. Si decides participar, eres libre de retirarte del estudio en cualquier momento.

Si tienes dudas sobre el estudio, puedes comunicarte con el investigador principal, Neyra Hidalgo, Antony William al celular: 959841590, o al correo: antony_wnh@hotmail.com.

Si tienes dudas acerca de tus derechos como participante de un estudio de investigación, puedes llamar a la Mg. Zoila Rosa Limay Herrera presidente del Comité institucional de Ética en Investigación de la Universidad Católica los Ángeles de Chimbote, Cel: (+51043) 327-933, Email: zlimayh@uladech.edu.pe

Obtención del Consentimiento Informado

Me ha sido leído el procedimiento de este estudio y estoy completamente informado de los objetivos del estudio. El (la) investigador(a) me ha explicado el estudio y absuelto mis dudas. Voluntariamente doy mi consentimiento para participar en este estudio:

Nombre del Participante:	Antony William Neyra Hidalgo

Anexo 06. Documento de aprobación de institución para la recolección de información

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

«Año de la Unidad, la Paz y el Desarrollo»

Chimbote, 18 de agosto 2023

CARTA N°001-2023-ULADECH CATÓLICA

Señor(a):
VALERIA VARGAS-MACHUCA RAMÍREZ
SOAINT S.A.C.

Presente.-

Asunto: Presentación y aceptación para la ejecución de proyecto de tesis.

Tengo el agrado de dirigirme a usted para saludarlo y al mismo tiempo permitame presentarme como NEYRA HIDALGO ANTONY WILLIAM, con código 2709070013, estudiante egresado de la Carrera Profesional de Ingeniería de Sistemas; quién solicita su autorización para ejecutar su proyecto de investigación denominado " IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS DE LA APLICACIÓN WEB DE SOAINT S.A.C – LIMA; 2023.", durante el periodo del 02-05-2023 hasta el 27-08-2023.

Agradeceré brinde su apoyo y facilidades a fin de ejecutar satisfactoriamente el proyecto de investigación, el mismo que beneficiará a la empresa y a los mis conocimientos.

En espera de su amable atención, quedo de usted.

Atentamente,

.....
Neyra Hidalgo, Antony William
DNI: 45905574

Anexo 07. Evidencias de ejecución (declaración jurada, base de datos)

1. Consentimiento Informado

Investigador principal del proyecto: Neyra Hidalgo Antony William

Consentimiento informado

Estimado participante,

El presente estudio tiene como objetivo: Implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023, para proteger la aplicación web de posibles amenazas y ataques.

La presente investigación informa que la Empresa SOAINT S.A.C, genera, almacena y comparte información a sus empleados a través de módulos y opciones que se encuentren en una aplicación web llamada SIGO, y se busca asegurar la aplicación web.

Toda la información que se obtenga del análisis de esta investigación, será confidencial y sólo los investigadores y el comité de ética podrán tener acceso a esta información. Será guardada en una base de datos protegidas con contraseñas. Tu nombre no será utilizado en ningún informe. Si decides no participar, no se te tratará de forma distinta ni habrá prejuicio alguno. Si decides participar, eres libre de retirarte del estudio en cualquier momento.

Si tienes dudas sobre el estudio, puedes comunicarte con el investigador principal, Neyra Hidalgo, Antony William al celular: 959841590, o al correo: antony_wnh@hotmail.com.

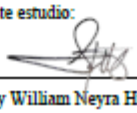
Si tienes dudas acerca de tus derechos como participante de un estudio de investigación, puedes llamar a la Mg. Zoila Rosa Limay Herrera presidente del Comité institucional de Ética en Investigación de la Universidad Católica los Ángeles de Chimbote, Cel: (+51043) 327-933, Email: zlimayh@uladech.edu.pe

Obtención del Consentimiento Informado

Me ha sido leído el procedimiento de este estudio y estoy completamente informado de los objetivos del estudio. El (la) investigador(a) me ha explicado el estudio y absuelto mis dudas. Voluntariamente doy mi consentimiento para participar en este estudio:

Diana Marroquín Ramirez

Nombre del Participante:



Antony William Neyra Hidalgo

2. Instrumento de recolección de información

TITULO: Implementación de un modelo de análisis de vulnerabilidades y riesgos de la aplicación web de SOAINT S.A.C – Lima; 2023

TESISTA: Antony William Neyra Hidalgo

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; y se le invita a participar respondiendo a cada pregunta de forma objetiva y precisa. La información que proporcione se tratará de manera confidencial y se mantendrá en reserva. Los resultados obtenidos se utilizarán exclusivamente con fines académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere su alternativa

DIMENSIÓN 1: NIVEL DE SATISFACCIÓN DE LA APLICACIÓN WEB Y LA PROTECCIÓN DE SUS DATOS			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿La navegación resulta fácil debido a que la interfaz web es intuitiva y dinámica?	x	
2	¿Considera que la información disponible en la aplicación web está segura, sabiendo que se puede acceder desde cualquier dispositivo con acceso a Internet?	x	
3	¿Considera que la aplicación web debe tener vínculos externos hacia páginas informativas referentes a Soaint?	x	
4	¿Los documentos o reportes que se generan y almacenan en la aplicación web cumplen con la calidad y disponibilidad?	x	

2

5	Los procesos de solicitudes como, por ejemplo: vacaciones, ¿Considera que son eficientes y cumplen con el tiempo de respuesta?	x	
6	¿Considera que la página de inicio de sesión de la aplicación web, debería contar con otros factores de autenticación adicionales a usuario y contraseña?		x
7	¿La gestión de olvido de contraseña o desbloqueo de usuario, considera que debe ser autogestionable o por el mismo trabajador?	x	
8	¿Considera que es importante contar con un directorio de contactos, general, dentro de la aplicación web?	x	

DIMENSIÓN 2: NECESIDAD DE PROPONER LA IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Ha identificado alguna vulnerabilidad o riesgos en la aplicación?		x
2	¿Ha experimentado incidentes de seguridad o problemas como caídas en la aplicación web que han generado indisponibilidad?	x	
3	¿Considera que las posibles amenazas y vulnerabilidades pueden afectar la disponibilidad y posible pérdida de información de la aplicación web?	x	
4	¿Considerar que integrar el directorio activo (AD) para autentificación e inicio de sesión en la aplicación web, sería más seguro y eficientes?	x	
5	¿Considera que la inversión en un modelo de análisis de vulnerabilidades y riesgos sería justificada en términos de la mejora de la seguridad y la reducción de riesgos?	x	

3

6	¿Conoce estándares y marcos de seguridad existentes que respaldan la implementación de un modelo de análisis de vulnerabilidades y riesgos?		x
7	¿Cree que un modelo de análisis de vulnerabilidades y riesgos proporcionaría una visión más clara de la infraestructura y sus componentes de red expuestos?	x	
8	¿Ha considerado que la evaluación de análisis de vulnerabilidades y riesgos ayudará a reestructurar la interfaz y/o adicionar nuevas opciones para la aplicación web?	x	

4

SI 1
NO 0

TABULACIÓN PARA LA VARIABLE / DIMENSIÓN NRO. 01

	1	2	3	4	5	6	7	8	9	10	Si	No	Si	No	
1	1	1	1	1	1	1	1	1	1	1	10	0	100.00	-	100.00
2	1	0	1	0	1	1	0	1	1	1	7	3	70.00	30.00	100.00
3	1	0	1	1	1	1	0	1	1	1	8	2	80.00	20.00	100.00
4	1	1	1	1	1	1	1	0	1	1	9	1	90.00	10.00	100.00
5	1	1	1	1	1	1	1	1	1	1	10	0	100.00	-	100.00
6	1	1	0	1	1	1	1	1	0	1	8	2	80.00	20.00	100.00
7	1	0	1	1	1	0	0	1	0	1	6	4	60.00	40.00	100.00
8	1	0	1	0	1	1	1	0	0	1	6	4	60.00	40.00	100.00
	1	1	1	1	1	1	1	1	1	1	10	0			
											64	16	80.00	20.00	

SI 1
NO 0

Tabla 1
Navegación web es intuitiva y dinámica

Alternativas	n	%
Si	10	100.00
No	0	0.00
Total	10	100.00

Tabla 2
Información en aplicación web está segura

Alternativas	n	%
Si	7	70.00
No	3	30.00
Total	10	100.00

Tabla 3
Vínculos externos a páginas referentes a Soaint

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Tabla 4
Calidad y disponibilidad de documentos o reporte

Alternativas	n	%
Si	9	90.00
No	1	10.00
Total	10	100.00

Tabla 5
Considera eficientes los tiempo de respuesta

Alternativas	n	%
Si	10	100.00
No	0	0.00
Total	10	100.00

Tabla 6
Factores de autenticación adicionales a usuario y contraseña

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Tabla 7
Autogestión de credenciales

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Tabla 8
Directorio de contactos general

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

TABULACIÓN PARA LA VARIABLE / DIMENSIÓN NRO. 02

	1	2	3	4	5	6	7	8	9	10	1	0			
1	0	0	0	0	1	0	0	0	0	0	1	9	10.00	90.00	100.00
2	0	0	1	0	1	1	0	1	0	0	4	6	40.00	60.00	100.00
3	0	1	1	1	1	1	0	1	1	1	8	2	80.00	20.00	100.00
4	1	1	1	1	1	1	1	1	1	1	10	0	100.00	0.00	100.00
5	1	1	1	1	1	1	1	1	1	1	10	0	100.00	0.00	100.00
6	1	1	0	0	1	1	0	0	1	1	6	4	60.00	40.00	100.00
7	1	1	1	1	1	1	0	1	1	1	9	1	90.00	10.00	100.00
8	1	1	1	1	1	1	0	1	1	1	9	1	90.00	10.00	100.00
	1	1	1	1	1	1	0	1	1	1	9	1			
											57	23	71.25	28.75	

Tabla 1

Vulnerabilidades y riesgos en aplicación

Alternativas	n	%
Si	1	10.00
No	9	90.00
Total	10	100.00

Tabla 2

Incidentes de seguridad en aplicación web

Alternativas	n	%
Si	4	40.00
No	6	60.00
Total	10	100.00

Tabla 3

Amenazas y vulnerabilidades afectan la disponibilidad y pérdida de información

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Tabla 4

Integrar AD para inicio de sesión

Alternativas	n	%
Si	10	100.00
No	0	0.00
Total	10	100.00

Tabla 5

Modelo de análisis de vulnerabilidades y riesgos m

Alternativas	n	%
Si	10	100.00
No	0	0.00
Total	10	100.00

Tabla 6

Conocimientos de estándares y marcos de seguridad

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Tabla 7

El Análisis de vulnerabilidades y riesgos ayuda

Alternativas	n	%
Si	9	90.00
No	1	10.00
Total	10	100.00

Tabla 8

Reestructurar la interfaz luego del analisis de v

Alternativas	n	%
Si	9	90.00
No	1	10.00
Total	10	100.00