BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN



"SEGURIDAD LÓGICA DE UNA RED, PRUEBAS E IMPLEMETACIÓN DIAGNÓSTICA"

TESIS PRESENTADA PARA OBTENER EL TÍTULO DE:

INGENIERÍA EN CIENCIAS DE LA COMPUTACION

PRESENTA:

GABRIELA GIOVANA PÉREZ LÓPEZ

ASESORA:

M.C. ADRIANA HERNÁNDEZ BERISTAIN

ABRIL 2024

AGRADECIMIENTOS

En primer lugar, quiero expresar mi sincero agradecimiento a mis padres, por el constante apoyo que ha sido fundamental para alcanzar mis metas tanto personales como académicas. Su amor y aliento han sido un motor que me ha impulsado a perseverar y superar los obstáculos que he enfrentado en el camino. Además, por ser el soporte económico para poder concentrarme en mis estudios y nunca abandonarlos.

También deseo expresar mi más sincero agradecimiento a mi asesora de tesis por su compromiso y comprensión. Su orientación experta y sus comentarios precisos fueron indispensables para alcanzar este importante hito en mi trayectoria académica. Agradezco su valiosa guía y consejos, que atesoraré como parte fundamental de mi formación profesional.

Quiero expresar mi gratitud a todos mis compañeros, quienes no solo han sido colegas, sino también amigos cercanos y confidentes. Agradezco sinceramente las horas compartidas, los proyectos colaborativos y las experiencias compartidas que hemos vivido juntos.

INDICE

CAPÍTULO 1. INTRODUCCIÓN *5*

1.1 Resumen **5**

1.2 Planteamiento del problema **6**

1.3 Justificación **7**

1.4 Objetivo general **7**

1.5 Objetivos Específicos **7**

CAPÍTULO 2. ESTADO DEL ARTE *8*

2.1Antecedentes **8**

2.2 Aplicaciones similares **9**

2.2.1 Rio Bravo Systems 9
2.2.2 Sonar 9
2.2.3 Fortra 10
2.2.4 Ivanti 10

CAPÍTULO 3. MARCO TEÓRICO *12*

3.1 Metodología **12**

3.2 Aplicaciones web **15**

3.2.1 Antecedentes 15
3.2.2 Interfaz 16
3.2.3 Inconvenientes 19
3.2.4 Ley de derecho al olvido 19
3.2.5 Historia de derecho al olvido 20

3.3 Software de la aplicación **20**

3.3.1 Servlets 20
3.3.2 Java Script 21

3.4 Bases de datos **22**

3.4.1 Tipos de Bases de Datos 22
3.4.2 Software que se utilizó para la base de datos 23

3.5 Seguridad Lógica **24**

3.5.1 Control de accesos 25
3.5.2 Control de accesos de Software 26
3.5.3 Control de accesos de Programas 27
3.5.5 Control de Privilegios 28
3.5.6 Control de Información 28

3.6 Evaluación de Amenazas Lógicas **29**

3.6.1 Seguridad informática 29
3.6.2 Amenazas a la seguridad informática 30
3.6.3 Amenazas lógicas de programas. 31
3.6.4 Amenazas Lógicas de Correos 33
3.6.5 Amenazas Lógicas de Páginas Web 33
3.6.6 Amenazas Lógicas de Software 34

3.7 Pruebas de Seguridad 34

CAPÍTULO 4. DISEÑO Y DESARROLLO DEL SISTEMA 38

4.1 Análisis y requerimientos de la aplicación web 38

4.1.1 Requerimientos no funcionales del sistema 39
4.1.2 Modelado del sistema 40
4.1.3 Diagrama entidad relación 44
4.1.4 Diagrama de clases 45
4.1.5 Diseño del sistema 46

4.2 Desarrollo de la aplicación web 54

CAPITULO 5 PRUEBAS Y RESULTADOS 70

5.1 Pruebas 70
5.1.1 Pruebas por exploración 70
5.2 Resultados 74

CAPÍTULO 6. CONCLUSIONES Y TRABAJO A FUTURO 76

6.2 Trabajo futuro 76

CAPITULO 7 BIBLIOGRAFIA 77

1.1 Resumen

En el presente proyecto, se desarrolló una aplicación web la cual fue nombrada como: Security and Audit I&G (SAIG) .Durante todo el documento se presentará el desarrollo y la implementación del mismo, este documento está compuesto por diferentes capítulos en donde se explicará en cada uno como se fue desarrollando el proyecto de tesis, el proyecto trata de otorgar sugerencias a los usuarios con base en la revisión de vulnerabilidades ante ataques cibernéticos la cual apoya al usuario en evitar algún tipo de problemática que lo lleve a ser víctima de un delitos cibernéticos, la mínima importancia que le otorgamos a la seguridad de nuestros sistemas es la causante de muchos de los delitos a los que el usuario que se queda expuesto, pero mediante el avance tecnológico van surgiendo métodos de robo, espionaje o daños a nuestros sistemas, por lo cual es necesario que un sistema o una aplicación web de cualquier tipo de sistema tecnológico que las organizaciones usen, este protegido ante amenazas de seguridad.

El proyecto de tesis presenta una aplicación web con un análisis completo en las áreas corporativas de la empresa. La aplicación web lleva al usuario a revisar las vulnerabilidades de su organización con base en un cuestionario que lo evalúa cada aspecto de sus sistemas internos, desde las contraseñas que colocan en sus diferentes accesos, que cumplen con estándares establecidos para una buena seguridad, y el cuestionario lleva al usuario a revisar softwares que involucren datos relacionados con la empresa y uso de datos personales.

Cuando el usuario obtuvo el análisis completo, se le evalúa cómo se encuentran sus áreas corporativas actualmente, y generar un informe final con sugerencias para mejorar la seguridad en sus áreas y sistemas, para disminuir un porcentaje de vulnerabilidad en los sistemas, mejorando con ello la seguridad tecnológica de la organización.

En el Capítulo 1: Introducción, se muestra el planteamiento del problema para conocer las necesidades que motivaron al presente proyecto, se especifica la justificación y se describen los objetivos.

En el Capítulo 2: Estado del arte, en él se encontrarán los antecedentes donde se conoce que en el año 2017 se incrementaron los ataques cibernéticos, otro tema que se da a conocer son las aplicaciones similares a Segurity and Audit I&G (SAIG) algunas de ellas son: Rio Bravo Systems, Sonar, Fortra, Ivanti .

En el Capítulo 3: Marco teórico, la metodología es desarrollar un análisis, ejecución y modelado de la aplicación Segurity and Audit I&G (SAIG), en donde encontramos las fases de análisis, planificación, formulación, modelado, producción y test. Con lo anterior se menciona la estructura de los menús requeridos dando un informe de la evaluación. Se define los conceptos de aplicación web que es un intercambio de información y proporciona servicios de forma remota, así como también se mencionan los softwares que se usaron para la aplicación los cuales son: Servlets, Script java, consultas con PHP, Servidores Web y Base de datos.
También se menciona la protección de datos, el encriptado de los datos, las pruebas de software y tipos de pruebas de software.

En el Capítulo 4: Diseño y desarrollo del sistema, se menciona el análisis y cada uno de los requerimientos de la aplicación Segurity and Audit I&G (SAIG), el caso de uso extenso de la aplicación, diagrama de clases y diagrama de secuencias.

1.2 Planteamiento del problema

Actualmente, existen distintas formas de realizar ataques cibernéticos que causan problemas tanto a empresas como a usuarios individuales. Es por ello por lo que surge la necesidad de proteger los sistemas, ayudar a erradicar dichos ataques y mejorar la seguridad de ellos.

Por tanto, en este proyecto de tesis se plantea el desarrollo de la aplicación web Security and Audit I&G (SAIG) para sistemas de empresas o usuarios individuales con la finalidad de brindar un análisis y sugerencias acerca de las vulnerabilidades con las que cuenta su sistema. De esta manera se contribuye al mejoramiento de seguridad corriendo por cuenta de cada usuario que tipo de sugerencia aplicar a su sistema para evitar seguir teniendo las vulnerabilidades encontradas y poder protegerse de los ataques.

1.3 Justificación

Actualmente se presentan con mayor frecuencia los ataques hacia la seguridad de redes como lo son de empresas, escuelas por mencionar algunos. Por eso es tan importante estar informado sobre los tipos de ataques que podría sufrir una organización y de qué manera poder protegernos de estos. Existen softwares con los que es más práctico y sencillo proteger ante los diferentes tipos de ataques, de los que se hablará después.

Cada organización es distinta y requiere de diferentes medidas de protección, ante esto es muy importante identificar qué tipo de protección es conveniente y eficiente usar. Cada ataque se comporta y funciona de distintas formas, pero los daños causados son en su mayoría de importancia ya que se habla de datos confidenciales.

1.4 Objetivo general

Diagnosticar la vulnerabilidad del control de acceso a una red en una Institución Educativa y una Empresa, a través de una aplicación web, para mitigar los posibles ataques cibernéticos y mejorar la seguridad lógica de la red.

1.5 Objetivos Específicos

- Analizar a detalle la bibliografía sobre los tipos de ataques cibernéticos existentes hacia una red.
- Analizar a detalle la bibliografía de las técnicas para mitigar los ataques cibernéticos.
- Modelar la base de datos necesaria.
- Implementar una aplicación web que permita realizar el diagnóstico de la seguridad lógica.
- Evaluar la seguridad lógica de una empresa y una universidad con la aplicación web.

- Mostrar cómo se aplican los diferentes tipos de técnicas para mitigar los ataques.
- Recomendar cambios en la seguridad lógica de la red.
- Generar reporte final de los resultados obtenidos en la evaluación de seguridad lógica.

CAPÍTULO 2. ESTADO DEL ARTE

2.1Antecedentes

Es importante conocer los porcentajes de los ataques cibernéticos ya que con esto se puede apreciar que, a pesar de tener algunas medidas de seguridad, en muchos casos no es suficiente por ello es recomendable evaluar las debilidades y reforzar la seguridad. A continuación, se muestran algunos porcentajes de ataques de años anteriores:

- El 78% de líderes de seguridad TI creen que sus organizaciones no tienen suficiente protección contra ciberataques a pesar de las inversiones en ciberseguridad realizadas en 2020.
- Más del 90 por ciento de todas las organizaciones de salud han reportado al menos una brecha de ciberseguridad en los últimos tres años.
- 43% de los ciberataques afectan a pequeños negocios.
- Las detecciones de malware y ransomware de endpoint superaron el volumen total observado en 2020 a fines del tercer trimestre de 2021, según los investigadores de WatchGuard Threat Lab.
- El 93% del malware observado el 2019 es polimórfico, puede modificar su programación para evitar ser detectado.
- A una compañía le toma aproximadamente 6 meses detectar una brecha de seguridad.
- Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar [1].

Actualmente, es fundamental tener buena seguridad en nuestra red para controlar quien accede a la información de una empresa, universidad o una red pequeña, por eso se requiere apoyo para evaluar la seguridad lógica, pero más adaptada a una organización o institución.

2.2 Aplicaciones similares

Hay algunas aplicaciones similares a SAIG, cada una con distintas variantes con propósito similar, para prevenir ataques y pérdida de datos confidenciales a continuación se describen las funcionalidades de algunas de estas aplicaciones.

2.2.1 Rio Bravo Systems

Especialistas en soluciones de ciberseguridad. Sus ingenieros “Red Team” son expertos en Vulnerability Assestment y Pruebas de Penetración para tu ambiente de TI [2].

Sus algunos servicios con los que cuenta son:

- Identificación y evaluación de brechas de seguridad
- Pruebas de explotación de vulnerabilidades
- Personal certificado Ethical Hacking
- Hackeo ético de caja blanca,caja gris o caja negra
- Pruebas en aplicaciones web, servidores, dispositivos finales o redes inalámbricas.
- Pruebas de ingeniería social
- Servicios para cumplimiento de controles ISO 27001
- Recomendaciones de remediación
- Entrega de análisis técnico y resumen ejecutivo

2.2.2 Sonar

Las vulnerabilidades de seguridad requieren una acción inmediata. Sonar proporciona descripciones detalladas de problemas y aspectos destacados del código que explican por qué

su código está en riesgo. Simplemente siga la guía, verifique una solución y asegure su aplicación [3].

2.2.3 Fortra

Fortra ofrece servicio de soporte orientado al cliente para darle una protección en cada paso del camino de la Ciberseguridad [4].

Cuenta con diferentes soluciones:

- Seguridad de la Información
- Clasificación de Datos
- Prevención de Pérdida de Datos (DLP)
- Transferencia Segura de Archivos (MFT)
- Encriptación
- Gestión de Identidades y Accesos

2.2.4 Ivanti

Gestiona las vulnerabilidades de su conjunto de aplicaciones con un enfoque basado en el riesgo. Ivanti Neurons for App Security Orchestration & Correlation (ASOC) ayuda a medir y controlar su verdadero riesgo de ciberseguridad para poder protegerse mejor contra el ransomware y otras amenazas cibernéticas [5].

Ivanti Neurons for ASOC correlaciona continuamente las aplicaciones de una organización con los datos de vulnerabilidad interna y externa, los conocimientos sobre amenazas, los resultados de las pruebas de penetración humana y la criticidad de los activos de la empresa para medir el riesgo, advertir de forma temprana sobre el emplazamiento de armas, predecir ataques y priorizar las actividades de reparación.

Sus características y funciones principales son:

- Motor de amenazas
- Clasificación de riesgo de vulnerabilidad (VRR)
- Alertas y notificaciones
- Paneles de control
- Filtros

Además, cuenta con las siguientes soluciones:

- Gestión de vulnerabilidades basada en el riesgo
- Gestión de parches
- Inteligencia de parches

A continuación, se muestra la tabla 1.1 en la cual se realiza la comparación en las aplicaciones antes mencionadas:

Tabla 1.1 comparación aplicaciones similares

Características	**Rio Bravo Systems**	**Sonar**	**Fortra**	**Ivanti**
• Enfocado a la ciberseguridad.	✓	✓	✓	✓
• Aplicación de paga	✓	✓	✓	✓
• Soluciones flexibles	✓	X	✓	X
• Clasificación de riesgos	✓	X	X	✓

CAPÍTULO 3. MARCO TEÓRICO

3.1 Metodología

La metodología para realizar este proyecto se basa en el desarrollo de un análisis, ejecución y modelado de una aplicación web que permitirá el análisis y evaluación de la seguridad lógica en una empresa y una institución, se considera realizar un análisis de los tipos de ataques cibernéticos, analizar los criterios, evaluar los sistemas informáticos por medio de la aplicación web. En la sección del desarrollo del sistema se muestran los resultados obtenidos en dicha

evaluación, la realización y modelado de una base de datos, el establecimiento de los cambios en la seguridad y, por último, el desarrollo de la aplicación web.

Se hará uso de metodologías sistemáticas, disciplinadas y cuantificables al desarrollo eficiente, operación y evolución de aplicaciones de alta calidad en la World Wide Web. En este sentido, la ingeniería Web hace referencia a las metodologías, técnicas y herramientas que se utilizan en el desarrollo de aplicaciones Web complejas y de grandes dimensiones. En esta tesis se utilizarán las siguientes fases basándose en la ingeniería web:

FASES

1)Fase de Análisis:

En esta etapa se definen los ataques cibernéticos, algunas propuestas de solución a vulnerabilidades con las que llegue a contar la empresa o institución, y también se describe el objetivo principal de la aplicación web, para obtener mayor conocimiento en el tema y para realizar dicho proyecto.

2)Fase de Planificación:

En esta etapa se planifican los tiempos de diseño, implementación y entrega. Para llevar un control de cada actividad a realizar y evitar contratiempos o errores. Así como también se plantea de qué manera se ira organizando la información para lograr un buen entendimiento sobre el tema en el que se basa este proyecto.

3)Fase de Formulación:

En esta etapa se realizan entregables de avance de diseños, esto a través de 3 módulos principales, cada uno de ellos tendrá submenús:

Seguridad Lógica, dividida en 4 submódulos: Control de Acceso, Control de Privilegios, Control de Uso y Control de Información.

Propuestas de Solución para Garantizar la Seguridad, se divide en 2 submódulos los cuales son: Evaluación y Pruebas de Seguridad

Informe Final de Seguridad Lógica que se divide en 4 submódulos los cuales son: Análisis, recomendación, crear Informe, e Imprimir Informe.

4)Fase de Modelado:

En esta etapa se trabaja con la estructura de la aplicación, casos de uso y diseño. Se hacen diseños de página y cómo ira escalando el usuario cuando esté dentro de la aplicación para que la navegación sea fácil.

5)Fase de Producción:

En esta etapa se integra la estructura de la base de datos resultante, la aplicación web y se realizan pruebas de las técnicas de mitigación de los diferentes tipos de ataques.

6)Fase de Test:

Esta es la última etapa del proyecto, en esta se realizan pruebas de navegación para correcciones en la interfaz y usabilidad de la aplicación web. Las pruebas se llevan a cabo por cada usuario con el que cuenta la aplicación para comprobar y observar que tan eficaz es la misma y con esto brindar una buena navegación al usuario y obtener el resultado esperado.

En la fig. 1 se muestran las fases que se llevaron acabo para este proyecto de tesis.

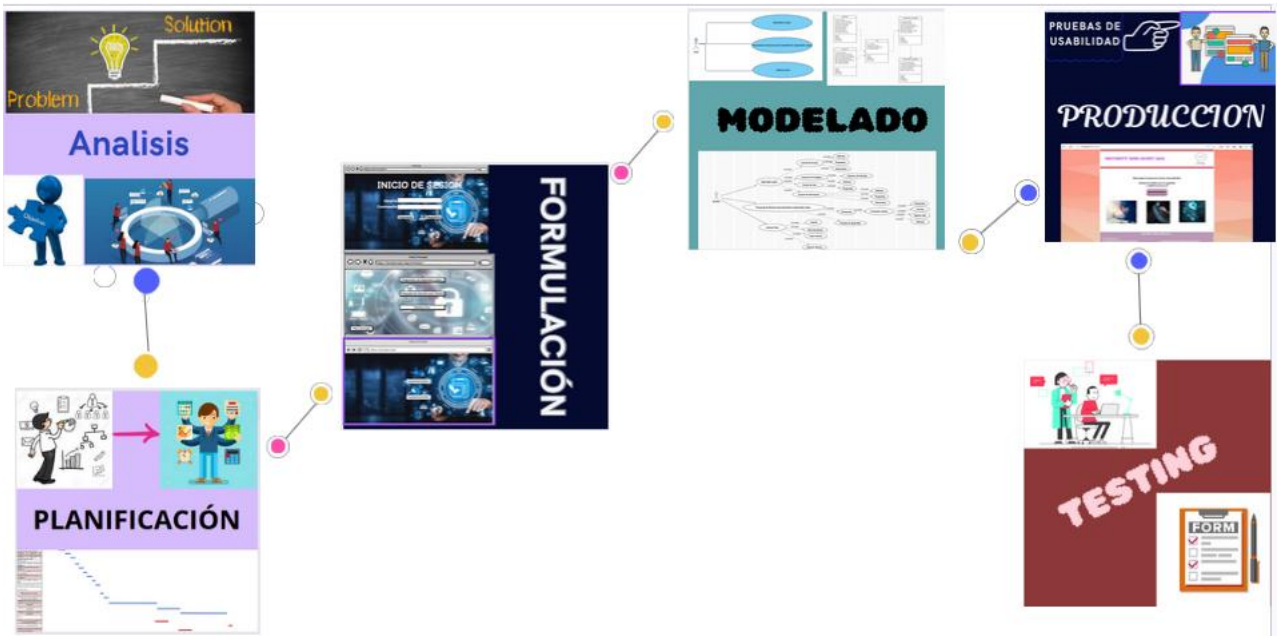


Fig. 1 diagrama de fases de la aplicación SAIG.

3.2 Aplicaciones web

Una aplicación web es un tipo de software que se codifica en un lenguaje que pueda ser soportado y ejecutado por los navegadores de Internet o por una intranet o red local [6].

Cada día es más común que empresas y negocios habiliten este tipo de soluciones informáticas ajustadas a los servicios que ofrecen y a los requerimientos de sus clientes.

Las aplicaciones web se ejecutan con un navegador web y no necesitan instalarse en tu PC o smartphone, ya que los datos o archivos utilizados se almacenan en una red o en la nube.

Las aplicaciones web se relacionan estrechamente con el almacenamiento de datos en la nube, ya que toda la información requerida está en servidores web, que además de alojar la información, la envían a nuestros dispositivos cuando es requerida.

Existen muchas empresas dedicadas a alquilar espacios en servidores web, lo que se conoce como servicio de Hosting; que se brinda a empresas para respaldar y almacenar toda la información que requieran y que puede ser consultada a través de aplicaciones, según los permisos otorgados.

Existen distintas tecnologías para el desarrollo de una aplicación, aunque las más comunes son:

- Para las bases de datos: SQL Server o MySQL
- Para la aplicación: NET (con diferentes lenguajes) o PHP
- El navegador suele recibir la información en HTML5 [6]

3.2.1 Antecedentes

Las primeras aplicaciones web eran simples páginas HTML estáticas que ofrecían información básica. A medida que la web avanzaba, surgieron las aplicaciones dinámicas con la introducción de lenguajes de programación como PHP y JavaScript. Esto permitió la creación de formularios interactivos y contenido que se actualizaba en tiempo real.

Con la llegada de la Web 2.0, las aplicaciones web se convirtieron en plataformas interactivas y sociales. Plataformas como MySpace y más tarde Facebook revolucionaron la forma en que las personas se conectaban en línea. Los usuarios podían compartir fotos, publicaciones y mantenerse en contacto con amigos y familiares en todo el mundo.[7]

3.2.2 Interfaz

Interfaz web es el nombre que se utiliza para referirse a la estructura diseñada en cualquier aplicación web y que le permite al usuario acceder a los contenidos de dicha web cuando esté navegando [8]. También se puede designar como interfaz de usuario o por sus siglas en inglés como GUI (graphical user interface). La interfaz utiliza un conjunto de componentes visuales (imagen o texto), interactivos (botones, casillas, cuadro de desplazamiento, controles) y de diseño para representar la información y acciones disponibles. Su principal uso consiste en proporcionar un entorno visual sencillo para permitir la comunicación con el sistema operativo de un ordenador o dispositivo móvil.

***Tipos de aplicaciones de una interfaz de usuario**

Navegador web:

Cuando el usuario visita la url del sitio web al que quiere acceder, éste se abre en un navegador que carga las instrucciones creadas en un lenguaje de programación lo que genera los elementos visuales de la página que permitirán al usuario interactuar con los contenidos de esta.

Móvil:

En la actualidad “mobile first” es la norma. Esto quiere decir que las interfaces se diseñan y se desarrollan pensando primero en el consumo de contenidos en el móvil. Hoy en España el 78% de las personas acceden a los contenidos digitales a través de su smartphone y tienen una media de 36 apps descargadas.

Software:

En este tipo de interfaces tienen como meta facilitar la experiencia del usuario para poder obtener un buen diseño.

***¿Qué criterios se deben considerar para hacer un buen diseño de interfaz de una web?**

Los criterios que se toman en cuenta para realizar una interfaz web con un buen diseño son: claridad, simpleza, flexibilidad y funcionalidad. Estos criterios se describen a continuación. [8]

Claridad:

Los elementos de diseño deben ser claros, estar distribuidos de forma clara y que su organización sea natural para el usuario. Algunos elementos básicos que suelen incluir la mayoría de las interfaces web son los menús de navegación, las ventanas, el contenido gráfico, el cursor, sonidos y en general, todos aquellos canales por los cuales se permite la comunicación entre el ser humano y la computadora.

Simpleza:

Se deben buscar referentes próximos al usuario para que pueda decodificarlos a simple vista. Elementos con los que esté familiarizado y le resulte cómodo relacionarse.

Flexibilidad:

Los componentes deben organizarse sí, pero ser flexibles para adaptarse a las experiencias de uso y situaciones que surjan durante la navegación sin perder la estructura clara.

Funcionalidad:

Nunca hay que perder de vista el objetivo con el que se esté diseñando la interfaz para crear y distribuir los diferentes elementos en vistas de la consecución de dicho objetivo.[8]

3.2.3 Estructura de las aplicaciones web

La arquitectura modular cliente-servidor de una aplicación web suele seguir un patrón de tres niveles o capas [9]:

1. Capa de presentación:

Está compuesta por componentes de interfaz de usuario como HTML, CSS y JavaScript que conforman la parte frontal de la aplicación.

2. Capa de negocio:

Esta capa consiste en la lógica de la aplicación, como scripts PHP, ASP.NET o Python, que definen cómo la aplicación maneja y procesa los datos en respuesta a las interacciones del usuario.

3. Capa de datos:

Esta capa contiene las bases de datos y otros almacenes de datos que guardan la información utilizada por la aplicación, como los usuarios, productos, pedidos, etc. [9]

3.2.4 Ventajas de la arquitectura de las aplicaciones web

1. Mejora del rendimiento:

Con la arquitectura adecuada, las aplicaciones web pueden ejecutarse de forma óptima y rápida, proporcionando a los usuarios una experiencia positiva.

2. Mayor seguridad:

Una arquitectura bien definida puede ayudar a garantizar que todos los componentes de la aplicación sean seguros y estén debidamente defendidos contra posibles ataques.

3. Escalabilidad:

La arquitectura debe estar diseñada para permiten una fácil escalabilidad, de modo que la aplicación puede crecer según sea necesario sin grandes cambios en su estructura.

4. Reutilización:

La arquitectura debe diseñarse de forma que los componentes y el código puedan reutilizarse en todos los proyectos. Esto facilita el mantenimiento y lo hace más eficiente.

5. Simplicidad:

Una arquitectura bien definida debe ser fácil de entender y utilizar, para facilitar a los desarrolladores el trabajo con el código.

6. Mantenimiento:

La arquitectura debe permitir un fácil mantenimiento, permitiendo a los desarrolladores realizar cambios rápida y fácilmente sin afectar a otras partes de la aplicación.

7. Eficacia:

Una arquitectura bien definida ayuda a garantizar que todos los componentes se utilizan de forma eficiente, sin código redundante o innecesario.

8. Automatización:

Una arquitectura bien definida puede ayudar a reducir el tiempo dedicado a tareas manuales y permitir a los desarrolladores centrarse más en mejorar la aplicación.[9]

3.2.4 Inconvenientes

- Habitualmente ofrecen **menos funcionalidades que las aplicaciones de escritorio**. Se debe a que las funcionalidades que se pueden realizar desde un navegador son más limitadas que las que se pueden realizar desde el sistema operativo.

- **La disponibilidad depende de un tercero**, el proveedor de la conexión a internet o el que provee el enlace entre el servidor de la aplicación y el cliente. Así que la disponibilidad del servicio está supeditada al proveedor. [9]

3.2.5 Ley de derecho al olvido

El concepto conocido como el "derecho al olvido", también referido con mayor precisión como el "derecho a la supresión", hace mención a la capacidad de requerir a plataformas de búsqueda comerciales u otros sitios web que recolectan datos personales con objetivos comerciales, como Google, que eliminen los vínculos que conducen a información privada bajo solicitud, siguiendo

criterios específicos. Este derecho encuentra su base en el principio reconocido a individuos por diversas leyes de protección de datos, las cuales establecen que la información personal almacenada sobre un individuo debe ser borrada si resulta inadecuada, irrelevante, ya no es pertinente o es excesiva con respecto a los propósitos originales para los cuales fue recopilada.

3.2.6 Historia de derecho al olvido

En 2013, María Verónica Martínez Espinosa, Senadora de la LXII Legislatura del Congreso de la Unión, propuso una iniciativa para modificar la Ley Federal de Protección de Datos Personales en Posesión de Particulares, con el fin de garantizar el derecho al olvido digital. Esto se basa en la protección constitucional del derecho a la privacidad y la intimidad, así como en el reconocimiento de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en la legislación mexicana. Estos derechos permiten a las personas controlar la información personal que está en posesión de terceros.[10]

3.3 Software de la aplicación

Existen distintos softwares para la realización de páginas web, a continuación, se describe el software utilizado para la realización de SAIG y la manera en trabaja:

3.3.1 Servlets

Los Servlets son clases Java que dinámicamente procesan peticiones y mandan respuestas. Las JSPs son documentos de texto que se ejecutan como Servlets pero que permiten una mayor aproximación a la creación de contenido estático. Aunque se pueden intercambiar, cada uno tiene sus virtudes. Los Servlets encajan mejor para las aplicaciones orientadas a servicio (los puntos finales de servicio se implementan como Servlets) y las funciones de control de una aplicación orientada a presentación, como el envío de peticiones y el tratamiento de datos que no son de texto. Las JSPs son más apropiadas para generar marcas de texto como HTML, y XML [11].

Finalidad y ventajas

La funcionalidad de los Servlets se resume en lo siguiente:

- Leer los datos enviados por el cliente.
- Extraer cualquier información útil incluida en la cabecera HTTP o en el cuerpo del mensaje de petición enviado por el cliente.
- Generar dinámicamente resultados.
- Formatear los resultados en un documento HTML.
- Establecer los parámetros HTTP adecuados incluidos en la cabecera de la respuesta (por ejemplo: el tipo de documento, cookies, etc.)
- Enviar el documento final al cliente.

3.3.2 Java Script

JavaScript es un lenguaje de alto nivel, dinámico e interpretado. Se define como orientado a objetos, basado en prototipos, imperativo y débilmente tipado. Junto al *HTML* y a *CSS*, es una de las tres tecnologías esenciales en la producción mundial webs: la mayoría de los sitios web la emplean y es compatible con todos los navegadores modernos sin necesidad de *plug-ins*. JavaScript posee una API para trabajar con texto, arrays, fechas y expresiones regulares.

A pesar de algunos nombres y similitudes en la biblioteca estándar, JavaScript y Java no poseen ninguna relación y tienen semánticas muy diferentes. La sintaxis de JavaScript en realidad se deriva de C, mientras que su semántica y el diseño están influenciados por los lenguajes de programación *Self* y *Scheme*.

El uso de JavaScript

JavaScript también se utiliza en entornos que no se basan en web, tales como documentos PDF, navegadores específicos del sitio y widgets de escritorio [12]. Máquinas virtuales de JavaScript (*VMs*) mucho más nuevas y rápidas, así como plataformas construidas sobre este lenguaje, han aumentado la popularidad de JavaScript para aplicaciones web. Por parte del cliente, JavaScript se ha aplicado tradicionalmente como un lenguaje interpretado, pero los navegadores más recientes pueden realizar la compilación al momento.

También se utiliza en el desarrollo de videojuegos, en la creación de aplicaciones de escritorio y móviles y en la programación de servidores con entornos de ejecución como *Node.js*. Para interactuar con una página web se provee al lenguaje JavaScript de una implementación del *Document Object Model (DOM)*.

Normalmente se utilizaba JavaScript en las páginas web HTML para realizar operaciones y solo en el marco de la aplicación cliente, sin acceso a funciones del servidor. Ahora se usa para enviar y recibir información del servidor junto con otras tecnologías como AJAX. JavaScript se interpreta en el agente de usuario mientras las sentencias se descargan junto con el código HTML [12].

3.4 Bases de datos

Una base de datos se define como una colección organizada de datos o información estructurada, generalmente almacenada electrónicamente en un sistema informático y típicamente gestionada por un sistema de gestión de bases de datos (DBMS). Este conjunto de datos, junto con el DBMS y las aplicaciones asociadas, constituyen lo que comúnmente se conoce como sistema de bases de datos.

Hoy las bases de datos más utilizadas suelen adoptar un formato de tablas compuestas por filas y columnas, lo que facilita la eficiencia en el procesamiento y consulta de datos. Esta estructura permite acceder, administrar, modificar, actualizar, controlar y organizar los datos de manera efectiva. En la mayoría de los casos, se emplea un lenguaje de consulta estructurada (SQL) para escribir y consultar datos en estas bases de datos.

3.4.1 Tipos de Bases de Datos

Existen una variedad de tipos de bases de datos, y la elección de la más adecuada para una organización depende de cómo se planea utilizar los datos [13].

- **Bases de datos relacionales**: Organizadas en tablas con columnas y filas, estas bases de datos ofrecen eficiencia y flexibilidad en el acceso a la información estructurada.
- **Bases de datos orientadas a objetos**: Representan la información como objetos, similar a la programación orientada a objetos.

- **Bases de datos distribuidas**: Compuestas por múltiples archivos ubicados en diferentes sitios, pueden estar almacenadas en varios ordenadores o distribuidas en diferentes redes.
- **Almacenes de datos**: Son repositorios centrales diseñados para consultas y análisis rápidos.
- **Bases de datos NoSQL**: Permiten almacenar y manipular datos no estructurados o semiestructurados, ganando popularidad con la creciente complejidad de las aplicaciones web.
- **Bases de datos orientadas a grafos**: Almacenan datos relacionales entre entidades y sus relaciones.
- **Bases de datos OLTP**: Son rápidas y analíticas, diseñadas para múltiples usuarios y transacciones.

Además de estos, hay otros tipos menos comunes adaptados a funciones específicas. Además, los avances tecnológicos como la nube y la automatización están dando lugar a nuevas direcciones en las bases de datos. Algunas de las más recientes incluyen:

- **Bases de datos de código abierto**: Su código fuente es accesible y pueden ser de tipo SQL o NoSQL.
- **Bases de datos en la nube**: Residen en plataformas de computación en la nube, con modelos tradicionales o como servicios gestionados.
- **Base de datos multimodelo**: Integran diferentes modelos de bases de datos en un solo servidor.
- **Bases de datos de documentos/JSON**: Almacenan datos en formato JSON, orientadas a documentos.
- **Bases de datos de autogestión**: Utilizan machine learning para automatizar tareas de gestión como ajustes, seguridad y copias de seguridad.

3.4.2 Software que se utilizó para la base de datos

Una base de datos es parte fundamental de una base de datos, como se mostro en el punto de arriba existen distintos tipos de bases de datos y es importante identificar que el tipo de base que utiliza la aplicación web SAIG. A continuación, se explica que tipo de base de datos se utiliza y el por qué:

La base de datos utilizada para la realización de la aplicación fue una base de datos relacional. El motivo por el que se usó dicha base de datos es porque el software XAMPP trabaja con MySQL, un sistema de gestión de bases de datos. Este software fue factible, ya que al ser una base de datos relacional como se decía en el punto anterior, cuenta con tablas formadas por columnas y filas que permiten llevar un buen manejo y control de la información manejada en la aplicación como: usuarios, preguntas, respuestas, etc.

Por eso este tipo de base de datos, como el software, fueron útiles y prácticos para desarrollar la aplicación web.

3.5 Seguridad Lógica

Se conoce seguridad lógica como la manera de aplicar procedimientos que aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo [14].

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos

2. Los operadores deben trabajar sin supervisión minuciosa y no podrán modificar ni programas archivos que no correspondan.

3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

4. Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido dirigida y por ningún otro.

5. Asegurar que la información que el destinatario ha recibido sea la misma que ha sido transmitida.

6. Se debe disponer de sistemas alternativos de transmisión de información entre diferentes puntos.

3.5.1 Control de accesos

El control de acceso es un elemento esencial de seguridad que determina quién puede acceder a ciertos datos, aplicaciones y recursos, y en qué circunstancias. De la misma forma que las claves y listas de invitados con aprobación previa protegen los espacios físicos, las directivas de control de acceso protegen los espacios digitales. En otras palabras, permiten a las personas adecuadas entrar y mantener a las personas equivocadas fuera. Las directivas de control de acceso se basan en gran medida en técnicas como autenticación y autorización, que permiten a las organizaciones comprobar explícitamente que los usuarios son quienes dicen ser y que a estos usuarios se les concede el nivel adecuado de acceso en función del contexto, como el dispositivo, la ubicación, el rol y mucho más.

El control de acceso evita que la información confidencial, como los datos de los clientes y la propiedad intelectual, sea robada por delincuentes u otros usuarios no autorizados. También reduce el riesgo de filtrado de datos por parte de los empleados y mantiene a raya las amenazas web. En lugar de gestionar los permisos manualmente, la mayoría de las organizaciones impulsadas por la seguridad recurren a soluciones de gestión de identidades y accesos para implementar directivas de control de acceso.

- **Objetivo del control de acceso**

El objetivo del control de acceso es evitar que la información confidencial entre en manos de actores malintencionados. Los Información sobre ciberataques ca datos confidenciales pueden tener consecuencias graves, incluidas fugas de propiedad intelectual, exposición de información personal de clientes y empleados e incluso pérdida de fondos corporativos.

El control de acceso es un componente fundamental de la estrategia de seguridad. También es una de las mejores herramientas para las organizaciones que desean minimizar el riesgo de seguridad del acceso no autorizado a sus datos, en particular a los datos almacenados en la nube.

Conforme crece la lista de dispositivos susceptibles al acceso no autorizado, también lo hace el riesgo en organizaciones sin directivas de control de acceso sofisticadas. Las soluciones de

administración de identidad y acceso pueden simplificar la administración de estas directivas, sin embargo, el primer paso consiste en reconocer la necesidad de gobernar cómo y cuándo se accede a los datos [15]. A continuación, se muestran dos preguntas propuestas para el análisis:

- ¿Se restringe el número de accesos de intentos fallidos para la autenticación del sistema?
- ¿Se realizan revisiones periódicas de los controles de accesos a los datos?

3.5.2 Control de accesos de Software

- Llevar un registro actualizado de licencias, que cuente con datos como nombre y versión del producto, autor, fecha de adquisición, vigencia de la licencia, número de usuarios permitidos por licencia, etc.
- Identificar quién tiene la competencia para la instalación, actualización y borrado del software. De esta forma nos aseguraremos de que únicamente el personal autorizado podrá ejecutar este tipo de acciones. Si no dispone de esta figura o es personal externo quien ejerza estas acciones, se documentará y notificará la autorización y operativa.
- Documentar y dar a conocer las sanciones disciplinarias derivadas del uso de software ilegal no autorizado, así como las responsabilidades civiles y penales según la legislación vigente en materia de protección de propiedad intelectual. La medida pretende concienciar de las consecuencias del uso de software ilegal.
- Contar con un repositorio de software. De esta manera, si se quiere instalar un determinado programa de forma rápida y eficiente, se establecerá una ubicación donde localizarlo, así como claves de activación, números de serie, licencias, etc.

- Realizar auditorías del software instalado en cualquier momento y en cualquier equipo para verificar que se cumple con las políticas establecidas.
- Comprobar tanto las autorizaciones como las licencias. Será necesario garantizar que los programas instalados (incluidos los dispositivos BYOD), estén debidamente autorizados y que cuenten con las licencias necesarias.

- No permitir que se realicen copias del software disponible sin el debido consentimiento [16].

3.5.3 Control de accesos de Programas

El administrador del equipo puede configurar las aplicaciones a las que puede acceder cada uno de los usuarios del PC, consiguiendo que ningún usuario con cuenta activa en el ordenador pueda ejecutar programas para los que no está autorizado.

3.5.4 Control de accesos de Información

La norma ISO/IEC 27001 establece los requisitos para poner en marcha, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SG-SI). El objetivo fundamental es ayudar a las compañías a preservar su confidencialidad e integridad, así como la disponibilidad de la información y los activos relacionados con ella.

La norma ISO 27001:2022 proporciona un marco que permite la gestión de los riesgos de seguridad de la información. Ayuda a todas las empresas a identificar y evaluar los posibles riesgos sobre la seguridad de la información. También permite implementar controles y medidas de seguridad necesarias para su mitigación y gestión de manera efectiva.

Además, la ISO 27001 mejora la confianza de los stakeholders, como clientes, socios comerciales y reguladores, al demostrar el compromiso de la empresa con la seguridad de la información. Con la certificación ISO/IEC 27001:2022, las empresas demuestran su cumplimiento con los estándares internacionales en materia de seguridad de la información, ayudándoles a diferenciarse en el mercado y así mejorar su reputación [17]. A continuación, se muestran dos preguntas para agregar al área de análisis:

- ¿Las copias de seguridad que contienen información confidencial son protegidas por mecanismos de cifrado?

3.5.5 Control de Privilegios

El **acceso privilegiado** es la puerta de entrada a los activos más valiosos de una organización y es el núcleo de casi todas las violaciones importantes de datos. Una de las formas más rápidas y efectivas para reducir el riesgo en tu fuerza de trabajo remota es **priorizar la gestión del acceso privilegiado** (PAM).

Para muchos empleados, cuando se mudaron de la oficina a trabajar fuera en sus hogares, los privilegios cambiaron para permitirles trabajar de manera más independiente o manejar nuevas tareas. Sin un plan sólido para la administración de acceso privilegiado en tiempos de crisis, es muy fácil que estos nuevos privilegios se conviertan en nuevas vulnerabilidades para las empresas.

En una época de cambios sin precedentes en la forma en que trabajamos, la incertidumbre económica global y las implacables ciber amenazas, hacen que la gestión del acceso privilegiado sea hoy más importante que nunca [18]. A continuación, se coloca una pregunta, pensada para añadirla como parte del análisis:

- ¿Se eliminan los derechos de acceso al sistema cuando los usuarios finalizan su actividad en la empresa?

3.5.6 Control de Información

Toda actividad de procesamiento de información no autorizada debe ser detectada. Todos los sistemas con los que cuenta el centro de datos deben ser monitoreados por sus respectivos administradores, con un registro de los usuarios y las operaciones realizadas en el sistema, para asegurar la identificación de los problemas.

Esta tesis pretende solucionar y mejorar la seguridad lógica, ya que, como se mostró antes, es un problema común hoy para el que se deben buscar soluciones. Es por esta razón que se realizará una aplicación web en la cual hará un diagnóstico de si se llevan a cabo las normas para tener una buena seguridad y poder dar recomendaciones de qué aspectos podrían cambiar, así como también se mostrará de qué manera pueden protegerse de ataques y perdida de información logrando así mejorar la seguridad lógica. Esta aplicación se basará en preguntas

con las cuales se ira haciendo el diagnóstico para que al final se muestre el informe final. A continuación, se en listan ejemplos de preguntas:

- ¿Los usuarios tienen acceso únicamente a los recursos que necesitan para desempegar su labor?

3.6 Evaluación de Amenazas Lógicas

La evaluación de amenazas es una parte fundamental para cualquier empresa o institución ya que se maneja información de suma importancia, por esto es necesario realizar evaluaciones periódicamente para evitar cualquier tipo de ataque cibernético. A continuación, se describe que es la seguridad informática, así como los tipos de amenazas lógicas. A continuación, se colocan dos preguntas pensadas para el análisis de esta sección:

- ¿Se utilizan antivirus para prevenir, detectar y eliminar malware?
- ¿Se realizan pruebas para verificar que los mecanismos de seguridad funcionan de manera correcta?

3.6.1 Seguridad informática

La seguridad informática es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado [19].

La seguridad informática debe cumplir con ciertas características para que sea eficiente. Estas son:

Confidencialidad: Las acciones de seguridad informativas están orientadas a proteger la confidencialidad, es decir, la información de acceso no autorizado y garantizar que solo las personas adecuadas tengan acceso a ella.

Integridad: Esta característica es la capacidad de mantener la precisión y la integridad de los datos, garantizando que no se alteren o manipulen sin autorización. Algo fundamental en esta época en la que se maneja una enorme cantidad de datos.

Disponibilidad: Las medidas de seguridad informática deben garantizar que los sistemas y la información estén disponibles para su uso en todo momento, y que cualquier interrupción en la disponibilidad sea mitigada y resuelta rápidamente.

Autenticidad: Parte fundamental de la labor de la seguridad informática es corroborar la identidad de un usuario o recurso, así que protegerá que dicha identidad no se falsifique.

Resiliencia: Por seguridad informática, una organización podrá recuperarse rápidamente de cualquier interrupción o ataque de seguridad, ya que es crucial para las empresas ser resilientes informáticos.

Seguridad en capas: Se refiere a la implementación de múltiples medidas de seguridad en diferentes niveles, para garantizar una mayor protección contra posibles amenazas.

Actualización constante: La seguridad informática es un campo en constante evolución, por lo que hay que actualizar y mejorar las medidas de seguridad para protegerse de nuevas amenazas.

3.6.2 Amenazas a la seguridad informática

Amenazas humanas

Las amenazas humanas pueden ser pasivas o activas. Los ataques pasivos buscan tener información, pero sin que esta sea modificada, de este modo son complicados de detectar. Se producen por usuarios con conocimientos simples que usan herramientas sencillas, o por usuarios con grandes conocimientos que atacan un sistema para ver sus puntos débiles y así poder corregirlos. Los ataques activos buscan perjudicar a la persona por simple gusto o para lograr un beneficio. Se pueden producir por los llamados crackers, que son grandes informáticos que buscan dañar un sistema con el fin de robar información y así obtener dinero u otras cosas [20].

3.6.3 Amenazas lógicas de programas.

1. SOFTWARE INCORRECTO: Defectos de instalación o programación Eliminación o sustitución de bibliotecas comunes a más de un programa o del sistema (DLL Hell). Reiniciar arbitrariamente la sesión de un usuario para que la instalación tenga efecto. Presuponer que el usuario tiene una conexión permanente a internet.
2. HERRAMIENTAS DE SEGURIDAD: El mal uso de estas herramientas puede concluir en situaciones de bloqueo, enlentecimiento e incluso denegación de servicio de las máquinas analizadas. Solo deben lanzarse contra máquinas ajenas únicas y solo cuando sus responsables nos hayan autorizado. En ningún caso deben emplearse contra máquinas ajenas a nuestra propiedad sin consentimiento de sus propietarios, informando de la actividad que vayamos a realizar.
3. PUERTAS TRASERAS: Lo peor que puede pasarle cuando está en el messanger o en el ICQ no es que contraiga su PC un virus informático. Lo peor es que alguien instale un backdoor en su PC. Las puertas traseras son fáciles de entender. Como todo en Internet se basa en la arquitectura cliente / servidor, sólo se necesita instalar un programa servidor en una máquina para poder controlarla a distancia desde otro equipo, si se cuenta con el cliente adecuado, ésta puede bien ser la computadora de un usuario descuidado o poco informado.
4. BOMBAS LÓGICAS: Ejemplos de acciones que puede realizar una bomba lógica: Borrar información del disco duro, Mostrar un mensaje, Reproducir una canción Enviar un correo electrónico, Apagar el Monitor provoca alucinaciones.
5. CANALES CUBIERTOS: Ruido Como cualquier canal de comunicación, oculto o no, los canales cubiertos pueden ser ruidosos o inmunes al ruido; idealmente, un canal inmune al ruido es aquél en que la probabilidad de que el receptor escuche exactamente lo que el emisor ha transmitido es 1: sin importar factores externos, no hay interferencias en la transmisión. Evidentemente, en la práctica es muy difícil conseguir estos canales tan perfectos, por lo que es habitual aplicar códigos de corrección de errores, aunque éstos reduzcan el ancho de banda del canal. Flujos de información De la misma forma que en las líneas convencionales de transmisión de datos se aplican técnicas (multiplexación en el tiempo, multiplexación en frecuencia...) para maximizar el ancho de banda efectivo, en los canales cubiertos se puede hacer algo parecido. A los canales en los que se transmiten varios flujos de información entre emisor y receptor se les denomina agregados, y

dependiendo de cómo se inicialicen, lean y reinicien las variables enviadas podemos hablar de agregación serie, paralela o híbrida; los canales con un único flujo de información se llaman no agregados.

6. VIRUS Amenazas: Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas. Ralentizar o bloquear el ordenador. Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo. Reducir el espacio en el disco. Molestar al usuario cerrando ventanas, moviendo el ratón...
7. GUSANOS: Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (a otras terminales en la red) y pueden llevarlo a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en métodos como SMTP, IRC, P2P, entre otros.
8. CABALLOS DE TROYA: Evitar la infección de un troyano es difícil, algunas de las formas más comunes de infectarse son: Descarga de programas de redes p2p y sitios web que no son de confianza. Páginas web que contienen contenido ejecutable (por ejemplo, controles ActiveX o aplicaciones Java). Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea). Ingeniería social (por ejemplo, un cracker manda directamente el troyano a la víctima a través de la mensajería instantánea). Archivos adjuntos en correos electrónicos y archivos enviados por mensajería instantánea.
9. PROGRAMA CONEJO O BACTERIA: Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina. Hemos de pensar hay ciertos programas que pueden actuar como conejos sin proponérselo; ejemplos típicos se suelen encontrar en los sistemas Unix destinados a prácticas en las que se enseña a programar al alumnado: es muy común que un bucle que por error se convierte en infinito contenga entre sus instrucciones algunas de reserva de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas para procesos de usuario pueda venirse abajo o degradar enormemente sus prestaciones.
10. TÉCNICAS SALAMI: El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesetas se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar una peseta de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad

de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima [21].

3.6.4 Amenazas Lógicas de Correos

Actualmente existen muchos tipos de amenazas al correo electrónico corporativo, entre las que podemos destacar:

- **Phishing:** ataques de phishing implican correos electrónicos fraudulentos que intentan engañar a los usuarios para que revelen información personal, como contraseñas o datos de tarjetas de crédito.
- **Ataques de pretexto (Pretexting):** en este tipo de ataque, los atacantes crean un escenario (o pretexto) para obtener la información de acceso de un usuario.
- **Malware:** los correos electrónicos pueden contener archivos adjuntos o enlaces que, cuando se abren, instalan un software malicioso en el dispositivo de la víctima.
- Ransomware: es un tipo específico de malware que cifra los datos del usuario y exige un rescate para descifrarlos.
- **Trojans:** disfrazado de software legítimo, los trojans proporcionan a los atacantes acceso no autorizado a un dispositivo comprometido.
- **Spam:** además de ser molestos y no solicitados, los correos electrónicos de spam pueden tener enlaces maliciosos, anexos infectados o intentos de phishing.
- **Ataques de ingeniería social:** normalmente, estos ataques utilizan la manipulación psicológica para convencer a los usuarios a realizar acciones específicas o revelar información confidencial [22].

3.6.5 Amenazas Lógicas de Páginas Web

- **Amenazas en redes privadas:** afectan a las subredes conectadas a una Internet global más amplia. Los ejemplos típicos pueden incluir redes Ethernet o Wi-Fi domésticas y redes internas corporativas o nacionales.
- **Amenazas en el host:** afectan dispositivos host de redes específicas. El término host hace referencia a endpoints corporativos y dispositivos personales, como teléfonos móviles, tablets y computadoras tradicionales.

- **Amenazas en servidores web:** afectan hardware y software específicos que admiten servicios e infraestructuras web.
- **Denegación de accesos:** se impide el acceso a una computadora o a un servicio de red.
- **Adquisición de accesos:** entrada no autorizada o no deseada a una computadora o un servicio de red privado.
- Uso no autorizado o no deseado de una computadora o un servicio de red.
- **Exposición de datos privados** sin consentimiento, como fotos, credenciales de cuentas e información confidencial de gobiernos [23].

3.6.6 Amenazas Lógicas de Software

Bugs o errores de programación: software mal diseñado que, por error, ocasiona un agujero de seguridad que puede acabar provocando los mismos riesgos que el malware [24].

Rootkit: En Windows es un programa que oculta ciertos elementos (archivos, procesos, entradas en el Registro de Windows, direcciones de memoria, conexiones de red, etc.) de otros programas o del sistema operativo [25].

3.7 Pruebas de Seguridad

Las aplicaciones web están expuestas a muchas amenazas, como el mal uso de los usuarios, ataques de seguridad, mala calidad del software o falta de desarrollo estructurado. Para evitar que estos ataques se aprovechen de las vulnerabilidades común es al software y causen un daño, es necesario que desde el principio en el ciclo de desarrollo se tomen medidas para disminuir el impacto, lo cual comienza desde la fase de levantamiento de requerimientos hasta la de entrega y soporte al cliente, pasando por las pruebas funcionales. Las empresas deben adoptar un modelo para estandarizar e implementar un proceso basado en el ciclo de desarrollo del software, que permita acompañar en cada fase y brinde la calidad y seguridad requeridas.

En la aplicación web SAIG se considera la ley del derecho al olvido, por lo que se agrega un botón que sirve para ello, como se muestra en la fig. 2, el usuario al acceder al botón puede eliminar su información sensible almacenada en la base de datos de la aplicación.

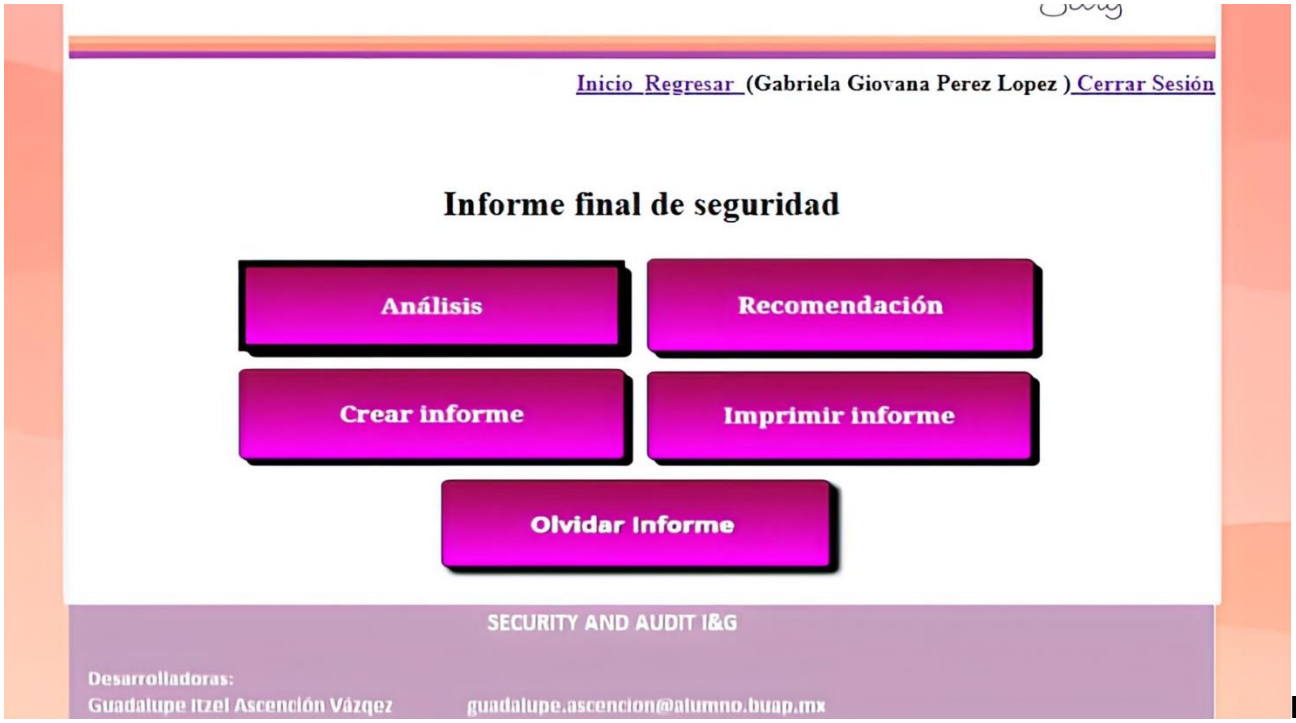


Fig. 2 Botón de olvidar informe el cual elimina todos los datos de cualquier organización que utilice la aplicación

3.7.1 Pruebas de software

Las pruebas de sistemas son un tipo de pruebas de software que siempre se realizan en un sistema completo. Comprueba si el sistema cumple sus requisitos, sean cuales sean. Los probadores realizan pruebas de sistemas para evaluar los requisitos funcionales y no funcionales del sistema una vez que se han integrado los módulos y componentes individuales. Las pruebas del sistema son una categoría de las pruebas de caja negra, lo que significa que sólo comprueban las características externas de funcionamiento del software, en lugar de probar el diseño interno de la aplicación. Los encargados de las pruebas no necesitan conocer la programación ni la estructura del código del software para evaluar por completo una compilación de software durante las pruebas del sistema. En cambio, los probadores se limitan a evaluar el rendimiento del software desde la perspectiva de un usuario [26].

3.7.2 Tipos de pruebas de sistemas

Hay más de 50 tipos de pruebas del sistema que se consideran si se desea comprobar cómo funciona la compilación de un software. En la práctica, la mayoría de los equipos de pruebas solo usan algunos tipos de pruebas de sistemas. El tipo de prueba del sistema que se utiliza en este proyecto depende de muchos factores, como el presupuesto, las limitaciones de tiempo, las prioridades y los recursos [27].

Tipo de prueba	Definición
Pruebas por exploración	Las pruebas exploratorias combinan diseño y ejecución, permitiendo libertad al probador y una optimización constante del trabajo. Son similares a las pruebas ad hoc pero con una documentación más rigurosa y un proceso de aprendizaje activo. Son útiles para detectar fallos como lo harían los usuarios, ya que estos suelen encontrar problemas de forma accidental, lo que las pruebas programadas no pueden detectar [28].
Pruebas por conjetura de fallos	Se encargan de enumerar una lista de errores posibles o de situaciones propensas a tener errores y con ello crean casos de prueba basados en esas situaciones [29].
Pruebas de integración	Las pruebas de integración evalúan la compatibilidad entre los diferentes módulos o servicios de una aplicación. Esto

	implica verificar la interacción con la base de datos y la correcta funcionalidad de los microservicios en conjunto [30].
Pruebas unitarias	Las pruebas unitarias se realizan a un nivel muy bajo, cerca del código fuente de la aplicación, evaluando métodos y funciones individuales de clases, componentes o módulos. Son económicas de automatizar y pueden ejecutarse rápidamente mediante un servidor de integración continua [30].
Pruebas funcionales	Las pruebas funcionales se enfocan en los requisitos empresariales de una aplicación, verificando solo el resultado de una acción sin considerar los estados intermedios [30].
Pruebas de rendimiento	Las pruebas de rendimiento evalúan cómo un sistema responde bajo una carga específica, midiendo su fiabilidad, velocidad, escalabilidad y capacidad de respuesta. Ayudan a determinar si una aplicación cumple con los requisitos de rendimiento, identificar cuellos de botella y medir la estabilidad durante picos de tráfico, entre otras funciones [30].
Pruebas de regresión	Las pruebas de regresión detectan errores y aseguran la estabilidad de la aplicación al evaluar el impacto de nuevas características en el código existente [31].
Pruebas de estrés	Las pruebas de estrés del software son fundamentales para identificar vulnerabilidades, puntos débiles y fallos potenciales bajo condiciones de alta carga o adversas [32].
Pruebas de usabilidad	Las pruebas de usabilidad son un tipo de pruebas de sistemas que consisten en comprobar la usabilidad de la aplicación. Esto significa que los probadores valoran y evalúan la facilidad de navegación y uso de la aplicación, lo intuitivas que son sus funciones y si hay fallos o problemas que puedan causar problemas de usabilidad [27].
Pruebas de extremo a extremo	Las pruebas integrales replican el comportamiento de un usuario con el software en un entorno de aplicación completo. Además, verifican que diversos flujos de usuario funcionen según lo previsto, y pueden ser tan sencillos como cargar una página web o iniciar sesión, o mucho más complejos, como

	la verificación de notificaciones de correo electrónico, pagos en línea, etc. [30] .
Pruebas de humo	Las pruebas de humo son pruebas básicas que verifican el funcionamiento esencial de una aplicación. Son rápidas de ejecutar y garantizan que las funciones principales del sistema operen correctamente [30].

CAPÍTULO 4. DISEÑO Y DESARROLLO DEL SISTEMA

4.1 Análisis y requerimientos de la aplicación web

La sección pretende mostrar el proceso del diseño para la solución practica con la aplicación web de la seguridad lógica.

Se describen las necesidades funcionales y no funcionales, el diagrama de casos de uso extendido, especificaciones de casos de uso, diagrama de clases y diagramas de secuencia.

Tabla 1 Requerimientos funcionales de la aplicación web

NoReq.	Tipo de Requerimiento	Nombre del requerimiento	Descripción
RF1	Requerimiento funcional del sistema	Inicio de sesión	El sistema cotara con un servicio de inicio de sesión con seguridad de los datos proporcionados por el usuario
RF2	Requerimiento funcional del sistema	Gestión de usuarios	El sistema contara con un menú para llevar el control de usuarios, cuenta con alta, bajas, modificaciones y consultas
RF3	Requerimiento funcional del sistema	Gestión de empresa	Ahora el sistema tiene un segundo menú para controlar las empresas que usaran esa aplicación contando con las opciones de altas, bajas, modificaciones y consultas.
RF4	Requerimiento funcional del sistema	Gestión de test	El sistema contara con un menú para gestionar las preguntas y respuestas en donde se podrán realizar altas, bajas, modificaciones y consultas de estas.

4.1.1 Requerimientos no funcionales del sistema

Tabla 2 Requerimientos no funcionales de la aplicación web

NoReq.	Tipo de Requerimiento	Descripción
RNF1	Requerimiento no funcional del sistema	La aplicación estará disponible 24/7 mientras se tenga conectividad para poder hacer uso del servidor.
RNF2	Requerimiento no funcional de seguridad	El sistema contara con una encriptación de datos para garantizar la privacidad de la información del usuario.
RNF3	Requerimiento funcional de usabilidad	La aplicación tendrá un diseño responsivo para adaptarse a pc de escritorio y de laptops.

RNF4	Requerimiento no funcional de usabilidad	El diseño de la aplicación será fácil de usar, ya que será intuitivo para que el usuario logre analizara eficazmente sin complicaciones de uso de la aplicación.
RNF5	Requerimiento funcional de fallas	El sistema tendrá soluciones inmediatas si alguna falla pudiera presentarse imprevistamente.

4.1.2 Modelado del sistema

En este apartado se muestra el modelado de la aplicación web Security and Audit A&G (SAIG), en este proyecto de tesis solo se muestra el modelado del botón de Seguridad Lógica ya que es la parte que se desarrollo para este proyecto.

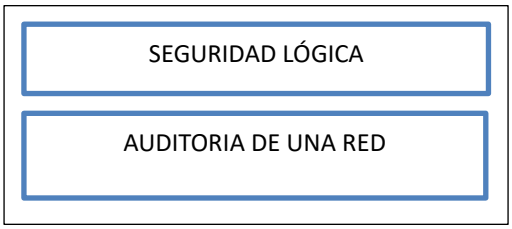


Fig. 3 Menú Principal de la aplicación SAIG

La opción de seguridad lógica cuenta con tres opciones: Seguridad lógica, Propuesta de solución para garantiza la seguridad lógica e importe final. En la fig. 4 se muestra dichas opciones del menú principal.

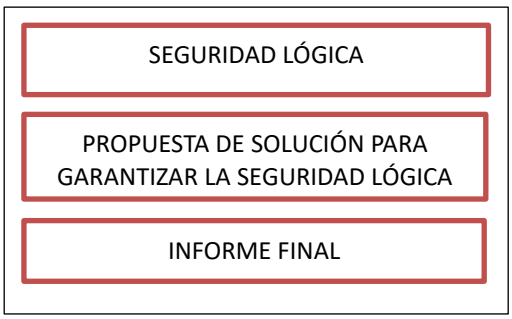


Fig. 4 Menú Principal de Seguridad Lógica

Este apartado se presenta el modelo de la aplicación iniciando por el diagrama de casos de uso; la fig. 5 muestra el caso de uso principal, donde se puede observar que el usuario puede acceder a las siguientes opciones:

- CASO DE USO 1: Seguridad Lógica
- CASO DE USO 2: Propuesta de Solución para Garantizar la Seguridad Lógica
- CASO DE USO 3: Informe final

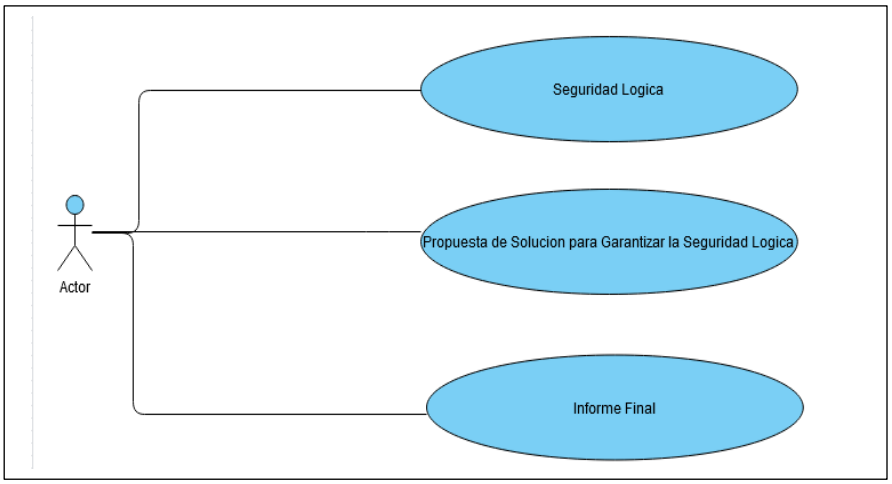


Fig. 5 Caso de uso de Menú Principal del sistema

Con objetivo de dar una visión completa de la aplicación la fig. 6 muestra el uso extendido del sistema, en el que se pueden observar todos los submenús y opciones con las que se puede interactuar.

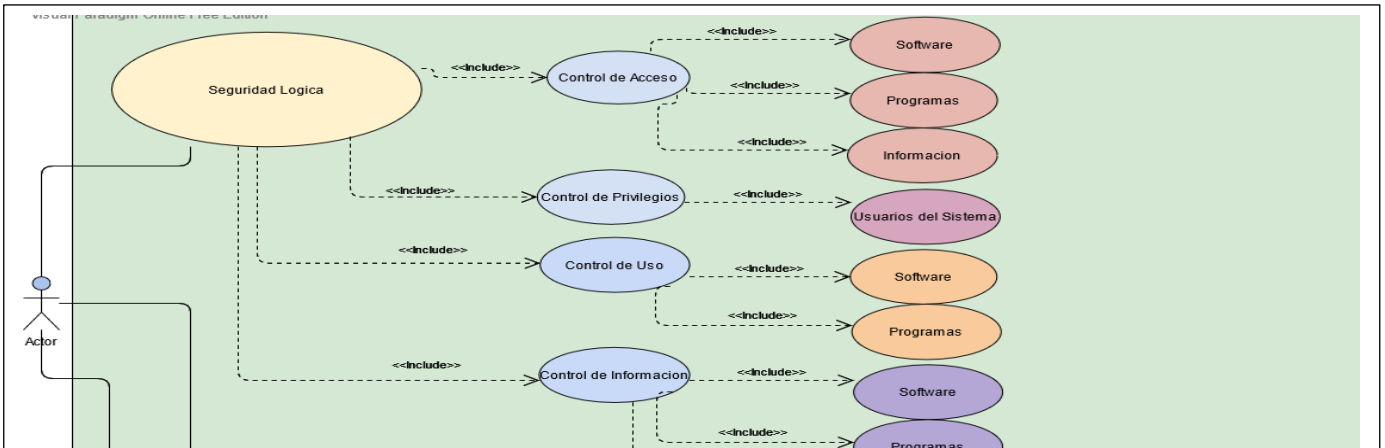


Fig. 6 Caso de Uso Extendido del sistema

Como se observa en la figura anterior cada uno de los tres casos de uso principales está compuesto por sub-opciones, se pretende mostrar la especificación textual de cada uno de ellos:

Caso de uso:	Seguridad Lógica
Actor principal:	Usuario
Ámbito:	Campus virtual
Stakeholders e intereses:	
Usuario:	Quiere saber qué nivel de seguridad tiene en la empresa o institución
Encargado del área:	Quiere realizar las encuestas para determinar el nivel de seguridad con la que cuenta la empresa o institución.
Precondición:	El usuario debe iniciar sesión en el sistema
Garantías mínimas:	El sistema realizara una encuesta por cada submenú
Garantías en caso de éxito: El sistema mostrara un informe sobre el nivel de seguridad que tiene la empresa o institución.	
Escenario principal de éxito:	
El usuario indicara en cuál de los submenús desea realizar la encuesta El sistema registrara las respuestas dadas por el usuario El sistema realizara la valoración de respuestas El sistema mostrará el informe del nivel de seguridad que tiene la empresa o institución.	

Tabla 3 Especificación textual de seguridad lógica

Caso de uso:	Propuesta de solución para garantizar la seguridad lógica
Actor principal:	Usuario
Ámbito:	Campus virtual
Stakeholders e intereses:	
Usuario:	Quiere saber qué tan vulnerable está a las amenazas lógicas
Encargado del área:	Quiere realizar las encuestas para determinar la vulnerabilidad de su sistema a las amenazas lógicas
Precondición:	El usuario debe iniciar sesión en el sistema
Garantías mínimas:	El sistema realizara una encuesta por cada submenú
Garantías en caso de éxito: el sistema mostrara un informe del nivel de vulnerabilidad del sistema ante amenazas lógicas	
Escenario principal de éxito:	
El usuario indicara en cuál de los submenús desea realizar la encuesta sobre amenazas lógicas El sistema registrara las respuestas dadas por el usuario El sistema realiza la valoración de respuestas El sistema mostrara el informe del nivel de vulnerabilidad ante amenazas lógicas que tiene la empresa o institución.	

Tabla 4 Especificación textual de Propuesta de solución para garantizar la seguridad lógica

Caso de uso:	Informe final
Actor principal:	Usuario
Ámbito:	Campus virtual
Stakeholders e intereses:	
Usuario: Quiere visualizar el informe completo de cada evaluación que realizo	
Encargado del área: Quiere visualizar el informe completo sobre el nivel con el que cuenta la empresa en cada uno de los submenús de evaluación	
Precondición: el usuario debe realizar las encuestas correspondientes	
Garantías mínimas:	el sistema mostrara el informe de cada submenú del cual se haya realizado la encuesta
Garantías en caso de éxito: el sistema entregara el informe final completo	
Escenario principal de éxito:	
El usuario indicara si desea visualizar el informe final El sistema mostrara el informe final El sistema preguntara si desea saber que técnicas de seguridad puede aplicar para mejorar la seguridad de la empresa. El sistema mostrara las técnicas para mejorar toda la seguridad lógica de la empresa o institución.	

Tabla 5 Especificación textual de Informe final

4.1.3 Diagrama entidad relación

En el desarrollo de la aplicación Segurity and Audit I&G (SAIG) se crea una base de datos con el nombre saig, compuesta por 5 tablas las cuales son:

- Usuario
- Empresa
- Test
- Repositorio_seguridad
- Respuestas_seguridad

En la fig. 7 se muestra cómo está compuesta cada tabla, cada una de ellas cuenta con llave primaria y llave foránea, cada tabla cuenta también con las conexiones correspondientes.

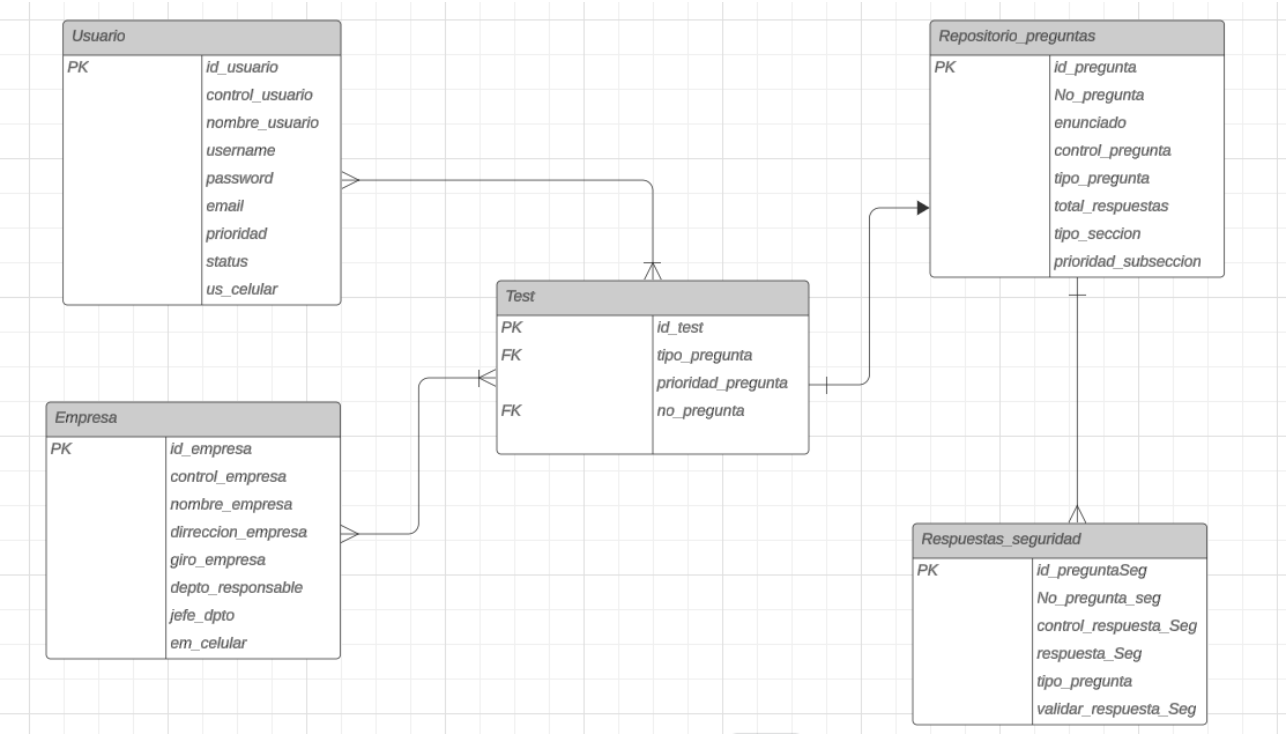


Fig. 7 Diagrama entidad relación de la base de datos saig.

4.1.4 Diagrama de clases

A continuación, en la fig. 8 se muestran las 5 tablas con las variables requeridas para la aplicación SAIG las cuales son:

- Usuario.
- Empresa.
- Test.
- Repositorio_preguntas.
- Respuestas_seguridad.

También se muestran los métodos con los que cuenta cada tabla los cuales son:
Tabla usuario:
Alta (), Bajas (), Modificar () y Consultas ().
Tabla empresa: Alta (), Bajas (), Modificar (), Consultas ().
Tabla test:Alta (), Bajas (), Modificar (), Consultas ().
Tabla repositorio_preguntas: Alta (), Bajas (), Modificar (), Consultas ().
Tabla respuestas_seguridad: Alta (), Bajas (), Modificar (), Consultas ().

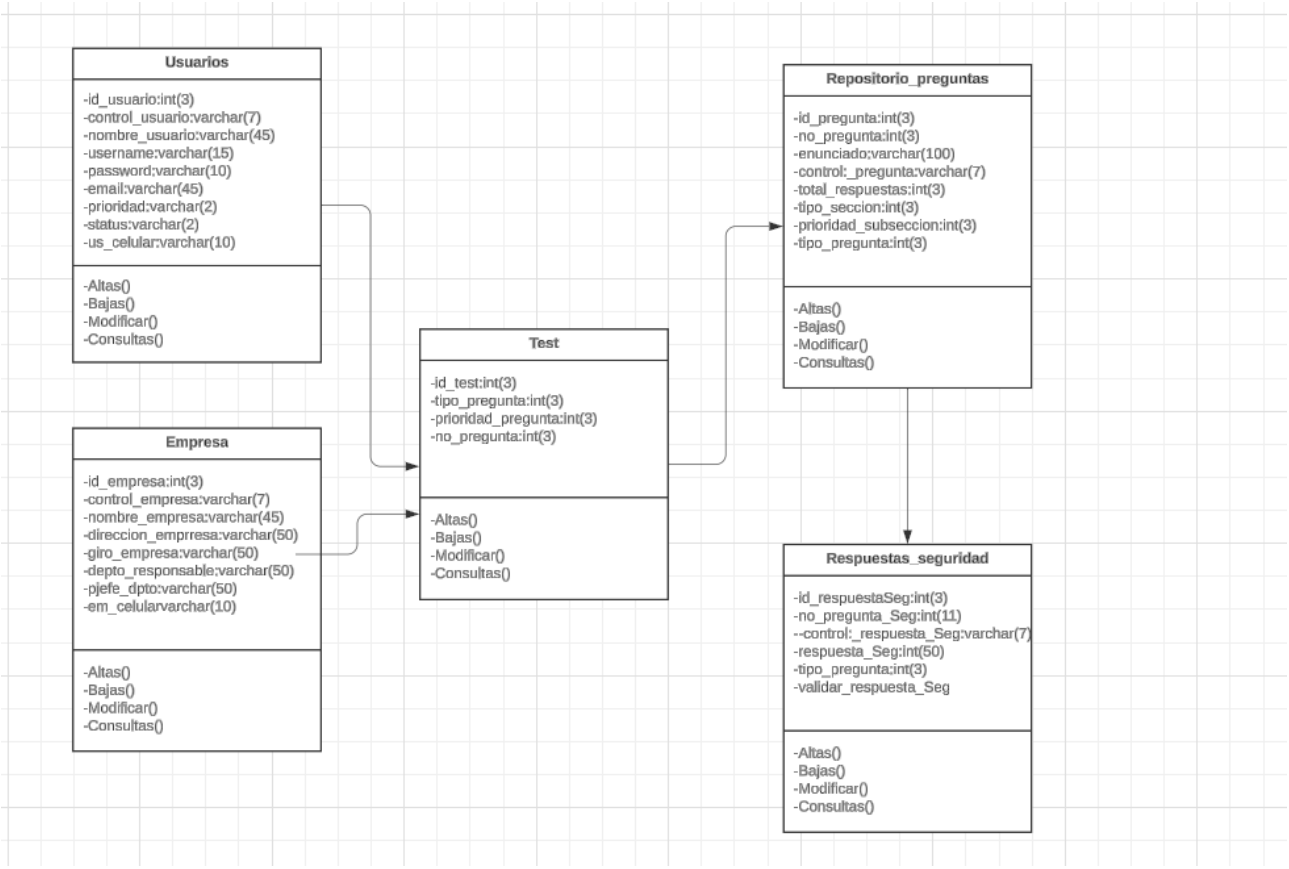


Fig. 8 Diagrama de clases de la aplicación SAIG.

4.1.5 Diseño del sistema

En este apartado, se presenta la simulación de la interfaz de la aplicación web a desarrollar, las siguientes imágenes son representaciones estáticas de las pantallasde la aplicación, diseñadas para mostrar cómo se las visualiza el usuario, y cómo se relacionan los diferentes elementos de la interfaz.

En la fig. 9 se muestra el inicio de sesión, compuesto por usuario y contraseña, que tiene dos botones ingresar y registro.



Fig.9 Pantalla de Inicio de sesión

Si no está registrado en la aplicación la fig. 10 se muestra un pequeño registro para crear una cuenta personal por empresa, donde se registran los campos de nombre de la empresa, usuario, responsable del departamento, nombre del departamento, contraseña, confirmar contraseña y correo electrónico.



Fig. 10 Registro de usuarios

La fig.11 muestra el menú principal de la aplicación, en cual cuenta se interactúa con dos botones: seguridad lógica y auditoría de red.



Fig.11 Menú principal de la aplicación

Como ya se mencionó anteriormente, solo se presenta la opción de seguridad lógica, por lo cual como se puede observar en la fig. 12 el submenú de este, el cual está compuesto por tres módulos, el primero es “Diagnóstico de Seguridad lógica, Propuesta de solución para garantizar la seguridad lógica e informe final”.



Fig. 12 Submenú de Seguridad lógica

Se muestra cuando el usuario desea acceder a la primera opción del menú, se muestran las opciones que tiene para empezar su verificación dentro de la organización, para ello el menú secundario muestra lo que puede hacer en la aplicación, la fig. 13 las detalla: Control de Acceso, Control de Privilegios, Control de Uso y Control de Información.

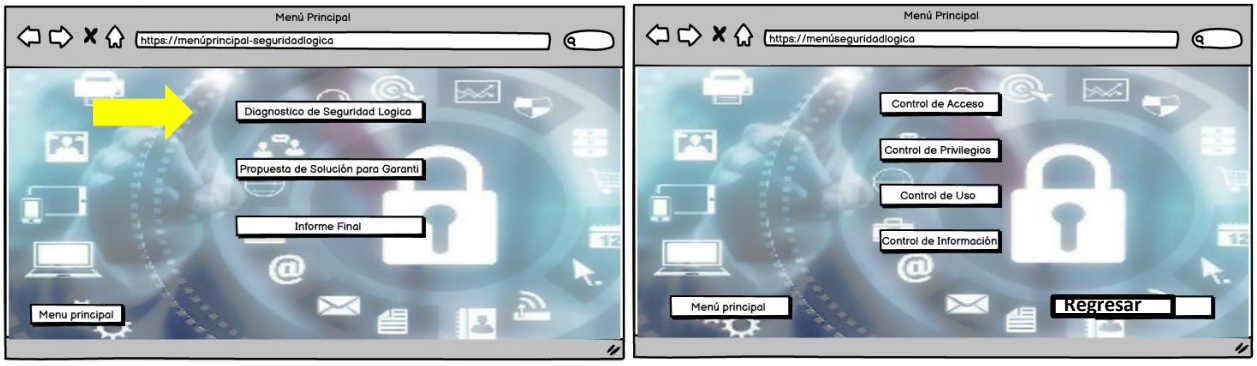


Fig. 13 Pantalla de submenú de Diagnostico de Seguridad lógica

La fig. 14 muestra las opciones del submenú "Control de acceso", el cual cuenta con las siguientes opciones: Software, Programas e Información, aquí el usuario puede verificar si su organización cumple con los linimientos de seguridad con respecto a el software, programas e información de datos personales o sensibles y de la organización.

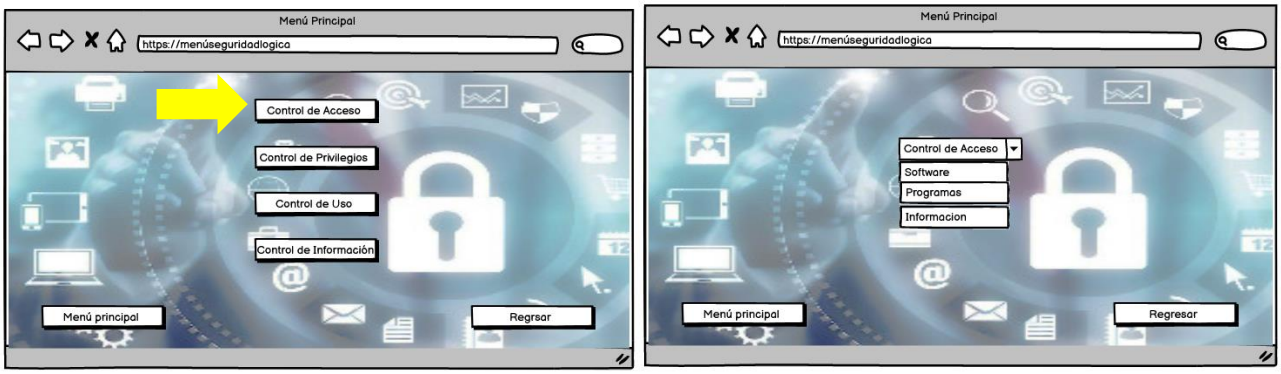


Fig. 14 Pantalla de opciones del submenú Control de acceso

Se muestra el segundo submenú, este es el encargado de verificar si se asignaron correctamente los privilegios a los usuarios dentro de la organización, la fig. 15 detalla esta opción, como se puede observar solo es una llamada "Usuarios del Sistema".



Fig. 15 Pantalla de opciones del submenú Control de privilegios

Ahora se muestran las opciones que tendrá el usuario, cuando este desee acceder a la opción de “Control de uso”, la cual es la tercera opción del submenú, esta opción se encarga de verificar y controlar el uso de aplicaciones de la organización, la fig.16 muestra las opciones con las que cuenta este submenú las cuales son: Software y Programas.



Fig.16 Pantalla de opciones del submenú Control de uso

Ahora se muestra las opciones con las que cuenta la última opción del submenú que es la encargada de verificar y controlar el uso de la información de la organización, de aplicaciones y datos personales, la fig. 17 muestra las opciones de “Control de Información”, que tiene las opciones de: Software, Programas e Información.



Fig. 17 Pantalla de opciones del submenú Control de información

La fig. 18 muestra las opciones que tiene usuario cuando este accede a la opción de información que se encuentra en la opción de “Control de información”. Esta opción consiste en preguntas, las cuales ayudan a verificar el nivel de control que tiene la organización respecto a la información que manejan.

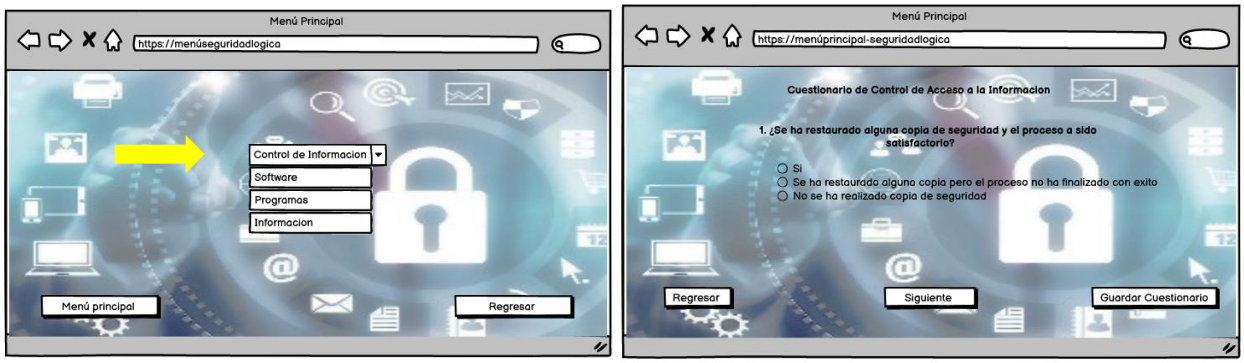


Fig.18 Pantalla de cuestionario de control de Información

Ahora mostraremos el caso en el que el usuario accede al segundo submenú, donde se muestran las opciones para mejorar la seguridad de la organización. En la fig. 19 se muestran las opciones del submenú “Propuesta de solución para garantizar la Seguridad lógica”, el cual cuenta con las siguientes opciones: Evaluación de Amenaza y Pruebas de Seguridad.



Fig. 19 Pantalla de submenús de Propuesta de solución para garantizar la Seguridad lógica

Después se presenta un ejemplo cuando el usuario accede a la opción de “Evaluación de amenazas”, en la que se presentan aquellas características que debe verificarse, para lograr una buena seguridad ante las amenazas cibernéticas existentes, la fig. 20 muestra las opciones de: Programas, Correos, Páginas Web, y Software.

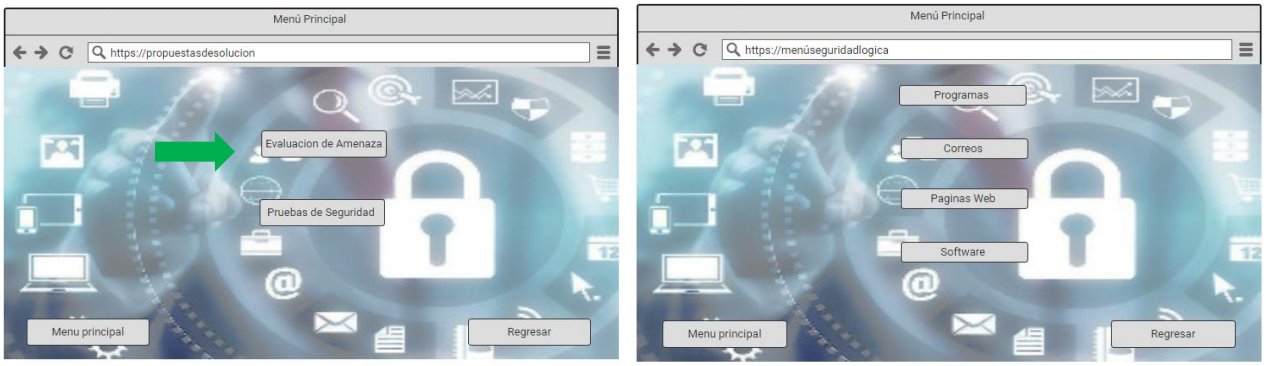


Fig. 20 Pantalla de opciones del submenú Evaluación de amenaza

Se muestra cuando el usuario accede al submenú “Informe final”, el cual muestra opciones para visualizar su informe de acuerdo con lo que desee este le reporte. La fig. 21 detalla esta opción, la cual cuenta con las siguientes opciones: Análisis, Crear Informe Final e Imprimir informe Final.



Fig. 21 Pantalla de opciones del submenú de Informe final

Se muestra cuando el usuario accede a la opción de “Análisis”, donde se le muestra la puntuación de cada submenú evaluada. La fig. 22 muestra la pantalla de análisis finalizado, presentando la puntuación obtenida en cada submenú donde realizo la encuesta dando la opción de ver una recomendación adecuada.



Fig.22 Pantalla de Analisis finalizado con puntuaciones

Se muestra cuando el usuario accede a la opción de “Recomendación”, en el cual se presentan algunas recomendaciones para mejorar la seguridad de la organización, en los aspectos en

donde la organización se encuentre más vulnerable a los ataques. La fig. 23 muestra en la aplicación web Segurity and Audit I & G un ejemplo de recomendaciones para sugerirle a la organización y/o institución.

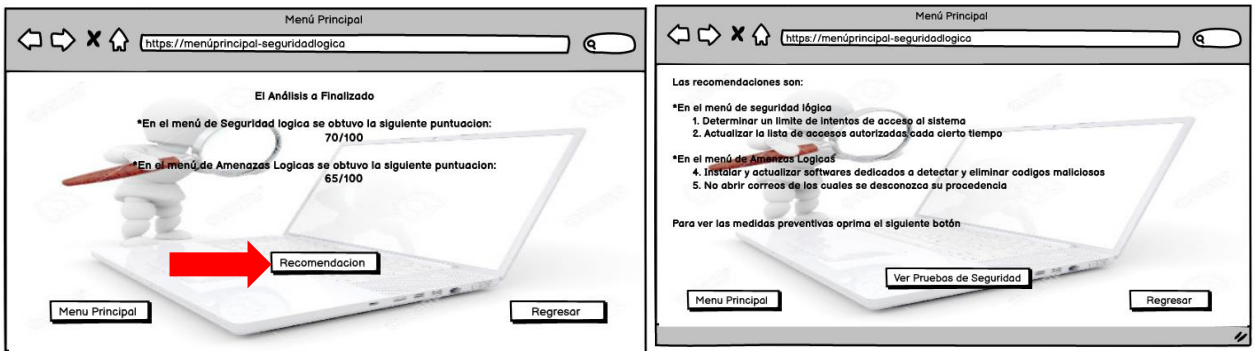


Fig. 23

Pantalla de Recomendaciónes para mejoras

Por último, se muestra cuando el usuario accede a la opción de “Ver pruebas de seguridad”, en la cual se presentan algunas recomendaciones de softwares que fueron antes valorados para solucionar los problemas de seguridad que se encuentren. La fig. 24 muestra en la aplicación web Segurity and Audit I & G un ejemplo de medidas preventivas para sugerirles a las empresas y/o instituciones.



Fig. 24

Pantalla de Pruebas de Seguridad

4.2 Desarrollo de la aplicación web

El presente apartado muestra las pantallas de la implementación de la aplicación, con la descripción de cada una de ellas para una mejor comprensión del funcionamiento de la aplicación.

En la fig. 25 se muestra la primera página que aparece al acceder a la aplicación.



Fig. 25 Pagina inicial de la aplicación (SAIG)

En la fig. 26 muestra el inicio de sesión el cual solicita la autenticación del usuario.



Fig. 26 Inicio de sesión, usuario y contraseña

En la fig. 27 se muestra la bienvenida que se le da al usuario, el cual está dado de alta con el perfil de Administrador.



Fig. 27 Bienvenida de un usuario que es Administrador.

En la fig. 28 se muestra el menú principal del perfil de usuario Administrador, el cual está conformado por gestión de usuarios, gestión de información de empresa y gestión de test.



Fig. 28 Menú principal de usuarios Administradores

En la fig. 29 se muestra el menú de “Administración de usuarios”, el cual está conformado por altas, bajas, modificar y consultas.



Fig. 29 Menú de Administración de usuarios.

En la fig. 30 se muestra el formulario para dar de alta a un usuario.



Fig. 30 Formulario de Alta de Usuarios

En la fig. 31 se muestra el letrero de confirmación de alta del usuario, así como el número el ID de usuario que se le asignó en la base de datos.



Fig. 31 Letrero de confirmación de alta del usuario.

Posteriormente en la fig. 32 se muestra la opción de eliminar un usuario, esta pantalla contiene una lista despegable con la clave de control del usuario para que, el usuario con perfil de Administrador seleccione la que desea y realice la eliminación.

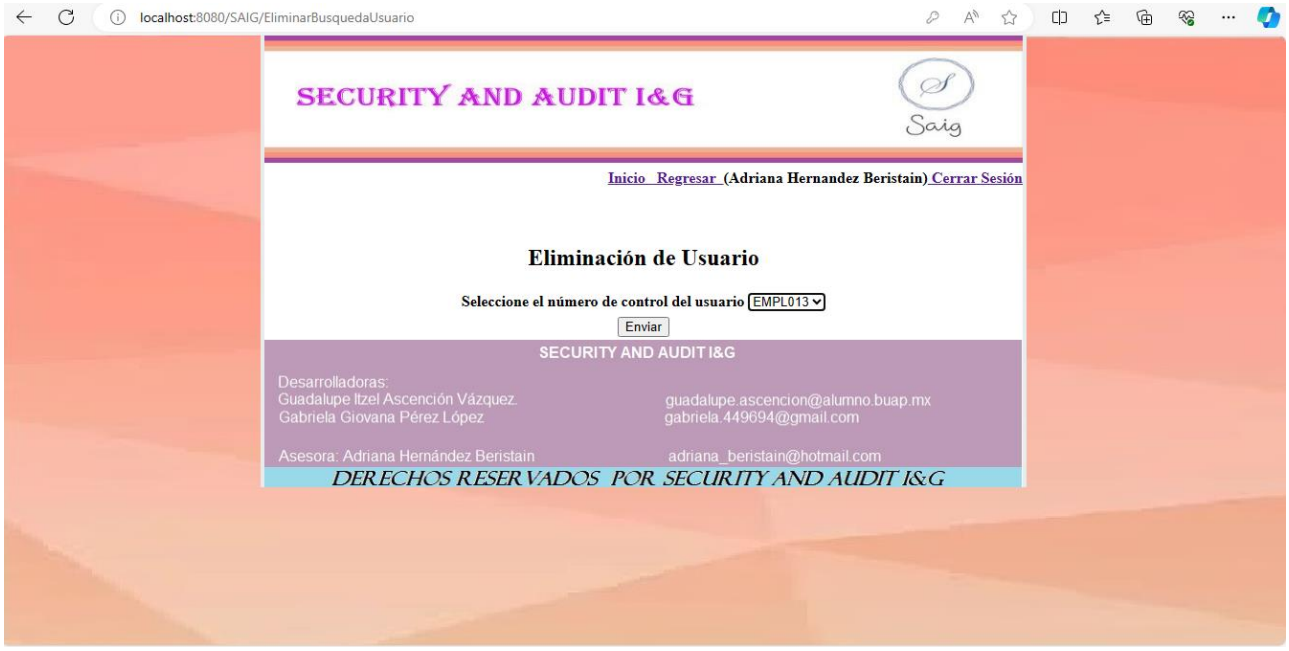


Fig. 32 Selección de clave de control del usuario a eliminar.

En la fig. 33 se muestra un letrero de confirmación, esto con la finalidad de corroborar la eliminación y así no cometer errores.

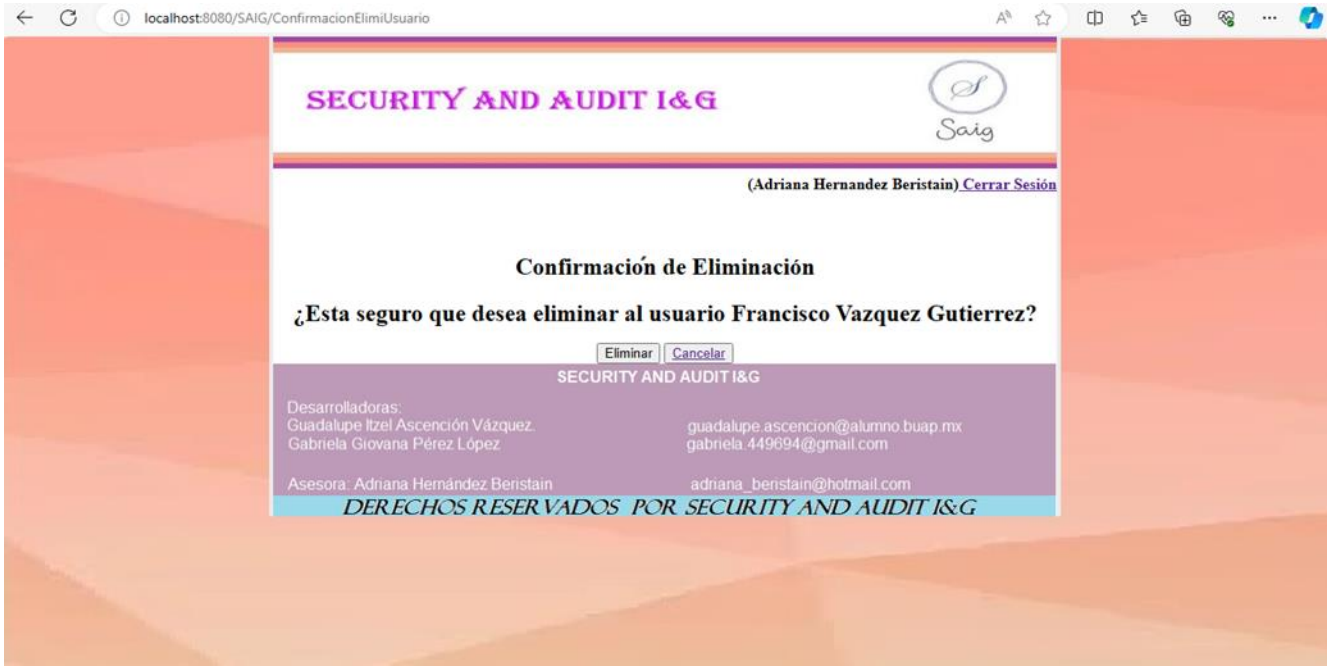


Fig. 33 Confirmación de Eliminación de Usuarios.

En la fig. 34 se muestra un letrero confirmando que se realizó correctamente la eliminación del usuario deseado.



Fig. 34 Letrero de confirmación de eliminación de usuario deseado.

En la fig. 35 se muestra el botón de modificación de usuarios, al igual que, en la opción de eliminar, se debe seleccionar la clave de control del usuario a modificar.



Fig. 35 Selección de clave de control del usuario a modificar.

En la fig. 36 Se muestra la tabla, la cual de lado izquierdo muestra la información almacenada en la base de datos de dicho usuario y en el lado derecho se muestran los campos que se pueden modificar. En este ejemplo se modifica el puesto del usuario.

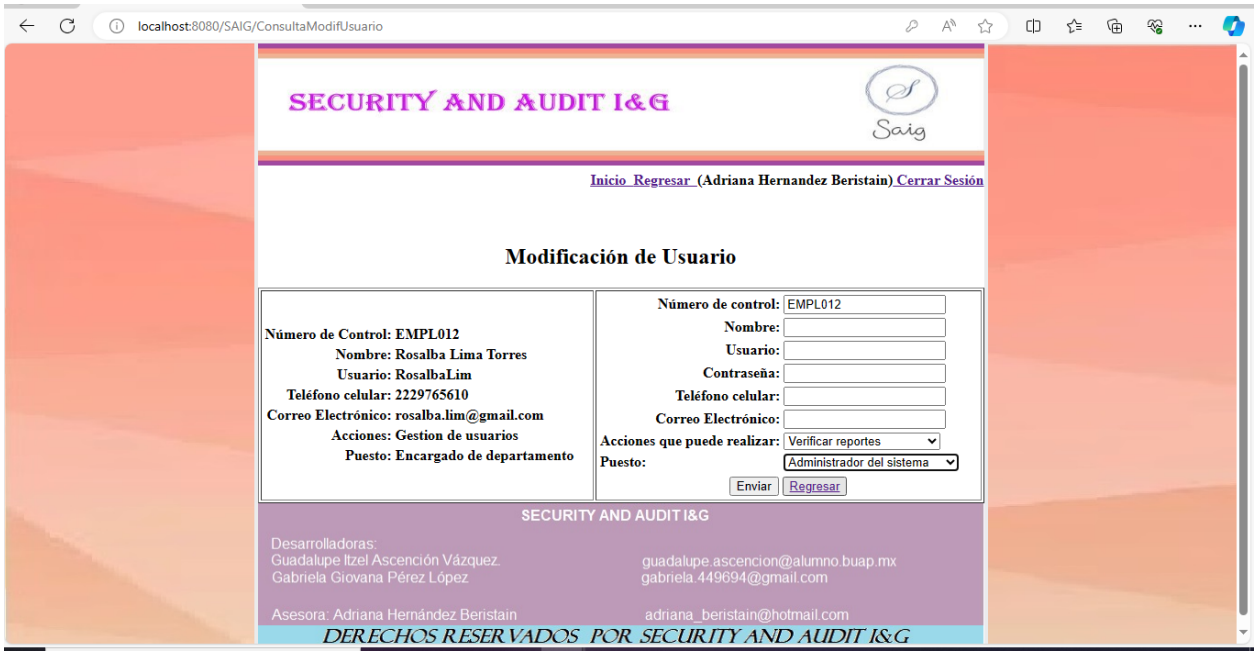


Fig. 36 Tabla con datos almacenados en la base de datos y campos que se pueden modificar.

En la fig. 37 se muestra la última pantalla del botón de modificar, la cual imprime el letrero de confirmación de cambios y la clave de control o ID del mismo.



Fig. 37 Letrero de Cambios realizados en el usuario deseado.

En la fig. 38 muestra el ultimo botón de la gestión de usuarios, el cual se encarga de realizar consultas. En esta primera pantalla se muestran dos opciones para la búsqueda del usuario a consultar, estas dos opciones son: por clave de control o por nombre del usuario.



Fig.38 Selección de usuario a consultar

En la fig. 39 se muestra la información del usuario seleccionado por la opción "Clave de control".



Fig.39 Información del usuario, buscado por la opción de clave de control.

En la fig. 40 muestra la consulta de información de un usuario, a través de la segunda opción "por nombre".



Fig. 40 Consulta de información de usuario seleccionado por la opción de nombre.

En la fig. 41 se muestra el submenú gestión de administración de empresas, el cual cuenta con altas, bajas, modificaciones y consultas de empresas.



Fig. 41 Menú de Administración de empresas

En la fig. 42 se muestra un formulario por el cual se realiza el alta de una empresa.



Fig. 42 Formulario de alta de empresa.

En la fig. 43 muestra la confirmación de alta de la empresa de manera correcta.



Fig. 43 Confirmación de alta realizada correctamente.

En la fig. 44 se muestra el segundo botón de administración de empresas, el cual se encarga de la eliminación de estas.



Fig. 44 Pantalla de búsqueda de empresa a eliminar.

En la fig.45 se muestra la pantalla de confirmación de eliminación.



Fig. 45 Confirmación de si es la empresa correcta que se dese eliminar.

En la fig. 46 se muestra el letrero, que confirma que se realizó la eliminación de la empresa seleccionada.



Fig. 47 Letrero de Eliminación correcta.

En la fig. 47 se muestra el botón de “Administración de empresas” el cual se encarga de realizar modificaciones a la información de estas.

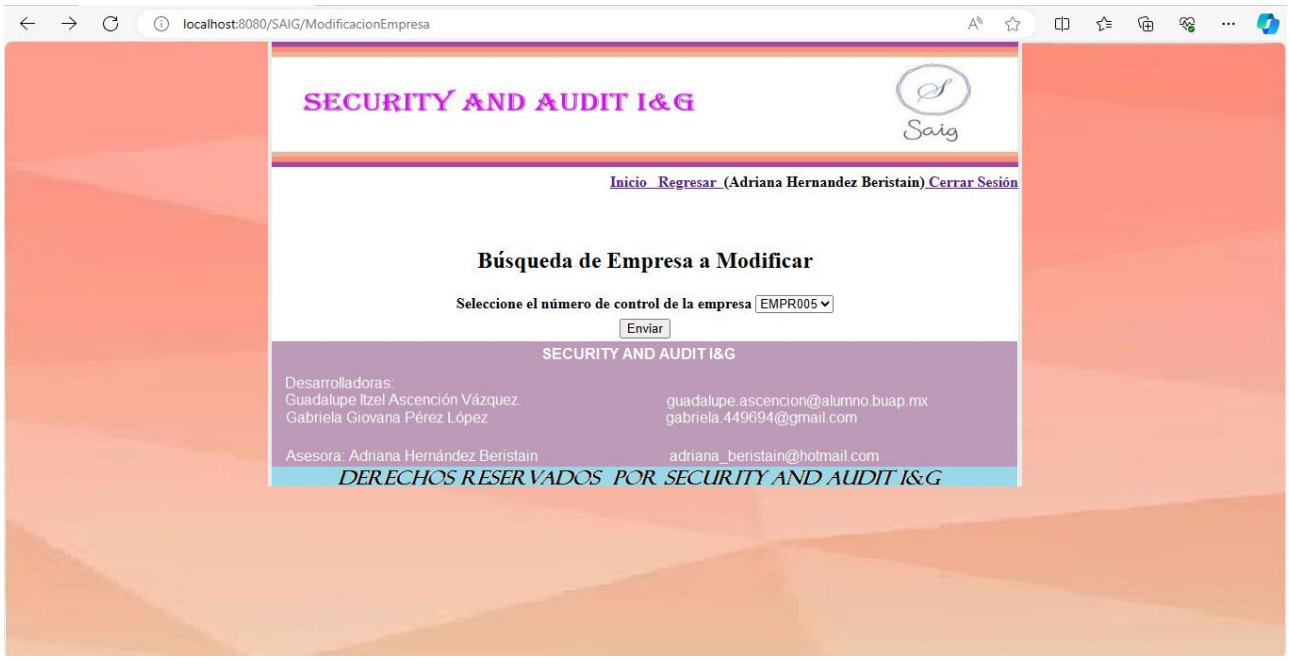


Fig. 47 Búsqueda de empresa de la cual se desea modificar la información.

En la fig. 48 se muestra del lado izquierdo la información almacenada en la base de datos y en el lado derecho los campos que se pueden modificar de una empresa.



Fig. 48 Datos que se pueden modificar de una empresa

En la fig. 49 se muestra la confirmación de que los cambios se realizaron correctamente en la información de una empresa.



Fig. 49 Confirmación de datos modificados correctamente

En la fig. 50 se muestran las opciones con las que cuenta el botón de consulta de empresas, este cuenta con dos opciones para realizar la búsqueda ya sea por la clave de la empresa o por el nombre de esta.



Fig. 50 Formas de búsqueda de empresa a modificar

En la fig. 51 se muestra un ejemplo de cuando el usuario selecciona la primera forma de buscar la empresa de la cual se desea visualizar la información.

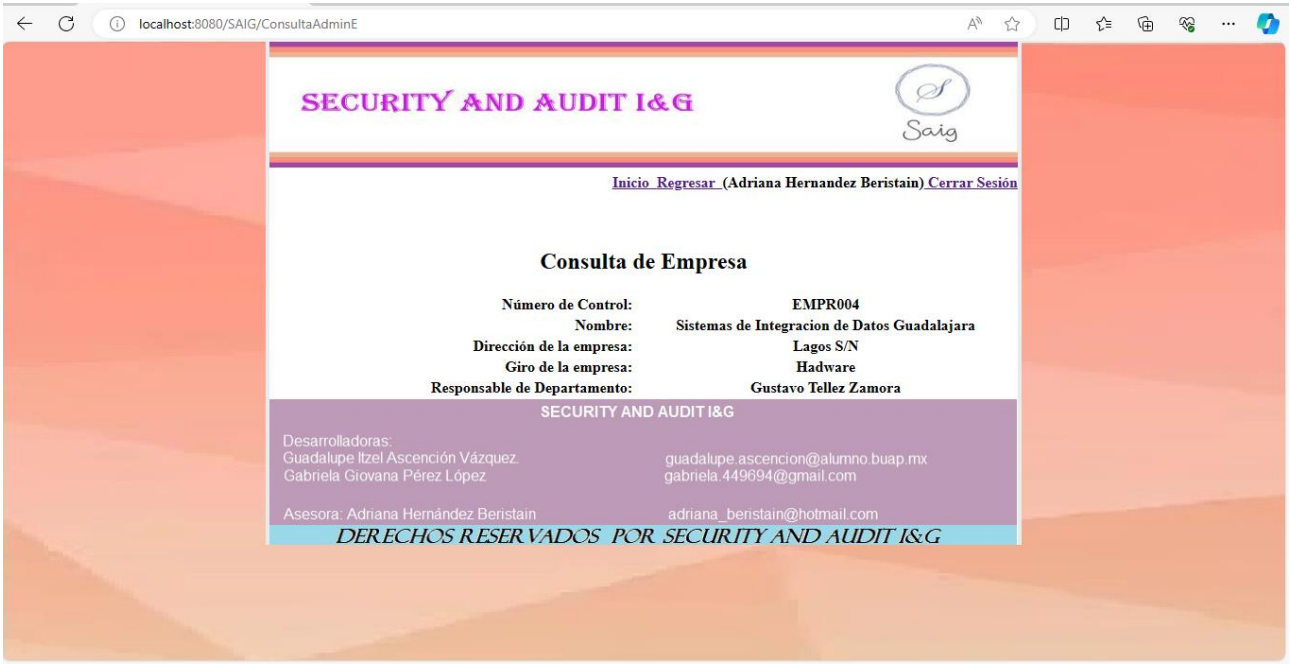


Fig. 51 Información de cliente empresa seleccionado por clave de la empresa

En la fig. 52 se muestra un ejemplo de cuando el usuario selecciona la segunda forma de buscar la empresa de la cual se desea visualizar la información.



Fig. 52 Información de cliente empresa seleccionado por nombre de la empresa

En la fig.53 se muestra el acceso de otro tipo de usuario del sistema, en este caso es un supervisor, el cual cuenta con un menú distinto al de un administrador.

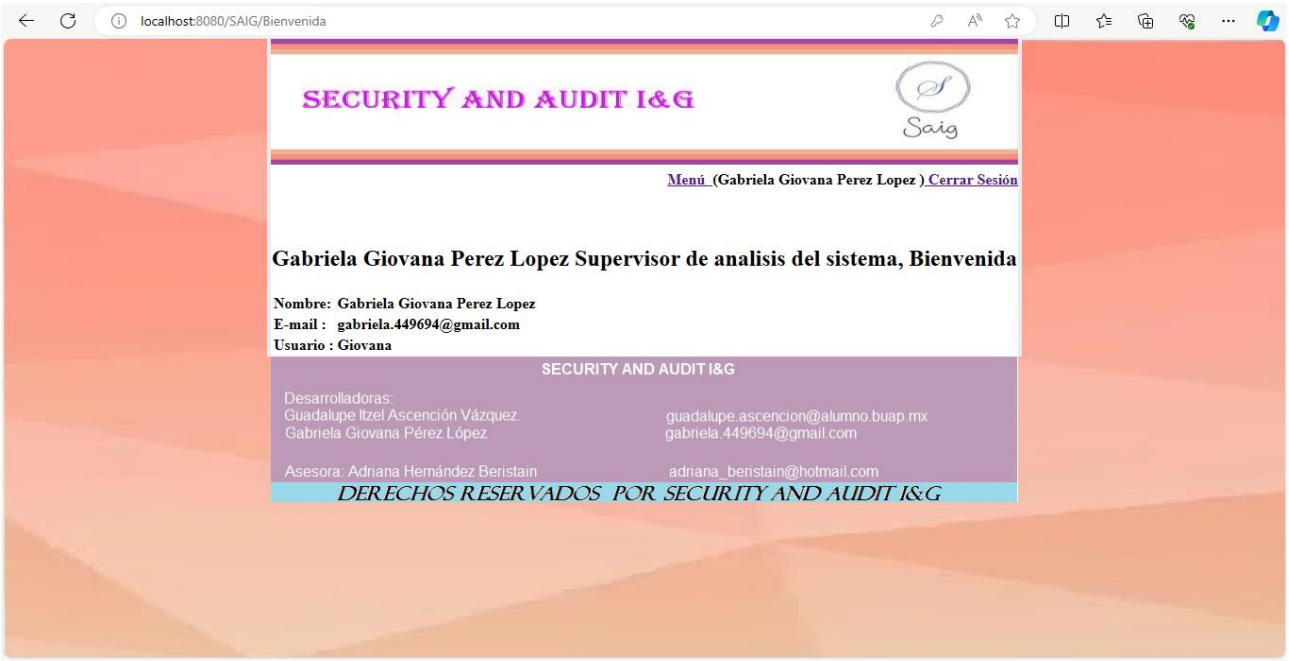


Fig. 53 Acceso de un supervisor al sistema

En la fig. 54 se muestra el menú al que tiene acceso un supervisor. En este caso solo se mostrarán las opciones con las que cuenta el botón de Seguridad lógica ya que es el tema que se desarrolla en este trabajo de tesis.



Fig. 54 Menú del supervisor

En la fig. 55 se muestra el submenú al que tiene acceso el supervisor por medio del botón de Seguridad lógica. El cual cuenta con tres opciones.



Fig. 55 Submenú del botón de Seguridad lógica

CAPITULO 5 PRUEBAS Y RESULTADOS

5.1 Pruebas

5.1.1 Pruebas por exploración

Las pruebas por exploración se evaluaron con las siguientes historias de usuario, además se anexan las observaciones que se identificaron en el proceso.

Tabla 1 - Historia de usuario del registro de usuario

Historia de usuario #1	
Nombre:	Registro de usuario
Usuario:	Administrador
Descripción:	Comprobar que el administrador logre registrar mediante el formulario de registro.
Observaciones:	Se validan que los datos estén completos además de que en los campos de teléfono sólo permite ingresar números. El administrador indicará que acciones podrá realizar el usuario seleccionando su puesto, su estatus.

Tabla 2 - Historia de usuario del inicio de sesión del usuario

Historia de usuario #2	
Nombre:	Inicio de sesión
Usuario:	Empleado
Descripción:	Cuando el empleado inicie sesión se le dirige a su menú correspondiente según el estatus con el que se registró el empleado.
Observaciones:	Se valida el estatus del usuario y según eso se dirige al usuario a sus menús a los que tiene acceso para lograr un mejor manejo de la aplicación.

Tabla 3 - Historia de usuario de la gestion de usuarios.

Historia de usuario #3	
Nombre:	Gestión de usuarios
Usuario:	Administrador
Descripción:	Realizar altas, bajas, modificaciones y consultas de usuarios.
Observaciones:	El administrador lleva el control de los usuarios y asigna los rangos a cada usuario, así como las acciones que puede realizar.

Tabla 4 - Historia de usuario de la gestion de la informacion de la empresas.

Historia de usuario #4	
Nombre:	Gestión de la información de empresas
Usuario:	Administrador
Descripción:	Realizar altas, bajas, modificaciones y consultas de empresas
Observaciones:	El administrador lleva el control de los empresas, para que tengan acceso a la aplicación web y con ello logren realizar sus análisis.

Tabla 5- Historia de usuario de la gestion de la informacion de la empresas.

Historia de usuario #5	
Nombre:	Gestión de test
Usuario:	Administrador
Descripción:	Realizar altas, bajas, modificaciones y consultas de test.
Observaciones:	El administrador es el encargado de las preguntas que conforman cada test para que realizar el análisis correspondiente.

Tabla 6- Historia de usuario de la gestion de test

Historia de usuario #6	
Nombre:	Gestión de test
Usuario:	Administrador
Descripción:	Realizar altas, bajas, modificaciones y consultas de test.
Observaciones:	El administrador es el encargado de las preguntas que conforman cada test para que realizar el análisis correspondiente.

Tabla 7- Historia de usuario de diagnostico de seguridad

Historia de usuario #7	
Nombre:	Diagnóstico de seguridad
Usuario:	Supervisor
Descripción:	Realiza diagnósticos de control de acceso, control de privilegios, control de uso, control de información.
Observaciones:	Cada supervisor realiza los diagnósticos cada uno se divide diagnósticos de software, programas e información.

Tabla 8- Historia de usuario de propuesta de solucion para garantizar la seguridad logica

Historia de usuario #8	
Nombre:	Propuesta de solución para garantizar la seguridad lógica
Usuario:	Supervisor
Descripción:	En este apartado el supervisor realiza evaluación de amenazas y propuestas de seguridad.
Observaciones:	Se realiza el análisis y con ellos se da un resultado y las propuestas para poder resolver dichas anomalías en la seguridad.

Tabla 9- Historia de usuario de evaluacion de amenazas.

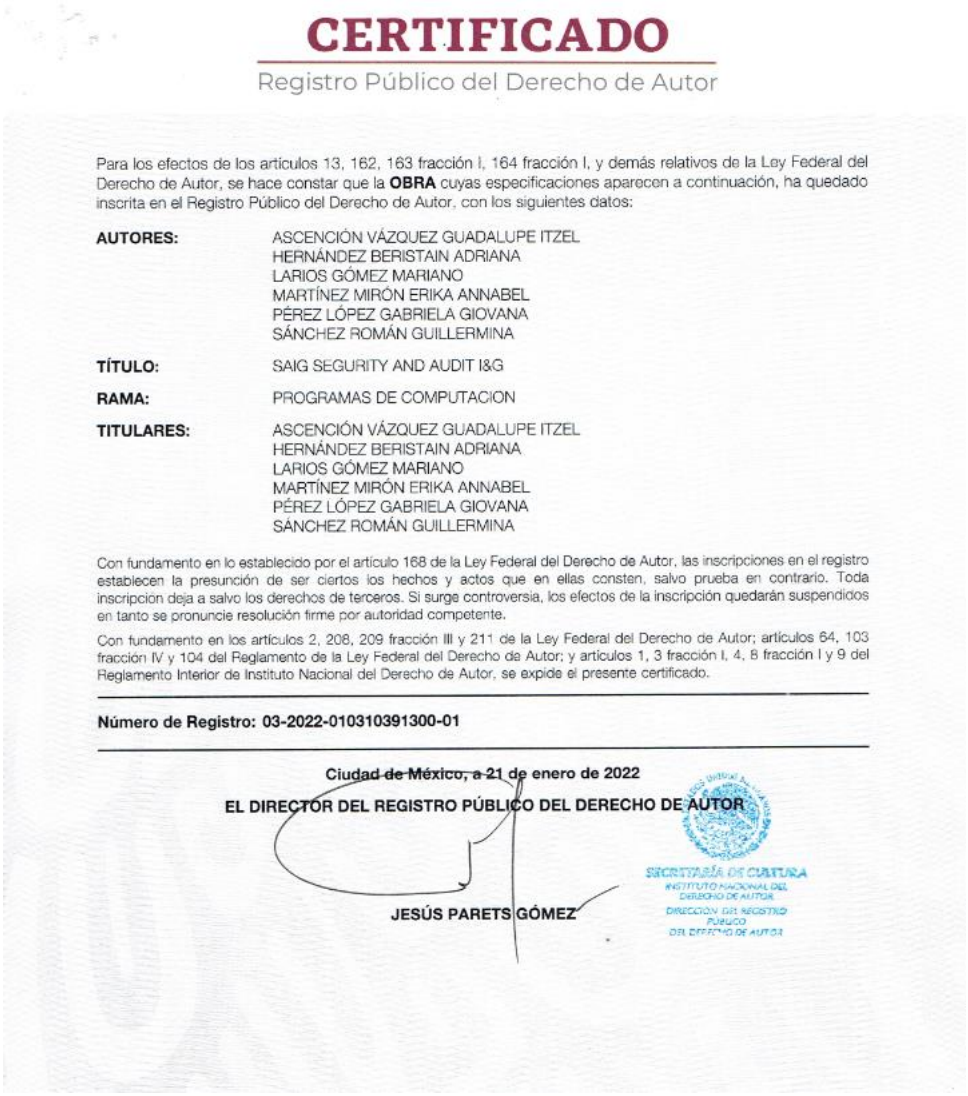
Historia de usuario #9	
Nombre:	Evaluación de amenazas
Usuario:	Supervisor
Descripción:	Realiza evaluaciones de amenazas, las cuales se dividen en evaluaciones de programas, correos, páginas web y software.
Observaciones:	Cada evaluación se conforma por cierta cantidad de preguntas las cuales irán determinando las debilidades de la seguridad y con ello lograr dar un buen análisis y así dar una buena propuesta para solucionarlo.

Tabla 10- Historia de usuario de informa final

Historia de usuario #10	
Nombre:	Informe final
Usuario:	Supervisor
Descripción:	Se muestra el informe final con los rubros que conforman el análisis completo.
Observaciones:	El informe final es detallado y en el también se encuentran las propuestas por cada rubro y detalladas para lograr u mejor entendimiento del usuario.

5.2 Resultados

- Se presentó el proyecto de tesis en el coloquio estudiantil para desarrollar habilidades del pensamiento complejo CE-DHPC de octubre 2021, con la evolución de otros estudiantes de la facultad, que sirve de apoyo para atender errores, observaciones y mejorar.
- Se realizo la protección de obra a través del Registro de Derecho de Autor de la Fase 1 de la aplicación donde se presentó el modelo de la aplicación web, simulación y casos de uso.



CERTIFICADO

Registro Público del Derecho de Autor

Para los efectos de los artículos 13, 162, 163 fracción I, 164 fracción I, y demás relativos de la Ley Federal del Derecho de Autor, se hace constar que la **OBRA** cuyas especificaciones aparecen a continuación, ha quedado inscrita en el Registro Público del Derecho de Autor, con los siguientes datos:

AUTORES: ASCENCIÓN VÁZQUEZ GUADALUPE ITZEL
HERNÁNDEZ BERISTAIN ADRIANA
LARIOS GÓMEZ MARIANO
MARTÍNEZ MIRÓN ERIKA ANNABEL
PÉREZ LÓPEZ GABRIELA GIOVANA
SÁNCHEZ ROMÁN GUILLERMINA

TÍTULO: SAIG SEGURITY AND AUDIT I&G

RAMA: PROGRAMAS DE COMPUTACION

TITULARES: ASCENCIÓN VÁZQUEZ GUADALUPE ITZEL
HERNÁNDEZ BERISTAIN ADRIANA
LARIOS GÓMEZ MARIANO
MARTÍNEZ MIRÓN ERIKA ANNABEL
PÉREZ LÓPEZ GABRIELA GIOVANA
SÁNCHEZ ROMÁN GUILLERMINA

Con fundamento en lo establecido por el artículo 168 de la Ley Federal del Derecho de Autor, las inscripciones en el registro establecen la presunción de ser ciertos los hechos y actos que en ellas consten, salvo prueba en contrario. Toda inscripción deja a salvo los derechos de terceros. Si surge controversia, los efectos de la inscripción quedarán suspendidos en tanto se pronuncie resolución firme por autoridad competente.

Con fundamento en los artículos 2, 208, 209 fracción III y 211 de la Ley Federal del Derecho de Autor; artículos 64, 103 fracción IV y 104 del Reglamento de la Ley Federal del Derecho de Autor; y artículos 1, 3 fracción I, 4, 8 fracción I y 9 del Reglamento Interior de Instituto Nacional del Derecho de Autor, se expide el presente certificado.

Número de Registro: 03-2022-010310391300-01

Ciudad de México, a 21 de enero de 2022

EL DIRECTOR DEL REGISTRO PÚBLICO DEL DERECHO DE AUTOR

JESÚS PARETS GÓMEZ

SECRETARÍA DE CULTURA
INSTITUTO NACIONAL DEL DERECHO DE AUTOR
DIRECCIÓN DEL REGISTRO PÚBLICO DEL DERECHO DE AUTOR

- Se cuenta con una aplicación web nombrada "Segurity and Audit I & G”, por sus siglas SAIG.

CAPÍTULO 6. CONCLUSIONES Y TRABAJO A FUTURO

En el desarrollo se utilizaron distintas aplicaciones que permitieron el desarrollo de la aplicación, logrando así el objetivo de este proyecto.

Los resultados obtenidos con un mantenimiento correcto generarían un gran impacto en la seguridad, ya que con la aplicación SAIG se puede obtener ayuda para la mejoría de la seguridad de las organizaciones que deseen aplicar medidas eficientes para no pasar por un ataque cibernético.

En conclusión, este proyecto y su investigación ha sido enriquecedora, gratificante y han complementado mis conocimientos previos que tenía antes de realizar el trabajo de tesis, espero que pueda servir como punto de partida u orientar a quienes estén interesados en temas relacionados a este.

6.2 Trabajo futuro

- Para trabajo a futuro se puede continuar la aplicación, para dar los reportes finales impresos a las organizaciones que usen la aplicación SAIG y continuar a que se implementaran las medidas de seguridad para volver a realizar un testeo de verificación.
- Una vez que este completo el desarrollo realizar y entregar los reportes, se pondrá un precio a la aplicación que vaya acorde con los servicios que ofrece.
- Realizar diferentes pruebas con organizaciones de distintas ramas, para que usen la aplicación y puedan corroborar que funciona correctamente según se describe en este trabajo de tesis.
- Que el reporte final sea enviado por sms o correo electrónico al responsable del departamento de TIC de la organización.

CAPITULO 7 BIBLIOGRAFIA

[1]Prey Project. (s.f.). 30 estadísticas sobre seguridad informática. Recuperado de https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

[2] Rio Bravo Systems. (s.f.). Sistemas Río Bravo: Vulnerability Pentesting. Recuperado de https://services.riobravosystems.com/es/sistemas-rio-bravo-vulnerability-pentesting/?utm_campaign=Pentesting&utm_term=vulnerability%20analysis&utm_source=adwords&utm_medium=ppc&hsa_ver=3&hsa_acc=8382277779&hsa_mt=b&hsa_src=g&hsa_cam=12001312774&hsa_grp=145188115851&hsa_tgt=kwd-10991870&hsa_kw=vulnerability%20analysis&hsa_ad=613732405862&hsa_net=adwords&gad=1&gclid=EAIaIQobChMI0tr9svrZ_wIVuBWtBh0F_w_SEAAYAiAAEgJdx_D_BwE

[3] SonarSource. (s.f.). Soluciones de seguridad. Recuperado de https://www.sonarsource.com/solutions/security/?gads_campaign=SQ-Mroi-Generic&gads_ad_group=Security&gads_keyword=application%20security%20tester&gclid=EAIaIQobChMItKCcl-bQ_wIVZg6tBh3ErAdvEAAYAyAAEgJVr_D_BwE

[4] Fortra. (s.f.). Escaneo de Vulnerabilidades. Recuperado de https://www.fortra.com/es/blog/escaneo-vulnerabilidades-

[5]vanti. (s.f.). Ivanti Neurons for Autonomous Security Operations Center. Recuperado de https://www.ivanti.com/es/products/ivanti-neurons-for-asoc

[6] Strapp Inc. (s.f.). ¿Qué es una aplicación web? Recuperado de https://www.strappinc.com/blog/strapp-datos/que-es-una-aplicacion-web

[7]Aprender Libre. (s.f.). Historia de las aplicaciones web. Recuperado de https://aprender-libre.com/historia-de-las-aplicaciones-web/

[8] ESIC Business & Marketing School. (s.f.). ¿Qué es el diseño de interfaces web? Recuperado de https://www.esic.edu/rethink/tecnologia/que-es-el-diseno-de-interfaces-web/

[9] Dongee. (s.f.). ¿Cuál es la arquitectura de una aplicación web? Recuperado de https://www.dongee.com/tutoriales/cual-es-la-arquitectura-de-una-aplicacion-web/

[10] Senado de la República. (s.f.). Gaceta de la Comisión Permanente. Recuperado de https://www.senado.gob.mx/65/gaceta_comision_permanente/documento/42432

[11]Biblus. (s.f.). Memoria del proyecto: Capítulo 3 - Tecnología Java Servlet. Recuperado de https://biblus.us.es/bibing/proyectos/abreproy/11416/fichero/MEMORIA_EDITOR_FORMATO_QTI%252FCap%C3%ADtulo+3+Tecnolog%C3%ADa+Java+Servlet.pdf

[12]Arimetrics. (s.f.). Glosario Digital de JavaScript. Recuperado de https://www.arimetrics.com/glosario-digital/javascript

[13]Oracle. (s.f.). ¿Qué es una base de datos? Recuperado de https://www.oracle.com/mx/database/what-is-database/

[14]UNAM. (s.f.). Administración de Centros de Cómputo (UNIDAD IV). Recuperado de https://www.fcca.umich.mx/descargas/apuntes/academia%20de%20informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20IV.pdf

[15] Microsoft. (s.f.). What is access control? Recuperado de https://www.microsoft.com/es-mx/security/business/security-101/what-is-access-control

[16] INCIBE. (s.f.). Toma el control: se instala la política de aplicaciones permitidas. Recuperado de https://www.incibe.es/empresas/blog/toma-el-control-se-instala-politica-aplicaciones-permitidas

[17] ISOTools. (s.f.). ISO 27001. Recuperado de https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

[18] Smartekh. (2022, agosto 29). 4 maneras en las que la gestión de acceso privilegiado asegura a los trabajadores remotos. Recuperado de https://blog.smartekh.com/4-maneras-en-las-que-la-gestion-de-acceso-privilegiado-asegura-a-los-trabajadores-remotos/

[19] HubSpot. (s.f.). ¿Qué es la seguridad informática? Recuperado de https://blog.hubspot.es/website/que-es-seguridad-informatica

[20] Megías, A. (s.f.). Amenazas a la seguridad. Recuperado de https://albertomegiasblog.wordpress.com/amenazas-a-la-seguridad/

[21] ML, G. (s.f.). Tipos de amenazas lógicas. Recuperado de https://geraldml66.weebly.com/tipos-de-amenazas-loacutegicas.html

[22] HostGator. (s.f.). Principales amenazas al correo electrónico corporativo. Recuperado de https://www.hostgator.mx/blog/principales-amenazas-correo-electronico-corporativo/

[23] Kaspersky Lab. (s.f.). Threats to Web. Recuperado de https://latam.kaspersky.com/resource-center/threats/web

[24] Universidad de Alicante. (s.f.). Catálogo de las principales amenazas lógicas de los sistemas informáticos. Recuperado de https://moodle2022-23.ua.es/moodle/pluginfile.php/196983/mod_resource/content/11/tema/catlogo_de_las_principales_amenazas_lgicas_de_los_sistemas_informticos.html

[25] Panda Security. (s.f.). Rootkit. Recuperado de https://www.pandasecurity.com/es/security-info/rootkit/

[26] ZapTest. (s.f.). ¿Qué es la comprobación de sistemas? Una inmersión en profundidad en enfoques, tipos, herramientas, consejos y trucos, y mucho más. Recuperado de https://www.zaptest.com/es/que-es-la-comprobacion-de-sistemas-una-inmersion-en-profundidad-en-enfoques-tipos-herramientas-consejos-y-trucos-y-mucho-mas

[27] ZapTest. (s.f.). Pruebas exploratorias: una inmersión profunda en tipos, procesos, enfoques, herramientas, marcos y más. Recuperado de https://www.zaptest.com/es/pruebas-exploratorias-una-inmersion-profunda-en-tipos-procesos-enfoques-herramientas-marcos-y-mas

[28] Capacitación Inclusiva. (2022). UNIDAD 8 - Software Testing [Documento PDF]. Recuperado de https://www.capacitacioninclusiva.com/wp-content/uploads/2022/04/UNIDAD-8-SoftwareTesting.pptx.pdf

[29] Atlassian. (s.f.). Tipos de pruebas de software. Recuperado de https://www.atlassian.com/es/continuous-delivery/software-testing/types-of-software-testing

[30] ZapTest. (s.f.). ¿Qué es la prueba de regresión? Aplicación, herramientas y guía completa. Recuperado de https://www.zaptest.com/es/que-es-la-prueba-de-regresion-aplicacion-herramientas-y-guia-completa

[31] ZapTest. (s.f.). Pruebas de estrés en pruebas de software: qué es, tipos, procesos, enfoques, herramientas, más. Recuperado de https://www.zaptest.com/es/pruebas-de-estres-en-pruebas-de-software-que-es-tipos-procesos-enfoques-herramientas-mas