UNIVERSIDAD JOSE ANTONIO PÁEZ

APLICACIÓN WEB PARA LA GESTIÓN DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN

Autores:

Alvarez Rashel

Tochon Bryan

Urb. Yuma II, calle Nº 3. Municipio San Diego

Teléfono: (0241) 8714240 (master) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN
CARRERA INGENIERÍA EN COMPUTACIÓN

APLICACIÓN WEB PARA LA GESTIÓN DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN

Proyecto del Trabajo de Grado para optar al título de
INGENIERO EN COMPUTACIÓN

Autor(a):
Alvarez Rashel
Tochon Bryan

Tutor(a):
Dra. Belkys Araujo

San Diego, Febrero 2020

FI-C -001-2019-3CR (TG)

Valencia, 10 de diciembre de 2019

Ciudadanos:
Alvarez H. Rashel M.,
26.246.666
Tochón M. Bryan O'.
26.047.849
Presente-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión Nº **06-2019** de fecha **12-09-2019** aprobó el proyecto de trabajo de grado titulado **APLICACIÓN WEB PARA LA GESTIÓN DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN** presentado por usted (es) como requisito para optar al título de Ingeniero en Computación.

Se ratifica la designación de la Ing. Belkys Araujo C.I: 6.906.234 como Tutora Académica que los asesorara en el desarrollo de este proyecto.

Atentamente.

UNIVERSIDAD JOSE ANTONIO PAEZ
UJAP
DECANATO INGENIERIA

Prof. Luis Lira
Decano de la Facultad de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado (1).

LL/a.a.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN
CARRERA INGENIERÍA DE COMPUTACIÓN

APROBACIÓN DEL TUTOR

Quien suscribe, Dra. Belkys Araujo, portador de la cédula de identidad N° **6.906.234** en mi carácter de tutor del trabajo de grado presentado por los ciudadanos: **Rashel Alvarez**, portador de la cédula de identidad N° 26.246.666, y el ciudadano: **Bryan Tochon,** portador de la cedula de identidad N° 26.047.849 titulado **APLICACIÓN WEB PARA LA GESTIÓN DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN**, presentado como requisito parcial para optar al título de **INGENIERO DE COMPUTACIÓN**, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los catorce días del mes de febrero del año dos mil veinte.

Dra. Belkys Araujo
C.I.: 6.906.234

DEDICATORIA

Primeramente a Dios, a ti te estoy infinitamente agradecida por protegerme, por nunca dejarme sola, por ser mi ejemplo, mi apoyo, mi consejero espiritual y moral, gracias por la vida, por la salud y por darme fuerzas para superar obstáculos y dificultades a lo largo de la vida.

A mis padres por estar siempre presente, apoyándome y guiándome para que nunca decaiga y pueda alcanzar mis logros.

A mi hermana por ser mi ejemplo a seguir y mi confidente.

A mis sobrinos a quienes adoro mucho y espero que cuando sean mayores puedan alcanzar todas sus metas.

A todos los miembros de mi familia y aquellas personas que creyeron en mí y a los que no, por impulsarme en las adversidades siempre.

A mis compañero Bryan Tochon por darme su amistad, por sus valiosos conocimientos aportados a este trabajo de grado y por ser un gran apoyo durante el transcurso de mi carrera.

Rashel Alvarez

DEDICATORIA

A Dios.

Por acompañarme siempre en mis pasos y decisiones para fortalecerme y poder superar todo tipo de obstáculo.

A mi madre Angelica.

Por darme la vida, por darme todas las cosas que he necesitado sin necesidad de lujos para convertirme en el hombre que soy, en el hijo mayor ejemplar, en una persona honesta y bondadosa y por darme tantos valores que hoy por hoy el que mas me caracteriza es el ser humanitario.

A mi tío Franklin.

Por ser parte importante en mi vida para cumplir esta meta, y estuvo siempre apoyándome a lo largo de mi carrera.

A mis familiares.

A pesar de no ser una familia tan grande se siente la fe y el orgullo que tienen hacia mí, a mi tía Luz Romero quien abrió las puertas de su hogar para yo estar y a mis primos por tantos momentos de alegría que me regalaron y que por supuesto conté con su ayuda para cumplir con muchas de mis obligaciones a lo largo de la carrera.

A mis compañeros de estudio.

Rashel Álvarez quien tuve el honor de ser su compañero de tesis, y compañero en la carrera, Estefanía Gainza por ayudarnos tanto en la elaboración de la tesis y convertirse en una gran amiga en tan poco tiempo, y demás compañeros de promoción.

A la Dra. Belkys Araujo, tutora de tesis y madrina de promoción, por su tiempo, momentos de alegría, dedicación y asesoramiento el cual eternamente estaré agradecido. A la MSc. Oneida Jiménez por confiar en mí, por permitirnos apoyarnos en ella y ser una guía. Y al MSc. Jetro López su valiosa guía.

A ustedes,
Gracias.
De Bryan Tochon.

AGRADECIMIENTOS

A dios por darnos la fortaleza, perseverancia y sabiduría para poder superar los obstáculos y así poder alcanzar los objetivos.

Gracias a nuestros padres, familiares y amigos por el apoyo, en el transcurso de nuestra carrera universitaria y por siempre estar presentes en todo momento.

A la Dra. Belkys Araujo por ser nuestra tutora, por la dedicación y el tiempo que nos dio para guiarnos y aconsejarnos en el desarrollo de este trabajo de grado.

De igual manera le damos gracias a todos los profesores de la Universidad José Antonio Páez en especial a la Msc Oneida Jiménez y al Msc Jetro López, por aportar sus valiosos conocimientos y formarnos como futuros profesionales.

A nuestra amiga Estefania por su valiosa amistad, por los buenos momentos y por todo su apoyo.

Rashel Alvarez, Bryan Tochon

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN
CARRERA INGENIERÍA EN COMPUTACIÓN

APLICACIÓN WEB PARA LA GESTIÓN DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Autores: Bryan Tochón O'Neill Moreno
Rashel Álvarez Mariana Henríquez
Tutor: Dra. Belkys Araujo
Fecha: Marzo 2020

RESUMEN

En la actualidad la masificación de los sistemas informáticos es un hecho, cada vez se producen avances en el campo tecnológico haciendo que estén a disposición de un mayor número de personas y sea usado en distintos ambientes de trabajo. El presente trabajo de grado se fundamenta en las auditorias de los sistemas informáticos, se puede definir que la auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos; por esta razón resulto importante desarrollar una aplicación web que facilite la evaluación de estos datos de forma rápida y eficiente, ya que muchos de los auditores aun trabajan de forma manual. El tipo de investigación es proyecto especial y un nivel de investigación de carácter descriptivo con un diseño de investigación de campo, bajo la metodología de desarrollo XP, el cual la población fue representada por 10 auditores de una empresa consultora. Siguiendo cada una de las fases metodológicas de la investigación, se profundizo en la problemática para optimizar los procesos de auditoría, además se llevo a cabo una entrevista no estructurada determinando así los requerimientos funcionales del sistema el cual unos de los más importantes son la generación de un modulo para los procesos de los Sistemas de Gestión de Seguridad de la Información y la generación del informe final de auditoría, luego se desarrollo la aplicación en el lenguaje de programación PHP y el gestor de base de datos MYSQL y finalmente se ejecutaron las pruebas necesarias para el correcto funcionamiento del sistema.
Descriptores: Auditoria, Aplicación Web, Sistemas de Información.

INTRODUCCIÓN

En la actualidad el mundo progresa cada vez más rápido, la constante lucha por mejorar y cumplir con los objetivos de las organizaciones, hacen prioritaria la incorporación de nuevas tecnologías como los sistemas de información, donde su base es la base de brindar soluciones con resultados favorables, significativos y que aporten valor al desarrollo de sus procesos. Pues, los sistemas de información han tenido una gran utilidad dentro de la sociedad y organizaciones conllevando una gran influencia en todos los ámbitos.

Muchas empresas utilizan un departamento de sistema donde diseñan, implementan, mantienen, y actualizan los sistemas de información y programas que permitirán lograr los innovadores cambios, resultando un medio aun más confiable para poder llevar el control de cualquier proceso dentro del mundo empresarial que hoy en día es tan competitivo.

Ahora bien, a pesar del impacto positivo que ofrece la implantación de estos sistemas, todavía existen organizaciones con una gran necesidad de estas tecnologías, el presente trabajo de grado tuvo como finalidad el desarrollo de una aplicación web para la gestión de auditoría de los sistemas de información, el cual su función se concentra en agilizar las auditorias de sistemas informáticos y como instrumento de apoyo para los auditores de sistemas de información. Además, obtener los beneficios inherentes de un proceso de evaluación manual a un sistema informático para automatizar este proceso y como mayor seguridad de la información, alto nivel de resguardo, almacenamiento en base de datos y otros.

El enfoque del proyecto de esta investigación se divide en cuatro (4) capítulos, los cuales describen lo siguiente:

Capítulo I: en este capítulo se describe el problema a solucionar en el proyecto, el objetivo general y específicos a lograr, el alcance y justificación.

Capítulo II: se resumen todos los conceptos y teorías que se utilizan para la realización del proyecto de investigación, así como la descripción de

antecedentes correlacionados y la definición de términos básicos para la comprensión del lector.

Capítulo III: describe el marco metodológico de la investigación, el cual consiste en describir el tipo, nivel y diseño de la misma, así como también la definición de las fases y los instrumentos de recolección de datos para el cumplimiento de los objetivos.

Capítulo IV: en este capítulo se interpretan los resultados de las fases previamente definidas en el proyecto, así como también el diseño y la construcción del sistema.

Capitulo V: se definen las conclusiones y recomendaciones.

CAPÍTULO I
EL PROBLEMA

1.1. Planteamiento del Problema

La información es un recurso vital para la organización, contar con información exacta, y precisa es muy valioso, ya que de ella pueden depender variables en el crecimiento de esta, a partir de una información se toman decisiones y se proyectan metas u objetivos. La información además de ser importante está expuesta a la vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, virus, desastres naturales, hurto de la información, conexión no autorizada a equipos y servidores, suplantación de identidad, modificación o eliminación de datos, falta de mantenimiento, manipulación indebida de usuarios no autorizados, abuso de privilegios, sabotaje, etc. La vulnerabilidad de un sistema permite al atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

La auditoría de sistemas es importante ya que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos para el excelente desempeño de los sistemas de información porque proporciona controles necesarios ya que los hace confiable en el nivel de seguridad. El proceso de auditoría de sistemas es de vital importancia ya que se encarga de determinar los hallazgos y vulnerabilidades más relevantes de seguridad física y lógica en una organización.

Es importante que la información que se encuentre integrada en una organización esté resguardada bajo unas medidas de seguridad. Es ahí donde nace la seguridad de la información para mantener a salvo todos los datos de la empresa, desde los que pertenecen a la propia organización como los vinculados con trabajadores y clientes. La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa. Principalmente este tipo de sistemas se basan en las nuevas tecnologías, por tanto,

la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán acceso usuarios autorizados.

Si se habla de los impactos que genera las auditorias vendrían siendo la automatización de los procesos, la simplicidad en el volumen y velocidad de las operaciones, la creciente disminución de documentos impresos, mejor control de los sistemas de información, las operaciones relacionadas con el proceso de información son más precisas, supervisa todos los accesos del medio informático, tanto la calidad del acceso lógico, acceso físico y sus controles.

Por ende, el impacto de las auditorias está en que las evaluaciones independientes de todas las áreas, actividades y funciones de una organización sean optimizadas para dar un dictamen profesional sobre la eficiencia de sus operaciones y resultados. La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: electrónicos, papel, audio, vídeo, etc.

Hoy en día la tecnología como hardware, software, bases de datos, redes y servidores son herramientas estratégicas que brindan ventajas ante la necesidad de crecimiento y competitividad a los negocios, pero pueden también ocasionar pérdidas si no se administran de la mejor manera. Por eso que es necesario mantener y realizar evaluaciones de estas herramientas y del personal calificado que cumpla con el objetivo de la empresa.

Se vio en la necesidad de implementar una aplicación web que permita establecer la gestión de auditoría de los sistemas de información para minimizar y solucionar los riesgos a los cuales se encuentra expuesta la organización.

1.2 Formulación del problema

¿Cómo se puede facilitar el proceso de auditoría de los Sistemas de Información?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Desarrollar una aplicación web para la gestión de auditoría de los sistemas de la información en la organización.

1.3.2 Objetivos Específicos

- Analizar el estado actual de los procesos de auditoría de los Sistemas de Información mediante las normas ISO 27001 y 19011 basado en los estándares de auditabilidad correspondientes.
- Determinar requerimientos funcionales y no funcionales utilizando las normativas ISO 27001 y 19011 optimizando los procesos de auditoría.
- Crear la aplicación web basado en el lenguaje de programación preprocesador de hipertexto (PHP) y el gestor de base de datos MYSQL.
- Verificar la funcionalidad y el rendimiento del sistema mediante un plan de pruebas.

1.4 Justificación de la investigación

La información es un activo que es esencial para una organización y en consecuencia necesita ser protegido adecuadamente. Por ende, se justificó la realización de una aplicación web que permita la gestión de auditoría de los sistemas de información. Evaluando cada uno de los ítems anteriormente nombrados para verificar, evaluar y analizar los diferentes hallazgos, así como sus posibles soluciones para que se realicen mejoras, esto con el fin de mejorar en los diferentes aspectos para un buen funcionamiento y mejoramiento del servicio de sus asociados y que serán expuestos en un informe final y totalmente confidencial.

Con los cambios de la ciencia y la tecnología, la auditoria ha sido beneficiada por estos, lo que ha conllevado a una mayor eficiencia en los controles que se practican en las diferentes organizaciones de forma manual, sin embargo, la auditoria de los sistemas de información aun mantiene como reto adaptar su esquema de trabajo ante los avances tecnológicos, y debe contribuir con sus evaluaciones de gestión y control interno a determinar la eficacia y eficiencia de las operaciones de la entidad, teniendo en cuenta que, los avances en la tecnología van incrementándose día a día impactando todos los aspectos de las operaciones de la empresa y viéndose más difícil de poder agilizar estos procesos, por eso es totalmente ideal la realización de una aplicación web para la auditoria de los sistemas de información.

1.5 Alcance

El diseño de esta aplicación web pretende identificar las condiciones actuales de los sistemas de información en una organización, dando así una calificación de los recursos y ofreciendo un informe como solución a la problemática que es parte del asesoramiento, con los siguientes ítems:

Seguridad Física: se verificará las condiciones ambientales que permiten estar protegidos mediante elementos que, combinados, ayudan a integrar una serie de medidas preventivo-disuasivas o represivas contra eventualidades de carácter ilícito.

Seguridad Lógica: verificar los diferentes controles de acceso a la información, como también los diferentes roles que tienen los clientes internos para utilizar el sistema de información comprobando la limitación al servicio que tienen dichos usuarios.

Infraestructura Tecnológica: se evaluará el tipo de mantenimiento que tiene cada uno de los terminales, comprobando su respectivo uso de acuerdo con el usuario.

Software: verificar las licencias de funcionamiento de los diferentes programas instalados en la empresa, Lo anterior con el fin de observar un conjunto de elementos para verificar el cumplimiento de normas y así optimizar el uso de los recursos para brindar un buen servicio a los asociados de dicha empresa lo cual saldrá dentro del informe final y será parte del asesoramiento. También verificar que el sistema de la empresa cumpla con los principios de calidad y diseño del software.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes

Para el estudio de "Aplicación Web para la Gestión de Auditoría de los Sistemas de Información", ha sido necesario indagar en investigaciones anteriores con el fin de ampliar el entendimiento del tema. Estas investigaciones constituyen estudios previos relacionados con el problema planteado y que guardan alguna vinculación con el problema en estudio. Dichas investigaciones se presentan a continuación:

Alonso, G. (2018), para la obtención del título de Magister en informática empresarial y que fue presentada en el año 2018 en Ecuador con el titulo denominado "**Auditoría Informática y la Calidad del Servicio de las Tecnologías de la Información en el Distrito de Educación Colta - Guamote."** Este proyecto de investigación se realizo con el motivo de llevar a cabo una auditoria informática para comprobar si se puede mejorar la calidad del servicio de las tecnologías de información en el Distrito de Educación. Luego de las acciones tomadas después de haber concluida la auditoría, la calidad de servicio de la Unidad de Tecnologías de la Información y Comunicación mejoró de un 67% a un 87% en los aspectos auditados. Se llego a la conclusión que mediante la realización de una auditoria informática se pueden tomar decisiones para mejorar la calidad del servicio ya sea en base a optimización de recursos, mejorar la planificación y la incorporación de elementos tecnológicos actualizados.

Así mismo Lascano, W. (2016), trabajo de grado titulado **"Auditoria Informática para Mejorar la Gestión de las Tecnologías de la Información en el Ministerio del Trabajo Regional Ambato"**, el motivo de la investigación fue realizar una auditoría Informática en el Ministerio del Trabajo Regional Ambato, con el fin de establecer métodos y estándares que se ejecutan en la institución. El Ministerio del Trabajo Regional Ambato por ser una institución del estado, su razón es el servicio, en tal virtud debe tener una gestión de las tecnologías acopladas a este beneficio. Se puede concluir que los procesos de auditoría permiten definir el estado real de la infraestructura tecnológica que maneja la

institución, también se puede deducir que mediante la utilización de la metodología COBIT se llega a obtener resultados evacuatorios de los procesos y de los equipos informáticos. Toda auditoría informática requiere de una planificación previa y de la definición de los instrumentos evacuatorios para hardware, para software y lógicamente para procesos.

Además Jiménez, A y Salazar, B. (2016), realizaron un trabajo de grado para optar por el título de Ingeniero en Sistemas, fue presentado en Bogotá, Colombia en la Universidad Piloto de Colombia, con el titulo denominado **"Análisis de riesgos, amenazas y vulnerabilidades de la compañía Pinzón Pinzón & Asociados en su área de TI y planteamiento de los controles a aplicar basados en la norma ISO 27001:2013".** La empresa Pinzón Pinzón & Asociados, cuenta con diferentes sistemas de información los cuales han sido implementados sin un esquema especializado de seguridad. El tratamiento que se le ha dado a los problemas en seguridad de la información es insuficiente, generando brechas de seguridad, repetitivas en lapsos muy cortos sobre los que nunca se identifica su causa, ni se hace un seguimiento a las oportunidades de mejora. Con este estudio se busca describir el análisis realizado a la compañía Pinzón Pinzón & Asociados, en el departamento de TI, y de allí poder obtener como resultado los riesgos, las vulnerabilidades y las amenazas que se presentan y de esta manera proponer un plan de controles los cuales ayudaran en la mitigación de los resultados obtenidos en el análisis.

Por último Velásquez, J. (2016), trabajo de grado para optar por el título de Ingeniero en Sistemas, fue presentado en Barcelona, Venezuela en el Instituto Universitario Politécnico Santiago Mariño en el año 2016 con el título **"Sistema de Información para el Manejo de Inventario en la Empresa Inversiones Camino Real C.A.".** En la empresa Inversiones Camino Real C.A., no se lleva un control para el inventario y seguimientos de las entradas y salidas de mercancía, es por ello que este proyecto se realizó con el fin de mejorar el sistema de información existente, en relación al seguimiento de las actividades más importantes que se llevan en el departamento de almacén, como lo son: la

reposición y venta de mercancía, así como los reportes correspondientes a su organización.

2.2. Bases Teóricas

La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía.

2.2.1 Sistemas de información (SI)

Los Sistemas de Información son reconocidos como una herramienta básica para usar y acceder a la información además de facilitar el proceso de toma de decisiones en las organizaciones.

Según Muñoz Cruz un sistema de información “es un conjunto de elementos o componentes relacionados con la información que interaccionan entre sí para lograr un objetivo: facilitar y/o recuperar información”

Según Arjonilla Domínguez, “un sistema de información está formado por un conjunto de elementos integrados e interrelacionados que persiguen el objetivo de capturar, depurar, almacenar, recuperar, actualizar y tratar datos para proporcionar, distribuir y transmitir información en el lugar y momento en el que sea requerido en la organización”. Laudon, K y Laudon J, los sistemas de información “son un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización” Laudon, K y Laudon J

Cuando se habla de un sistema de información (SI) se refiere a un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente. Todo sistema de información se compone de una serie de recursos interconectados y en interacción, dispuestos del modo más conveniente en base al propósito informativo trazado, como puede ser recabar información personal, procesar estadísticas, organizar archivo, etc. Estos recursos pueden ser:

- Recursos humanos: personal de variada índole y destrezas.
- Datos: cualquier tipo de información masiva que precisa de organizarse

- Actividades: procedimientos, pasos a seguir, estaciones de trabajo, etc.
- Recursos informáticos: aquellos determinados por la tecnología.

2.2.1.1 Activos

> Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008].

En un sistema de información hay 2 cosas esenciales:

- La información que maneja
- Los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Ahora nos preguntamos, ¿Por qué interesa un activo? Por lo que vale. No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger. La valoración se puede ver desde la perspectiva de la ‘necesidad de proteger’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en los principios de información que sean pertinentes.

De un activo puede interesar tomar en cuenta los siguientes principios de la información:

- Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos. Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.
- Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falsos o, incluso, faltar datos. Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.
- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios. Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves. Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño. La disponibilidad es una característica que afecta a todo tipo de activos. A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). En el caso de esta investigación se utilizo la norma ISO 27005 definida como el sistema de gestión de riesgos para la

seguridad de la información la cual se utilizo como referencia para la valoración de los activos, así como también, la definición de los criterios y los colores para cada uno.

C = Confidencialidad

I = Integridad

D = Disponibilidad

Cuadro 1 **Valoración de Activos**

Criterio	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

Fuente: Norma ISO 27005

2.2.2 Amenazas

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información.

- Infraestructura: fallos de suministro eléctrico, refrigeración, contaminación, etc.
- Origen natural: inundaciones, terremotos, incendios, rayos, etc.
- Origen industrial: explosiones, derrumbes, contaminación química, etc.
- Fallos de los sistemas informáticos y de comunicaciones: aplicaciones o equipos de transmisión, caída del servicio, virus, troyanos, falta de mantenimiento, etc.
- Humano: errores accidentales o deliberados de las personas que actúan con la información.

2.2.3 Impacto

El impacto generado sobre un activo de información según la norma ISO 27001 es la consecuencia de la materialización de una amenaza. A continuación se muestra los criterios definidos para la valoración del impacto y una breve descripción.

Cuadro 2 **Criterios de Impacto**

Valor – Criterio		**Descripción**	**Pérdida de utilidad operacional**
1	Insignificante	No genera pérdidas financieras ni compromete de ninguna forma la imagen pública de la institución y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos.	Menor de ½ día
2	Menor	Puede generar pérdidas financieras que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la institución y del Gobierno. Su materialización causaría un bajo daño en del desarrollo del proceso y no afectaría el cumplimiento de los objetivos.	½ día o 1 día
3	Serio	Puede generar pérdidas financieras que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la institución y del Gobierno. Su materialización causaría un deterioro en del desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente de forma normal	De 1 día a una semana
4	Desastroso	Generación de pérdidas financieras que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la institución y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal.	De una semana a un mes
5	Catastrófico	Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren.	Más de un mes

Fuente: Norma ISO 27001

2.2.4 Probabilidad

Es una cuantificación para determinar en que nivel un evento de riesgo pueda producirse. En este caso aplicado a la probabilidad de que una amenaza explote una vulnerabilidad para que se produzca o se materialice un riesgo.

Cuadro 3 **Valoración de la probabilidad**

Valor	Criterio	Descripción
1	Muy improbable	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad
2	Improbable	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad.
3	Posible	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad.
4	Muy probable	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad.
5	Casi Seguro	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente (90%-100%)

Fuente: Norma ISO 27001

2.2.5 Riesgos

> "El Riesgo, producto de la interrelación de amenazas y vulnerabilidades es, al final de cuentas, una construcción social, dinámica y cambiante, diferenciado en términos territoriales y sociales. Aun cuando los factores que explican su existencia pueden encontrar su origen en distintos procesos sociales y en distintos territorios, su expresión más nítida es en el nivel micro social y territorial o local. Es en estos niveles que el riesgo se concreta, se mide, se enfrenta y se sufre, al transformarse de una condición latente en una condición de pérdida, crisis o desastre". (Humboldt, 2004).

A continuación se mencionan los niveles de riesgos que pueden presentar los activos bajo una amenaza identificada:

Cuadro 4 **Nivel de Riesgo**

Nivel de riesgo	Descripción
Baja	Baja exposición y severidad para lo cual se recomienda monitoreo.
Moderado	Se recomienda que estos riesgos sean gestionados en niveles básicos de la compañía pero con supervisión directa del responsable.
Alta	Riesgos que requieren controles y alarma permanente que permitan su gestión constante.
Extremo	Riesgos de alta severidad y exposición para los cuales se deben implementar controles para su adecuado tratamiento, debido a su importancia y criticidad son de máxima prioridad para la compañía.

Fuente: Norma ISO 27001

Para la fundamentar un poco mas esta investigación para la ejecución de los tratamientos del riesgo se utilizo la metodología COSO esta metodología permite implementar un control interno en cualquier tipo de compañía a través de marcos reguladores globales. De esta forma, se asegura la consecución de objetivos y la rentabilidad de la empresa.

Clasificación del control

Cuadro 5 **Tipo de control**

Clasificación	Descripción
Preventivo	Controles que actúan antes o al inicio de un proceso
Correctivo	Controles que actúan durante el proceso y que permiten corregir las deficiencias

Fuente: Metodología COSO

Cuadro 6 **Periodicidad del control**

Clasificación	Descripción
Permanente	Controles que se aplican durante todo el proceso, es decir en cada operación
Periódico	Controles que se aplican en forma constante solo cuando ha transcurrido un periodo especifico de tiempo
Ocasional	Controles que se aplican de forma ocasional en un proceso

Fuente: Metodología COSO

Cuadro 7 **Automatización del control**

Clasificación	Descripción
Automatizado	La aplicación del control es completamente automatizada
Manual	No está considerado el uso de sistema automatizados

Fuente: Metodología COSO

2.2.6 Auditoria

Según Alvin Arens (2007) auditoria es "la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos, se debe realizar por una persona independiente y competente"

> La auditoria es un proceso sistemático, independiente y documentado, mediante el cual podemos obtener evidencia y declaraciones, que permite verificar el cumplimiento de requisitos solicitados por una determinada norma o algún documento como la política o estrategia impuestos por la alta dirección de una organización. (ISO 19011).
>
> La auditoria de sistemas de información se puede definir como la revisión sistémica organizada de los sistemas de información en una organización, para evaluar el correcto manejo de controles, seguridad, información, funcionalidad, procedimientos, políticas y normas. Para así emitir una evaluación profesional de la eficiencia de los sistemas de información. (Vieites, 2004).

La historia de las auditorías se registra desde tiempos remotos cuando los soberanos exigían el mantenimiento para comprobar la veracidad de las operaciones financieras, posteriormente con el desarrollo del comercio surge la

necesidad de las primeras auditorias en Inglaterra en el año de 1862. Por otra parte, la teoría administrativa y las aportaciones de Taylor y Farol, proponen cinco funciones que todo administrador o gerente debe poseer: planear, organizar, ordenar, coordinar y controlar, lo anterior, da paso junto a la función del control en la que se integra la auditoria lo cual, permite acumular y evaluar datos y evidencias que se han realizado de determinadas áreas y actividades para posteriormente realizar una información cuantificable, con el propósito de terminar un informe y así poder tomar decisiones correctas y optimas.

En resumen, las primeras auditorías que se realizaron fueron para evaluar el funcionamiento de las áreas contables de las organizaciones, para analizar las finanzas de las empresas, esto debido que los dueños consideraban a las finanzas como lo único interesante en la empresa. Durante mucho tiempo las organizaciones solo se preocupaban de ver por el buen funcionamiento de sus cuentas, sin embargo a lo largo del tiempo y al gran desarrollo tecnológico han tomado importancia otros aspectos, como los sistemas de información.

Por otro lado, gracias al crecimiento del comercio y las sociedades, nació la necesidad de implementar mejoras continuas en todos los procesos, productos y servicios que se consumen. Asimismo, con la finalidad adicional de obtener una optimización de recursos para la empresa, se hace necesario contar con estructuras de organización dedicadas a uniformizar la forma de hacer las cosas. Con esta necesidad de estandarización, nacen algunas normas de calidad que empiezan a aplicarse en organizaciones de todos los sectores productivos. En la parte de auditorías de sistemas de información esta las normas ISO 27001 y 19011, lo cual ayudan a las empresas que puedan hacer un análisis de riesgo de seguridad periódicamente siempre que se propongan o se establezcan cambios significativos dentro de esta, logrando así controlar estos cambios.

La norma ISO 19011 llegó en el año 2002, y su denominación dentro de las normas ISO fue minuciosamente pensada y meditada, puesto que se pretendió evitar que fuese relacionada con las familias de las normas ISO 9000 e ISO 14000, pero manteniendo la relación con las normas de auditoría previas, ISO 10011 e ISO 14011. Los dos primeros dígitos de la norma (19xxx) corresponde al

número que se encontraba disponible en el momento en que se realizó el trabajo, mientras que los otros tres que la componen (xx011) se mantuvieron de las anteriores normas mencionadas. El número 19011 puede entenderse como una simbología que defiende el proyecto más allá de la grieta actual entre la gestión de calidad y ambiental (2002) y en el 2011 se enfoca como directrices para la auditoría de los sistemas de gestión en función del programa de Auditoría.

Además, la norma ISO 27001 hace referencia al British Standard 7799, publicado en 1995. Después de sufrir una serie de revisiones, este patrón originó la norma conocida como ISO/IEC 17799.Con una segunda parte del BS 7799 referente a la implantación de un Sistema de Gestión de Seguridad de la Información y publicada en 1999, se creó la norma que hoy se conoce como ISO 27001. Esta norma se estableció en 2005, con la publicación de una nueva revisión hecha en 2013 para incorporar las adaptaciones necesarias, ya que la computación en la nube, por ejemplo, pasó a ser una realidad del universo TI.fue publicada en octubre de 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional siendo estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

Se considera como un estándar internacional, debido a que hace referencia a un compendio de requisitos que exige que los sistemas de gestión de seguridad de la información en la organización garanticen la mejora continua y la administración adecuada de la información. El interés por gestionar la seguridad de la información surgió por los riesgos a los que está expuesta en medio del tránsito hacia la digitalización; el principal problema fue la forma en la que se manejó la información y su control público-privado, independientemente de su formato: datos, video y voz, en medios tradicionales o en medios magnéticos. Otro de los factores que, en gran medida, influyó en la necesidad de implementar esta norma fue la activación de la cultura móvil, pues se puede manejar una gran cantidad de datos; además, esto permite que la información se cree y se regenere.

2.2.6.1 Principios de Auditoria ISO 19011

Integridad:

- Los auditores y la persona que maneja el programa de auditoría deben llevar a cabo su trabajo con honestidad, diligencia y responsabilidad.
- Observar y cumplir con todos los requisitos legales aplicables.
- Demostrar su competencia durante el desarrollo del trabajo.
- Llevar a cabo su trabajo de manera imparcial; es decir, ser justo e imparcial en todos sus negocios.
- Ser sensible a cualquier influencia ejercida sobre su juicio durante el curso de una auditoría.

Presentación ecuánime:

- Obligación de reportar con veracidad y exactitud: los hallazgos, conclusiones e informes de la auditoría deberían reflejar con veracidad y exactitud las actividades de la auditoría.
- Se informa de los obstáculos significativos encontrados durante la auditoría y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado. La comunicación debería ser sincera, exacta, objetiva, clara y completa.

Debido cuidado profesional:

- Aplicación de diligencia y juicio al auditar
- Los auditores deben proceder con el debido cuidado, de acuerdo con la importancia de la tarea que desempeñan y la confianza depositada en ellos por el cliente de la auditoría y por otras partes interesadas. Un factor importante en el desempeño de su trabajo con el debido cuidado profesional es tener la habilidad de hacer juicios razonables en toda situación de auditoría.

Confidencialidad:

- Seguridad de la información: los auditores deben ejercitar la discreción en el uso y protección de la información adquirida en el curso de sus labores. La información de auditoría no debería ser usada de manera inapropiada

para ganancia personal del auditor o del cliente de auditoría ni de manera tal que vaya en detrimento de los intereses legítimos del auditado. Este concepto incluye el adecuado manejo de información confidencial sensible.

Independencia:

- La base para la imparcialidad de la auditoria y la objetividad de las conclusiones de la auditoria.

Enfoque basado en la evidencia:

- El método racional para alcanzar conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático. La evidencia de la auditoría debería ser verificable. En general, está basada en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un período de tiempo delimitado y con recursos finitos. Se debería aplicar un uso adecuado del muestreo, ya que éste está estrechamente relacionado con la confianza que puede depositarse en las conclusiones de la auditoría.

2.2.6.2 Evidencia

> Material físico o digital que permita probar un proceso, un dicho o una afirmación (Amaya, 2015).

2.2.6.3 Hallazgos

> Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría. Los hallazgos de la auditoria indican conformidad o no conformidad. Los hallazgos de la auditoria pueden conducir a la identificación de oportunidades para la mejora o el registro de buenas prácticas. (ISO 9000)

Los hallazgos de auditoría están clasificados como: conformidad y no conformidad.

Una conformidad puede tener matices que se clasifican en: observaciones y oportunidades de mejora. Una observación es un hallazgo en el cual sí existe un cumplimiento pero que en el futuro puede convertirse en un incumplimiento debido a cómo se está desarrollando una actividad, tarea o proceso concreto. Una oportunidad de mejora es un hallazgo en el cual sí existe un cumplimiento, pero a pesar de ello se determina, bajo

criterios objetivos, que existe un margen de mejora para optimizar más una actividad, tarea o proceso concreto.

2.2.6.4 Aspectos a evaluar en las auditorias

Existen ciertas áreas a las que se deben evaluar cuando se hace una auditoria de los sistemas de información, estos aspectos se pueden clasificar en las siguientes categorías.

2.2.6.4.1 Control de acceso

> El control de acceso se realiza por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. (ISO 27001)

2.2.6.4.2 Seguridad Física y Ambiental

> El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. (ISO 27001)

2.2.6.5 Seguridad Lógica

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La seguridad lógica involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. El Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados emitido por la Contraloría General de la República, establece en la norma Nº 305-03 sobre seguridad lógica, que el acceso a los archivos de

datos y programas sólo se permitirá al personal autorizado. Los principales objetivos que persigue la seguridad lógica son:

- Restringir el acceso a los programas y archivos
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

2.2.7 Organización Internacional de la Estandarización (ISO)

Las normas ISO son normativas internacionales para la optimización de los procesos empresariales, fueron elaboradas por la Organización Internacional de la Estandarización (ISO, International Standard Organization). Las normas ISO son documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo. Hasta el momento ISO, ha publicado alrededor de 19.500 normas internacionales que se pueden obtener desde la página oficial.

El objetivo es asegurar que los productos y/o servicios alcancen la calidad deseada. Para las organizaciones son instrumentos que permiten minimizar los costos, ya que hacen posible la reducción de errores y sobre todo favorecen el incremento de la productividad. Los estándares internacionales ISO son clave para acceder a mercados nacionales e internacionales y de este modo, estandarizar el comercio en todos los países favoreciendo a los propios organismos públicos.

Podemos nombrar algunas ISO relacionadas como por ejemplo:
ISO/IEC27000: consiste en un vocabulario estándar para el SGSI.
ISO/IEC27001: es la certificación que deben de tener las organizaciones, además es una norma que especifica los requisitos necesarios para la implantación del SGSI. Se la considera la norma más importante de la familia. Está centrada en la mejora continua de los procesos y de la gestión de riesgos.
ISO/IEC27002: tecnología de la información, técnicas de seguridad y código para la práctica de la seguridad de la gestión de la información.
ISO/IEC27003: directrices para la implementación de un SGSI. También se le considera el soporte de la norma ISO/IEC27001.

ISO/IEC27004: Métricas para la gestión de seguridad de la información. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

ISO/IEC27005: guía para la gestión del riesgo en relación a la seguridad de la información.

ISO/IEC27006: en ella se especifican los requisitos para la acreditación de entidades de certificación de sistemas de gestión de seguridad de la información y auditoría.

2.2.8 ISO 27001. Sistema de Gestión de la Seguridad de la Información

La norma/estándar UNE ISO/IEC 27001 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

Los requisitos de la Norma ISO 27001 nos aporta un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa. Los Objetivos del Sistema de Gestión de la Seguridad de la Información son preservar la: Confidencialidad Integridad y Disponibilidad.

La información es un activo que, como otros activos importantes del negocio, tiene valor para la Organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio elenco de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. La información adopta diversas formas: puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación. Debería protegerse

adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se caracteriza aquí como la preservación de su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información; su integridad, asegurando que la información y sus métodos de proceso son exactos y completos; su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Implementar la norma ISO 27001 le aporta valor a cualquier organización ya que se desarrollan un conjunto de estrategias que la hacen más confiable, a continuación se menciona los aspectos que se pueden llevar a cabo con el uso de esta norma:

- Evitar virus, fraudes, espionajes, vandalismo, desastres naturales, hacking, denegación de servicios, etc.
- Reducción del riesgo de pérdida o hurto de la información.
- Mejora la confianza de cliente y socios.
- Cumplimiento de las legislaciones vigentes referente a la seguridad de la información.
- Mejora de la reputación.
- Diferencia competitiva frente a otra organización que no tiene un estándar o que no vela por la seguridad de la información.
- Reducción de costos y tiempo.

2.3. Bases Legales

Ley Especial contra los Delitos Informáticos

> **Articulo 6. Acceso Indebido.** Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. (p. 6)
>
> **Articulo 7. Sabotaje o Daño a Sistemas.** Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será

penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo. (p. 7)

Articulo 11. Espionaje Informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenida en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentara de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado. (p. 8)

Articulo 13. Hurto. Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolas a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. (p. 9)

Articulo 14. Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias. (p. 9)

2.4. Definición de Términos Básicos

Información: es un conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento.

Base de Datos: es una colección de información organizada de tal modo que sea fácilmente accesible gestionada y actualizada.

Sistema: la palabra sistema procede del latín

Impacto: la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.

Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Activo: cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste.

Control: comprobación, inspección, fiscalización e intervención.

CAPÍTULO III

MARCO METODOLÓGICO

Los fundamentos metodológicos son los que servirán para orientar el proceso de investigación del estudio desarrollado intentando dar respuesta a las interrogantes objeto de la investigación. En tal sentido, el marco metodológico constituye según Balestrini A. (1998, p. 114) “la instancia referida a los métodos, las diversas reglas, registros y protocolos con los cuales una teoría y su método calculan las magnitudes de lo real”. Su fin esencial es el de situar en el lenguaje de investigación los procedimientos e instrumentos que serán empleados en el estudio y que permitirán darle direccionalidad.

3.1 Tipo de la Investigación

La presente investigación al tener como objetivo general el desarrollo de una aplicación web para la gestión de auditoría de los sistemas de la información en la organización, se fundamenta en la modalidad de proyecto especial, que se puede definir como: un estudio “que consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales” (UPEL, 1998, p. 7).

3.2 Diseño de la Investigación

Basado en la investigación de, Sabino (2006, p. 32), “en los diseños de campo los datos de interés se recogen en forma directa de la realidad, mediante el trabajo concreto del investigador y su equipo. Este diseño nos permite estudiar las verdaderas condiciones en que se encuentra el proyecto el cual se va a realizar, al aplicar dicho diseño ayuda cerciorándolos de la realidad y las condiciones en que se encuentra los datos, esta es una de las maneras más confiables y directa de conocer los mismos”. Este estudio se enmarcó en una investigación de campo, ya que los datos fueron extraídos de forma directa del lugar de la problemática y descrito por los afectados., la cual brindo todos los elementos necesarios para la realización de la presente investigación.

Así mismo, Fidias G. Arias (2012, p. 27), define: “la investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos.” De igual manera, el presente estudio es una investigación documental, ya que la información adicional que respalda la presente investigación, fue extraída de autores pasados.

3.3 Nivel de la Investigación

. Con respecto al nivel de la investigación la misma se encuentra ubicada dentro de los parámetros de la investigación descriptiva. Para Tamayo (1998, p. 54) la investigación descriptiva: “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, composición o procesos de los fenómenos. El enfoque que se hace sobre conclusiones es dominante, o como una persona, grupo o cosa, conduce a funciones en el presente. La investigación descriptiva trabaja sobre las realidades de los hechos y sus características fundamentales es de presentarnos una interpretación correcta”. El trabajo de investigación se enmarco en un ámbito descriptivo debido a que se llevo a cabo un análisis de los procesos actuales de auditoría de los sistemas de información utilizando normas estándares ISO, de tal manera que, mediante el desarrollo de un software optimizar los métodos de auditoría.

3.4 Población y muestra

3.4.1 Población

La población es definida por Arias (2006, p. 81) como “un conjunto finito o infinito de elementos con características comunes para los cuales serán extendidas las conclusiones de la investigación. Esta queda determinada por el problema y por los objetivos del estudio”. Por lo tanto, la población fue representada por 10 auditores de una empresa consultora.

3.4.2 Muestra

Según Tamayo (2004, p. 38): afirma que la muestra “es el grupo de individuos que se toma de la población, para estudiar un fenómeno estadístico”. En lo que se refiere a la muestra para el desarrollo de esta investigación se encontró representada por 3 auditores de una empresa consultora.

3.5 Técnicas e instrumentos de recolección de datos

Para la recolección de los datos fue necesario aplicar algunas técnicas que permitiera obtener la información necesaria para determinar los requerimientos funcionales y no funcionales para el desarrollo del software en relación con los procesos de auditoría de los sistemas de información que se llevan a cabo en una organización.

Arias (2006, p. 376) define como las técnicas de recolección de datos "como el conjunto de procedimientos y métodos que se utilizan durante el proceso de investigación, con el propósito de conseguir la información pertinente a los objetivos formulados en una investigación”. Para esta investigación las técnicas de recolección de datos fueron establecidas de la siguiente forma: observación directa y entrevista no estructurada.

Arias (2006, p. 69) “la observación es una técnica que consiste en visualizar o captar mediante la vista, en forma sistemática, cualquier hecho, fenómeno o situación que se produzca”. Esta técnica se utiliza como propósito de captar como se lleva a cabo la auditoria en la organización.

Por último, se utilizara la entrevista no estructurada con la finalidad de realizar preguntas de manera libre y espontanea. Hurtado (2007, p. 44) las define como: “la formulación de preguntas libres, cada una basada en la respuesta que va dando el interrogado, por lo cual, las preguntas pueden variar de un interrogatorio a otro”. Es por esto que se plantea una entrevista no estructurada a los auditores o ex auditores, ya que con ello se lograra satisfacer los requerimientos establecidos en la investigación, haciendo uso de instrumentos tales como cuadernos de apuntes.

3.6 Fases Metodológicas

La descripción del desarrollo de una aplicación web para la gestión de auditoría de los sistemas de información, se llevo a cabo aplicando la metodología XP. Pinciroli (2011) dice que XP: “se trata de una metodología de desarrollo liviana, cuenta con pocas herramientas de modelado y se cuida bastante de incorporar otras adicionales”, y define a UML como (2003): “la funcionalidad completa del sistema desde la perspectiva de los actores que interactúan con él”, donde expresa que, si existe alguna funcionalidad en el sistema, por menor que esta sea, debe quedas representada dentro del modelo de casos de uso, mientas que las historias de usuario no solo no deben contener la funcionalidad completa del sistema, sino que solo deben plantear los diferentes objetivos de los usuarios en un nivel de generalidad tal que permita cumplir con ciertas restricciones básicas y el detalle se obtendrá en discusiones cara a cara entre los programadores y los usuarios. De esta manera, se emplea casos de uso para complementar lo que hacen las historias de usuario.

El Lenguaje de Modelado Unificado (UML), puede utilizarse para visualizar, especificar y documentar los procesos de un sistema, permitiendo la comunicación, explicar comportamientos deseados, comprender el proceso de construcción y visualizar oportunidades de optimización. Las fases en la que está dividido el proyecto se contemplan a continuación:

Fase I: Análisis del estado actual de los procesos de auditoría de los Sistemas de Información mediante las normas ISO 27001 y 19011 basado en los estándares de auditabilidad correspondientes.

Durante esta fase se realizó una investigación de los procesos que forman parte del funcionamiento de las auditorias en los sistemas informáticos, con el fin de conocer como se manejan los auditores actualmente y saber las expectativas que tienen con la intención de que puedan ser plasmadas en el desarrollo de la aplicación web. Por supuesto que, describiendo todo el proceso manual de los auditores como también las necesidades para que el sistema pueda cubrirla, por lo tanto, esta es la parte más importante ya que con ella obtendremos una idea real

del problema y de lo que se quiere lograr para satisfacer las necesidades de los usuarios.

Fase II: Determinación de los requerimientos funcionales y no funcionales utilizando las normativas ISO 27001 y 19011 optimizando los procesos de auditoría. Esta fase tiene como objetivo determinar los requerimientos funcionales y no funcionales del sistema tomando en cuenta las normas ISO y las técnicas de recolección de datos.

Fase III: Creación de la aplicación web basado en el lenguaje de programación preprocesador de hipertexto (PHP) y el gestor de base de datos MYSQL.

En esta fase de desarrollo se encarga de toda el área funcional del sistema a través de la codificación ateniendo a estándares de codificación ya creados. Programar bajo estándares mantiene el código consistente y facilita su compresión y escalabilidad. Al empezar el desarrollo del sistema se prestó atención a los requerimientos funcionales y no funcionales ya dados anteriormente. Por otro lado es importante destacar que en dicha fase es necesario dar a conocer los diagramas de caso de uso, diagramas de entidad-relación, además de mantener el contacto con el usuario y cliente, es importante desarrollar código reutilizable o prototipo para implementar futuros sistemas partiendo de lo creado previamente.

Fase IV: Verificación de la funcionalidad y el rendimiento del sistema mediante un plan de pruebas.

Por último, esta fase se encarga de realizar las distintas pruebas del sistema para corroborar que lo hecho previamente funcione según lo planificado, en caso de existir errores y/o fallas deberán corregirse. Por otra parte, esta etapa se ha de conseguir el aceptamiento tanto del cliente como el de los usuarios, ya que esto será primordial para la posterior implantación del sistema para uso completo con las mejoras realizadas.

CAPÍTULO IV

RESULTADOS

En este capítulo se describe los resultados obtenidos de la investigación de tal manera que se llevo a cabo un análisis e interpretación de los procesos actuales de auditoría según la normas ISO 27001 y 19011, así como también la aplicación de una entrevista no estructurada a las organizaciones de auditoría que se encuentran dentro del municipio Valencia, por medio de los cuales se busco obtener los métodos idóneos para lograr los aspectos que permitan argumentar esta investigación.

4.1 Fase I: Análisis

En esta primera fase se presenta el análisis de los procesos actuales que se llevan a cabo en una auditoria mediante el uso de las normas ISO 27001 y 19011. De tal manera que la información reunida en esta investigación sirve como apoyo para una mejor optimización del sistema de gestión.

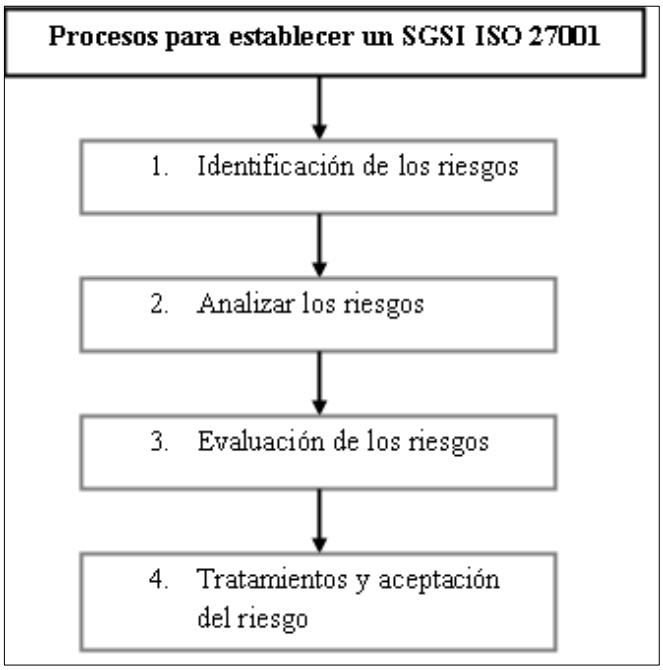

Figura 1: **Procesos de SGSI Fuente: ISO 27001**

- Identificación de los riesgos: se identifican los activos, luego evaluar la confidencialidad, integridad y disponibilidad de los activos de información. Después de tener una valoración de la condición actual del

activo, se han de conocer las amenazas que tiene cada uno y que pueden causar daños en la información.

- Analizar los riesgos: se determinaran una serie de criterios que serán las directrices para la evaluación de los riesgos. Son los que servirán para medir las consecuencias o impacto y la probabilidad de ocurrencia de que se materialice o se lleve a cabo las amenazas.
- Evaluación de los riesgos: una vez se han valorado las consecuencias o impactos y la probabilidad de los incidentes para los activos del ámbito elegido, se ha de realizar el producto de ambos para calcular los riesgos. Los resultados obtenidos se compararán con los criterios de tratamiento y aceptación de riesgo.
- Tratamiento y aceptación del riesgo: Identificar y evaluar las distintas opciones de tratamiento de los riesgos para aplicar controles adecuados para cada riesgo, los cuales irán orientados a: aceptar, reducir, eliminar o transferir el riesgo. Además se utilizaron controles que son medidas de protección para reducir el riesgo. La norma ISO 27001:2013 en su anexo A incluye una lista de controles de aplicación a la mayoría de empresas.

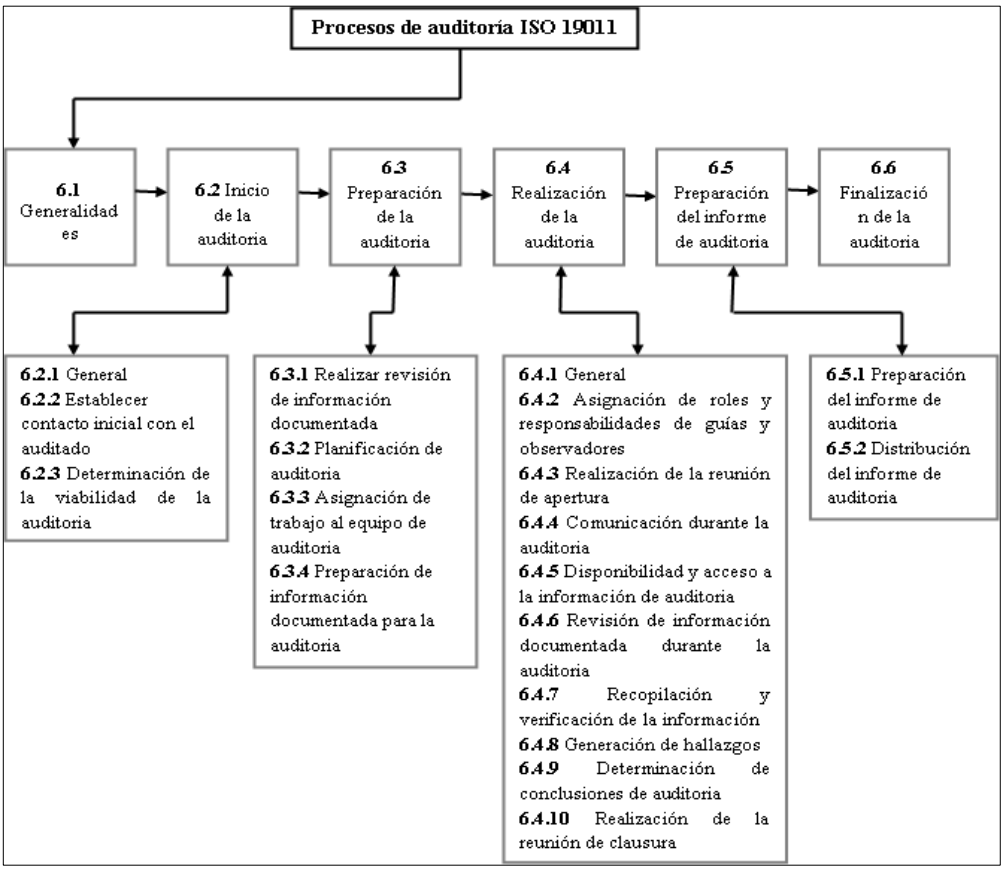

Figura 2 **Procesos de auditoría Fuente: ISO 19011**

Inicio de la auditoria

- General: la responsabilidad de llevar a cabo la auditoría debería corresponder al líder del equipo auditor, hasta que la auditoría finalice. Es por esto, que lo principal es la designación del mismo.
- Establecer contacto inicial con el auditado: el contacto inicial con el auditado para el desarrollo de la auditoría puede ser formal o informal y debe hacerlo el líder del equipo auditor. Además, el auditor líder debe conseguir tener acceso a la información pertinente para proceder a realizar la planificación de la auditoria.
- Determinación de la viabilidad de la auditoria: se debe tener en cuenta factores tales como la disponibilidad de lo siguiente; la información suficiente y apropiada para planificar y llevar a cabo la auditoria, la cooperación adecuada del auditado, el tiempo y los recursos adecuados para llevar a cabo la auditoria.

Preparación de las actividades de auditoria

- Realizar revisión de la información documentada: la información documentada debería incluir, pero no limitarse a: documentos y registros del sistema de gestión, así como a informes de auditoría previos. La revisión debería tener en cuenta el contexto de la organización, incluyendo su tamaño, naturaleza, complejidad, sus riesgos y oportunidades.
- Planificación de la auditoria: definir objetivos, criterios de auditoría, documentos de referencia, alcance, identificación de la organización y de sus funciones, fechas, horario y duración de las actividades de auditoría, definir horario de las reuniones con el auditado y miembros del equipo auditor, asignación de recursos.
- Asignación de las tareas al equipo auditor: el líder del equipo auditor, consultando con el equipo auditor, debería asignar a cada miembro del equipo la responsabilidad para auditar procesos, actividades, funciones o lugares específicos y, según sea apropiado, la autoridad para la toma de decisiones.
- Preparar los documentos de trabajo: los miembros del equipo auditor deberían recopilar y revisar la información pertinente a las tareas de auditoría asignadas y preparar la información documentada para la auditoría, usando cualquier medio apropiado.

Realización de la auditoria

- Se debe realizar una reunión de apertura para confirmar plan de auditoría y proporcionar un breve resumen de la planificación.
- Luego de lo ya mencionado anteriormente, cada persona empezara a cumplir con las tareas asignadas.
- La evidencia de la auditoria debe ser registrada, estos pueden indicar una conformidad o una no conformidad.
- El auditor líder debe planificar una reunión de clausura para verificar detalles, revisar hallazgos, cualquier otra información recopilada durante la auditoria y preparar recomendaciones.

Preparación del informe de auditoría

- El auditor líder es el responsable de la preparación y el contenido del informe.

Finalización de la auditoria

La auditoria finaliza cuando todas las actividades descritas en el plan de auditoría se hayan realizado y el informe aprobado se entregue al cliente.

En otras palabras, cabe destacar que no todos los procesos anteriormente mencionados en la Figura 2 que se encuentra en la pág. (35) aplican para el sistema, debido a que la ejecución de esas tareas no son consideradas para ser establecidos en un software de gestión de auditoría de modo que no afectaría al funcionamiento de la misma ni al resultado final de la auditoria, esto quiere decir que, fácilmente se pueden llevar a cabo de manera manual. Los procesos que se encuentran definidos en el sistema son: contacto inicial con el auditado, determinación de la viabilidad de la auditoria, planificación de auditoría, disponibilidad y acceso de la información de la auditoria, revisión de la información documentada de la auditoria, generación de evidencias y hallazgos, determinación de recomendaciones y conclusiones, preparación del informe de auditoría.

4.2 Fase II: Determinación

Luego del análisis de los procesos mencionados anteriormente, se presenta a continuación la interpretación de los resultados obtenidos en la entrevista no estructurada que se realizó a un auditor de la empresa KPMG, esto con la finalidad de fundamentar un poco más la investigación y además determinar los requerimientos funcionales y no funcionales para la optimización del sistema.

Cuadro 8 **Pregunta 1**

Nº	¿Cuáles son los procesos de auditoría de Sistemas de gestión de seguridad de la información que están aplicados en su empresa?
1	-Identificar los activos de información de la Compañía (hardware, software, bases de datos, redes, instalaciones, personas, entre otros). -Realizar una evaluación de riesgos para identificar las amenazas y determinar la probabilidad de ocurrencia, el impacto resultante y las medidas adicionales que mitigaran este impacto a un nivel aceptable para la compañía. .-Identificar controles para mitigar los riesgos identificados. -Realizar evaluaciones de riesgos de manera periódicas.

Fuente: Alvarez y Tochon (2020)

Cuadro 9 **Pregunta 2**

Nº	¿Qué le gustaría usted que controlara un software de auditoría?
2	Que incluya la valoración de riesgos, planificación, vista dinámica que despliegue todos los hallazgos para la auditoria, elaboración de informes, seguimiento global de asuntos, administración de problemas y fácil implementación e instalación.

Fuente: Alvarez y Tochon (2020)

Cuadro 10 **Pregunta 3**

Nº	¿Como las tics pueden mejorar o dar aporte a la auditoria?
3	Las tics nos aportan las tres perspectivas que son: -La auditoría alrededor del computador. -La auditoría a través del computador. -La auditoría con el computador.

Fuente: Alvarez y Tochon (2020)

Cuadro 11 **Pregunta 4**

Nº	Según usted, ¿Qué debe llevar un informe de auditoría?
4	Información de las personas que aporto el cliente para realizar la auditoria, los puntos de los hallazgos de la auditoria, las recomendaciones en que debe mejorar el cliente por punto (que es la que va directamente al cliente) ya que esa información le sirve a la directiva de la empresa para la toma de decisiones.

Fuente: Alvarez y Tochon (2020)

Cuadro 12 **Pregunta 5**

Nº	Según su experiencia, ¿Cuáles son los problemas o riesgos más comunes que se presentan al realizar una auditoría?
5	La vulnerabilidad de la red que pueda existir, una de ellas es el hackeo. Otros de los casos es el desorden en la sala de servidores (para evitar un circuito o caídas de la red) como también falta de ups (para mantener operativos los servidores por una caída de luz y no ocurran daños bruscos). Algo muy importante a mencionar es la vulnerabilidad de la información como es la base de datos ya que de allí parte el principio del sistema matriz de las empresas, acceso a la sala de servidores, control de roles en sistema administrativo (ya que existe información confidencial), los equipos fuera de un dominio para prevenir fuga de información, no contar con antivirus causa problema ya que puede encriptar información importante de los servidores, el estado actual de los equipos, Determinar si la navegación en Internet por los usuarios de la red interna se realiza de manera segura.

Fuente: Alvarez y Tochon (2020)

4.2.1Definición de requerimientos funcionales y no funcionales

4.2.1.1 Requerimientos funcionales:

- Inicio de sesión de usuarios con sus respectivos roles en el sistema.El administrador podrá crear, modificar y mostrar usuarios, auditorias, tareas, informes, hallazgos, etc.
- El líder podrá crear, modificar y mostrar las auditorias e informes además de ver la información que los demás auditores suben al sistema.
- El rol de auditor solo podrá realizar las tareas que le sean asignadas por su auditor líder y ver la información que lo demás auditores suben al sistema siempre y cuando este en la misma auditoria.
- Si los auditores no están asignados a una auditoria no podrán ver dicha información.
- Gestión de los procesos de auditoría.
- Modulo para los procesos de los Sistemas de Gestión de Seguridad de la Información
- Generación de evidencias y hallazgos.
- Generación de graficas pertinentes al sistema.
- Generación de informe final de auditoría.

4.2.1.2 Requerimientos no funcionales

- La interfaz debe ser agradable y comprensible para el usuario
- El sistema debe ser capaz de operar adecuadamente
- La aplicación debe cumplir con la confidencialidad, disponibilidad e integridad de la información.

4.3 Fase 3: Creación

Después de la determinación de los requerimientos funcionales y no funcionales para el sistema, se presenta a continuación las herramientas utilizadas para la visualización de las actividades que podrá realizar cada usuario dentro del sistema, el cual consta de diagramas que definen las tareas o actividades que llevarán al cumplimiento de los requerimientos anteriormente planteados.

4.3.1 Diagrama entidad-relación

Para la creación del presente sistema, se requiere una base de datos relacional que almacene la información necesaria en distintas tablas. Cada tabla contiene ciertos atributos o columnas que clasifican la información almacenada y la relaciona con el resto de las tablas. Para detallar dichas tablas, se plantea el diagrama entidad-relación en la siguiente figura:

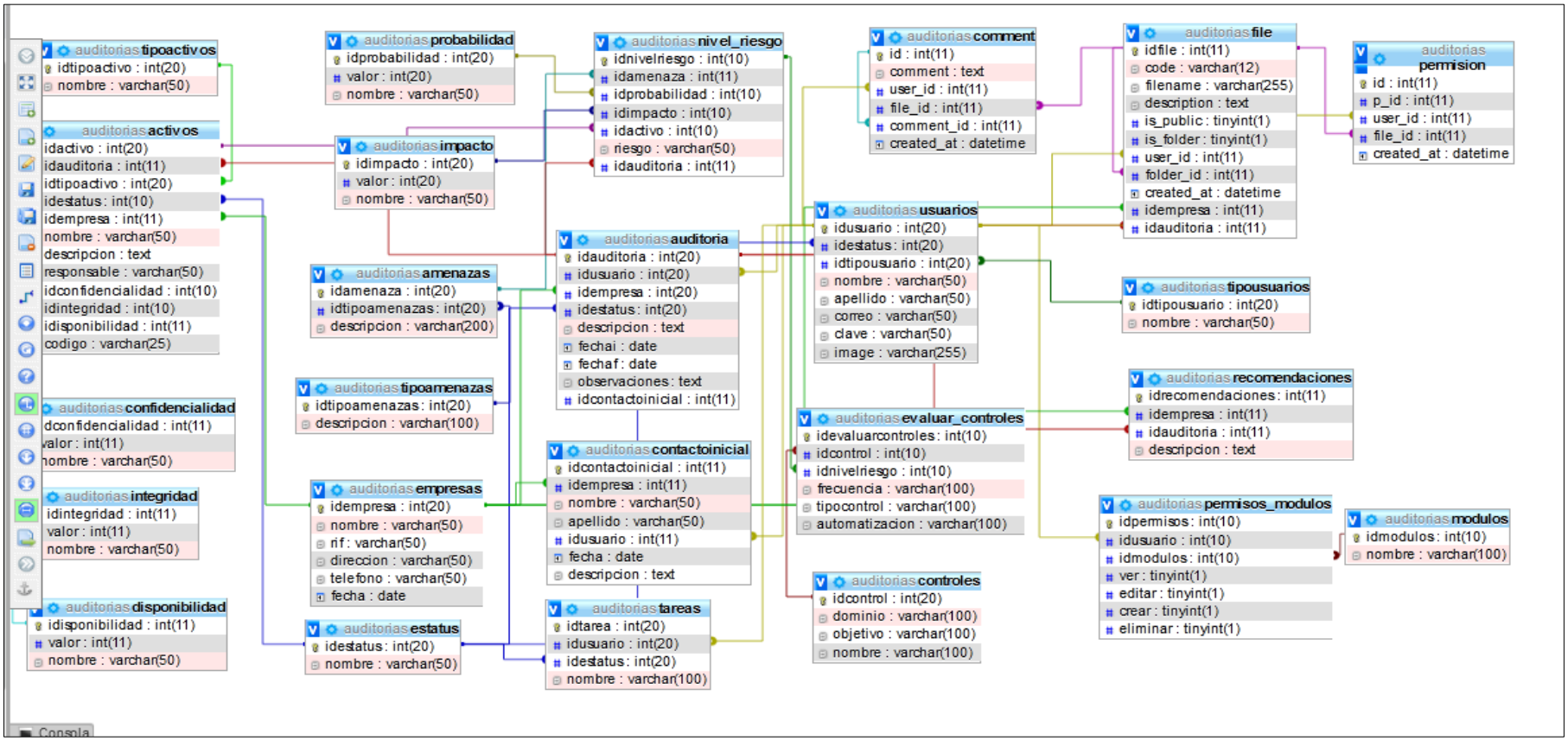

Figura 3 **Diagrama entidad-relación**

Fuente: Alvarez y Tochon (2020)

Cuadro 13 **Tabla Activos**

Columna	**Tipo**	**Nulo**	**Comentarios**
idactivo	Int(20)	No	Identificados de la tabla
idauditoria	Int(20)	No	foreignkey tabla auditoria
idtipoactivo	Int(20)	No	foreignkey tabla tipo de activos
idestatus	Int(10)	No	foreignkey tabla estatus
nombre	Varchar(50)	No	Nombre del activo
descripcion	Varchar(100)	No	Descripcion del activo
responsable	Varchar(50)	No	Responsable a cargo del activo
idconfidencialidad	Int(10)	No	Confidencialidad del activo
idintegridad	Int(10)	No	Integridad del activo
iddisponibilidad	Int(11)	No	Disponibilidad del activo

Fuente: Alvarez y Tochon (2020)

Cuadro 14 **Tabla Amenazas**

Columna	**Tipo**	**Nulo**	**Comentarios**
idamenaza	Int(20)	No	Identificados de la tabla
idtipoamenazas	Int(20)	No	foreign key tablatipoamenazas
descripcion	Varchar(200)	No	Descripcion de la amenaza

Fuente: Alvarez y Tochon (2020)

Cuadro 15 **Tabla comment**

Columna	Tipo	Nulo	Comentarios
id	Int(11)	No	Identificados de la tabla
comment	text	No	Comentarios de los Usuarios
user_id	Int(11)	No	Id usado para saber usuario que comentó
file_id	Int(11)	No	Id del documento
comment_id	Int(11)	No	Id para registrar el comentario
created_at	datetime	No	Fecha del comentario

Fuente: Alvarez y Tochon (2020)

Cuadro 16 **Tabla confidencialidad**

Columna	Tipo	Nulo	Comentarios
idconfidencialidad	Int(11)	No	Identificados de la tabla
valor	Int(11)	No	Valor de la confidencialidad
nombre	varchar(50)	No	Nombre del tipo de confidencialidad

Fuente: Alvarez y Tochon (2020)

Cuadro 17 **Tabla Auditoria**

Columna	Tipo	Nulo	Comentarios
idauditoria	Int(20)	No	Identificados de la tabla
idusuario	Int(20)	No	foreignkey tabla usuario
idempresa	Int(20)	No	foreign key tablaempresa
idestatus	Int(10)	No	foreignkey tabla estatus
descripcion	Varchar(100)	No	Descripcion de la auditoria
fechai	date	No	Fecha de inicio de la auditoria
fechaf	date	No	Fecha final de la auditoria
observaciones	text	No	Observaciones de auditoria

Fuente: Alvarez y Tochon (2020)

Cuadro 18 **Tabla Empresa**

Columna	Tipo	Nulo	Comentarios
idempresa	Int(20)	No	Identificados de la tabla
nombre	varchar(50)	No	Nombre de la empresa
rif	varchar(50)	No	Rif de la empresa
direccion	varchar(50)	No	Dirección de la empresa
telefono	varchar(50)	No	Teléfono de la empresa

Fuente: Rashel Alvarez y Bryan Tochon (2020)

Cuadro 19 **Tabla Estatus**

Columna	Tipo	Nulo	Comentarios
idestatus	Int(20)	No	Identificados de la tabla
nombre	varchar(50)	No	Nombre del estatus

Fuente: Alvarez y Tochon (2020)

Cuadro 20 **Tabla Controles**

Columna	Tipo	Nulo	Comentarios
idcontrol	Int(20)	No	Identificados de la tabla
dominio	varchar(100)	No	Dominio del Control
objetivo	varchar(100)	No	Objetivo del Control
nombre	varchar(100)	No	Nombre del Control

Fuente: Alvarez y Tochon (2020)

Cuadro 21 **Tabla Disponibilidad**

Columna	Tipo	Nulo	Comentarios
iddisponibilidad	Int(11)	No	Identificados de la tabla
valor	Int(11)	No	Valor de la disponibilidad
nombre	varchar(50)	No	Nombre del tipo de disponibilidad

Fuente: Alvarez y Tochon (2020)

Cuadro 22 **Tabla file**

Columna	Tipo	Nulo	Comentarios
idfile	Int(11)	No	Identificados de la tabla
code	varchar(12)	No	Codigo del documento
filename	varchar(225)	No	Nombre del documento
description	varchar(100)	No	Descripcion del documento
Is_public	tinyint(1)	No	Variable para saber si el documento es público o no
Is_folder	tinyint(1)	No	Variable para saber si esta dentro de una carpeta publica o no
User_id	Int(11)	No	Id usado para saber usuario que subió el documento
Folder_id	Int(11)	Yes	Id de la carpeta
Created_at	datetime	No	Creado para saber cuándo se creo el documento

Fuente: Alvarez y Tochon (2020)

Cuadro 23 **Tabla evaluar_controles**

Columna	Tipo	Nulo	Comentarios
idevaluaciorcontroles	Int(10)	No	Identificados de la tabla
idcontrol	Int(10)	No	foreignkey de la tabla controles
idnivelriesgo	Int(10)	No	foreignkey de la tabla nivel_riesgo
frecuencia	varchar(100)	No	Frecuencia con la que se evaluará el control
tipocontrol	Varchar(100)	No	Tipo de control que se aplicará
automatizacion	Varchar(100)	No	Forma en la que se evaluará el control

Fuente: Alvarez y Tochon (2020)

Cuadro 24 **Tabla modulos**

Columna	Tipo	Nulo	Comentarios
idmodulos	Int(10)	No	Identificados de la tabla
nombre	Varchar(100)	No	Nombre de los modulos

Fuente: Alvarez y Tochon (2020)

Cuadro 25 **Tabla Impacto**

Columna	Tipo	Nulo	Comentarios
idimpacto	Int(20)	No	Identificados de la tabla
valor	Int(20)	No	Valor del impacto
nombre	varchar(50)	No	Nombre del impacto

Fuente: Alvarez y Tochon (2020)

Cuadro 26 **Tabla integridad**

Columna	Tipo	Nulo	Comentarios
idintegridad	Int(11)	No	Identificados de la tabla
valor	Int(11)	No	Valor de la integridad
nombre	varchar(50)	No	Nombre de la integridad

Fuente: Alvarez y Tochon (2020)

Cuadro 27 **Tabla nivel_riesgo**

Columna	Tipo	Nulo	Comentarios
idnivelriesgo	Int(10)	No	Identificados de la tabla
idamenaza	Int(11)	No	foreignkey de la tabla amenazas
idprobabilidad	Int(10)	No	foreignkey de la tabla probabilidad
idimpacto	Int(10)	No	foreignkey de la tabla impacto
idactivo	Int(10)	No	foreignkey de la tabla activos
riesgo	Varchar(50)	No	Nombre de los riesgos
idauditoria	Int(10)	No	Foreignkey de la tabla auditoria

Fuente: Alvarez y Tochon (2020)

Cuadro 28 **Tabla tareas**

Columna	Tipo	Nulo	Comentarios
idtarea	Int(20)	No	Identificados de la tabla
idusuario	Int(20)	No	foreignkey de la tabla usuarios
idestatus	Int(20)	No	foreignkey de la tabla estatus
nombre	Varchar(100)	No	Nombre del a tarea

Fuente: Alvarez y Tochon (2020)

Cuadro 29 **Tabla probabilidad**

Columna	**Tipo**	**Nulo**	**Comentarios**
idprobabilidad	Int(10)	No	Identificados de la tabla
valor	Int(20)	No	Valor de la probabilidad
nombre	Varchar(50)	No	Nombre de las probabilidades

Fuente: Alvarez y Tochon (2020)

Cuadro 30 **Tabla tipoactivo**

Columna	**Tipo**	**Nulo**	**Comentarios**
idtipoactivo	Int(20)	No	Identificados de la tabla
nombre	varchar(50)	No	Nombre del tipo de activo

Fuente: Alvarez y Tochon (2020)

Cuadro 31 **Tabla tipoamenazas**

Columna	**Tipo**	**Nulo**	**Comentarios**
idtipoamenazas	Int(20)	No	Identificados de la tabla
descripcion	varchar(100)	No	Descripción de la amenaza

Fuente: Alvarez y Tochon (2020)

Cuadro 32 **Tabla tipousuario**

Columna	**Tipo**	**Nulo**	**Comentarios**
idtipousuario	Int(20)	No	Identificados de la tabla
nombre	varchar(50)	No	Nombre del tipo de usuario

Fuente: Alvarez y Tochon (2020)

Cuadro 33 **Tabla usuarios**

Columna	**Tipo**	**Nulo**	**Comentarios**
idusuario	Int(20)	No	Identificados de la tabla
idestatus	Int(20)	No	foreignkey de la tabla estatus
idtipousuario	Int(20)	No	foreignkey de la tabla tipousuarios
nombre	varchar(50)	No	Nombre del usuario
apellido	varchar(50)	No	Apellido del usuario
correo	varchar(50)	No	Correo del usuario
clave	varchar(50)	No	Clave del usuario
image	varchar(255)	No	Imagen del usuario

Fuente: Alvarez y Tochon (2020)

Cuadro 34 **contactoinicial**

Columna	**Tipo**	**Nulo**	**Comentarios**
idcontactoinicial	Int(11)	No	Identificador de la tabla
idempresa	int(11)	No	Foreignkey de la tabla empresa
nombre	Varchar(50)	No	Nombre del auditado
apellido	Varchar(50)	No	Apellido del auditado
idusuario	int(11)	No	Foreignkey de la tabla usuario
fecha	date	No	Fecha de la creación del registro
descripcion	text	No	Descripción de la reunión

Fuente: Alvarez y Tochon (2020)

Cuadro 35 **recomendaciones**

Columna	Tipo	Nulo	Comentarios
idrecomendaciones	Int(11)	No	Identificador de la tabla
idempresa	Int(11)	No	Foreignkey de la tabla empresa
idauditoria	Int(11)	No	Foreignkey de la tabla auditoria
descripcion	text	No	Descripción de las recomendaciones

Fuente: Alvarez y Rashel (2020)

4.3.2 Diagramas de caso de uso

En el sistema planteado existen tres tipos de usuarios: administrador, líder y usuario, en donde se mostrara las tareas o actividades de cada uno. Para el desglose de dichas tareas, se plantean los siguientes diagramas de caso de uso:

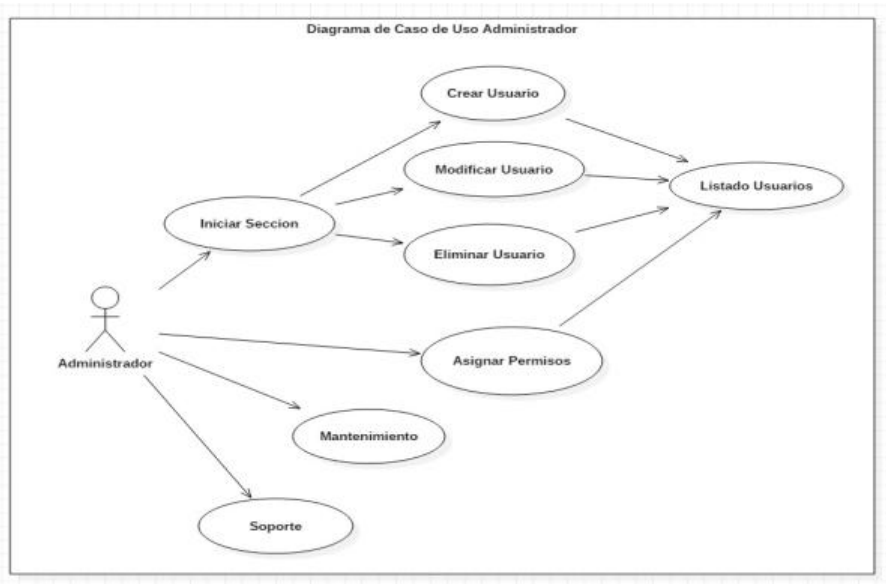

Figura 4 **Diagrama caso de uso del usuario administrador**

Fuente: Alvarez y Tochon (2020)

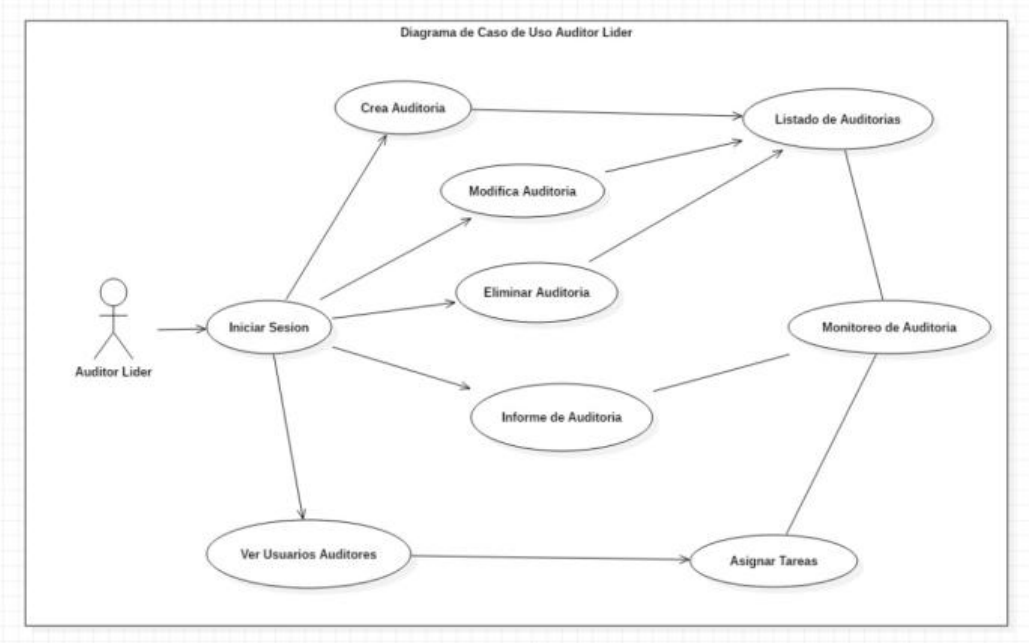

Figura 5 **Diagrama caso de uso del usuario auditor líder**

Fuente: Alvarez y Tochon (2020)

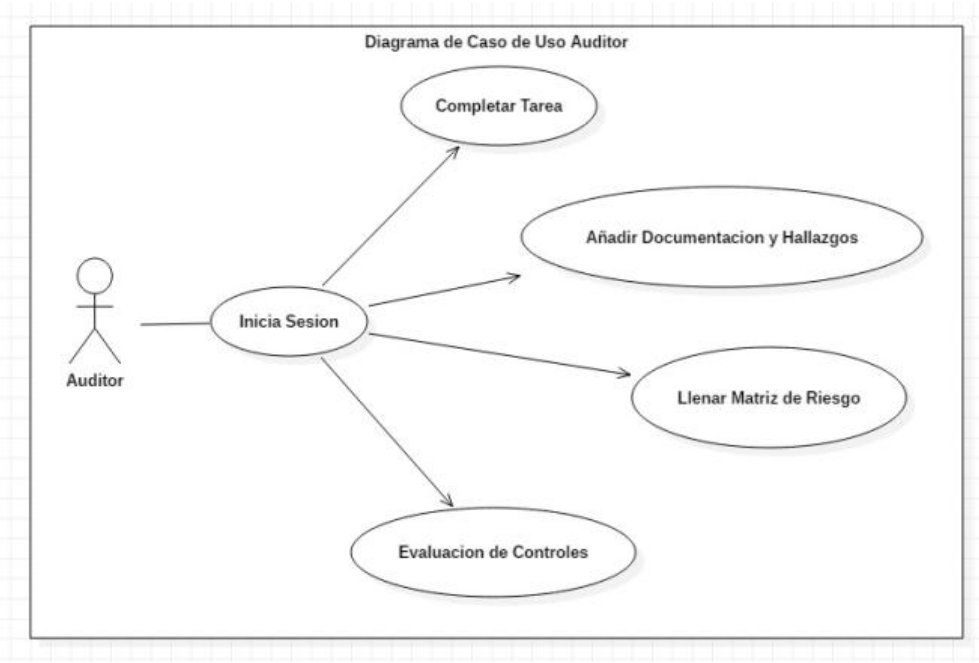

Figura 6 **Diagrama de caso de uso del usuario auditor**

Fuente: Alvarez y Tochon (2020)

4.3.3 Funcionamiento del sistema

En las siguientes figuras se muestra el funcionamiento de los módulos principales del sistema:

Figura 7 **Inicio de Sesión**
Fuente: Alvarez y Tochon (2020)

Descripción: el usuario al ingresar a la aplicación web podrá visualizar un formulario donde deberá ingresar el correo y la clave para tener acceso al sistema.

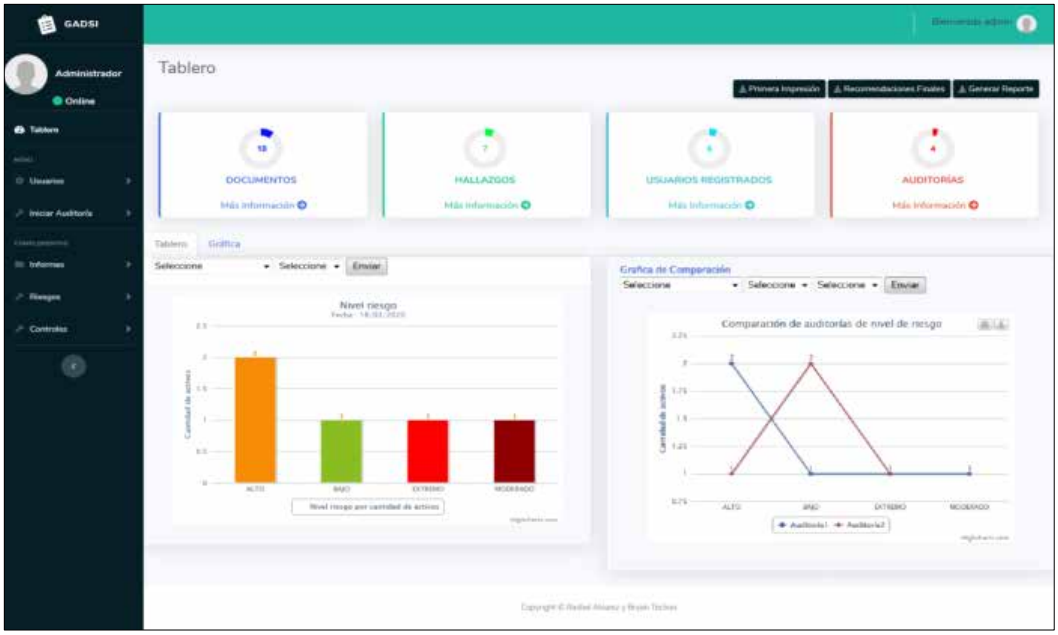

Figura 8 **Dashboard del usuario**
Fuente: Alvarez y Tochon (2020)

Descripción: una vez ya autentificado el usuario ingresara automáticamente a la pantalla inicial.

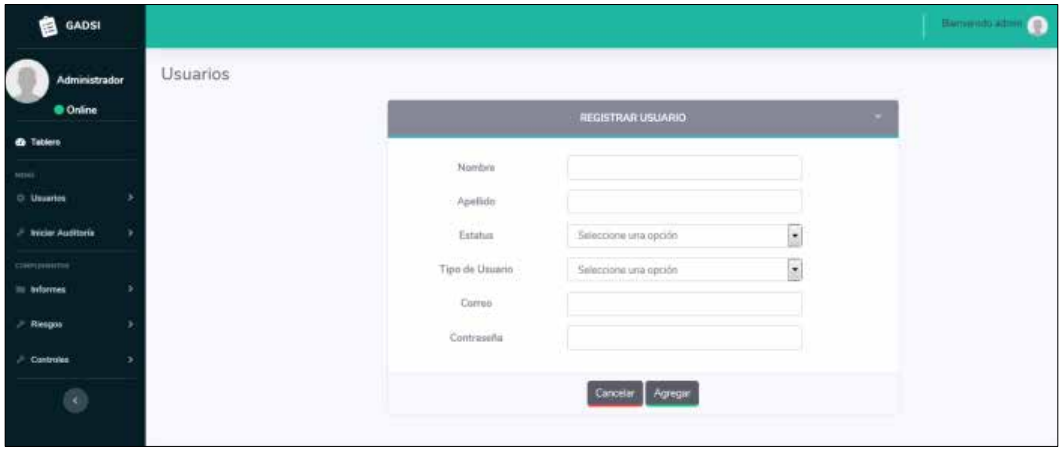

Figura 9 **Registro de usuarios**

Fuente: Alvarez y Tochon (2020)

Descripción: se muestra el formulario de registro de usuarios.

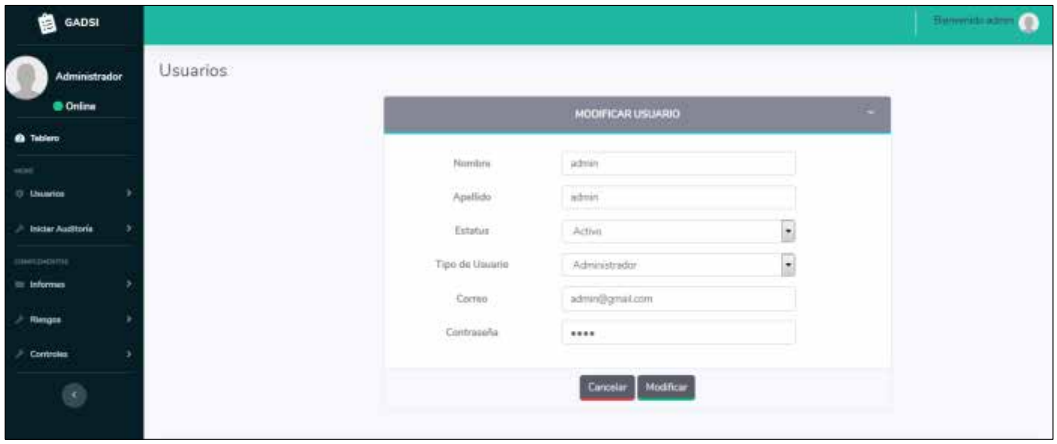

Figura 10 **Modificacion de usuarios**

Fuente: Alvarez y Tochon (2020)

Descripción: se muestra el formulario de modificación de usuarios.

Figura 11 **Visualización de usuarios**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información ya registrada en la base de datos.

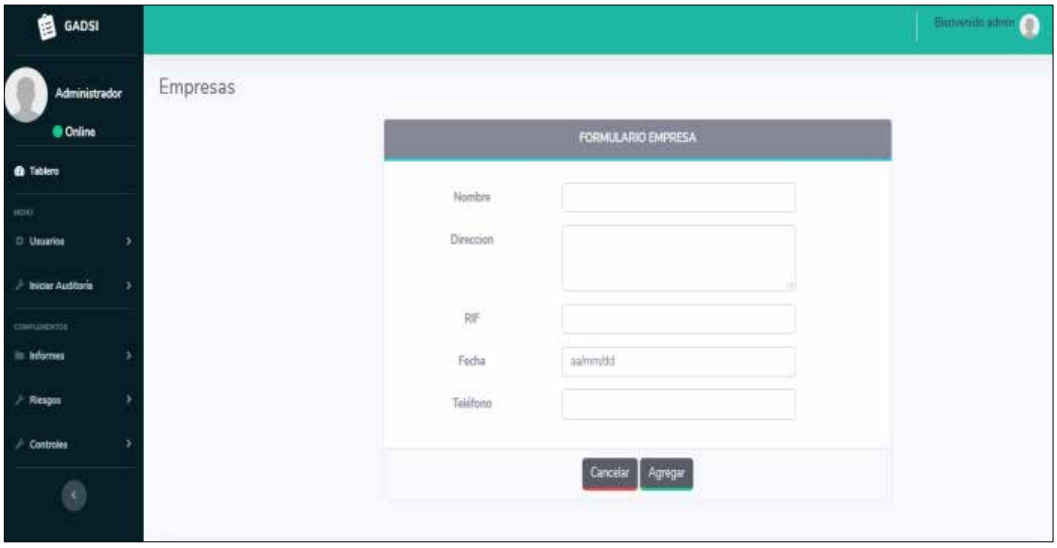

Figura 12 **Registro de empresas**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de las empresas.

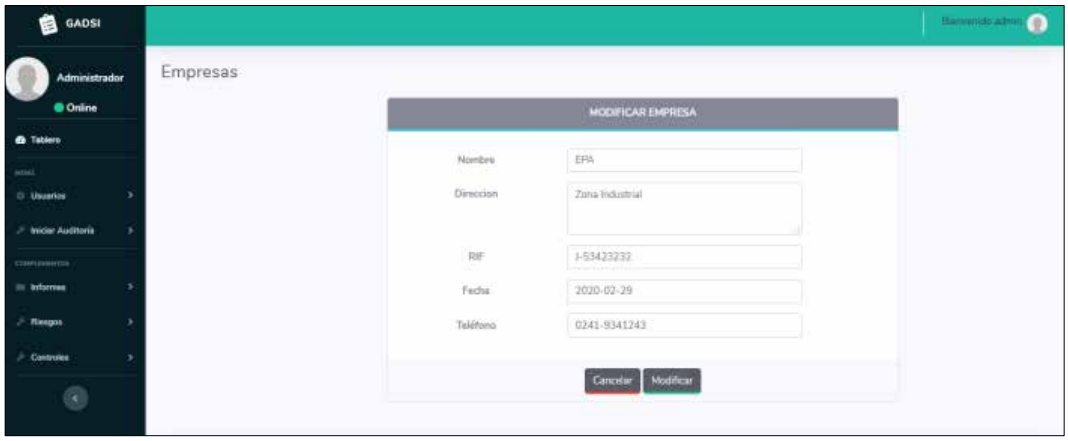

Figura 13 **Modificación de empresas**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de modificación de las empresas.

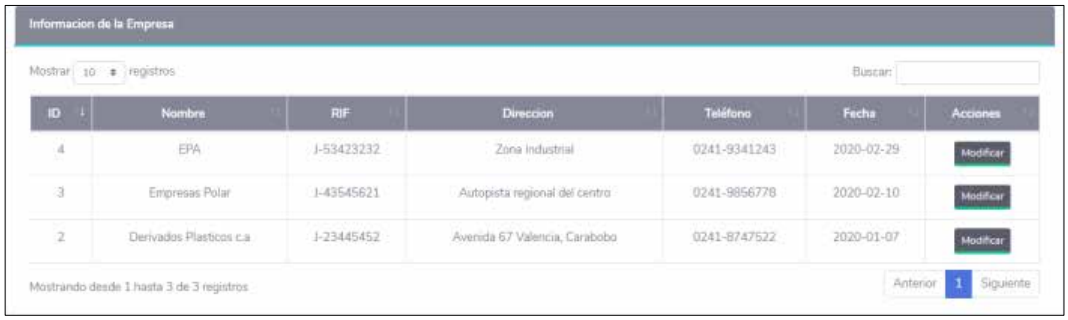

Figura 14 **Visualización de empresas**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información ya registrada en la base de datos.

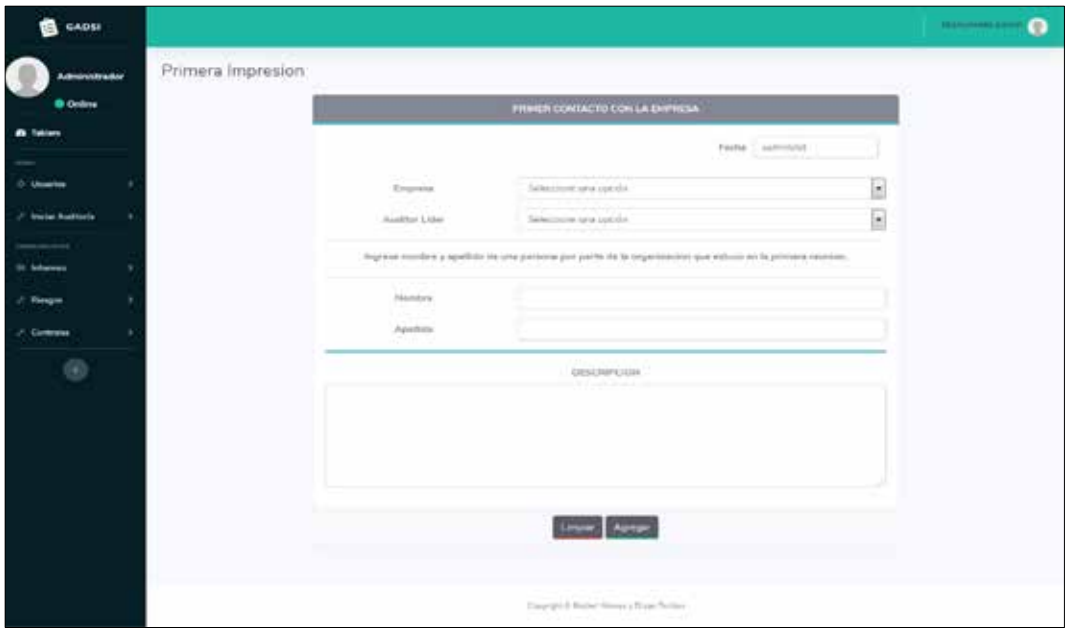

Figura 15 **Registro del primer contacto con la empresa**

Fuente: Alvarez y Tochon (2020)

Descripción: en la pantalla se puede ver un formulario que sirve para registrar la información de la primera reunión que se tuvo con la empresa.

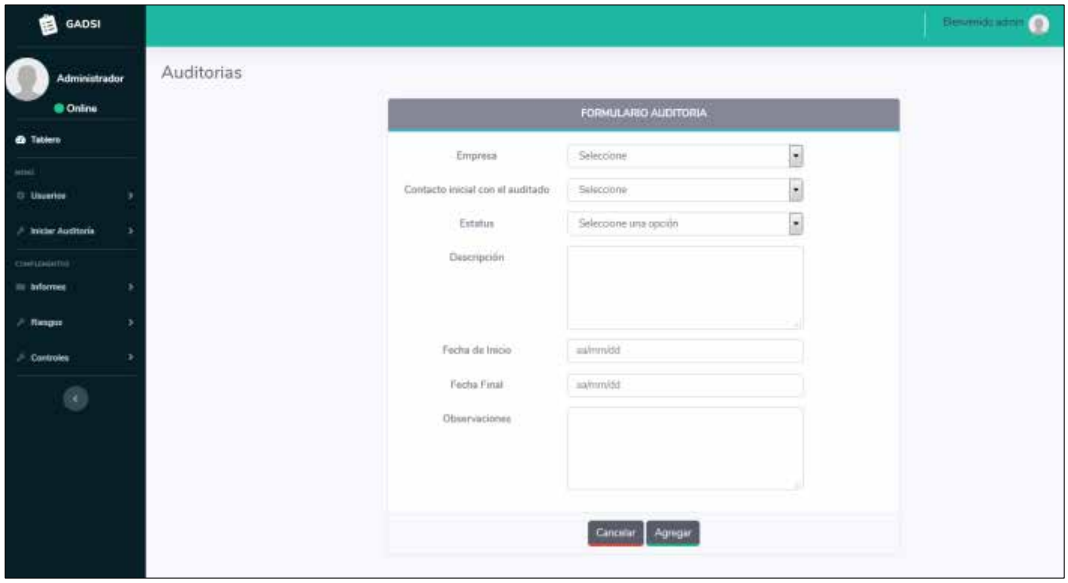

Figura 16 **Registro de auditorias**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de auditorías.

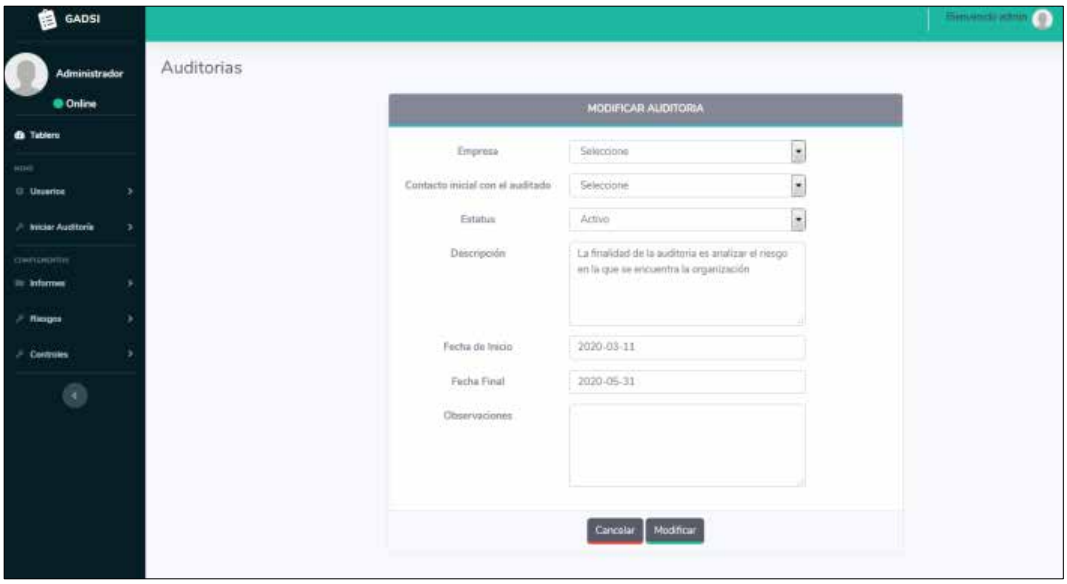

Figura 17 **Modificación de auditorias**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de modificación de auditorías.

Figura 18 **Visualización de auditorías**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información de las auditorías ya registrada en la base de datos.

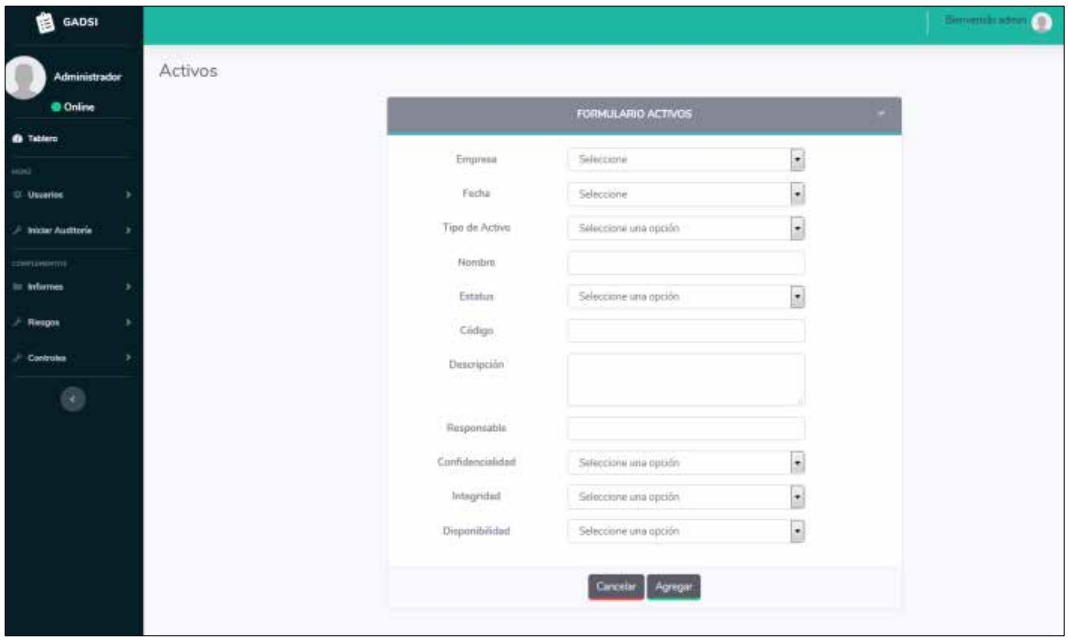

Figura 19 **Registro de activos**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de activos.

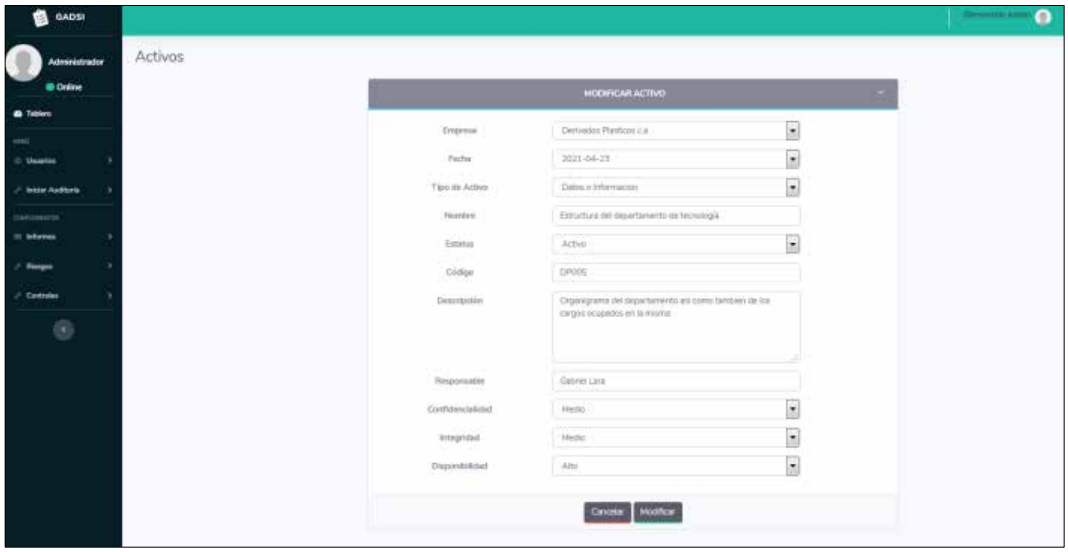

Figura 20 **Modificación de activos**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de modificación de activos.

Figura 21 **Visualización de activos**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información de los activos ya registrados en la base de datos.

Figura 22 **Registro de amenazas**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de las amenazas.

Figura 23 **Modificación de las amenazas**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de modificación de las amenazas.

Figura 24 **Visualización de las amenazas**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información de las amenazas ya registrados en la base de datos.

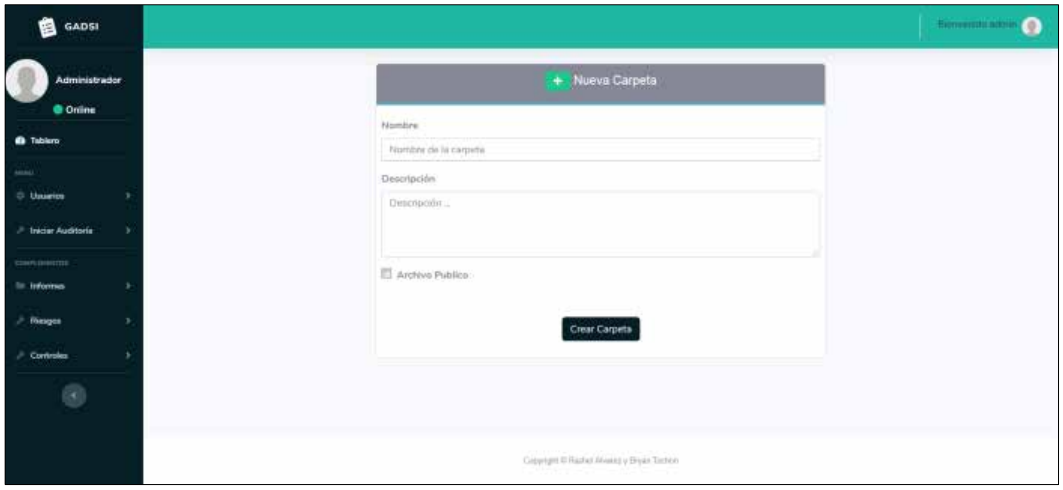

Figura 25 **Registro de nueva carpeta**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de una nueva carpeta.

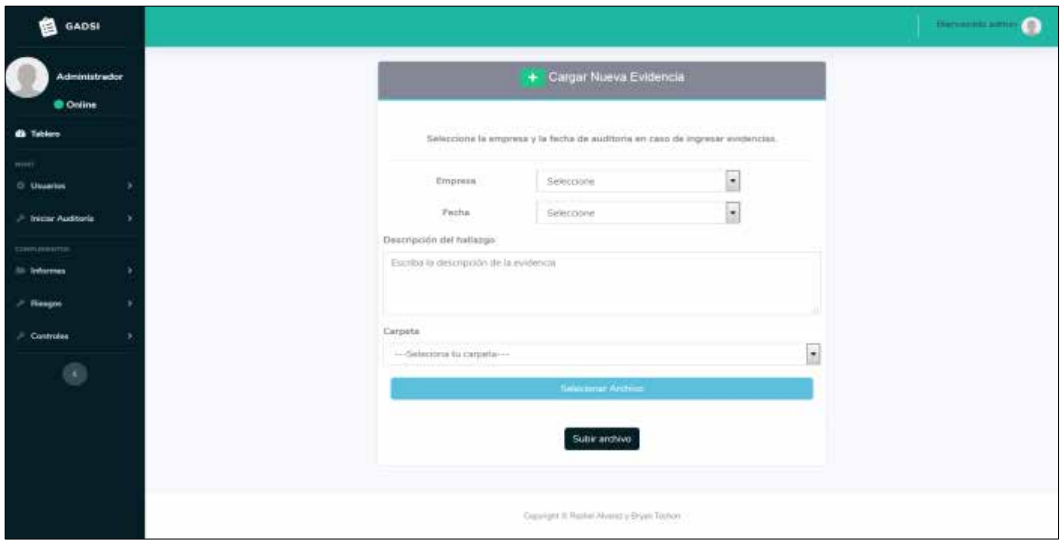

Figura 26 **Registro de nueva evidencia y hallazgo**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de una nueva evidencia junto con la descripción del hallazgo.

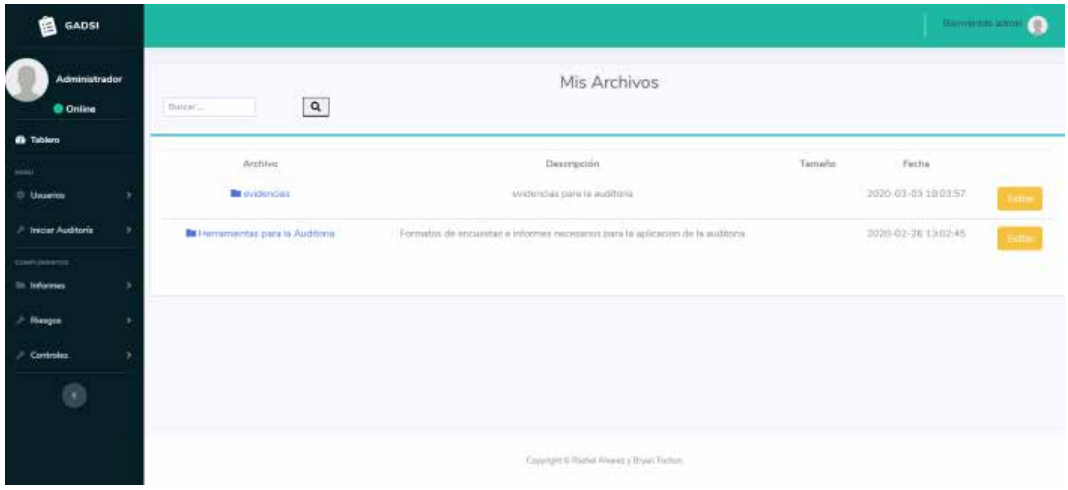

Figura 27 **Visualización de archivos**

Fuente: Alvarez y Tochon (2020)

Descripción: pantalla de la carpetas, evidencias y archivos ya registrados en la base de datos.

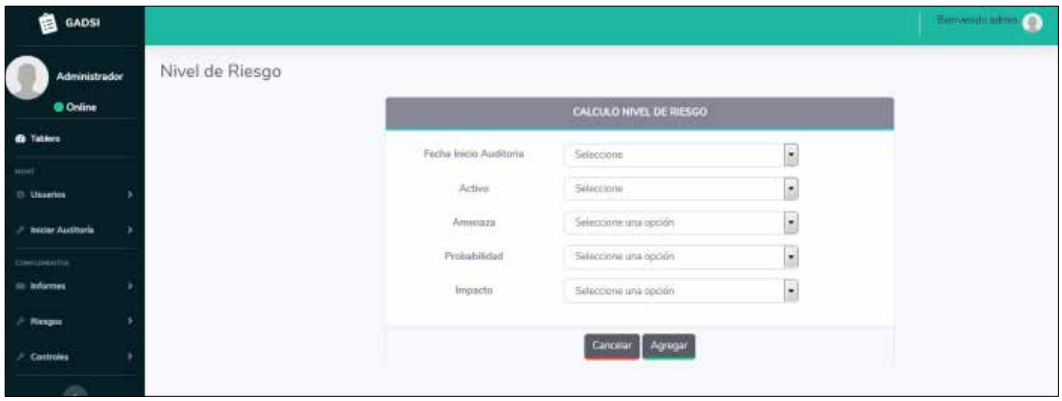

Figura 28 **Registro del cálculo del nivel de riesgo**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de registro de nivel de riesgo.

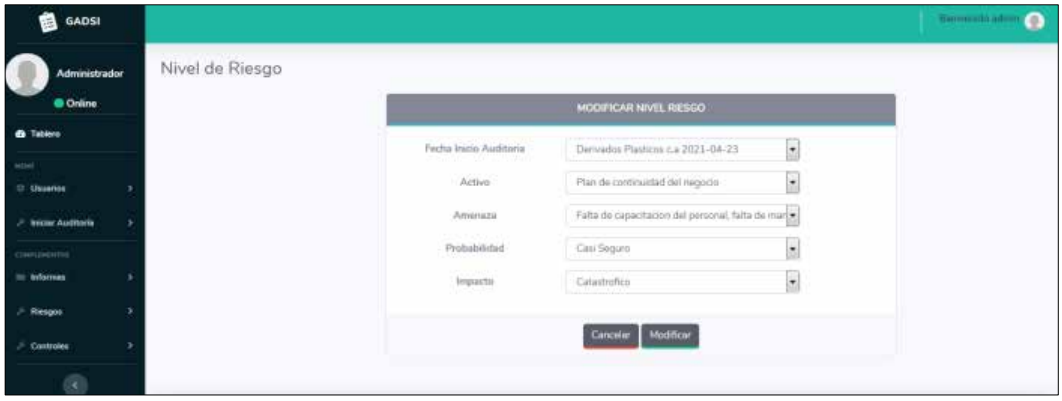

Figura 29 **Modificación del nivel de riesgo**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario de modificación de nivel de riesgo.

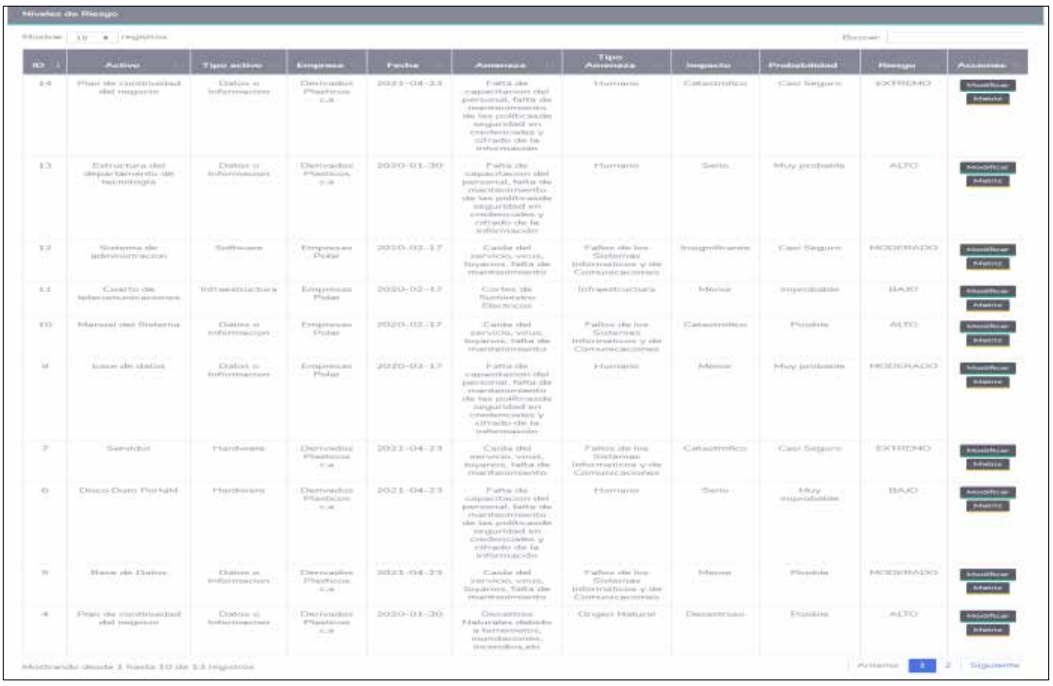

Figura 30 **Visualización del cálculo de nivel de riesgo**

Fuente: Alvarez y Tochon (2020)

Descripción: mediante un Datatable el usuario puede ver la información del cálculo de nivel de riesgo ya registrados en la base de datos.

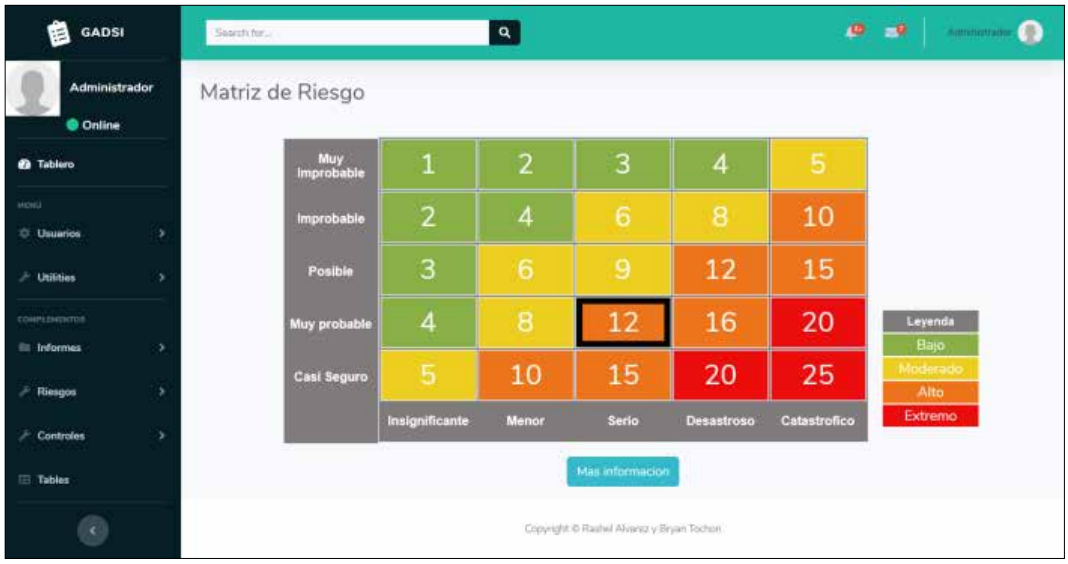

Figura 31 **Matriz de riesgo**

Fuente: Alvarez y Tochon (2020)

Descripción: generación de la matriz de riesgo del activo seleccionado.

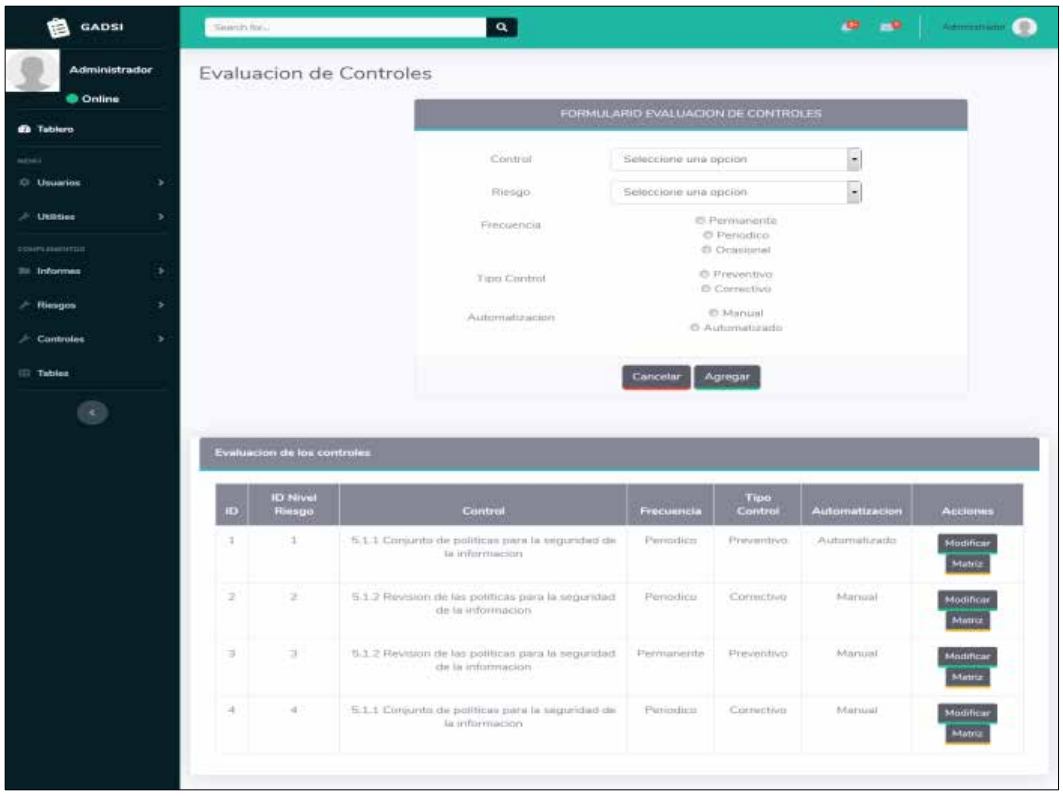

Figura 32 **Evaluación de controles**

Fuente: Alvarez y Tochon (2020)

Descripción: formulario y visualización de la evaluación de controles

Figura 33 **Escenario Schwartz de riesgos**

Fuente: Alvarez y Tochon (2020)

Descripción: en la pantalla se puede visualizar el escenario de schwartz el cual cuando se selecciona la empresa y la fecha de auditoría se obtiene de la base de datos los activos que corresponde a cada nivel de riesgo.

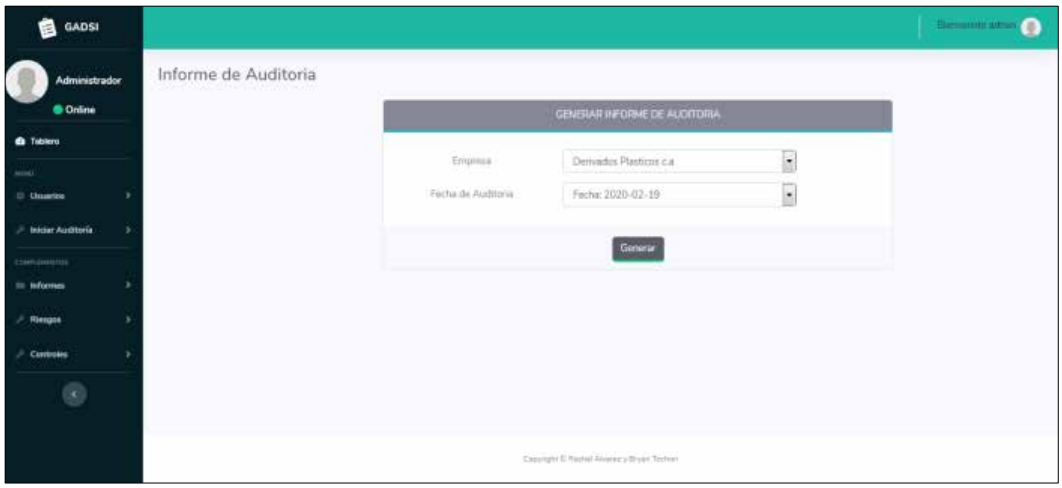

Figura 34 **Formulario para generar informe final de auditoria**

Fuente: Alvarez y Tochon (2020)

Descripción: en la pantalla se puede visualizar el formulario para generar el informe final de auditoría

.

Figura 35 **Informe final de auditoria**

Fuente: Alvarez y Tochon (2020)

Descripción: en la pantalla se puede visualizar el informe final de auditoría en formato PDF.

4.4 Fase 4: Verificación

En esta fase se procedió a realizar las pruebas para la comprobación del funcionamiento óptimo de dicho sistema, el cual se llevo a cabo pruebas de caja negra y caja blanca

Cuadro 36: **Caso de Prueba 1**

Programa:	Aplicación Web para la gestión de Auditoria de Sistemas de Información.	
Pruebas:	**Numero:**	**1**
	Estrategia:	**Caja Blanca**
Técnica de Prueba:	Verificar que solo puedan acceder personas registradas.	
Resultados:	El botón de ingresar del login, envía al usuario directamente al index con o sin datos en el formulario.	
Decisión:	Corregir el código de validación de datos en el formulario del login en el archivo validar.php para que pueda entrar solo personas registradas.	

Autores: Tochon, Bryan y Alvarez, Rashel (2020).

Cuadro 37: **Caso de Prueba 2**

Programa:	Aplicación Web para la gestión de Auditoria de Sistemas de Información.	
Pruebas:	**Numero:**	**2**
	Estrategia:	**Caja Negra**
Técnica de Prueba:	El usuario inicia sesión en el sistema y se debe mostrar el menú según el tipo de usuario.	
Resultados:	El proceso de inicio fue exitoso, pero no se establecen los permisos y menú correspondientes según el tipo de usuario con el que se inicia sesión.	
Decisión:	Establecer correctamente las variables de Sesión en el sistema.php para que establezca los permisos y menú correspondientes a cada usuario.	

Autores: Tochon, Bryan y Alvarez, Rashel (2020).

Cuadro 38: **Caso de Prueba 3**

Programa:	Aplicación Web para la gestión de Auditoria de Sistemas de Información.	
Pruebas:	**Numero:**	**3**
	Estrategia:	**Caja Blanca**
Técnica de Prueba:	Registrar Usuario	
Resultados:	El botón agregar del formulario registrar usuarios, no llama la función agregar.php correctamente.	
Decisión:	Corregir el código donde está la ruta de agregar.php en el botón del formulario de registro de usuarios para que funcione.	

Autores: Tochon, Bryan y Alvarez, Rashel (2020).

Cuadro 39: **Caso de Prueba 4**

Programa:	Aplicación Web para la gestión de Auditoria de Sistemas de Información.	
Pruebas:	**Numero:**	**4**
	Estrategia:	**Caja Blanca**
Técnica de Prueba:	Prueba para registrar una amenaza	
Resultados:	En el formulario de amenazas es necesario agregar un campo de descripción para especificar más la amenaza.	
Decisión:	Corregir el código del formulario de amenazas y añadirle la variable $descripcion dentro del archivo frmAmenazas.php para poder capturar la información pertinente de ese campo, y además añadir el campo descripción en el formulario.	

Autores: Tochon, Bryan y Alvarez, Rashel (2020).

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Luego de haber concluido el desarrollo de la Aplicación web para la gestión de auditoría de los sistemas de información y cumpliendo con el funcionamiento de las fases correspondientes y tomando como referencia los resultados obtenidos en la presente investigación, se desprende las siguientes conclusiones:

El diagnóstico de la situación con relación al proceso de recolección de datos permitió un entendimiento y planificación completa de la estructura del sistema referente a las auditorias de los sistemas de información, permitiéndonos centrarnos en la seguridad de la información y automatización de los procesos de auditabilidad, pudiendo así hacer todo el levantamiento de información necesario para fundamentar el sistema de información a desarrollar.

A través de las técnicas de recolección de datos como lo fue la entrevista no estructurada y observación directa, se logró ser más preciso con los requisitos fundamentales para el desarrollo del sistema propuesto.

El programa está parametrizado bajo las normas ISO 27001 y 19011 de auditabilidad correspondiente, los cual fueron de ayuda en gran parte para los requisitos funcionales y no funcionales dándole una mejor estructura a las bases de auditabilidad; El modelo de implementación sistemática maneja mejor la representación de la confidencialidad, la integridad y la disponibilidad de la información de una organización auditada, y además dando respaldo al auditor de dar un trabajo más eficiente.

Con el desarrollo de una aplicación web se logró una fácil demostración de los riesgos de cada activo de una organización bajo una Matriz de Riesgo, demostrando en qué nivel crítico está cada activo de la organización y la visualización grafica casi inmediata de cada activo con su riesgo correspondiente.

Adicional a esto, le logró que el auditor pueda aplicar los controles necesarios para disminuir dichos riesgos según las normas ISO 27001 y 19011 de auditabilidad, mostrando la disminución de este en una Matriz de Riesgo para

demostrar el valor critico en el que se encuentra ya después de haber sido aplicado dicho control.

Con el respaldo de documentos, hallazgos y evidencia por parte de los auditores, se elabora un informe final donde se obtiene de forma legible y agradable el análisis estadístico generando de manera clara y transparente el rendimiento de los activos de una organización, siguiendo las normas ISO 27001 y 19011 de auditabilidad correspondiente.

Con el desarrollo de una interfaz práctica, portable, segura y cómoda se busca el mayor confort para los usuarios que podrían usar la aplicación de una forma fluida y agradable, se logró comprender la necesidad del desarrollo de una interfaz intuitiva para el correcto funcionamiento de cualquier sistema siendo parte principal del cuerpo de cualquier proyecto.

Por medio del uso de pruebas de tipo caja negra y caja blanca se logró obtener un grado de respuesta adecuado verificando que los resultados obtenidos a través de ellos sean los correctos para la realización de los distintos procesos que el sistema posee.

5.2 Recomendaciones

Para mejorar el funcionamiento de sistema, se plantean las siguientes recomendaciones:

Se recomienda un modulo para evaluar el desempeño del auditor el cual se visualizara mediante una barra de progreso o una grafica.

También se recomienda un modulo para el cálculo del presupuesto de auditoría en base a las horas dedicadas al proyecto desde que se inicio hasta que finalizo la auditoria.

Agregar al informe final los gráficos correspondientes.

Además, se recomienda la aplicación de colores personalizados para la matriz de riesgo.

También es necesario implementar una mensajería privada entre usuarios para que estén siempre comunicados.

Alertas para avisar al usuario líder que la auditoria está por finalizar.

Por otro lado, es necesario la implementación de un modulo que gestione los permisos personalizados para el auditor líder.

Implementación de diferentes metodologías para el Sistema de Gestión de Seguridad de la Información.

REFERENCIAS

Bibliográficas

Gaceta Oficial Nº 37.313 **Ley Especial contra los Delitos Informáticos** (2001)

Electrónicas

Aguilar (2014) **"Evaluación del diseño y efectividad de los controles internos"** https://es.slideshare.net/miguelserrano5851127/evaluacin-del-diseo-y-efectividad-de-los-controles-internos-12mar2014-dr-miguel-aguilar-serrano

Alonso, G. (2018), "**Auditoría Informática y la Calidad del Servicio de las Tecnologías de la Información en el Distrito de Educación Colta - Guamote."**

Alvarez, L. (2005). **"Seguridad en Informática"**. Universidad Iberoamericana de México D.F. http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Damani, N. (2014). **"Gestión de riesgos"** https://www.theific.org/wp-content/uploads/2014/08/Spanish_ch27_PRESS.pdf

Escuela Europea por Excelencia (2019). **"Como evaluar la consecuencia y la probabilidad en el análisis de riesgos ISO 27001"** https://www.escuelaeuropeaexcelencia.com/2019/03/como-evaluar-las-consecuencias-y-la-probabilidad-en-el-analisis-de-riesgos-iso-27001/

Fernández, C. (2012). **"La Norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información".** https://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

Guillermo, G. (2019). **"Vulnerabilidades Informáticas".** https://tecnologia-informatica.com/vulnerabilidades-informaticas/

INCIBE (2015). **"Gestión de riesgos".** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf.

INCIBE (2015). **"Implantación de un SGSI en una empresa".** https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27002. (2012). **"Control de Accesos".** http://www.iso27000.es/iso27002_9.html

ISO 27002. (2012). **“Seguridad Física y Ambiental”.** http://www.iso27000.es/iso27002_11.html

ISO 19011. **“Norma ISO 19011 Directrices para la auditoria de los sistemas de gestión”.** https://www.cecep.edu.co/documentos/calidad/norma-iso-19011-2018.pdf

Lascano, W. (2016). **“Auditoria Informática para Mejorar la Gestión de las Tecnologías de la Información en el Ministerio del Trabajo Regional Ambato”**

Martínez, L. (2016). **“Medir los efectos de la auditoria, tarea primordial”.** Universidad de Cienfuegos en Cuba. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000200006.

Melo, J. (2013). **“Auditoria de sistemas aplicada al sistema de información de la cooperativa del magisterio de Tuquerres Coacremat”.** http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/89740.pdf

NovaSec (2018) **“ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI”** https://www.novasec.co/en/blog/62-gestion-integral-de-la-seguridad-de-la-informacion

Pedraza, A. (2018). **“Auditoría de los Sistemas de Información en la Organización”.** https://www.gestiopolis.com/auditoria-de-sistemas- de-informa cion -en-la-organizacion/

Salazar, A. (2016). **“Análisis de riesgos, amenazas y vulnerabilidades de la compañía pinzón pinzón & asociados en su área de ti y planteamiento de los controles a aplicar basados en la norma iso 27001:2013”** http://polux.unipiloto.edu.co:8080/00003291.pdf

Velásquez, J. (2016). **“Sistema de Información para el Manejo de Inventario en la Empresa Inversiones Camino Real C.A.”.**

Villalobos, J. (2008). **“Auditando en las bases de datos”.** Universidad Nacional de Costa Rica. https://dialnet.unirioja.es/descarga/articulo/5381374.pdf