BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

“AUDITORÍA DE RED Y PROPUESTA DE IMPLEMENTACIÓN DIAGNÓSTICA”

TESIS PRESENTADA PARA OBTENER EL

TÍTULO DE: LICENCIATURA EN

INGENIERÍA EN CIENCIAS DE LA

COMPUTACIÓN

PRESENTA:

GUADALUPE ITZEL ASCENCIÓN VÁZQUEZ

ASESORA:

M.C ADRIANA HERNÁNDEZ BERISTAIN

ABRIL 2024

DEDICATORIA

Dedico el siguiente trabajo de tesis a mis padres, que, con su apoyo incondicional, me otorgaron fuerzas para seguir adelante, también a mis abuelos que estuvieron conmigo siempre. A una persona muy especial, que me ha enseñado que la vida está llena de obstáculos y, a pesar de todo, si le pones empeño y dedicación, se lograrán los objetivos.

AGRADECIMIENTOS

Quiero agradecer a toda mi familia Betsabé Vázquez Hernández, Alberto Ascención Carrera y Candelaria Hernández Calderón por el gran apoyo a mi proyecto de tesis del cual me siento orgullosa de compartir con todos ellos.
En especial, a mi bisabuelita Teresa Mora Jiménez y mis abuelos Susana Carrera Garces, Juan Ascención Evangelista, aunque no se encuentran presentes, en su momento me motivaron para salir adelante y aprender de la vida.
A mi abuelo Armando Joel Vázquez Mora, por enseñarme a superarme en cada momento.
A mi tía Lorena Erika Vázquez Toscano, el enseñarme que los obstáculos solo están en mi mente y no en el poder hacerlos.
A mi asesora de tesis, la M.C, Adriana Hernández Beristain que, con sus conocimientos y experiencias, me dio a conocer el gran mundo de la ciberseguridad.

Contenido

CAPÍTULO 1. INTRODUCCIÓN *6*

1.1 RESUMEN **6**

1.2 Planteamiento del problema **7**

1.3 Justificación **8**

1.4 Objetivo general **9**

1.5 Objetivos Específicos **9**

CAPÍTULO 2. ESTADO DEL ARTE *10*

2.1 Antecedentes **10**

2.2 Aplicaciones similares **11**

2.3 Benchmark Gensuite **11**

2.4 WinAudit **11**

2.5 Planning Advisor **11**

2.6 Auditoría **12**

CAPÍTULO 3. MARCO TEÓRICO *13*

3 Metodología **13**

3.1 Tipos de pruebas de software **19**

3.1.1 Pruebas por exploración **19**

3.1.2 Pruebas por conjetura de fallos **19**

3.1.3 Pruebas de aceptación **19**

3.1.4 Pruebas de integración **19**

3.1.5 Pruebas de unidad **19**

3.1.6 Pruebas funcionales **19**

3.1.7 Pruebas de rendimiento **20**

3.1.8 Pruebas de regresión **20**

3.1.9 Pruebas de estrés **20**

3.1.10 Pruebas de usabilidad **20**

3.1.11 Pruebas unitarias **20**

3.1.12 Pruebas de extremo a extremo **20**

3.1.13 Pruebas de humo **21**

3.2 Aplicaciones web **21**

3.3 Software de la aplicación **23**

3.3.1 Servlets **23**

3.3.2 Script java **24**

3.3.3 Consultas con PHP **24**

3.3.4 Servidores web **24**
3.4 Bases de datos **24**
3.5 Protección de los datos **26**
3.6 Ley de derecho del olvido **27**
3.7 Cifrado de los datos **28**
3.8 Prueba de software **29**
CAPÍTULO 4. DISEÑO Y DESARROLLO DEL SISTEMA ***30***
4.1 Análisis y requerimientos de la aplicación web **30**
4.1.1 Requerimientos funcionales y no funcionales **30**
4.1.2 Casos de uso **32**
4.1.3 Especificaciones de casos de uso **34**
4.1.4 Diagrama relacional **36**
4.1.5 Diagrama de clases **37**
4.1.6 Diseño de la interfaz **38**
4.2 Desarrollo de la aplicación web **43**
CAPÍTULO 5. PRUEBAS Y RESULTADOS ***56***
5.1 Pruebas por exploración **56**
5.2 Resultados **59**
CAPÍTULO 6. CONCLUSIONES Y TRABAJO ***62***
6.1 Conclusiones **62**
6.2 Trabajo a futuro **63**
CAPÍTULO 7 BIBLIOGRAFÍA ***64***
CAPÍTULO 8 ANEXOS ***66***
Anexo A ***66***
Anexo B ***66***
Anexo C ***67***
Anexo D ***67***
Anexo E ***68***
Anexo F ***68***
Anexo G ***69***
Anexo H ***69***
Anexo I ***70***

CAPÍTULO 1. INTRODUCCIÓN

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 compartir estrategias de protección a los usuarios con base en la revisión de una auditoría la cual apoya al usuario en evitar algún tipo de problemática que lo lleve a ser víctima de un delito cibernético. La mínima importancia que le otorgamos a la seguridad de nuestros sistemas es la causante de muchos de los delitos a los que quedamos expuestos, pero mediante el avance tecnológico van surgiendo métodos de robo, espionaje o daños a nuestro sistema, por lo cual, es necesario que un sistema o una aplicación web o cualquier tipo de sistema tecnológico que las organizaciones usen, deba ser auditado.

El proyecto de tesis presenta una aplicación web con un análisis completo en las áreas corporativas de la empresa. La aplicación web va llevando al usuario a la revisión de su organización con base en un cuestionario que lo ayuda a evaluar cada aspecto de sus sistemas internos, como las contraseñas que colocan en sus diferentes accesos, para que cumplan con estándares establecidos para una buena seguridad. El cuestionario también lleva al usuario a una revisión de las funciones de QoS, respaldos, verificación de datos personales, políticas de seguridad, seguridad física y programas.

Cuando el usuario obtiene el análisis completo, se le otorga al usuario una evaluación de cómo están sus sistemas tecnológicos, mediante un informe con las respectivas sugerencias que le permitan implementar seguridad en sistemas y disminuir un porcentaje de vulnerabilidad en los sistemas, mejorando la seguridad tecnológica de la organización.

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

En Capítulo 2 se presenta el Estado del arte, el cual nos muestra los antecedentes del 2025 donde se da a conocer un incremento en la tecnología, por consecuencia, los delitos cibernéticos también aumentaron. Además, se dan a conocer algunas aplicaciones con el mismo objetivo de Security and Audit I&G (SAIG) como son: Benchmark Gensuite , WinAudit, Planning Advisor, Auditoría. Cada una se basa en el objetivo de proteger al usuario con base en varios métodos de recopilación de datos.

En el Capítulo 3 se presenta el Marco teórico, donde se describe la metodología para desarrollar la aplicación Security and Audit I&G (SAIG), donde se presentan las fases de análisis, planificación, formulación, modelado, producción y test.

Basándose en la metodología, se muestra una estructura sobre los menús de la aplicación Security and Audit I&G (SAIG), para dar un informe de la evaluación mediante los datos obtenidos.

La aplicación web se define como un intercambio de información que proporciona servicios de manera remota, los programas usados para la aplicación de SAIG son: *Servlets, script java, consultas de php, servidores web y base de datos.*

También se menciona la protección de datos del usuario, encriptado de datos por seguridad, la realización de pruebas de software para la valoración de su respectivo funcionamiento, los tipos de pruebas para evaluar el software.

En el Capítulo 4 se presenta el diseño y desarrollo del sistema, el análisis y requerimientos de la aplicación Security and Audit I&G (SAIG) mencionando cada uno de ellos como el inicio de sesión entre otros, también se presentan se presentan los caso de uso, donde observamos la estructura de los menús referente a la aplicación, los diagramas de clases y diagrama de secuencias.

1.2 Planteamiento del problema

Los delitos cibernéticos siempre han existido para dañar a los usuarios en diversas modalidades, con el aumento de las nuevas tecnologías, también los delitos se van incrementando con nuevas funcionalidades.

Por tal motivo, se propone una solución a esta problemática, a través de la

implementación de una plataforma web llamada Security and Audit I&G (SAIG) totalmente intuitiva que puede brindar apoyo a los departamentos de TIC de cualquier organismo, mediante cuestionarios para el pronto análisis de ellos y mostrar las sugerencias para protección del usuario. Se pretende analizar cada departamento en el cumplimiento de ciertos requisitos para aumentar la protección de los datos.

1.3 Justificación

Actualmente, hay muchas funcionalidades con la tecnología que pueden estar asociadas a buenas o malas acciones. Por lo tanto, se define mediante la ética de cada persona, la utilización de la tecnología, con forme está pasando el tiempo los investigadores realizan publicaciones sobre descubrimientos tecnológicos, con el fin de dar a conocer diversos temas para mejorar de manera personal o profesional también se nos presentan herramientas con el fin de realizar las tareas de una manera más eficiente y efectiva.

Con el avance de la tecnología, los ciberdelincuentes están al día, para vulnerar el software. El primer ciberdelincuente fue Nevil Maskelyne en 1903, se interceptó la primera transmisión de telégrafo inalámbrico. En la década de los 70´s surgió el primer *malware llamado "Creeper",* un software que se replicaba así mismo. Se eligió este tema debido al gran mundo de la tecnología y los avances que ha tenido la misma, nos ayuda a mejorar en muchos ámbitos o hacer acciones indebidas, esto conlleva a la ética de cada persona, es un tema muy amplio ya que con el exceso de información encontrada y las herramientas podemos obtener los conocimientos para vida diaria o en el caso profesional. Con el gran mundo de la ciberseguridad, se da a conocer los delitos que existen como la suplantación de identidad, los virus, ransomware entre otros, con dicha aplicación web se pretende salvaguardar a los usuarios que ocupan nuestras plataformas ya sean de estudio, trabajo, entre otros.

El objetivo principal de este proyecto es enseñar a la población el cómo prevenir alguna circunstancia de riesgo para el usuario, como es el robo de información, que es uno de los principales delitos, por ello, se intenta dar medidas de precaución para no caer en algún delito que afecte económicamente o en lo personal.

1.4 Objetivo general

Diagnosticar la vulnerabilidad del acceso informático en una institución educativa y una empresa, a través de una aplicación web diagnóstica, para mitigar los posibles ataques cibernéticos.

1.5 Objetivos Específicos

- Analizar exhaustivamente la bibliografía sobre los tipos de auditorías.
- Analizar criterios de posibles ataques al sistema.
- Modelado de la base de datos requerida.
- La implementación de una aplicación web donde permita la realización de una auditoría informática.
- Evaluar los sistemas informáticos, instalaciones y programas, de una empresa y una universidad con la aplicación web realizada.
- Detallar los resultados obtenidos en la auditoría informática.
- Recomendar ciertos cambios para evitar la vulnerabilidad de ciertas áreas de la empresa y la universidad.
- Generar un reporte final de los resultados obtenidos en la auditoría informática.

CAPÍTULO 2. ESTADO DEL ARTE

2.1 Antecedentes

Con el desarrollo de las tecnologías, se han ido generando beneficios y amenazas para cada usuario, se espera que para el año 2025 sean 300 millones de dispositivos conectados en México [1].

Surgirá un crecimiento acelerado de un 70% de dispositivos para 2025, esto requiere más del 30% del poder computacional de centros de datos, más del 94% de dicho poder estará en la nube [1].

Con este surgimiento también se presentan más riesgos para los usuarios, en México, más de 33 millones de personas fueron afectadas por el cibercrimen en 2017, en otras palabras, de cada cuatro personas, una tiene la probabilidad de ser afectada por algún tipo de delito cibernético. Se calculó que en el 2019 las pérdidas por ciberataques fueron de hasta 2 billones de dólares a nivel mundial [1].

Por la situación de contingencia que se vivió, las industrias y todas las áreas dedicadas a la educación y más se encontraron en una modalidad en línea, y se enfrentaron a la necesidad de analizar las situaciones individuales de cada empresa u organización con respecto a las vulnerabilidades en el área de ciberseguridad, es por ello que es de mayor prioridad realizar un testeo de dichas vulnerabilidades, las empresas corrieron el riesgo de estar expuestas a algún ataque en sus sistemas, al igual que entonces, hoy en día pueden sufrir la sustracción o robo de su información, que es valiosa e importante para ellos y para todos. Se espera que, con la herramienta propuesta en este trabajo, se evite o mitiguen algunos o los más posible los ataques a los que estén expuestos, ya que el robo de información es una latente amenaza, por todo ello, se considera relevante dar a conocer o proponer algunas sugerencias a empresas u organizaciones educativas de cómo reducir el riesgo de ser hackeados o hasta estafados. Por todo lo anterior, hay motivos para realizar el análisis de una auditoría informática basada en una implementación diagnóstica para esas áreas afectadas.

2.2 Aplicaciones similares

Actualmente existen aplicaciones similares a SAIG, aun así, cada una tiene varios distintivos el propósito que tienen es prevenir un ciberdelito ya que se pierde información, ya sea a un usuario o empresa.

A continuación, se menciona una breve descripción para dar a conocer cada una de ellas:

2.3 Benchmark Gensuite

Benchmark Gensuite es un conjunto de soluciones basadas en la nube para organizaciones y funciones para gestionar riesgos y lograr el cumplimiento. La suite ofrece aplicaciones funcionales integradas e intuitivas disponibles para un despliegue rápido e inmediato del retorno de inversión [2].

Gensuite ofrece más de 65 aplicaciones web que abarcan todo el aspecto de salud, seguridad y medio ambiente , con capacidades adicionales para funciones relacionadas como calidad, contraloría , abastecimiento responsable, seguridad / gestión de crisis y cumplimiento de productos.

2.4 WinAudit

WinAudit permite inspeccionar el sistema para obtener un informe muy completo y detallado sobre todo el hardware y software y el sistema operativo [3].

El análisis de las categorías se subdivide en subcategorías como servicio, archivos del sistema, pantallas, ejecutables, variables de entorno, programas en ejecución, BIOS, programas de inicio o estadísticas de usuario, se puede activar o desactivar las casillas de verificación [3].

2.5 Planning Advisor

Planning advisor se basa en riesgos que simplifican el proceso de planteamiento

de auditoría [4]. Sus funciones con las que cuentan son:

- Automatiza el enfoque de planeamiento de auditoría para ahorrar tiempo.

- Definir y ponderar factores de riesgo para reflejar los aspectos de la auditoría.
- Brindar mayor seguridad a los gerentes principales, a la dirección y al comité de auditoría, dando a conocer las áreas de alto riesgo para ser revisadas.
- Actualizar de forma continua el plan de auditoría para solucionar los problemas generados.
- Priorizar los riesgos y orientar los recursos necesarios a las áreas de alto riesgo.

2.6 Auditoría

La auditoría permite a las compañías administrar integral del proceso de acuerdo con las mejoras globales y las normas o estándares de gestión [5].

Auditoría basada en riesgos.
Automatiza los procesos de auditoría o autocontrol con un enfoque de administración de riesgos.

La Tabla 1 muestra la comparativa de las aplicaciones antes mencionadas, la tabla muestra las características que cumplen y las que no se considera para cada una de las aplicaciones.

Tabla 1 Comparativa de aplicaciones similares

CARACTERÍSTICAS	BENCHMARK GENSUITE EHS	WINAUDIT	PLANNING ADVISOR	AUGE SOFTWARE AUDITORIA
Acceso móvil	X	X	X	X
Alertas y notificaciones	X	X	X	X
Auditoría de elementos de control	X	X	X	
Creación de informes / Análisis	X	X	X	X
Detección de etiquetado de servicio		X		
Evaluación de riesgos	X	X		X
Gestión de auditorías	X			
Gestión de conformidad	X		X	X
Gestión de problemas	X			X
Gestión de tareas	X	X		X
Mantenimiento de las auditorías		X	X	
Planificación de auditorías			X	X

CAPÍTULO 3. MARCO TEÓRICO

3 Metodología

La metodología para realizar este proyecto de tesis estuvo basada en un análisis, un modelado, un diseño, la implementación y la evaluación de una aplicación web en la auditoría informática en una empresa y una institución educativa. Esto involucra realizar un análisis de los tipos de auditorías, analizar los criterios, evaluar los sistemas informáticos por medio de la aplicación web, detallar los resultados obtenido en dicha evaluación, creación y modelado de la base de datos, 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 este proyecto se utilizarán las siguientes fases basándose en la ingeniería web:

FASES

Fase 1 de Análisis:

En esta etapa, se define la composición de una auditoría de red para evaluar en instituciones y/o empresas con resultados, se evalúa el buen funcionamiento de la aplicación y se da a conocer el objetivo principal, teniendo en cuenta los resultados se realiza la aplicación correcta.
A continuación, en la Ilustración 1se muestra la representación de una empresa que será requerida para hacer el análisis de la aplicación SAIG.

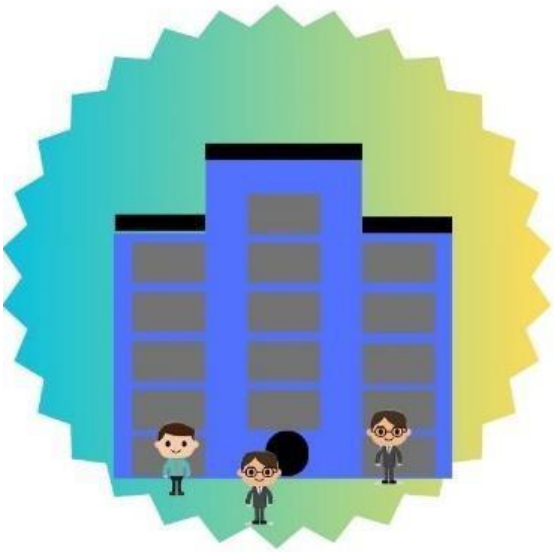


Ilustración 1. Empresa con los usuarios a auditar.

Fase 2 Planificación:

En esta etapa, se planifican los tiempos de diseño, implementación y entrega. Se realiza un control de tiempos de diseño para la realización correcta de la aplicación y corregir los errores del tiempo de desarrollo del software y no afectar la fecha final de entrega y cómo se implementaría para una correcta interpretación al usuario. A continuación, la Ilustración 2 muestra el manejo de tiempos para el diseño ya que se tiene un reporte de entregas.

Actividad	Fecha inicio	Fecha fin	Duración en días
Análisis:	4/01/20	10/01/21	7 días
Planificación:	11/01/21	13/01/21	3 días
Formulación:			
Simulador de aplicación web módulo 1 Preparación auditoria.	14/01/21	17/01/21	4 días
Simulador de aplicación web módulo 2 Desarrollo de la auditoria.	18/01/21	20/01/21	3 días
Simulador de aplicación web módulo 3 Informe final.	21/01/21	23/01/21	3 días
Modelado:			
Casos de uso módulo 1 Preparación auditoria.	24/01/21	25/01/21	2 días
Diseño de módulo 1 Preparación auditoria	26/01/21	28/01/21	3 días
Casos de uso módulo 2 Desarrollo de la auditoria.	29/01/21	30/01/21	2 días
Diseño de módulo 2 Desarrollo de la auditoria.	31/01/21	02/02/21	3 días
Casos de uso módulo 3 Informe final.	03/02/21	04/02/21	2 días
Diseño de módulo 3 Informe final.	05/02/21	07/02/21	3 días
Producción:			
Modelado base de datos	8/02/21	09/02/21	2 días
Integración de la estructura de la base de datos resultante	10/02/21	12/02/21	3 días
Módulo 1 de la aplicación web (3 submenús con sus respectivos sub-submenú	13/02/21	13/03/21	30 días
Módulo 2 de la aplicación web (2 submenús)	14/03/21	27/03/21	14 días
Módulo 3 de la aplicación web (4 submenús)	28/03/21	24/04/21	28 días
Test:			
Pruebas y correcciones de interfaz y funcionalidad Módulo 1	13/03/21	20/03/21	7 días
Pruebas de usabilidad Módulo 1	26/04/21	27/04/21	2 días
Pruebas y correcciones de interfaz y funcionalidad Módulo 2	27/03/21	3/04/21	7 días
Pruebas de usabilidad Módulo 2	28/04/21	29/04/21	2 días
Pruebas y correcciones de interfaz y	25/04/21	30/04/21	6 días

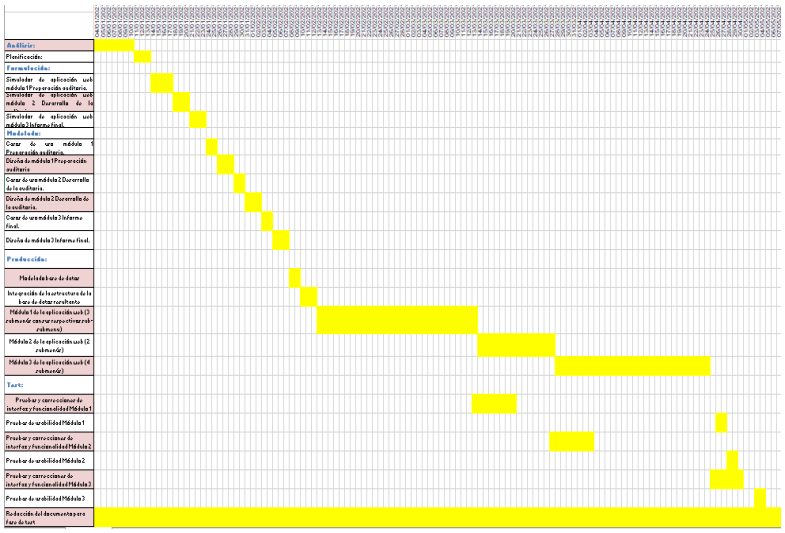


Ilustración 2. Reporte de tiempos y fechas de la planificación.

Fase 3 Formulación:

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

- La **preparación auditoría** se divide en 3 submenús: Auditoría de sistemas en desarrollo, Auditoría de instalaciones informáticas y de aplicaciones.
  - ✔ Auditoría de sistemas en desarrollo se divide en 5 sub-submenús de los cuales son: Contraseñas en sistemas, Definición de funciones, Qos, Respaldos, Datos personales.
  - ✔ Auditoría de instalaciones informáticas se divide en 3 sub-submenús los cuales son: Contraseñas en instalación, Políticas de seguridad, Seguridad física.
  - ✔ Auditoría de aplicaciones se divide en 1 sub-submenú que es: Programas.

- **Desarrollo de la auditoría** se divide en dos submenús que son: Propuesta de herramientas y Propuestas de mejoras usando herramientas.

- **Informe final** se divide en 4 submenús: Análisis, Recomendaciones, Crear informe e Imprimir informe.

A continuación, en la Ilustración 3 se muestra los menús con los que contiene la aplicación web Security and Audit I&G (SAIG).

Ilustración 3. Menú principal de la aplicación Security and Audit I&G (SAIG)

Fase 4 Modelado:

En esta etapa se trabajó con la estructura de la aplicación, casos de uso y diseño. Se realizó el diseño de las pantallas de la aplicación, también la estructura de estas para un eficiente manejo de la aplicación con el usuario. En la Ilustración 4 se muestra el caso de uso principal de la aplicación Security and Audit I&G (SAIG). Además, se muestra una pantalla de ésta, con los menús de informe final.

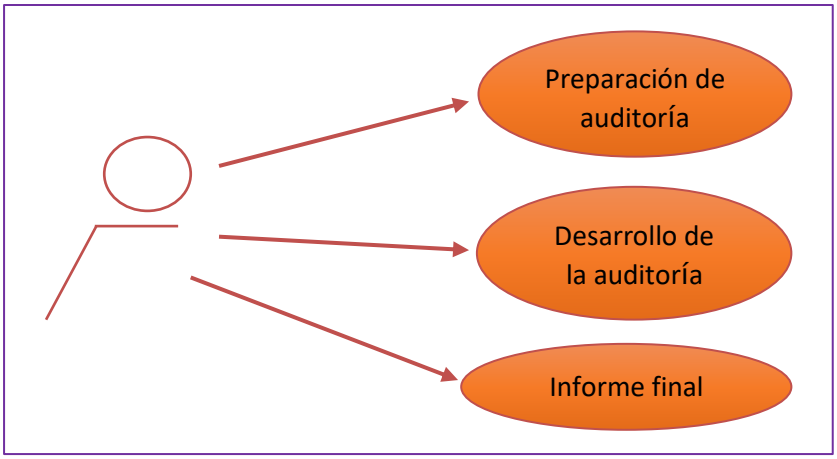


Ilustración 4. Caso de uso y pantalla de informe final de la aplicación Security and Audit I&G (SAIG).

Se muestra en la Ilustración 5 el menú del supervisor de análisis de la aplicación Security and Audit I&G (SAIG) que está compuesto de dos botones: Gestión de seguridad y Gestión auditoría. En el presente trabajo de tesis realiza el análisis de auditoría informática.

Ilustración 5 Menú del supervisor de análisis del sistema.

Fase 5 Producción:

En esta etapa se integró la estructura de la base de datos, la aplicación web y se realizaron las pruebas del análisis de auditoría informática. Se describe la composición de la base de datos en la aplicación con las diversas tablas requeridas, también se realizan pruebas con cuestiones de la vida real para un mejor análisis de la auditoría informática. En la Ilustración 6 se muestra el uso de bases de datos para un almacenamiento correcto de información y la producción de la aplicación con pantallas reales.

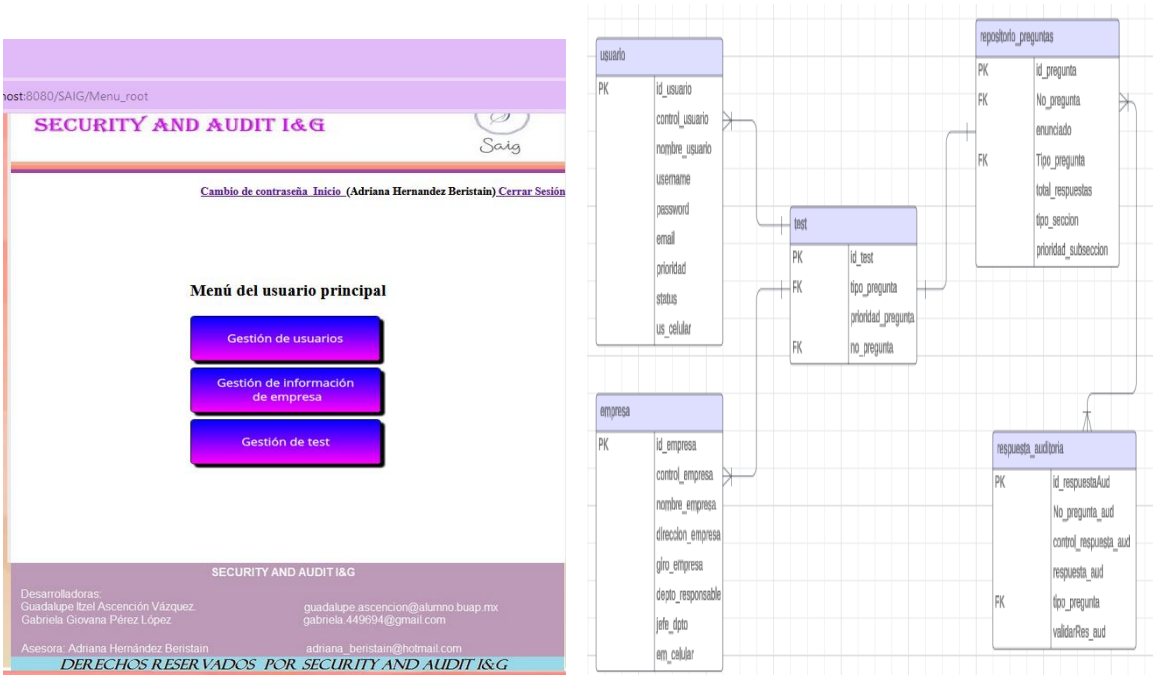


Ilustración 6. base de datos requerida y pantalla de la aplicación Security and Audit I&G (SAIG)

Fase 6 Test:

En la última etapa, se realizan pruebas de evaluación para correcciones en la interfaz y evaluación de la ejecución de la aplicación web. Las pruebas se realizan con usuarios finales para tener un mejor análisis del comportamiento de la aplicación con esto se confirma la eficacia y la navegación correcta de la aplicación desarrollada. Por último, en la Ilustración 7 hacemos referencia a la aplicación terminada y en la ejecución de esta por los usuarios para realizar las evaluaciones pertinentes.

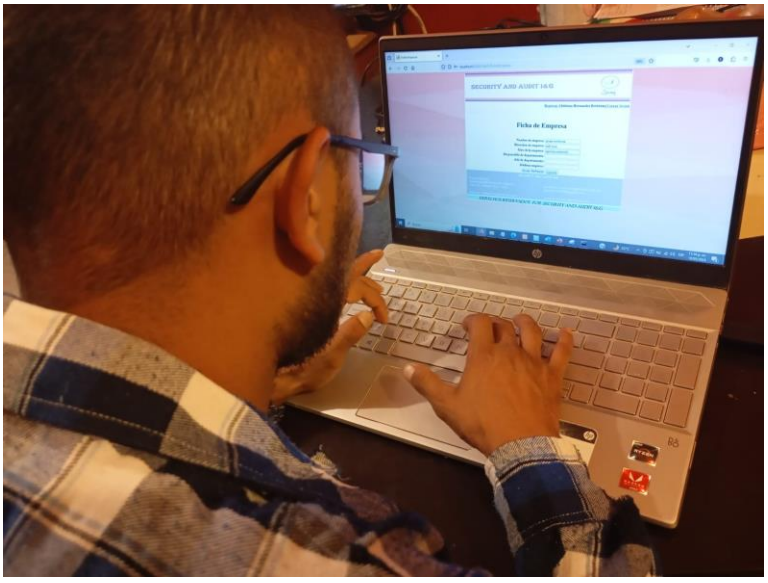


Ilustración 7. Pantalla de la aplicación Security and Audit I&G (SAIG) , aplicada a usuario.

3.1 Tipos de pruebas de software

Existen diferentes tipos de pruebas de software, cada uno cuenta con objetivos específicos y estrategias bien definidas, a continuación, se describen.

3.1.1 Pruebas por exploración

Las pruebas por exploración se realiza el aprendizaje del sistema, diseño y ejecución, implica examinar el resultado y utilizarlo para nuevas pruebas. Se ejecutan para tener una mayor exploración en el sistema, poder analizar el pensamiento del tester en tiempo real y son adaptadas en los modelos ágiles [16].

3.1.2 Pruebas por conjetura de fallos

Las pruebas por conjetura de fallos se realizan una lista enumerada de las equivocaciones que pueden surgir mientras desarrollas en sistema, es generar casos de prueba en base a la lista antes generada, para la creación de la lista muchas veces se genera a la intuición de cada persona o con la experiencia con la que se cuenta [17].

3.1.3 Pruebas de aceptación

Las pruebas de aceptación son pruebas formales donde verifican si un sistema satisface los requisitos del usuario. Es necesario ejecutar toda la aplicación durante las pruebas y se centran en replicar las acciones de los usuarios, también se mide el rendimiento del sistema y rechazar cambios si no cumplen determinados objetivos[18] [19].

3.1.4 Pruebas de integración

Las pruebas de integración amparan que los componentes o funciones de la aplicación operen de manera conjunta [18] [19].

3.1.5 Pruebas de unidad

Las pruebas de unidad se realizan la validación de cada unidad de software donde funcione correctamente, la unidad es el componente de pruebas más pequeño en la aplicación web [18] [19].

3.1.6 Pruebas funcionales

Las pruebas funcionales verifican las funciones realizando una imitación de los diferentes escenarios, mediante los requisitos funcionales. Las pruebas de la caja negra es una forma más habitual de verificar funciones [18] [19].

3.1.7 Pruebas de rendimiento

Se hacen pruebas del funcionamiento del software bajo varias cargas de trabajo para evaluar el rendimiento en situaciones reales [18] [19].

3.1.8 Pruebas de regresión

Las pruebas de regresión son la verificación de nuevas características para observar que no ocasionan degradación en la funcionalidad. Las pruebas de cordura se utilizan para verificar menús, funciones y comandos a nivel superficial, por si no se cuenta con tiempo para realizar una prueba de regresión completa [18].

3.1.9 Pruebas de estrés

Pruebas de estrés conoce la tensión que puede soportar el sistema para prevenir antes de que falle [18].

3.1.10 Pruebas de usabilidad

Pruebas de usabilidad realiza la validación de qué tan bien el cliente puede usar el sistema o en este caso la aplicación web para completar una tarea [18].

3.1.11 Pruebas unitarias

Pruebas unitarias se realizan cerca de la fuente de la aplicación. Consiste en probar métodos y funciones individuales de las clases, componentes o módulos que usa la aplicación web. Son muy baratas de automatizar y se pueden ejecutar rápidamente por medio de un servidor de integración continua [20].

3.1.12 Pruebas de extremo a extremo

Las pruebas de extremo a extremo se realiza la réplica del comportamiento del usuario en un entorno de la aplicación web. Verifican diversos flujos de usuarios que funcionen correctamente, pueden ser métodos muy sencillos como son cargar la aplicación web o

un inicio de sesión, también hay más complejos como la verificación de notificaciones de correo electrónico, pagos en línea, etc [19].

3.1.13 Pruebas de humo

Las pruebas de humo son pruebas básicas, se realizan para comprobar el funcionamiento de la aplicación web. Se utilizan para ejecutarse rápidamente, el objetivo principal es ofrecer seguridad de que las principales funciones del sistema funcionen correctamente como se pensaron.

Con la prueba de humo se puede hacer una compilación nueva para decidir si es posible ejecutar o no pruebas más caras o inmediatamente después de una implementación para verificar que la aplicación funcione correctamente [19].

3.2 Aplicaciones web

La aplicación web es un software que se ejecuta en el navegador web. Las empresas tienen que intercambiar información y proporcionar servicios de forma remota. Las utilizan para comunicarse con los clientes cuando se requiera y es una forma segura.

En la Ilustración 8 muestra el funcionamiento de una aplicación web del cliente-servidor, en algunos casos se presenta varios clientes conectados a un solo servidor mediante el proceso se tienen que usar protocolos específicos para la comunicación e intercambio de datos.

Se caracteriza por la implementación de una arquitectura distribuida para optimizar recursos y favorecer los accesos para usuarios finales.
Su estructura se basa en:

Comportamiento el cliente:

- Primero el navegador web (Browser) envía una solicitud (Request).
- Después el servidor envía una respuesta donde incluye un código que el navegador web (Browser) entiende.
- Por último, el navegador web (Browser) comprende el código enviado para el servidor y desarrolla la tarea solicitada.

Comportamiento el servidor:

- Primero el navegador web (Browser) envía una solicitud (Request).
- A continuación, el servidor ejecuta una aplicación para efectuar una determinada tarea.

- El servidor envía el resultado de la misma aplicación al cliente.
- Finalmente, el navegador web (Browser) muestra el resultado que recibe del servidor.

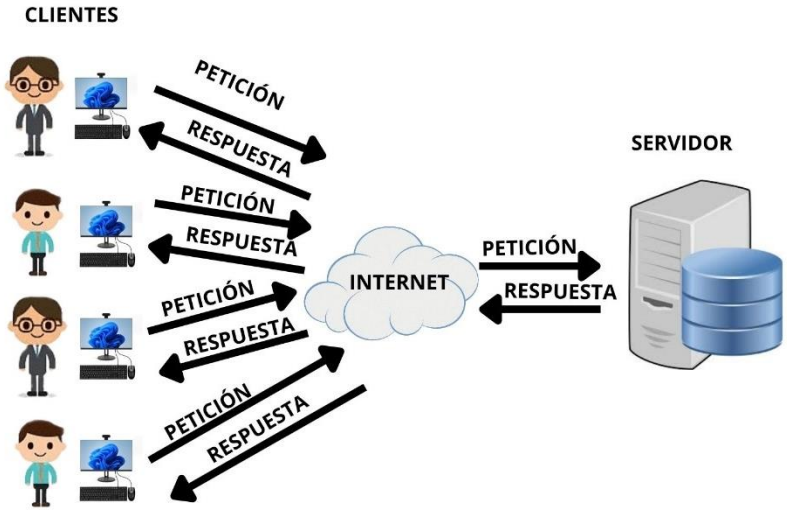


Ilustración 8. Esquema representativo del cliente - servidor.

Las desventajas presentadas son:

- El uso de aplicaciones web requiere navegadores compatibles con ella y a veces hay que tener las extensiones y actualizaciones necesarias para su uso.
- A diferencia de las aplicaciones descargables, su creador puede eliminarlas y dejar al usuario sin ella, en cambio las descargadas pueden seguir funcionando independiente de su desarrollo.
- El usuario no puede elegir la versión de la aplicación que sea usar, simplemente existe una sola disponible online.
- El creador de la aplicación web conozca los movimientos y acciones del usuario en la aplicación web puede ser negativo para la privacidad.
- Ofrecen menos funcionalidades que las aplicaciones descargables, a causa de las limitaciones de los navegadores a los que se accede desde los sistemas operativos.
- Las posibilidades dependen de otros, un ejemplo son los que proveen el servicio de conexión a internet y lo que puede ir surgiendo [6].

Existen cuatro tipos de aplicaciones web de los cuales son:

- Aplicaciones web estáticas son únicamente las que muestra un único contenido y no existe ningún tipo de interacción por ejemplo, una aplicación web empresarial donde muestra solo los teléfonos y dirección de la misma.
- Aplicaciones web dinámicas el usuario puede interactuar con la aplicación como por ejemplo, se puede ingresas a sus cuentas, la modificación de diversos

parámetros entre otros.

- Aplicaciones web Tienda Online o E-Commerce forma una parte de las aplicaciones web dinámicas, sin embargo, cuenta con mas funciones de las cuales son comercio electrónico, pagos en línea , direcciones de envió, etc.
- Aplicaciones web Gestor de contenido están diseñadas para que un administrador publique contenido sin la necesidad de tener conocimientos mayores en la programación de la misma.

3.3 Software de la aplicación

Para la realización de la aplicación Security and Audit I&G (SAIG) se ocuparon diversas herramientas, ya sea software de los cuales son: Servet, Java script , Consultas de php, Servidores web, Base de datos y a continuación se menciona una breve descripción de cada uno de ellos también de requirió hardware en donde fue instalada la aplicación web Security and Audit I&G (SAIG).

3.3.1 Servlets

Los servlets son programas de Java, que utilizan la interfaz de programación de aplicaciones (API) de Servlet Java. Se empaquetan los *servlets* en un archivo *WAR* o un módulo web para su demostración en el servidor de aplicaciones.

Además, los *servlets* se ejecutan en un servidor web habilitado para Java, amplían las funciones de un servidor web, es una forma similar a como se ejecutan *applets* en un navegador, y amplían las funciones de un navegador.

De igual forma, los *servlets* pueden dar soporte al contenido dinámico de páginas web, proporcionando acceso a base de datos y dar servicio a varios clientes al mismo tiempo y filtrar datos.

El navegador (Cliente) pide una página al servidor HTTP es un contenedor de *servlets.* Procesa los argumentos de la petición, en otras palabras, el contenedor de *servlets* delega la petición a un *Servlet* en particular elegido de entre los *servlets* que contiene.

¿Quién? Se encarga de generar el texto de la página web donde se entrega al contenedor.

El contenedor devuelve la página web al navegador (Cliente) que la solicitó, en HTML. Se encuentra en una arquitectura Cliente – Servidor para utilizar *servlets* es con *Apache Tomcat* [7].

3.3.2 Script java

Script java es un lenguaje de programación o de secuencias de comandos, donde los desarrolladores utilizan para realizar páginas web interactivas.
Primeramente, actualizar fuentes de redes sociales a mostrar animaciones y mapas interactivos, con las funciones que presentan pueden mejorar la experiencia del usuario en algún sitio web [8].

3.3.3 Consultas con PHP

Las consultas con php son acrónimos recursivos Preprocesador de hipertexto. Es un lenguaje de código abierto muy popular específicamente para el desarrollo web y puede ser incrustado en HTML.

Las consultas usan el modo de almacenamiento en buffer por omisión. Los resultados de las consultas son transferidos inmediatamente del servidor MySQL a PHP, donde después se mantienen en la memoria del proceso de PHP. Con esto permite operaciones adicionales como la cuenta del número de filas y mover el puntero actual del resultado.

Permite emitir más consultas en la misma conexión mientras se trabaja con un conjunto de resultados [9].

3.3.4 Servidores web

El servidor web es un ordenador que almacena, procesa y entrega archivos de sitios web a los usuarios desde un navegador. Están formados por hardware y software utilizan el protocolo de Transferencia de Hipertexto (HTTP) para dar una respuesta a las peticiones de los usuarios de la web realizadas a través de la World Wide Web.

Mediante este proceso los servidores web cargan y entregan la página solicitada al navegador del usuario [10].

3.4 Bases de datos

La base de datos es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Está controlada por un sistema de gestión de bases de datos (por sus siglas en inglés, Sistema de administración de base de datos, DBMS). En conjunto, los datos, el sistema de administración de base de datos y las aplicaciones reciben el nombre de base de datos [11].

Sirve para controlar todas las funciones de un sistema gestor de base de datos a los usuarios, creando la propia base de datos, gestionando su seguridad, actualizar sus contenidos, recuperar los datos y compartirlos entre usuarios.

En la Tabla 2 se muestra una comparativa sobre las características que debe cumplir una base de datos y las características de la aplicación web Security and Audit I&G (SAIG).

Tabla 2 Comparación de características de la base de datos

CARACTERISTICAS DE UNA BASE DE DATOS	BASE DE DATOS	BASE DE DATOS DE LA APLICACIÓN SAIG
Compatibles con varios sistemas operativos y con múltiples accesos simultáneos.	X	X
Permiten una gestión segura de usuarios.	X	X
Flexibilidad al gestionar la información.	X	X
Son independientes al código lo que permite que se pueda utilizar diversos lenguajes de información.	X	X
Independencia de datos.	X	X
Acceso por múltiples usuarios.	X	X
Respaldo y recuperación.	X	
Seguridad	X	X
Son sistema de almacenamiento que contribuyen a reducir la redundancia al mínimo.	X	X
Permiten realizar consultas complejas de diferentes tipos de datos.	X	X

Bases de datos relacionales

La base de datos relacionales es un conjunto de datos que está en tablas formalmente descritas se puede acceder a los datos o volver a ocupar los de diversas maneras sin tener que reorganizarlas.
La interfaz estándar, es el lenguaje de consulta estructurada SQL. Es utilizado para realizar consultas interactivas y también la recopilación de datos.

Cumple con la organización de información de una manera más pequeña mediante identificadores, contrario de las bases de datos no relacionales; también cuentan con un tamaño más robusto para el almacenamiento de información, son menos vulnerables frente a una falla.

En la aplicación web Security and Audit I&G (SAIG) se trabajó con base de datos relacionales por el uso de tablas donde son llenadas con los datos a ocupar, con un buen manejo de acceder a cada una de las tablas en el momento que lo requerimos sin tener la necesidad de reorganizar la información.
Obteniendo fácilmente los resultados, también se usaron por tener un tamaño robusto donde la base de datos puede aumentar sin tener problemas por almacenamiento, y son menos vulnerables al presentarse una falla en el sistema.

3.5 Protección de los datos

Los datos personales es información referente a una persona física, identificada o identificable. También si son anonimizados , cifrados o presentados con un seudónimo aun así, se utilizan para volver a identificar a la persona. Por lo tanto, se tiene el derecho de elegir que se desea compartir con las demás personas tanto por medio tecnológico o personal.

La protección de datos son medidas que tienen como objetivo garantizar la privacidad y seguridad de estos, para evitar el robo de información personal, ya sea de usuarios, empresas o del gobierno, para evitar estafas económicas, suplantación de identidad entre otros delitos. En Security and Audit I&G (SAIG) se considera la protección de los datos, por ello se cifran los datos sensibles que el usuario agrega a la aplicación, además de tener derecho al olvido, se consideró la creación de un botón dentro de la aplicación donde le permite al usuario eliminar sus datos una vez usada la aplicación y tras obtener el reporte final.

3.6 Ley de derecho del olvido

La ley de derecho del olvido se refiere al derecho de una persona en la solicitud de eliminar datos personales ya que considera obsoleta su información o si afecta el desarrollo de sus derechos.

La Dra. María Marvan Laborde da a conocer que, “es la posibilidad de desaparecer de los sistemas de registro de los datos personales, son aquellos datos perjudiciales, son socialmente reprobables, o desfavorecen a la persona, es usado como una fecha de caducidad para no afectar a las personas”.

En México, el derecho al olvido fue añadido en la Constitución del Estado de Durango y en la ciudad de México se cuenta con la ley de protección de datos personales.

Artículo 1. La ley es de orden público y de observancia general en la Ciudad de México, en protección de datos personales en posesión de sujetos obligados.

Tienen por objetivo disponer las bases, principios y los procedimientos adecuados para proteger el derecho que tienen todas las personas al tratarse de sus datos personales.

La senadora a la LXII legislatura del congreso de la unión María Verónica Martínez Espinoza sugiere de la soberanía la iniciativa con proyectos de decreto por el cual se adicionan diversas disposiciones a la ley federal de protección de datos personales en posesión de particulares, a efecto de garantizar el derecho al olvido digital.

Los motivos presentados son:

La carta magna defiende el derecho a la privacidad, en el artículo 16. Es un derecho que absolutamente nadie puede ser incomodado en su persona, familia, domicilio, documentos, o posesiones, a menos que por mandato escrito de las autoridades competentes se funde y motive la causa legal.

El día 5 de Julio del 2010 la ley federal de protección de datos personales en posesión de los particulares, su propósito es salvaguardar la información contenida en

bases de datos, garantizando la privacidad y el derecho a la autodeterminación de las personas. Por primera vez en México se consideran los derechos de Acceso, Rectificación, Cancelación y Oposición .

Los derechos de Acceso, Rectificación, Cancelación y Oposición son derechos de acceder a titulares, rectificar, cancelar u oponerse al tratamiento de datos personales, el titular puede autodeterminar el uso de su información [13] [14].

En la aplicación web Security and Audit I&G (SAIG) se encuentra la ley de derecho al olvido haciendo de su uso con, la creación del botón “Borrar datos sensibles” que se encuentra en dicha aplicación con el objetivo de eliminar la información delicada de las empresas agregada en la base de datos después de la obtención del informe final.
A continuación, en la Ilustración 9 se muestra una pantalla de la aplicación web donde se observa el menú de informe final con sus respectivos botones.

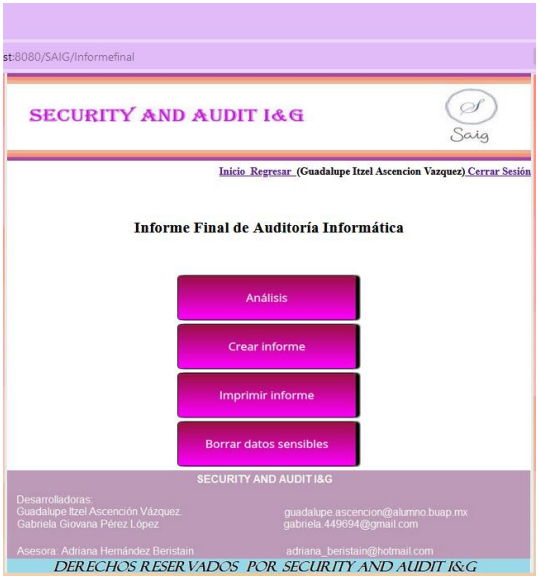


Ilustración 9. Pantalla de menú informe final de auditoría informática.

3.7 Cifrado de los datos

La encriptación es un proceso en el que la información se hace ilegible, alterando el contenido para ocultar datos, con base a esto, se realiza con un algoritmo matemático donde altera los bits de dichas cadenas; existen dos formas de cifrar, por ejemplo, si es texto escrito solo se cambia el orden de las letras basando en un patrón ya determinado, sin que la información digital se altere bit a bit [15].

Se conocen tres tipos de cifrado, los cuales se describen a continuación:

- ✔ Cifrado simétrico: Se ejecuta con una clave secreta cifrada, el emisor y receptor son los únicos que comparten dicha clave, el proceso se realiza con algoritmos

sencillos. Los algoritmos de sustitución o permutación no son recomendables por tal motivo, son los menos seguros.

- ✔ Cifrado asimétrico: Se ejecutan con dos claves secretas cifradas, una es privada y la otra es pública.
- ✔ Cifrado híbrido: Se ejecuta mediante los dos anteriores encriptados, se utiliza la encriptación asimétrica para transmitir la clave simétrica por un canal que no esté protegido.

El Reglamento General de Protección de Datos y la Ley Organica de Protección de Datos Personales y Garantía de los Derechos Digitales obligan al cifrado de los datos si se trata de lo siguiente:

- ✔ Datos protegidos, se encuentran en el Artículo .9 del reglamento general de protección de datos.
- ✔ Datos recolectados para fines policiacos sin el consentimiento del implicado.
- ✔ Datos derivados de violencia de género.
- ✔ Cuando sea dictamine alguna ley.
- ✔ Tratamiento de datos cuando sea aplicado como medida de seguridad.

3.8 Prueba de software

Las pruebas de software son procesos de evaluación y verificación de la aplicación web se analiza si realiza las tareas deseadas correctamente, las ventajas de realizar este proceso es la prevención de errores, reducción de costos en el desarrollo y mejorar el rendimiento para el usuario.

Se analiza que el tipo de prueba a presentar en la aplicación web es la de usabilidad, hay un grupo de usuarios que responden un corto cuestionario para conocer si se comprende el manejo de la aplicación, haciendo intuitiva la aplicación para un buen manejo por el usuario.

CAPÍTULO 4. DISEÑO Y DESARROLLO DEL SISTEMA

4.1 Análisis y requerimientos de la aplicación web

Esta sección pretende mostrar el proceso del diseño para la solución práctica con la aplicación web de una auditoría informática.
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.

4.1.1 Requerimientos funcionales y no funcionales

A continuación, se realiza un análisis y requerimientos de la aplicación web basándose en el desarrollo de esta, para un mejor funcionamiento. La Tabla 3 describe cuatro requerimientos funcionales, mientras que la Tabla 4 muestra cinco requerimientos no funcionales.

Tabla 3 Requerimientos funcionales de la aplicación web SAIG

No. Req.	Tipo de requerimiento	Nombre del requerimiento	Descripción
RF1	Requerimiento funcional del sistema	Inicio de sesión	La aplicación contará con un inicio de sesión, también incluida la seguridad
RF2	Requerimiento funcional del sistema	Gestión de usuarios	La aplicación permite dar de alta a los usuarios con sus respectivos datos, también el eliminarlos, consultar si deseas conocer su información y hasta modificar por algún error en la hora de captura.

RF3	Requerimiento funcional del sistema	Gestión de empresa	La aplicación considera el dar de alta a las empresas con sus respectivos datos, también el eliminarlos, consultar si se desea conocer su información y hasta modificar por algún error en la hora de captura.
RF4	Requerimiento funcional del sistema	Gestión de prueba	La aplicación ofrece dar de alta, baja, consulta y modificación en los tres apartados: configuración de test, repositorio y administración de respuestas.

Tabla 4 Requerimientos no funcionales de la aplicación web SAIG

No. Req.	Tipo de requerimiento	Descripción
RF1	Requerimiento no funcional de soporte	La aplicación estará disponible excepto cuando no tenga conexión al servidor.
RF2	Requerimiento no funcional de privacidad	La aplicación cumple con las leyes de no compartir los datos con otros usuarios.
RF3	Requerimiento no funcional de usabilidad	La aplicación se usará en un entorno de computadora de escritorio o una laptop para una mejor ejecución.
RF4	Requerimiento no funcional de usabilidad	La interfaz tendrá un diseño cómodo y fácil para el usuario siguiendo los requerimientos del usuario.

4.1.2 Casos de uso

A continuación, se muestra el caso de uso extendido de la aplicación web, como se sabe el diagrama de casos de uso apoya en observar el comportamiento que se espera del sistema, en este caso la aplicación web SAIG, se observa lo que el usuario se va a encontrar al clicar en un botón del sistema.

En la Ilustración 10 muestra el diagrama de casos de uso en UML, de la aplicación web SAIG donde tenemos tres menús de Preparación de auditoría, Desarrollo de auditoría e Informe final, para garantizar que el diagrama de casos de uso sea comprensible para todo el mundo de un vistazo, se utilizan elementos estandarizados para elaborarlo.

Elementos principales:

- Actor: puede ser un usuario o puede ser otro sistema, se representa con el dibujo de una figura humana esquemática.
- Sistema: el sistema al que se refiere el caso de uso tiene forma de rectángulo (rectángulo verde en este caso)
- Caso de uso: se coloca como una elipse que incluye texto que describe el proceso de forma breve.

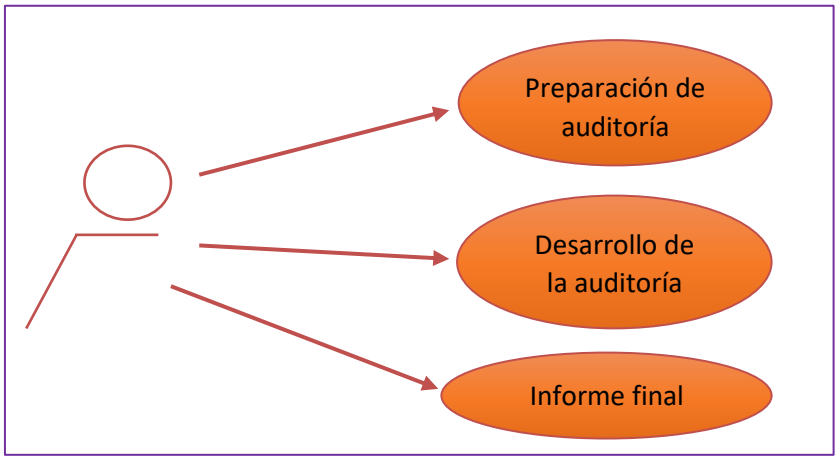


Ilustración 10. Diagrama de casos de uso en UML.

De la aplicación web Security and Audit I & G se muestra a continuación la pantalla de Gestión de auditoría , como se puede observar en la Ilustración 11 Muestra el menú principal de la aplicación. En este menú hay tres opciones que tendrá el usuario: Preparación Auditoría, Desarrollo de la Auditoría e Informe Final.

Ilustración 11 Menú Principal de la aplicación Security and Audit I & G.

En el caso de la Ilustración 12 existen 3 casos de uso: Preparación auditoría, Desarrollo de la auditoría e informe final, cada caso de uso tiene casos extendidos cada uno.

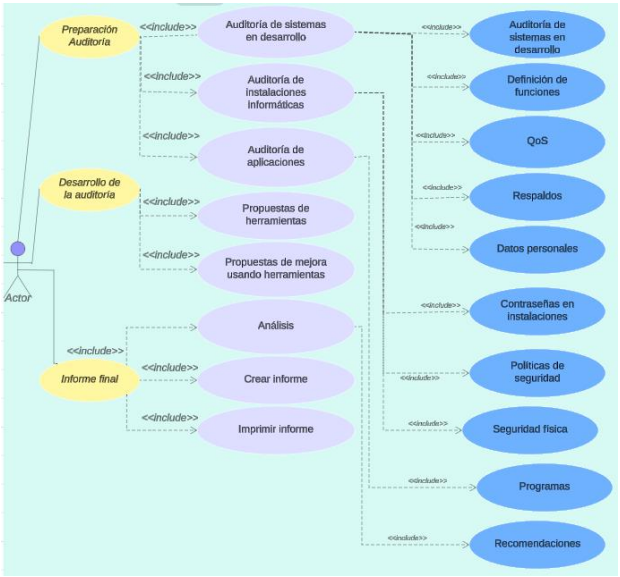


Ilustración 12 Diagrama de Caso de uso extendido

4.1.3 Especificaciones de casos de uso

A continuación, se presentarán tres especificaciones generales de los casos de uso de la aplicación web.

- Preparación de Auditoría.
- En la Desarrollo de la auditoría.
- Informe final.

En la Tabla 5 se muestra la especificación textual de Preparación Auditoría, donde nos da a conocer quién es el actor principal, el interés que se plantea para el área correspondiente, cuáles son las precondiciones que debe cumplir el usuario y el escenario principal donde selecciona en el sistema. Es importante realizar un análisis de cada caso de uso por los errores que puedan surgir en cada sección.

Tabla 5. Especificación textual caso de uso de Preparación de auditoría.

Caso de uso: Preparación Auditoría
Actor principal: Usuario
Ámbito: Campus virtual
Nivel objetivo: Usuario
Stakeholders e intereses:
Usuario: Se quiere conocer el nivel de seguridad de diferentes áreas de la empresa.
Encargado de área: Quiere conocer el nivel seguridad de las diferentes áreas con un informe final para realizar las debidas modificaciones y evitar algún tipo de ataque o daño a la empresa.
precondición: El usuario debe de estar registrado e iniciar sesión.
Garantías mínimas: La aplicación web realizara encuestas por cada submenú requerido.
Garantías en caso de éxito: La aplicación web mostrará un informe final donde evaluará el nivel de seguridad de la empresa.
Escenario principal de éxito:
1. El usuario seleccionara que submenú requiere realizar para la encuesta.
2. El sistema almacenará las respuestas obtenidas por el usuario.
3. El sistema realiza la evaluación de cada una de las respuestas obtenidas.
4. El sistema muestra el informe final del análisis realizado a la empresa sobre su seguridad.

Continuamos con la segunda especificación textual.

En la Tabla 6 se muestra la especificación textual de Desarrollo de Auditoría, donde nos da a conocer quién es el actor principal, el interés en este caso es conocer las propuestas de mejora para las empresas , las precondiciones es seleccionar la opción de Desarrollo de auditoría para lograr ingresar a los submenús y el escenario principal observara las propuestas de herramientas. Es importante realizar un análisis de cada caso de uso por los errores que puedan surgir en cada sección.

Tabla 6. Especificación textual caso de uso de Desarrollo de la auditoría.

Caso de uso: Desarrollo de la Auditoría.
Actor principal: Usuario
Ámbito: Campus virtual
Nivel objetivo: Usuario
Stakeholders e intereses:
Usuario: Se quiere conocer las propuestas de mejora para las empresas.
Encargado de área: Que le muestren ejemplos de propuestas de mejoras con la descripción de cada una.
precondición: El usuario debe elegir la opción de Desarrollo de Auditoría para usar los submenús.
Garantías mínimas: La aplicación web mostrará ejemplos de las herramientas a usar.
Garantías en caso de éxito: La aplicación web mostrará sugerencias para el cuidado de la información
Escenario principal de éxito:
El usuario seleccionará que submenú de propuesta de herramientas.
El sistema mostrará las herramientas almacenadas.
El sistema mostrará información de cada una.

Última especificación textual.

En la Tabla 7 se muestra la especificación textual de Informe Final, donde nos da a conocer quién es el actor principal, el interés en este caso es conocer la evaluación de los cuestionarios que se realizaron a cada usuario, las precondiciones es contestar los cuestionarios de cada área y el escenario principal dará a conocer las recomendaciones otorgadas después del análisis realizado. Es importante realizar un análisis de cada caso de uso por los errores que puedan surgir en cada sección.

Tabla 7. Especificación textual caso de uso de Informe final.

Caso de uso: Informe Final
Actor principal: Usuario
Ámbito: Campus virtual
Nivel objetivo: Usuario
Stakeholders e intereses:
Usuario: Observará el informe final de la evaluación total del cuestionario solicitado.
Encargado de área: Visualizará el informe final completo de la empresa para conocer en donde existe menos seguridad para reforzarla y donde exista buena seguridad para mantenerla así.
precondición: El usuario debe contestar los cuestionarios anteriores
Garantías mínimas: La aplicación web mostrará el informe final de la empresa.
Garantías en caso de éxito: La aplicación web mostrará un informe final donde evaluará el nivel de seguridad de la empresa.
Escenario principal de éxito:
El usuario selecciona si quiere realizar el análisis de los submenús.
El sistema mostrará un submenú de recomendaciones
El usuario selecciona crear informe final de todo lo analizado.
El sistema muestra nos proporciona la opción de imprimir el informe final.

4.1.4 Diagrama relacional

El desarrollo de la aplicación Security and Audit I&G (SAIG) requirió la implementación de una base de datos con el nombre SAIG, compuesta por 5 tablas las cuales son:

- Usuario.
- Empresa.
- Test.
- Repositorio_preguntas.
- Respuesta_auditoría

En la Ilustración 13 se observa cómo está compuesta cada tabla, cuentan con llave primaria y llave foránea, cada tabla se cuenta con las conexiones pertinentes.

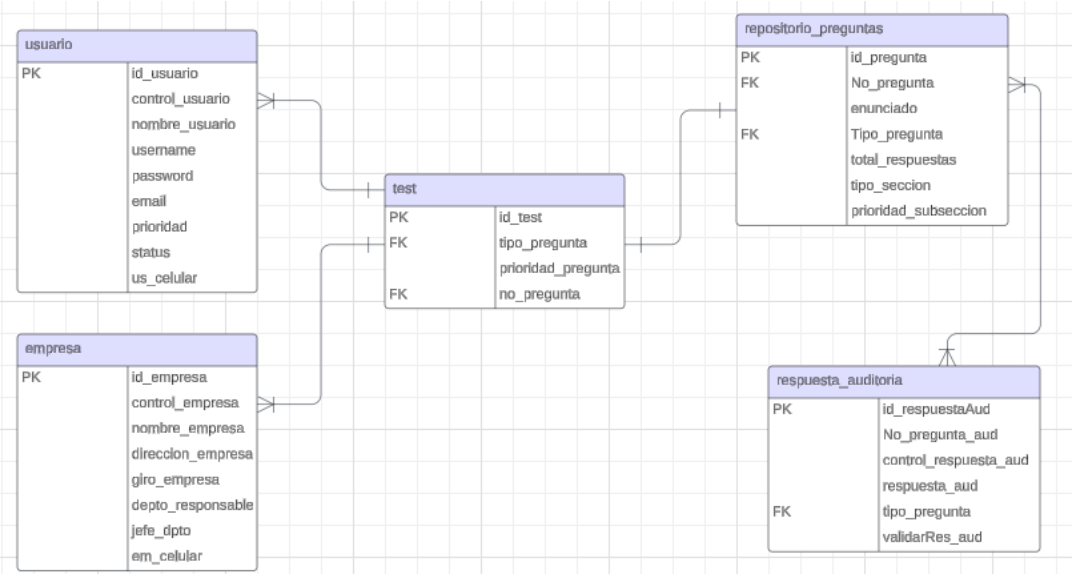


Ilustración 13 Diagrama de la aplicación Security and Audit I&G (SAIG)

4.1.5 Diagrama de clases

A continuación, en la Ilustración 14 se muestra la creación 5 clases que componen la aplicación web Security and Audit I&G (SAIG) de las cuales son:

- Usuario.
- Empresa.
- Test.
- Repositorio_preguntas.
- Respuesta_auditoría

Se muestra en la aplicación Security and Audit I&G (SAIG) las variables requeridas para realizarlo.

En la clase usuario tenemos cuatro métodos de los cuales son: Alta (), Bajas (), Modificar () y Consultas (). Esto conlleva al registro de los usuarios ocupando cada método para realizar diversas tareas las cuales son dar de alta al usuario nuevo, el poder dar de baja algún usuario requerido, el modificar su información por si surgiera algún error en su captura de datos y la consulta de información del usuario.

Clase empresa tiene cuatro métodos: Alta (), Bajas (), Modificar (), Consultas ().Se realiza el alta a la empresa nueva, el poder dar de baja alguna empresa requerida, modificar su información por si surgiera algún error en su captura de datos y la consulta de información de la empresa.

Clase test tiene cuatro métodos: Alta (), Bajas (), Modificar (), Consultas ().Realiza el alta de test en donde se selecciona si la pregunta cuenta con una única respuesta, múltiples respuestas o respuesta abierta y la prioridad de la pregunta donde se divide si es seguridad lógica o auditoría de red. Podemos dar de baja el test si lo deseamos, modificar si se ingresa incorrectamente la información por último, se logra realizar la consulta del número de pregunta.

Clase repositorio_preguntas tiene cuatro métodos: Alta (), Bajas (), Modificar (), Consultas (). Realizamos el alta de la pregunta en donde se ingresa la pregunta , tipo de pregunta, total de

respuestas y tipo de sección, si requerimos dar de baja se requiere seleccionar el número de control de repositorio , modificaciones seleccionamos el numero de control para realizar las modificaciones pertinentes , consultas se visualiza la información de la pregunta .

Clase respuesta_auditoría tiene cuatro métodos: Alta (), Bajas (), Modificar (), Consultas (). Se realizan las altas de

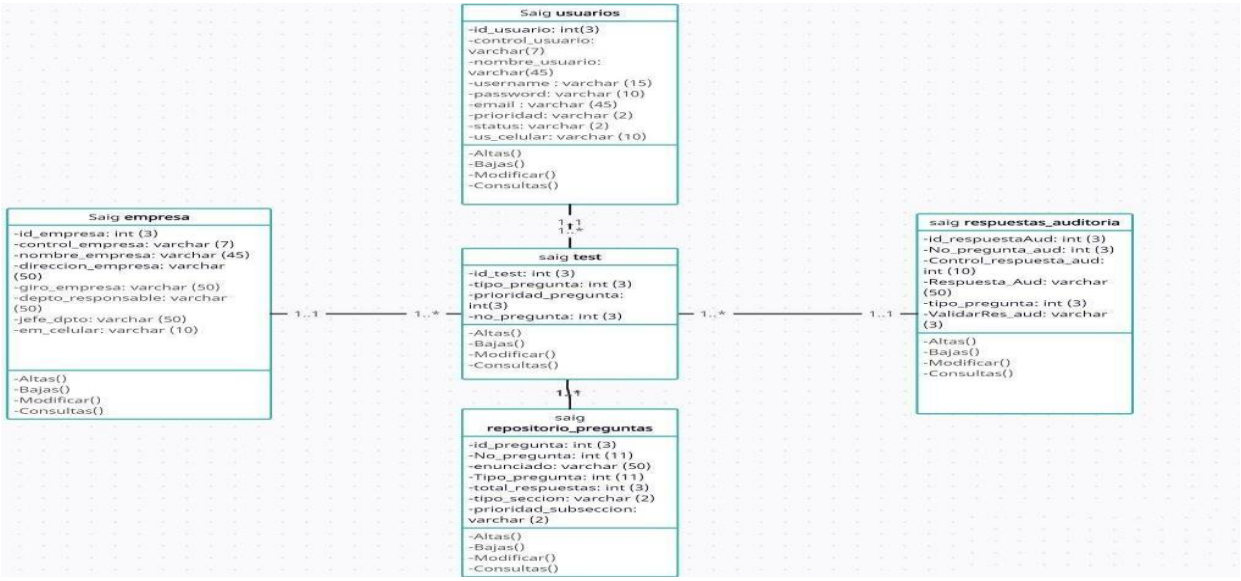


Ilustración 14. Diagrama de clases de aplicación Security and Audit I&G (SAIG).

4.1.6 Diseño de la interfaz

A continuación, se muestra la simulación de la aplicación web Security and Audit I & G, en la Ilustración 15 se puede observar la interfaz del inicio de sesión, compuesta con dos campos de texto (usuario y contraseña), así como dos botones: “ingresar” y “registro”.

Ilustración 15 Pantalla de inicio de sesión.

Si el usuario no está registrado en la aplicación web Security and Audit I & G, en la Ilustración 16 se observa un pequeño registro para tener una cuenta personal de cada empresa, donde llenaremos los campos de nombre de la empresa, usuario, responsable del departamento, departamento, contraseña, confirmar contraseña, correo electrónico también contara con un botón de cancelar por si aún no desea registrar se.

Ilustración 16. Pantalla de Registro.

Después se observa, en la Ilustración 17 el menú principal de la aplicación web Security and Audit I & G donde hay dos botones que son: “seguridad lógica y auditoría de red”.

Ilustración 17 .Pantalla de menú principal de la aplicación.

En el proyecto de tesis solo se realiza la opción de Auditoría de red, por lo que se observa en la Ilustración 18 el menú principal de una auditoría de red se compone por tres módulos el primero es preparación de auditoría, segundo, desarrollo de auditoría y tercero, informe final.

Ilustración 18 Submenú de una Auditoría de red.

Se muestra una prueba del acceso del usuario cuando este desee acceder a la primera opción del menú, en la Ilustración 20 se muestran las opciones que tiene para empezar a verificarse dentro de la organización, en la Ilustración 19 se detallan estas opciones: Auditoría de sistemas, Auditoría de instalación y Auditoría de aplicación (ver Anexo A).

Ilustración 20 Menú de Preparación de Auditoría

Se muestran las opciones del submenú Auditoría de sistemas, Auditoría de instalación y Auditoría de aplicación. En la Ilustración 22 se muestra las siguientes opciones del menú de Auditoría de sistemas: Contraseñas en sistemas, Definición de funciones, Qos, Respaldos y Datos personales, aquí el usuario podrá verificar si su organización si cumple con los lineamientos de la auditoría con respecto a contraseñas en sistemas (ver Anexo B).

. *Ilustración 22 Menú de opciones para Auditoría de Sistemas.*

Muestran las opciones del submenú Auditoría de sistemas, Auditoría de instalación y Auditoría de aplicación, ingresando a la opción de auditoría de instalación en la Ilustración 24 se muestran las opciones de dicho menú de las cuales son: contraseñas en instalaciones, políticas de seguridad y seguridad física (Ver anexo C).

Ilustración 24 Menú de opciones para la Auditoría de Instalación.

El ingreso al botón de Auditoría de aplicaciones, en la Ilustración 26 cuenta con la opción de programas para la evaluación correcta sobre los programas utilizados si cumple con la seguridad apropiada (Ver anexo D).

Ilustración 26 Menú de opciones para la Auditoría de Aplicaciones.

Se accede al botón de Desarrollo de la auditoría, en la que se observa en la Ilustración 28 un submenú que consta de dos opciones propuestas de herramientas y propuestas de mejora usando herramientas para conocer cómo podemos proteger diversos archivos de la organización (Ver anexo E).

Ilustración 28 Menú de opciones para el desarrollo de auditoría.

Se muestra el menú de desarrollo de auditoría clicando en propuesta de mejoras, la Ilustración 30, al seleccionar la opción de mejora con herramientas, se muestran las diversas propuestas de mejoras, mencionando su nombre, la interfaz de esta y, por último, una descripción. También se cuenta con dos botones para visualizar la

herramienta anterior y la siguiente información. Con esto se da a conocer algunas herramientas para el uso de seguridad sobre la información usada en la organización (Ver anexo F).

Ilustración 30 Pantalla de propuesta de mejoras.

El usuario ingresa al botón de informe final, en la Ilustración 32 se muestran tres botones: análisis, creación de informe final e imprimir informe y borrar datos sensibles, ahora se analizan las respuestas de los cuestionarios debidamente llenados para analizarlos y dar el reporte final (Anexo G).

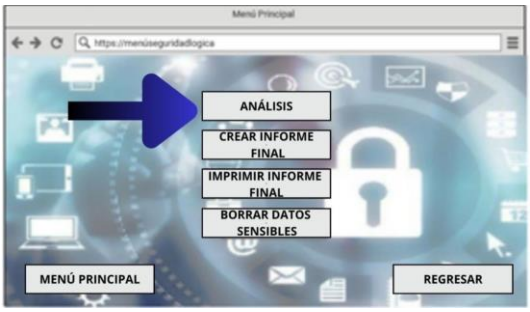


Ilustración 32 Menú de informe final.

Se indica el menú de informe final donde el usuario ingresa a la opción de análisis. Luego en la Ilustración 34 se muestra una pantalla de análisis finalizado en donde muestra el porcentaje de cada auditoría, donde se obtiene el de la organización /un 100% si cumple con todo. Así observaremos donde tenemos un menor porcentaje y debemos de realizar cambios para una mejor seguridad en la organización (Ver anexo H).

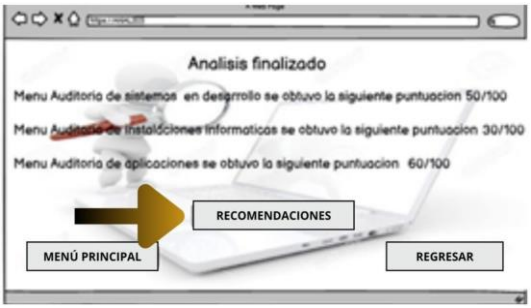


Ilustración 34 Análisis finalizado de cada sección.

Se muestra el análisis finalizado con los porcentajes del menú de auditoría. El usuario tiene que ingresar a recomendaciones, en la Ilustración 36 se muestran recomendaciones donde aparece un listado para sugerirle a las empresas y/o instituciones para tener mejor seguridad en sus sistemas, instalaciones y programas (Ver anexo I).

Ilustración 36 Informe de recomendaciones.

4.2 Desarrollo de la aplicación web

En esta sección se explica cada pantalla de la aplicación SAIG, también con los apartados que se encontrará el usuario para su ejecución.

En la Ilustración 37 se muestra la pantalla principal de Security and Audit I&G (SAIG) en donde se observa la bienvenida, la información de las desarrolladoras de la aplicación, también de la asesora de tesis.

Ilustración 37 Pantalla de bienvenida de la aplicación Security and Audit I & G.

En la Ilustración 38 Muestra dos apartados, usuario y contraseña, cada usuario ingresa con sus datos correspondientes después se da clic en entrar.

Ilustración 38 Pantalla de login a la aplicación Security and Audit I & G.

En la Ilustración 39 nos muestra la bienvenida de la aplicación Security and Audit I & G en donde aparecen los datos del usuario que ingreso a dicha aplicación y el tipo de usuario.

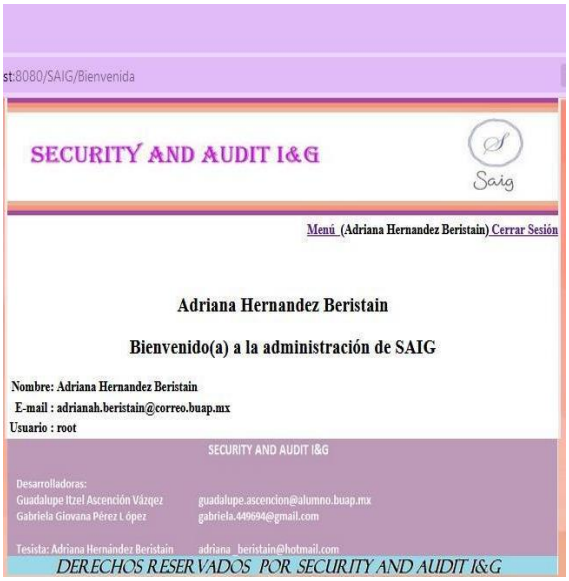


Ilustración 39 Pantalla de bienvenida de la aplicación Security and Audit I & G.

En la Ilustración 40 se muestra el menú del usuario principal con tres botones: Gestión

de usuarios, Gestión de información de empresas y Gestión de test.

Ilustración 40 Pantalla del menú de usuario principal

En la Ilustración 41 se muestran los submenús de gestión de usuarios que constituye el menú de administración de usuarios y cuenta con cuatro botones: Altas usuario, Bajas usuario, Modificaciones usuario, y Consultas usuarios.

Ilustración 41 Pantalla del menú de Administración de usuarios.

En la Ilustración 42 nos muestran la ficha usuario en la cual tenemos que llenar los datos solicitados del usuario como son: Nombre, Nombre de usuario, Contraseña, Correo electrónico, Acciones que puede realizar, Puesto y Teléfono celular.

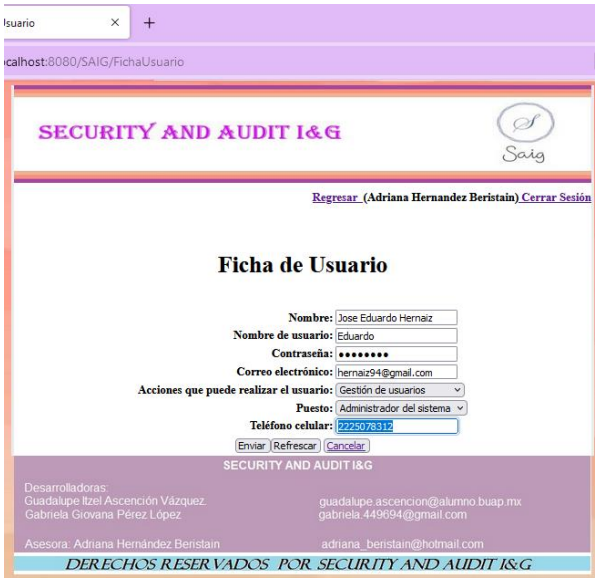


Ilustración 42 Ficha de Usuario

En la Ilustración 43 nos muestra un mensaje del cual nos informa que fue registrado correctamente y a qué número pertenece en la base de datos de usuario.

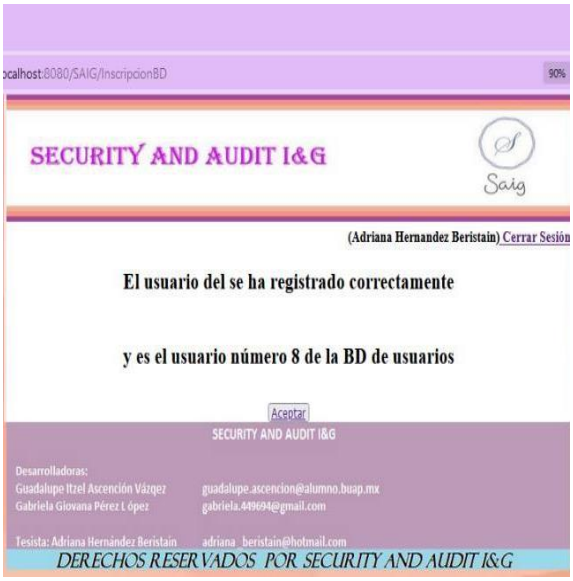


Ilustración 43 Mensaje de registro correctamente del usuario.

En la Ilustración 44 se muestra la pantalla de eliminación de usuario del cual presenta la opción de elegir con el control de usuario, despliega un listado de los usuarios existentes, se selecciona el deseado.

Ilustración 44 Pantalla de Eliminación de usuario.

En la Ilustración 45 se muestra una pantalla de confirmación donde se cuestiona si desea eliminar el usuario seleccionado del que muestra el nombre del usuario.

Ilustración 45 Pantalla de confirmación de eliminación de usuario seleccionado

En la Ilustración 46 se muestra el mensaje de satisfacción que el usuario fue eliminado correctamente.

Ilustración 46 Mensaje de eliminación satisfactoriamente.

En la Ilustración 47 se muestran las opciones para seleccionar el número de control de usuario, desplegando una lista de los usuarios dados de alta.

Ilustración 47 Pantalla de modificación al usuario

En la Ilustración 48 nos muestra la pantalla de modificación de usuario en la cual nos presenta la información del usuario en el lado izquierdo a diferencia de lado derecho en donde podremos modificar la información.

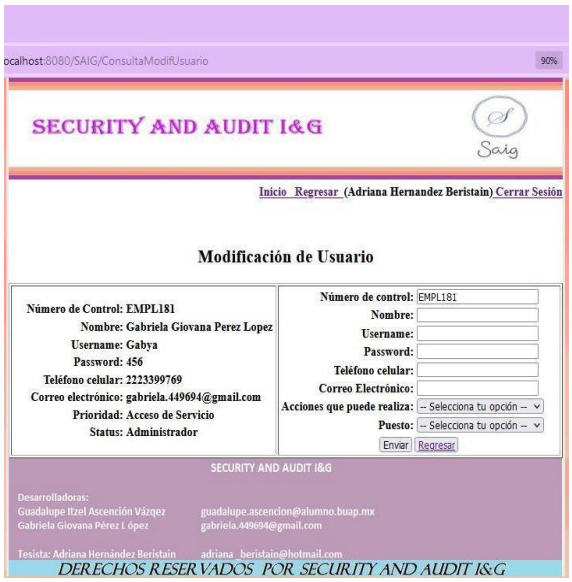


Ilustración 48 Pantalla de modificación del usuario.

En la Ilustración 49 se muestra el mensaje de la correcta modificación del usuario por medio del control de usuario.

Ilustración 49 Mensaje de la realización de la modificación del usuario.

En la Ilustración 50 se muestra la pantalla de búsqueda de usuario, en dicha pantalla se presentan dos opciones a elegir mediante el número de control o por nombre de usuario por si no se recuerda el número de control del usuario deseado.

Ilustración 50 Pantalla de Búsqueda de usuario.

En la Ilustración 51 se muestra la consulta del usuario mediante la opción de control de usuario, se proporciona toda la información de dicho usuario.

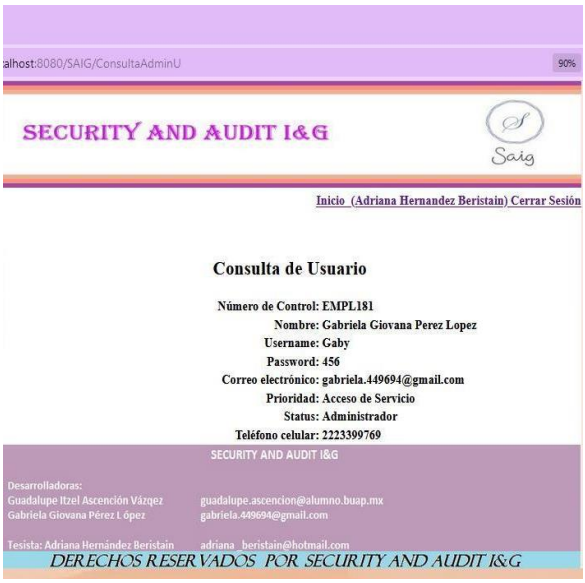


Ilustración 51 Consulta de usuario mediante control de usuario.

En la Ilustración 52 nos muestra la consulta de usuario mediante la opción de nombre de usuario de la misma manera nos proporciona la información del usuario seleccionado.

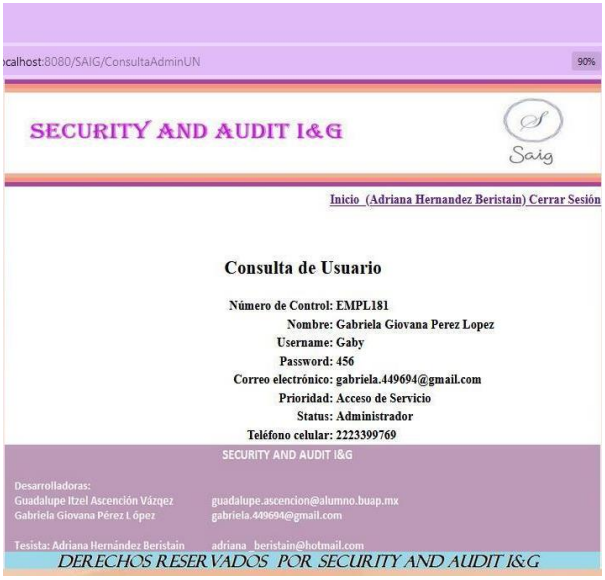


Ilustración 52 Consulta de usuario mediante el nombre de usuario.

En la Ilustración 53 se muestra el menú de administración de empresas del cual está conformado por altas empresas, bajas empresas, modificaciones empresa y consultas empresa.

Ilustración 53 Menú de Administración de empresas.

En la Ilustración 54 se muestra la ficha empresa para anotar los datos solicitados para dar de alta a la empresa.

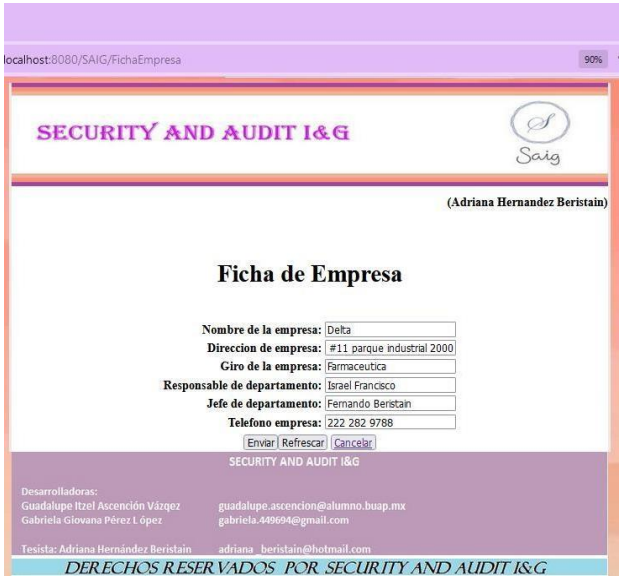


Ilustración 54 Ficha de alta de empresa.

En la Ilustración 55 se muestra la pantalla de eliminación buscando a la empresa a eliminar por el número de control seleccionando el deseado.

Ilustración 55 Pantalla de eliminación de la empresa.

En la Ilustración 56 se muestra un mensaje de confirmación para aceptar que dicha empresa se elimina de la base de datos.

Ilustración 55 Mensaje de confirmación para eliminar una empresa.

En la Ilustración 56 se muestra un mensaje de satisfacción en donde avisa que dicha empresa fue eliminada satisfactoriamente.

Ilustración 56 Mensaje de eliminación satisfactoriamente.

En la Ilustración 57 se muestra la pantalla de modificación por si deseamos corregir algún dato mediante el control de la empresa.

Ilustración 57 Pantalla de modificación seleccionando por control de empresa.

En la Ilustración 58 se muestra la pantalla de modificación de empresa en la cual de lado izquierdo se muestra la información almacenada en la base de datos mientras que en el lado derecho nos proporciona los recuadros para las modificaciones pertinentes.

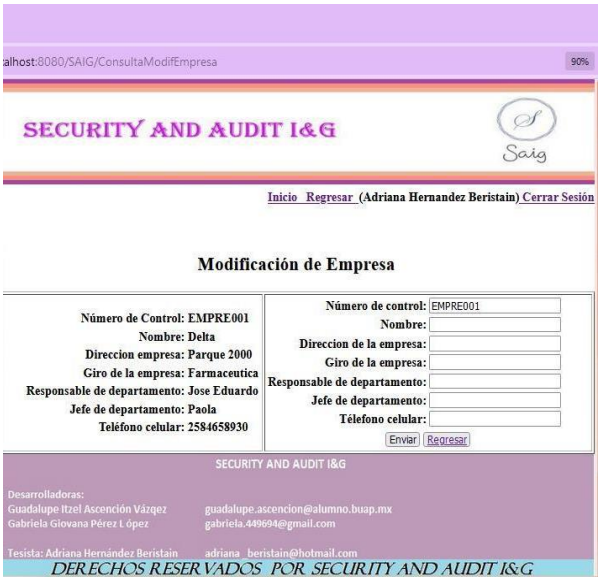


Ilustración 58 Pantalla de modificación de empresa.

En la Ilustración 59 nos muestran el mensaje del cual se realizaron exitosamente las modificaciones de la empresa.

Ilustración 59 Pantalla de modificación realizada.

CAPÍTULO 5. PRUEBAS Y RESULTADOS

5.1 Pruebas por exploración

Las pruebas por exploración se evaluaron con las siguientes historias de usuario de la aplicación Security and Audit I&G (SAIG) de las cuales son:

- Registro de usuario.
- Inicio de sesión.
- Gestión del usuario.
- Gestión de la empresa.
- Gestión de test.
- Preparación auditoría.
- Desarrollo de la auditoría.
- Informe final.

Por otro lado, se anexan las observaciones que se identificaron en el proceso de su elaboración.

Tabla 8 - Historia de usuario del registro de usuario.

Historia de usuario #1	
Nombre:	Registro de usuario
Usuario:	Administrador
Descripción:	Verificar el usuario se registre exitosamente según el debido llenado de un pequeño formulario del que cuestiona los datos de usuario.
Observaciones:	Se hace un chequeo de los datos, en el que deben estar completos y también se cuentan con restricciones en ciertos campos porque corresponde si son caracteres o números. Tras finalizar el registro, ingresaremos con nuestro usuario y contraseña correspondiente.

Tabla 9 - Historia de usuario de inicio de sesión.

Historia de usuario #2	
Nombre:	Inicio de sesión
Usuario:	Empleado
Descripción:	Se ingresa el usuario y contraseña correspondiente se realiza una comprobación para dar ingreso a la sesión.
Observaciones:	Se hace la verificación de los datos para dar acceso a la sesión correspondiente.

Tabla 10 - Historia de usuario de gestión de usuario.

Historia de usuario #3	
Nombre:	Gestión de usuario
Usuario:	Administrador
Descripción:	Se realizan las altas, bajas, consultas y modificaciones. Se da de alta al usuario con los datos solicitados. Las bajas se elimina los datos del usuario. En consultas nos muestra la información proporcionada. Modificación es editar algún dato ingresado erróneamente.
Observaciones:	Los datos son llenados correctamente respetando los caracteres o números. Con la información ingresada se logra ingresar a la sesión de supervisor.

Tabla 11- Historia de usuario de gestión de empresas.

Historia de usuario #4	
Nombre:	Gestión de empresas
Usuario:	Administrador
Descripción:	Se realizan las altas, bajas, consultas y modificaciones. Se da de alta a las empresas con los datos solicitados. Las bajas se elimina los datos de la empresa. En consultas nos muestra la información proporcionada. Modificación es editar algún dato ingresado erróneamente.
Observaciones:	Los datos son llenados correctamente respetando los caracteres o números. Con la información ingresada se logra ingresar a la sesión de supervisor.

Tabla 12- Historia de usuario de gestión de test.

Historia de usuario #5	
Nombre:	Gestión de test
Usuario:	Administrador
Descripción:	Se realizan las altas, bajas, consultas y modificaciones. Se da de alta al usuario con los datos solicitados. Las bajas se elimina los datos del usuario. En consultas nos muestra la información proporcionada. Modificación es editar algún dato ingresado erróneamente.
Observaciones:	Los datos son llenados correctamente respetando los caracteres o números.

Tabla 13- Historia de usuario de preparación de la auditoría.

Historia de usuario #6	
Nombre:	Preparación de auditoría
Usuario:	Supervisor
Descripción:	Se cuenta con un menú para la selección de auditoría de sistemas en desarrollo, auditoría de instalaciones informáticas y, por último, auditoría de aplicación. Se nos presenta un cuestionario de cada submenú para tener un conocimiento amplio de las áreas.
Observaciones:	Con los resultados obtenidos en dicho cuestionario se logra tener las sugerencias otorgadas para un mejor cuidado en sus áreas vulnerables cada usuario dependerá si las toma en cuenta para una mejor seguridad.

Tabla 14- Historia de usuario de desarrollo de la auditoría.

Historia de usuario #7	
Nombre:	Desarrollo de la auditoría
Usuario:	Supervisor
Descripción:	Proponemos herramientas para una seguridad estable del mismo modo proponemos mejoras con el uso de herramientas. Contamos con diversas herramientas de ayuda para proporcionar al usuario y las conozca para una mejor ejecución de estas
Observaciones:	Se mostrarán las diversas herramientas con una breve descripción para conocer las de una manera más explícita para su ejecución.

Tabla 15- Historia de usuario de Informe final.

Historia de usuario #8	
Nombre:	Informe final
Usuario:	Supervisor
Descripción:	Se muestras los resultados obtenidos en base al análisis de los cuestionarios para mostrar el porcentaje obtenido por cada área. Se crea un informe final mostrando la información del usuario. También se mostrarán las recomendaciones que aportamos basando nos en los resultados obtenidos, para un mayor conocimiento de estas.
Observaciones:	Las recomendaciones tendrán variantes debido a que cada usuario tendrá un resultado diferente o un poco similar.

5.2 Resultados

Originalmente el problema es la falta de protección de información en las empresas con forme a los sucesos ocurridos de los delitos cibernéticos, se realizó la aplicación web Security and Audit I&G (SAIG), donde se pretende realizar auditorías de red para analizar, cuáles son las debilidades de las distintas áreas, y brindar sugerencias de una

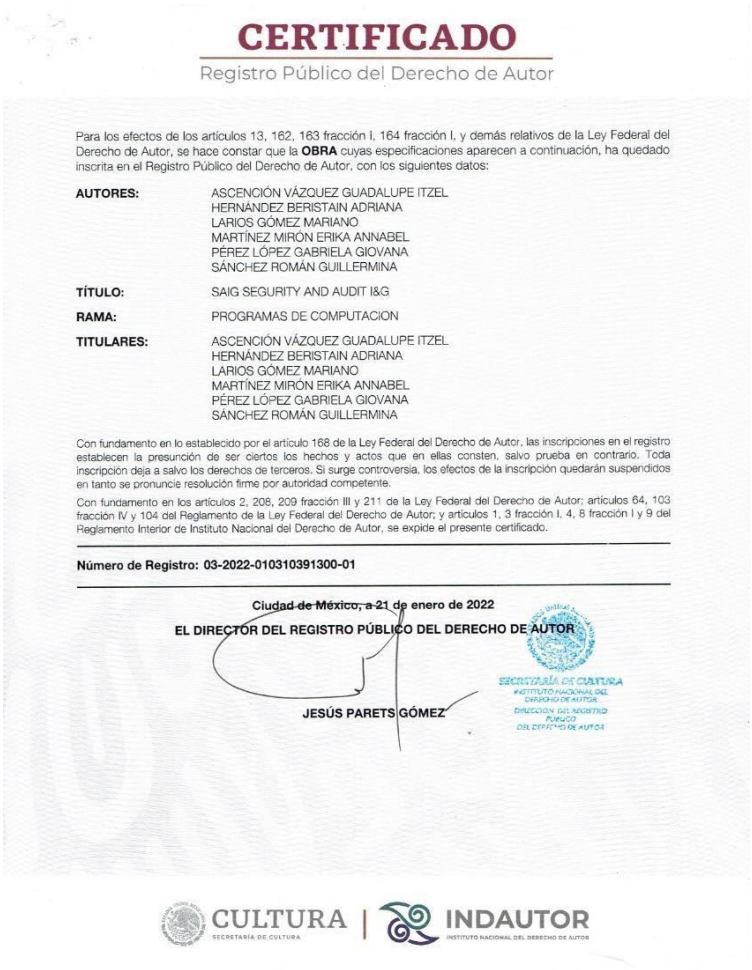
mejor protección y generando un informe final.

Se realizó la prueba de usabilidad, de este modo se evaluó la aplicación web Security and Audit I&G (SAIG), teniendo como resultado las evaluaciones de los usuarios y las empresas.
Mediante un cuestionario para la preparación de auditoría donde tienen diferentes menús. Como resultado se obtuvieron las sugerencias para los usuarios y tener mejor conocimiento de su seguridad.

También se obtuvieron los puntos de vista sobre la aplicación web, dado que es una aplicación funcional para los usuarios y es de forma intuitiva para ellos.

Además, se realizó una presentación de los avances de la tesis Auditoría de red y propuesta de implementación en el coloquio estudiantil para el desarrollo de habilidades del pensamiento complejo, CE-DHPC con el fin de obtener opiniones acerca del proyecto de Security and Audit I&G (SAIG) para mejorar la usabilidad y corrección de errores surgidos durante el desarrollo.

En la Ilustración 60, se realizó el registro público del derecho de autor 2022 de la aplicación Security and Audit I&G (SAIG) con número de registro: 3-2022-010310391300-1 se registró presentando simulación de la aplicación, los casos de uso, códigos de la aplicación.



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 COMPUTACIÓN

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

CULTURA | INDAUTOR

Ilustración 60 Certificado de Registro Público de Derecho de Autor

CAPÍTULO 6. CONCLUSIONES Y TRABAJO A FUTURO

6.1 Conclusiones

Mediante el planteamiento del problema se decide una manera ofrecer los conocimientos de cómo proteger al usuario mediante diversas herramientas, es notorio que con el avance de la tecnología existen mayores riesgos.

Por eso, se desarrolla una aplicación web en la que, a través de una serie de cuestionarios, se analiza cómo se constituye la protección de la empresa para diversas áreas de esta.

Se obtuvieron las carencias de protección de las áreas de las empresas, con los resultados obtenidos se realizó un análisis para atender las necesidades del usuario y generar un ambiente de trabajo más consciente de los riesgos informáticos para evitar daños a la persona, institución o empresa.

Se concluye que, con este trabajo de tesis es muy importante conocer una manera de salvaguardar nuestra información. Sabemos que las empresas siempre se arriesgan a sufrir algún ataque; aun así, debemos tener los conocimientos pertinentes.

La auditoría de red es un tema muy extenso y enriquecedor, ya que da una visión más extensa de la ciberseguridad.

6.2 Trabajo a futuro

Primeramente, debemos dar a conocer el tema de la ciberseguridad de varias maneras para que cada vez más y más personas se concienticen, para así difundir la aplicación realizada Security and Audit I&G (SAIG).

Teniendo el conocimiento se logra ofrecer a las empresas o usuarios, que desean conocer las maneras de protegerse en la red teniendo sugerencias de cambio hacia sus áreas de trabajo, para una mayor seguridad de esta.

CAPÍTULO 7 BIBLIOGRAFÍA

[1] Categoría: Ciberseguridad. (s. f.). Centro de Ética Judicial. https://www.centroeticajudicial.org/blog/category/ciberseguridad

[2] (No date) Benchmark gensuite EHS - reseñas, Precios Y Funciones - Capterra México 2024. Available at: https://www.capterra.mx/software/150242/gensuite (Accessed: 08 April 2024).

[3] Programación en Castellano, S.L. (no date a) Realiza auditorías de Tu Equipo Con Winaudit, Programación en Castellano. Available at: https://programacion.net/noticia/realiza_auditorias_de_tu_equipo_con_winaudit_1977 (Accessed: 08 April 2024).

[4] Automatice su enfoque de planeamiento de auditoría para Ahorrar Tiempo y mejorar La Precisión de las evaluaciones defina y pondere factores de Riesgo Para. - PPT descargar (no date) SlidePlayer. Available at: https://slideplayer.es/slide/1062776/ (Accessed: 08 April 2024).

[5] Auge software auditoría: Precios, funciones y opiniones (no date) ComparaSoftware. Available at: https://www.comparasoftware.com/auge-software-auditoría (Accessed: 08 April 2024).

[6] Escuela especializada en ingeniería. Tema 1: ESTRUCTURA DE APLICACIONES WEB. https://virtual.itca.edu.sv/Mediadores/daw/tema_1____estructura_de_aplicaciones_web.html

[7] Fernández, E. C. (2024, 26 febrero). Qué es un Servlet en Java y para qué sirve. Tokio School. https://www.tokioschool.com/noticias/que-es-servlet/#:~:text=Un%20servlet%20es%20un%20componente,Independencia.

[8] ¿Qué es JavaScript? - Aprende desarrollo web | MDN. (s. f.). MDN Web Docs. https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

[9] PHP: ¿Qué es PHP? - Manual. (s. f.). https://www.php.net/manual/es/intro-whatis.php#:~:text=PHP%20(acr%C3%B3nimo%20recursivo%20de%20PHP,puede%20ser%20incrustado%20en%20HTML.

[10] V, B., & V, B. (2023, 27 abril). ¿Qué es un servidor web y cómo funciona? Tutoriales Hostinger. https://www.hostinger.mx/tutoriales/que-es-un-servidor-web

[11] ¿Qué es una base de datos? - Explicación de las bases de datos en la nube -

AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/database/#:~:text=Una%20base%20de%20datos%20es,almacenar%2C%20recupera r%20y%20editar%20datos.

[12] Rendón, Y. A. (s. f.). Bases de datos relacionales vs. no relacionales. https://www.pragma.com.co/academia/lecciones/bases-de-datos-relacionales-vs.-no-relacionales#:~:text=Las%20bases%20de%20datos%20relacionales%20se%20basan%20en%20la%20organizaci%C3%B3n,o%20m%C3%A1s%20conjuntos%20de%20datos.

[13] Gaceta parlamentaria. (s. f.). https://www.senado.gob.mx/65/gaceta_comision_permanente/documento/42432

[14] El derecho Al Olvido (2023) Foro Jurídico. Available at: https://forojuridico.mx/el-derecho-al-olvido/ (Accessed: 08 April 2024).

[15] Ramírez, H. (2024, 29 enero). Encriptación de datos ¿Qué es, ¿cómo y cuándo realizarla? Grupo Atico34. https://protecciondatos-lopd.com/empresas/encriptacion-datos/

[16] Atlassian. (s. f.-b). Pruebas exploratorias | Atlassian. https://www.atlassian.com/es/continuous-delivery/software-testing/exploratory-testing

[17] Singureanu, C. (2023, 19 abril). Pruebas de caja negra: qué son, tipos, procesos, enfoques, herramientas y mucho más. ZAPTEST. https://www.zaptest.com/es/pruebas-de-caja-negra-que-son-tipos-procesos-enfoques-herramientas-y-mucho-mas

[18] ¿Qué es la prueba de software y cómo funciona? | IBM. (s. f.). https://www.ibm.com/mx-es/topics/software-testing

[19] Atlassian. (s. f.). Los distintos tipos de pruebas en software | Atlassian. https://www.atlassian.com/es/continuous-delivery/software-testing/types-of-software-testing

[20] Yeeply. (2022, 6 septiembre). ¿Qué son las pruebas unitarias y cómo llevar una a cabo? Yeeply. https://www.yeeply.com/blog/tendencias-habilidades/que-son-pruebas-unitarias/

CAPÍTULO 8 ANEXOS

Anexo A

Menú de auditoría de red.

Anexo B

Menú de Preparación de Auditoría

Anexo C

Menú de preparación de Auditoría.

Anexo D

Menú de Preparación de Auditoría.

Anexo E

Menú de auditoría de red.

Anexo F

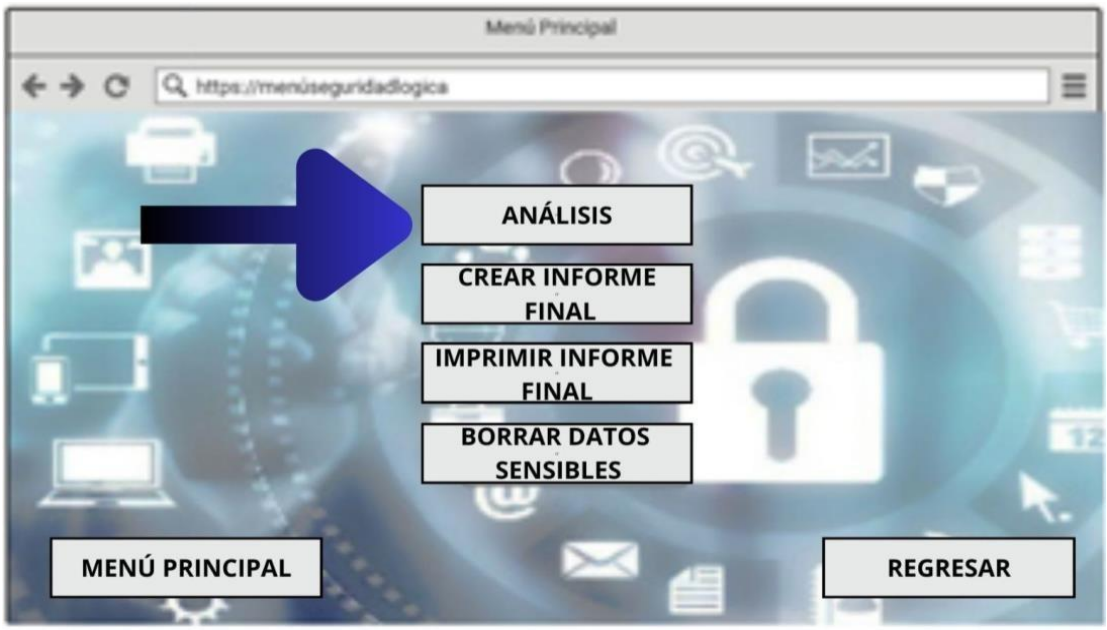
Menú de opciones para el desarrollo de auditoría.

Anexo G

Menú de auditoría de red.

Anexo H

Menú de informe final.



Anexo I

Análisis finalizado de cada sección.