UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

DISEÑO DE UN MODELO DE AUTOMATIZACIÓN PARA LA TOMA DE EVIDENCIAS DOCUMENTALES DE LAS PRUEBAS DE CUMPLIMIENTO EN LA AUDITORÍA DE TI

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ

ANDRÉS FELIPE QUEVEDO VEGA

ANDRÉS FELIPE SÁNCHEZ SÁNCHEZ

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

BOGOTÁ D.C 2017

DISEÑO DE UN MODELO DE AUTOMATIZACIÓN PARA LA TOMA DE EVIDENCIAS DOCUMENTALES DE LAS PRUEBAS DE CUMPLIMIENTO EN LA AUDITORÍA DE TI

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ

ANDRÉS FELIPE QUEVEDO VEGA

ANDRÉS FELIPE SÁNCHEZ SÁNCHEZ

Trabajo de grado para obtener el título de especialista en auditoria de sistemas df información

ASESOR: ALEXANDRA LÓPEZ

INGENIERA DE SISTEMAS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

BOGOTÁ D.C 2017

Nota de aceptación

_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., diciembre de 2017.

DEDICATORIA

Dedicamos este proyecto primeramente a Dios por ser nuestro faro en cada paso en nuestras carreras profesionales, a nuestros padres por ser nuestro apoyo y fortaleza en cada nuevo reto que tomamos en nuestras vidas y con los que contamos en todo momento; a nuestros parejas, quienes nos han apoyado de manera incondicional en el desarrollo de nuestra especialización, a todos los profesores que compartieron su conocimiento con nosotros cuyo trabajo nos ayuda en la formación como especialistas y a nuestros compañeros que nos apoyaron y crecimos como especialistas en auditoria de sistemas de información durante este año.

AGRADECIMIENTOS

Este trabajo de grado es el consolidado de un proceso de crecimiento personal, intelectual y profesional en nuestras vidas. Agradecemos a Dios el creador del universo que me permite construir otros mundos mentales.

A nuestras familias por el apoyo incondicional y su acompañamiento en este proceso de crecimiento.

A los profesores de la especialización, que con su profesionalismo lograron transmitir sus mejores conocimientos.

A nuestra asesora de trabajo de grado ALEXNDRA LOPEZ, por su apoyo y colaboración en la consolidación de los conocimientos adquiridos en este trabajo de grado.

A todas aquellas personas que de una u otra manera participaron y nos acompañaron en este proceso tan significativo para nosotros.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

RESUMEN

En la actualidad la auditoria de TI es una prioridad para las grandes, medianas y pequeñas empresas, por este motivo se han desarrollado técnicas y metodologías para gestionar las auditorias de TI, con el motivo de evitar la difusión de amenazas y vulnerabilidades dentro de las organizaciones.

Para el desarrollo del proyecto se investigó sobre las metodologías, buenas prácticas con el fin de gestionar las auditoria de TI, buscando las más alineadas a la recolección de la evidencias como también la ejecución de las pruebas que se hacen a los controles en los sistemas de información, lo anterior con el fin de realizar un diagnóstico de selección de las metodologías aplicables para la toma de evidencias de auditoria de TI, así mismo se identificaran las características de las aplicaciones utilizadas en la gestión de auditorías de TI también llamadas herramientas CAAT con sus características funcionales para categorizar su eficacia versus metodologías aplicada, para continuar con el análisis de los resultados de las metodologías y así plantear un modelo para automatizar la toma de evidencias documentales en las pruebas de cumplimiento en auditoría de TI, basado en una metodología.

Palabras clave: auditorias de TI, amenazas, vulnerabilidades, evidencias, pruebas, CAAT.

ABSTRACT

Nowadays IT audit is a priority for large, medium and small companies, for this reason techniques and methodologies have been developed to manage IT audits, in order to avoid the spread of threats and threats within organizations.

For the development of the project, methodologies and good practices were investigated in order to manage IT audits, looking for the most aligned to the collection of evidences as well as the execution of the tests that are done to the controls in the systems of information, the foregoing in order to make a diagnostic selection of the available methodologies for the taking of IT audit evidence, as well as identify the characteristics of the applications used in the management of IT audits also called CAAT tools with their Functional aspects to categorize their effectiveness against applied methodologies, for the analysis of the results of the methodologies and thus propose a model to automate the taking of documentary evidence in compliance tests in IT audit, based on a methodology.

Key words: IT audits, threats, vulnerabilities, evidence, tests, CAAT.

INTRODUCCIÓN

Uno de los activos más importantes de las organizaciones es la información. Por esta razón, las organizaciones se están ocupando por realizar una mejor gestión de sus activos de forma eficiente y segura (infysis, 2009).

Por lo anterior, en las organizaciones se aplica el proceso de auditoría a los sistemas de información, que consiste en verificar los controles y su cumplimiento. De igual manera, se implementan diversos tipos de pruebas, dentro de ellas está la prueba de cumplimiento. Esta prueba es la que determina que un sistema de control interno en una organización funciona adecuadamente y según las políticas y procedimientos de la organización.

Actualmente, el proceso más complejo en la ejecución de una auditoría de TI para un auditor es la creación y ejecución de pruebas de auditoría (Salgado, 2012). Este proceso involucra un diseño previo, la aplicación manual, la toma de evidencia de los resultados de su aplicación y por último con mayor complejidad la creación del reporte donde se evidencien los resultados de las pruebas aplicadas.

Este proyecto se enfoca en el diseño de un modelo funcional para la creación y ejecución de pruebas de cumplimiento para las auditorías de TI, presentando una alternativa para la gestión de pruebas que permita facilitar el proceso y además emitir juicios basados en metodologías de análisis y gestión de riesgos.

Por consiguiente, se desarrolla un diagnóstico donde se involucran varias metodologías para la gestión de auditoria de TI con el fin de seleccionar una metodología aplicable para la toma de evidencias de auditoria de TI, paso siguiente se identifican las características funcionales de las aplicaciones utilizadas en la gestión de pruebas de auditoria TI y así categorizar su eficacia con respecto a la metodología que estas aplican.

Basados en lo anterior analizar los resultados de las metodologías y la categorización de las aplicaciones utilizadas en las pruebas de auditoria de TI, para efectuar el desarrollo de un prototipo funcional enfocado a la toma de evidencias documentales en las pruebas de cumplimiento en las auditorias de TI siguiendo las buenas prácticas de una metodología.

1. GENERALIDADES

1.1.Línea de Investigación

El proyecto se en marca en la modalidad de "Software inteligente y convergencia tecnológica", toda vez que, al realizar el desarrollo y estudio de esta problemática, se pueden identificar diferentes variables que evidencian alguna falencia que hay en los procesos de la auditoria de TI.

De la misma forma, el proyecto está desarrollado en torno a la necesidad de los auditores de mejorar el proceso de las pruebas a los controles en auditoria de TI y por el contexto validar las metodologías más usadas para gestionar la auditoria con enfoque a las evidencias y a las pruebas.

Por otro lado, se analizarán las técnicas de auditoria asistidas por computadora para definir los requerimientos funcionales y así plantear un prototipo funcional en la toma de evidencias de una auditoria de TI.

1.2.Alcance del proyecto

Este proyecto está sujeto al diseño de un modelo de automatización para recopilar las evidencias documentales que puedan surgir en las pruebas de cumplimiento en la auditoría de TI, con un tiempo estimado de cuatro meses. En el desarrollo de este proyecto se hará un diagnóstico de las diversas metodologías para la gestión de auditorías de TI basadas en la gestión de riesgos y verificación de controles. Al realizar el diagnóstico se genera una matriz

donde se observarán las principales ventajas de cada una de ellas y los criterios de escogencia que se tendrá para definir una metodología.

Por consiguiente, se identifica las aplicaciones utilizadas en la gestión de auditoria TI y las características funcionales de las herramientas automatizadas, con el fin de analizar que metodología y el valor agregado que tiene el prototipo funcional para tomar evidencias documentales en las pruebas de cumplimiento con el propósito de elaborar un listado de requisitos priorizados.

Por último, se validará el prototipo funcional por medio de la ejecución de una auditoria TI en un proceso y organización específica para generar un informe de resultado, con el propósito de saber si la automatización de la toma de evidencias documentales en las pruebas de cumplimiento si cumplen con la optimización el proceso de la auditoria de TI.

1.3.Planteamiento del Problema

1.3.1. Antecedentes del problema

El origen de la auditoría surge con el advenimiento de la actividad comercial y por la incapacidad de intervenir en los procesos tanto productivos como comerciales de una empresa.

Por estas razones surge la necesidad de buscar personas capacitadas, de preferencia externas (imparciales), para que se desarrollen mecanismos de supervisión, vigilancia y control de los empleados que integran y desempeñan las funciones relativas a la actividad operacional de la empresa (Sama, 2011).

Hoy en día con los avances de las tecnologías de la información e internet, la seguridad de la información ha tomado una gran importancia para las empresas tanto públicas como privadas ya que la información que estas tiene de su negocio es uno de los activos más importantes. En este sentido las organizaciones día a día se enfrentan a diversos problemas (Rodriguez, 2011).

"La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, esta deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además deberá evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información (Auditoria superior, 2010).

Por lo tanto, la auditoría de sistemas se ha vuelto un proceso que se ejecuta de manera global, por lo que se han venido desarrollando herramientas y metodologías para gestionar la auditoria de TI como: Cobit, ISO 27000, winAudit, MeycorCobiT, entre otros (WinAudit, 2015).

Por lo anterior, se busca realizar la automatización de la toma de evidencias en la pruebas de auditoria de TI, basado en la metodología de Magerit V.3 para ejecución y validación de pruebas de cumplimiento aplicadas a los controles establecidos para la tecnología, promoviendo la trazabilidad y portabilidad del proceso de la auditoria de TI.

1.3.2. Formulación de problema

Uno de los niveles de la ciencia de la computación es la auditoría de TI que nace como una rama que se encarga de verificar los controles en los sistemas de información, para realizar pruebas de cumplimiento de controles con el fin de obtener una evidencia documental y analizarlas; así poder emitir un informe con hallazgos y recomendaciones. Por lo que se han desarrollado metodologías y técnicas asistidas por computadora para el desarrollar una auditoría de TI.

La auditoría de TI es algo determinante para los sistemas de información, al comprobar si se protege los activos de una empresa y mantiene la integridad de los datos. Para ejecutar una auditoria existen metodologías y buenas prácticas para su ejecución como los son: Cobit, Iso27001, Iso 27002, magerit 3 entre otras (Solarte, 2015). Por lo anterior el talento humano que ejecuta la auditoría debe tener conocimiento en estas metodologías.

Por otra parte, existen aplicaciones para gestionar la auditoria de TI también llamadas CAATs (Computer Assisted Audit Techniques), que optimizan este proceso, no obstante, las gestiones de la auditoría de TI por metido de las CAATs pocas veces permiten gestionar la toma de evidencias documentales en el instante que se realizan las pruebas de cumplimiento ya que son de uso local (Villa, 2016).

De esta forma, se propone un modelo funcional como alternativa para la toma de evidencias en la ejecución de pruebas de cumplimiento en las auditorias de sistemas, que permite facilitar el proceso para el auditor y generar reportes basados en las metodologías estudiadas.

1.3.3. Pregunta de investigación

¿La automatización de la toma de evidencias documentales en las pruebas de cumplimiento optimiza el proceso de la auditoria de TI?

1.3.4. Variables del problema

Teniendo en cuenta la importancia que está tomando la auditoría de TI en Colombia y la necesidad de gestionar correctamente la auditoria en las compañías se establecen las variables descritas a continuación.

Variable	Descripción
Pruebas de cumplimientos	Es un proceso que tiene como propósito probar los riesgos internos y externos y la efectividad de los sistemas de control.
Control	Es una de las principales actividades administrativas dentro de las organizaciones para tratar de garantizar el dominio sobre algún proceso o sistema.
Evidencias	Es la certeza que se obtiene a través de la ejecución de las pruebas.
Hallazgos	Los hallazgos son las debilidades, oportunidades y fortalezas que se encontraron en el sistema de control interno.
Recomendaciones	Es un instrumento que se emite cuando se ha demostrado un hallazgo en un proceso.
Activos	Son bienes o derechos que la empresa posee

Tabla 1: variables del problema Fuente: los autores.

1.4.Justificación

La tecnología ha tomado importancia vital para la gestión de la información en las compañías porque facilita el diario vivir evitando procesos manuales existentes en épocas pasadas que hacían más tardíos dichos métodos, pero todo este auge tecnológico también ha llevado a personas de poca ética a buscar errores en el software para explotarlos y realizar daños a las compañías (Auditoria superior, 2010).

Este proyecto tiene como finalidad crear un prototipo para agilizar las tareas en la toma de evidencias de las pruebas de auditoria de T.I no obstante en la actualidad se lleva a cabo este proceso de forma correcta pero manualmente. Este prototipo ayudará agilizar el proceso, tener una trazabilidad, integridad en la información y beneficiará a los auditores de T.I en la digitalización en tiempo real dichas pruebas, por lo que se hará una revisión de las metodologías para gestionar auditorías de TI con el fin de seleccionar una para que el prototipo funcional este basado en una de ellas y así generar automáticamente el informe de auditoría.

El manejo de auditorías de T.I en la actualidad, con los importantes y constantes avances tecnológicos que se presentan, ha tomado gran importancia para la mejora de procesos al interior de compañías en Colombia (Sama, 2011), por tal razón este proyecto tiene la finalidad de mejorar el proceso, crear nuevas formas para abordar las auditorias, reducir los costos de papelería y contribuir con el medio ambiente.

1.5.Objetivos

1.5.1. Objetivo general

Diseñar un modelo de automatización para la toma de evidencias documentales de las pruebas de cumplimiento en la auditoría de TI.

1.5.2. Objetivos específicos

- Realizar un diagnóstico con el fin de seleccionar las metodologías aplicables para la toma de evidencias de auditoria de TI.

- Identificar características de las aplicaciones utilizadas en la gestión de pruebas de auditoria TI para categorizar su eficacia en la metodología aplicada.

- Analizar los resultados de las metodologías y la categorización de las aplicaciones en las pruebas de auditoria de TI.

- Desarrollar un prototipo funcional enfocado a la toma de evidencias documentales en las pruebas de cumplimiento en las auditorias de TI.

2. MARCOS DE REFERENCIA

2.1.Marco conceptual

2.1.1. Software.

Software es todo programa o aplicación creada o desarrollada para realizar una tarea específica" (Tecnologia, 2017).

2.1.2. Hardware.

El hardware hace referencia a cualquier componente físico que interactúa de alguna manera con el computador (Tecnologia, 2017).

2.1.3. Riesgo

La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades (Australiano, 2000).

2.1.4. Riesgo residual

Riesgo residual: el nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo (Australiano, 2000).

2.1.5. Riesgo informático.

"Un riesgo es un problema potencial que puede ocurrir en un proceso de la organización o entidad" (Huerta, 2017).

2.1.6. Transferir riesgos

Cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo físico, o parte el mismo a otro sitio (Australiano, 2000).

2.1.7. Probabilidad

La probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación con la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto (Australiano, 2000).

2.1.8. Frecuencia

Una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado. Ver también Probabilidad (Australiano, 2000).

2.1.9. Aceptación de riesgo

Es una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular (ISO EN ESPAÑOL, 2012).

2.1.10. Monitoreo

Comprobar, supervisar, observar críticamente, o registrar el progreso de una actividad, acción o sistema en forma sistemática para identificar cambios (tecnologicas, 2008).

2.1.11. Proceso

Es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico. (Tecnologia, 2017).

2.1.12. Tecnología.

“Es la aplicación coordinada de un conjunto de conocimientos (ciencia) y habilidades (técnica) con el fin de crear una solución (tecnológica) que permita al ser humano satisfacer sus necesidades o resolver sus problemas" (CAMPAGNAT, 2017).

2.1.13. Activo

"Se considera un activo a aquello que es de alta validez y que contiene información de vital la cual es importante proteger" (Tecnologia, 2017).

2.1.14. Amenaza

"Se define como un peligro potencial a la información a sistema. Una amenaza se presenta cuando un atacante identifica una vulnerabilidad sobre un activo y es usada para generar daños que afectan la compañía" (Tecnologia, 2017).

2.1.15. Vulnerabilidad

"Una vulnerabilidad es una debilidad a nivel de software, hardware, procedimientos o error humano que permite a un atacante aprovecharla para causar daño. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada" (Tecnologia, 2017).

2.1.16. Pruebas

Proceso utilizado para demostrar una acción, Son aquellas pruebas que diseña el auditor con el objeto de conseguir evidencia que permita opinar sobre la integridad, razonabilidad y validez de los datos producidos por el sistema contable de la empresa auditada (Consultoría, 2017).

2.1.17. Pruebas de Cumplimiento

Son aquellas que proporcionan evidencia de que los controles claves existen y que son aplicables, efectivos y congruentes (Consultoría, 2017).

2.1.18. Evidencia

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

2.1.19. Ingeniería de software

Es una disciplina formada por un conjunto de métodos, herramientas y técnicas que se utilizan en el desarrollo de los programas informáticos (Tecnologia, 2017).

2.1.20. Desarrollo de Software

Desarrollar un software significa construirlo simplemente mediante su descripción. Está es una muy buena razón para considerar la actividad de desarrollo de software como una ingeniería. En un nivel más general, la relación existente entre un software y su entorno es clara ya que el software es introducido en el mundo de modo de provocar ciertos efectos en el mismo (Tecnologia, 2017).

2.1.21. Prototipo Funcional

El prototipo es una fase esencial en el desarrollo de un producto. Los prototipos permiten a los diseñadores ver y sentir los resultados de su trabajo (Tecnologia, 2017).

2.1.22. Sistema web

"Es un sistema que apoya parte de sus procesos a través de una red de computadoras o la Word Wide Web" (Huerta, 2017).

2.1.23. Auditoría TI

"Es la revisión y evaluación de procesos implementados en la empresa con respecto a sus equipos de cómputo, como se están utilizando y su eficiencia. Estas auditorías son necesarias también para lograr una utilización más eficiente y segura de la información" (Moyano, 2017).

2.1.24. Marcas de auditoría

"Son aquellos símbolos convencionales que el auditor adopta y utiliza para identificar, clasificar y dejar constancia de las pruebas y técnicas que se aplicaron en el desarrollo de una auditoria. Son los símbolos que posteriormente permiten comprender y analizar con mayor facilidad una auditoria" (Moyano, 2017).

2.1.25. Seguridad de la información

"Cuando existe una información y la misma tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger" (Huerta, 2017).

2.1.26. CAATS

"Técnicas de auditoria asistidas por computadoras, Son de gran ayuda para el auditor en el momento de aplicar una auditoría de TI" (Quesada, 2013).

2.1.27. Política de seguridad

"Reglas establecidas, de acuerdo con el comportamiento de los usuarios y de los atacantes que permiten minimizar ataques hacia los activos de la información. Las políticas van de la mano con el modelo de seguridad corporativo y son independientes de las demás organizaciones ya que su objetivo es cubrir las necesidades y requerimientos específicos de cada empresa" (Huerta, 2017).

2.1.28. Metodologías

Se denomina la serie de métodos y técnicas de rigor científico que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado teóricamente válido (Auditoria superior, 2010).

2.1.29. ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización ISO y describe cómo gestionar la seguridad de la información en una empresa (UCatabria, 2017).

2.1.30. Controles

"Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los bienes de la compañía" (ISO EN ESPAÑOL, 2012).

2.2.Marco teórico

2.2.1. Magerit 3

Es una metodología para el análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, está directamente relacionada con el uso de las tecnologías de la información, que supone unos beneficios evidentes para las empresas; pero también da lugar a riesgos que gestionarse con medidas de seguridad que generen confianza. La gestión del riesgo es un proceso que mantiene un ambiente seguro, radica en identificar los elementos que podrían afectar los datos, y en implementar medidas que generen solución para mitigar o reducir el riesgo (PAE, 2014).

Como parte de la gestión de riesgos Magerit 3 enuncia unos principios que se trasforman en unos mandatos y compromisos, con el fin de diseñar un marco de trabajo donde se gestionan los riesgos dando pautas para el análisis y tratamiento como se ve en la siguiente figura.

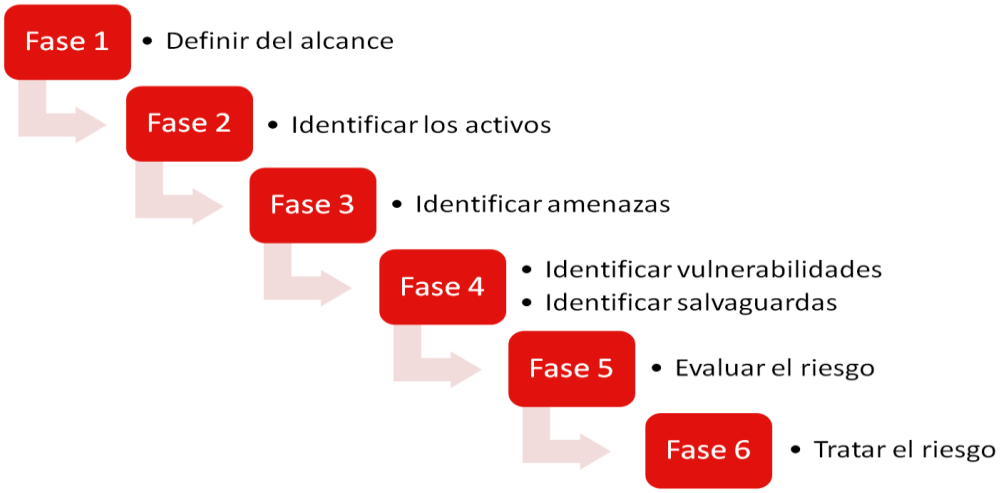


Figura 1: fases de majerit v3. “https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo”

Adicionalmente proporciona algunas técnicas para llevar a cabo el análisis y gestión de riesgos, donde se puede adoptar alguna de las siguientes técnicas: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, arboles de ataque, técnicas generales, técnicas gráficas, entrevistas, reuniones y presentaciones que se usaran para gestionar el prototipo funcional.

2.2.2. ISO 27002

La norma ISO/IEC 27002 es un estándar para la seguridad de la información y está enfocada a todo tipo de organizaciones para aplicar y evaluar controles en seguridad de la información.

Esta norma es una especificación de los controles publicados en el anexo A de la norma ISO/IEC 27001 (ISO EN ESPAÑOL, 2012).

Los controles establecidos para la norma inspeccionan puntos en la siguiente figura.

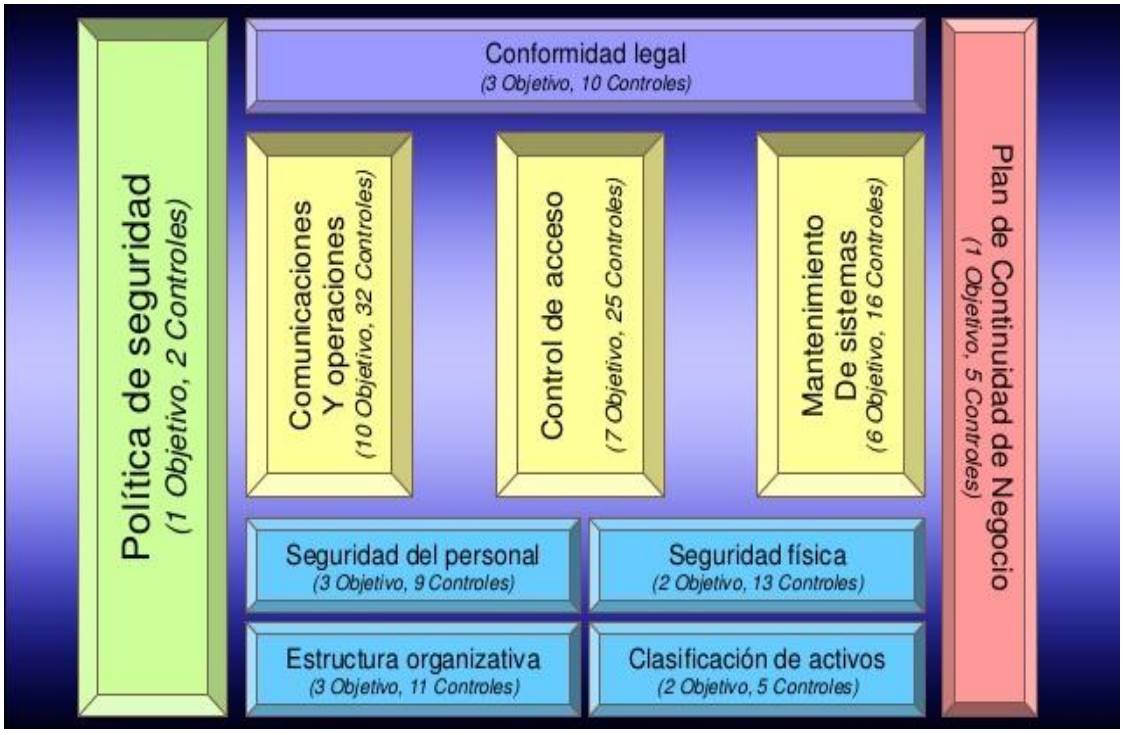


Figura 2: controles de ISO 27002. "Tomada de https://es.slideshare.net/cirobonilla/estndar-iso- iec-27002-2005

Los controles se clasifican según la norma se clasifican de la siguiente forma: Políticas, organización, recursos humanos, activos, acceso, cifrados, físico, ambiental, telecomunicaciones, adquisiciones, suministradores, indicies, continuidad del negocio y cumplimiento. Para que se establezcan el análisis de los controles y así asumirlos para la gestión de la auditoria.

2.2.3. ISO 31001

La norma ISO 31000 es un estándar internacional que brinda las pautas y principios para realizar la gestión del riesgo de las organizaciones.

Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización y tiene por objetivo que las todo tipo de organizaciones puedan gestionar los riesgos de forma efectiva, por lo que la norma encomienda a las organizaciones que desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades (IsoTools, 2016).

Como complemento a esta norma se ha desarrollado el estándar ISO 31010 que gestiona el riesgo como en la siguiente figura (IsoTools, 2016).

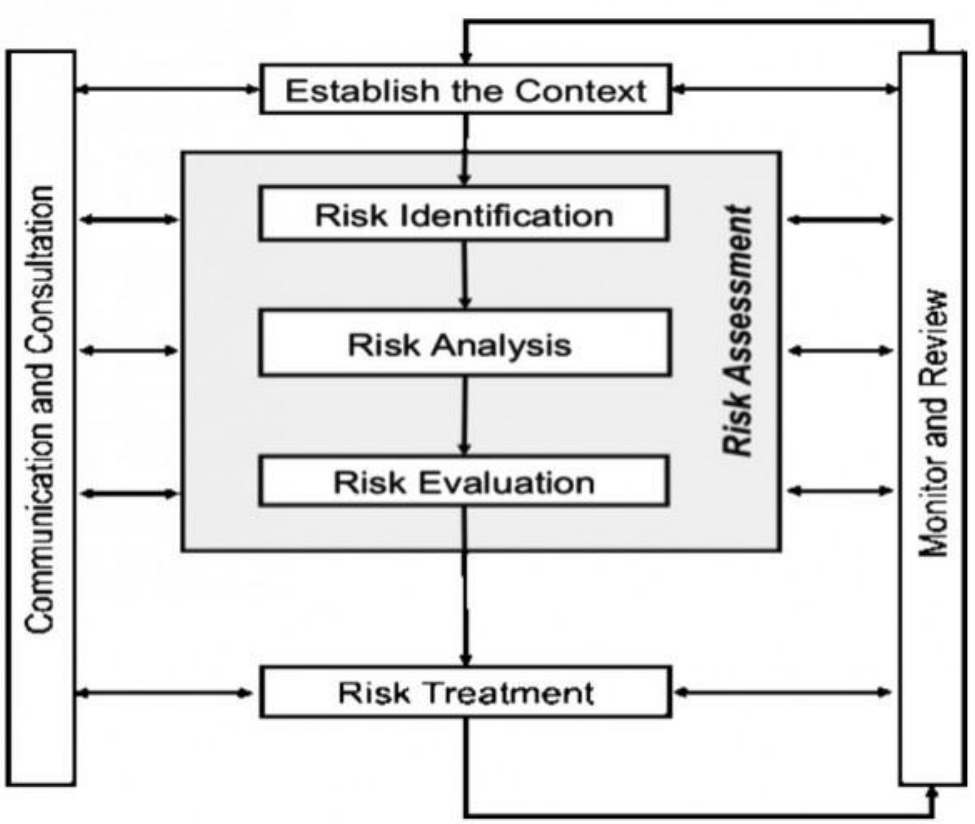


Figura 3: gestión de riesgo según iso 31000. "Tomada de http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management/"

2.2.4. Guías de Auditoria

Es una técnica para el análisis de las pruebas de que se hacen en las auditorias de TI, es una buena práctica dada por COBIT. Estándar que apliquen especialmente a las auditorías y aseguramiento de SI. El desarrollo y diseminación de los estándares de auditoría y aseguramiento de SI son la piedra angular de la contribución profesional de ISACA a la comunidad de auditoría donde se gestiona (Cobit, 2014).

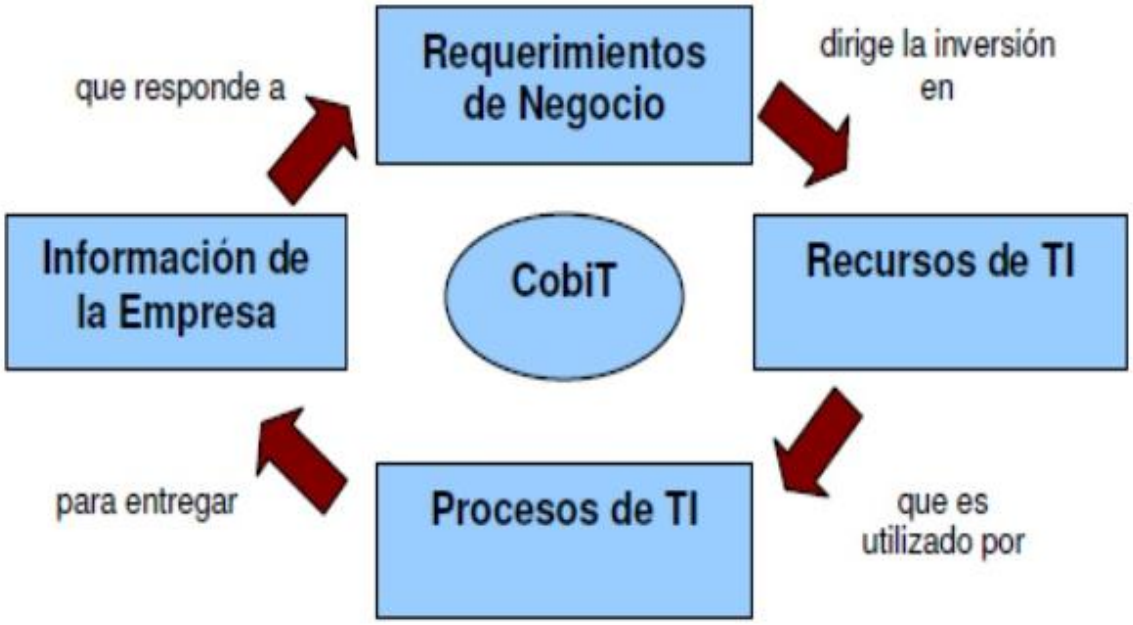


Figura 4: proceso de cobit en guias e auditoria"Tomada de https://es.slideshare.net/pedrogarciarepetto/ai10-isaca"

2.2.5. Matriz de riesgos

Es una técnica específica para analizar riesgos sus amenazas, vulnerabilidades y los controles que se establecen para gestionarlos. La matriz de riesgos es adaptable a diferentes metodologías como: cobit, Iso 27001, isaca, magerit entre muchas otras teniendo como procedimiento lo estipulado en la siguiente figura (Matriz de Riesgos , 2016).

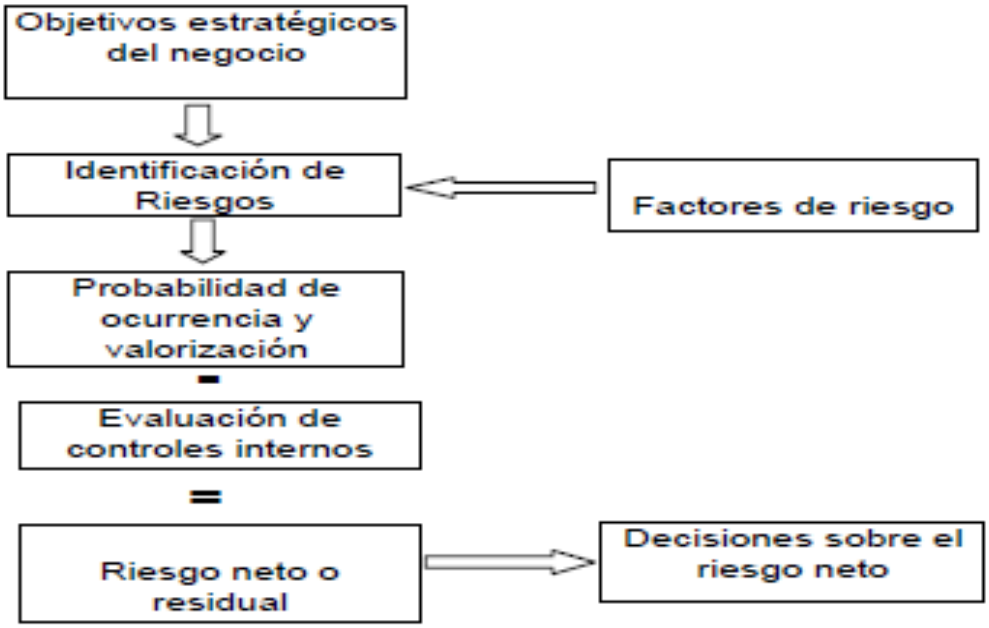


Figura 5: Pasos para hacer una matriz de riesgos. "Tomada de http://12302154.blogspot.com.co/2011/06/matriz-de-riesgos-ii.html"

2.3.Marco jurídico

2.3.1. Derechos de Autor

La normalización con respecto a los derechos que adquiere el autor de soporte lógico o de software, y las consecuencias jurídicas que sobrevienen a su licenciamiento, transferencia, distribución, reproducción o, en general, cualquier utilización que se haga de ellos, están contempladas en la Ley 23 de 1982, la Decisión 351 del Acuerdo de Cartagena y el Decreto 1360 de junio 23 de 1989 (Consultoría, 2017).

Según el Acuerdo de Cartagena, tanto los programas operativos como a los aplicativos, ya sea en forma de código fuente o código objeto, están cobijados por la Ley, que establece, entre otras, las siguientes normas: El propietario de un ejemplar de programa de computador de circulación lícita, puede realizar copias o adaptaciones del mismo, siempre y cuando sean

indispensables para su utilización o se realicen con fines de archivo o sustitución del original en caso de daño o pérdida (ACCIS, 2015).

Por lo que en nuestro desarrollo del prototipo estamos seguros de que los derechos que sobre él tiene se respetarán a nivel nacional e internacional.

2.3.2. El Hábeas Data

Es el derecho a su intimidad personal y familiar y a su buen nombre", que está consagrado desde 1991 en la Constitución Política, los ciudadanos pueden saber cómo y para qué se usa la información que se brinda a las distintas entidades en el país. La Ley además faculta al Estado para controlar a estas entidades en la administración de las bases de datos. En avisos en medios de comunicación, en atención a la Ley 1581 de 2012 y el Decreto 1377 de 2013, las empresas informaron que habían recolectado algunos datos personales con la intención de registrarlos en sus bases y así desarrollar diferentes actividades (Salcedo, 2013).

Por lo que debemos respetan en nuestro desarrollo y en la recolección de nuestros datos que sean sensibles los siguientes riesgos que a continuación se detallan:

- Acceso abusivo a un sistema informático: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema
- Interceptación de datos informáticos: El que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte (Salcedo, 2013).

- Violación de datos personales: La persona que con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
- Suplantación de sitios web para capturar datos personales: Este delito es para quien diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

2.4.Marco demográfico

El constante avance de las tecnologías ha hecho que surjan nuevas disciplinas en las ciencias de la computación, por lo que se requiere personal idóneo y capacitado para estas disciplinas. La auditoría de TI es una de las ramas de la computación de más importancia ya que garantiza la seguridad y el correcto funcionamiento de los procesos y sistemas en las compañías.

No obstante, la auditoria de TI no es la excepción y requiere personal capacitado para que puedan ejercer la funciones de la auditoria, ya que está basada en buenas prácticas y normas nacionales e internacionales, que son utilizadas para revisar el diseño, desempeño y cumplimiento de los controles implementados en el ambiente de TI (Consultoría, 2017).

En Colombia la auditoria de TI ha nacido a nivel empresarial y organización para asegurar la fiabilidad, eficacia, rentabilidad, seguridad y privacidad de la información, La necesidad de contar con personas expertas en lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación postgrados y certificaciones en auditoria para

el desarrollo de la misma teniendo en cuenta mejores prácticas como COBIT, COSO e ITIL (ACCIS, 2015). Entre enero y septiembre de 2016, en el país se han creado 243.093 empresas, de este total de empresas, 59.626 son sociedades (Protafolio, 2016), por lo que la necesidad de que los auditores estén presente en estas empresas crece, así como la necesidad de mejorar los procesos internos de las empresas y proteger sus activos.

Los auditores deben estar capacitados para ejecutar una auditoria de TI, así como para gestionarla a través de una herramienta CAAT, por lo que este proyecto conducente al diseño de un modelo de automatización para la toma de evidencias documentales de las pruebas de cumplimiento en la auditoría de TI enfocando su uso a los auditores que están capacitados para el uso de herramientas CAAT´s.

2.5.Marco geográfico

A continuación, se realiza la descripción de la ubicación geográfica donde se centra el levantamiento de información que se realizara para el desarrollo de un prototipo funcional enfocado a la toma de evidencias documentales en las pruebas de cumplimiento en las auditorias de TI.

Colombia es un país latino americano ubicado en sur américa, cuya capital es la cuidad de Bogotá, ubicada en el centro del país en el departamento de Cundinamarca, es una de las capitales más grandes de américa latina, donde se concentra la mayor parte de empresas grandes y medianas del país que han llevado a la ciudad a un crecimiento del 22% en 2015, del total de empresas registradas y renovadas, el 87% son microempresas, el 9% pequeñas empresas, el 3% medianas y el 1% grandes empresas (Dinero.com, 2016). Muchas de estas empresas son dedicadas a la gestión de tecnología por lo que está presente la auditoria de TI,

el proyecto está orientado en la zona del distrito de Bogotá, así como se ve en el siguiente mapa.

Figura 6: Mapa de Bogotá "Tomada https://www.google.de/maps/place/Bogot%C3%A1,+Colombia/@4.6462306,-74.0316005,11z/data=!4m5!3m4!1s0x8e3f9bfd2da6cb29:0x239d635520a33914!8m2!3d4.7109886!4d-74.072092"

Como una de la tanta empresa ubicada en Bogotá, también se encuentra Mac center que es una compañía que ofrece una experiencia Premium en la compra de productos Apple en las tiendas se puede encontrar accesorios de las mejores marcas de tecnología, servicio técnico confiable y cursos de entrenamiento sin costo, en toda Colombia, tiene sus oficinas principales y administrativas en Bogotá en el sector de Usaquén. Uno de los procesos que maneja la empresa es la seguridad física del centro de cómputo, el cual será auditado al completar el desarrollo de prototipo funcional y así tener evidencias documentales del estado en el proceso como caso de estudio.

2.6.Estado del arte

En el presente capítulo se presentan, datos e información correspondientes a el área de auditoria de TI en la que se enfoca el desarrollo de este proyecto. En primer lugar, se hace una reseña histórica sobre los comienzos de la auditoria de TI, la seguridad de la

información, las herramientas CAAT`s. En segundo lugar, se analizan algunas de las metodologías para las pruebas de auditoría de TI donde se gestionen riesgos. Por último, se define un criterio de selección de la metodología a usar dentro del desarrollo del proyecto de investigación en las fases de diseño e implementación.

2.6.1. Reseña histórica

El término de auditoría de sistemas se remonta a 1862 donde aparece por primera vez la profesión de auditor o de desarrollo de auditoria bajo la supervisión de la ley británica de Sociedades anónimas, donde se dieron los primeros pasos para realizar las auditorías contables. Con el auge de las redes y sistemas de información, se vio la necesidad de implementar sistemas más seguros que tuvieran los principios de la seguridad de la información. Es ahí donde nace la auditoría de TI (Historia de la Auditoria, 2015).

El objetivo de la auditoría de TI es evaluar el sistema de control interno, verificar los sistemas para obtener evidencias, para finalmente emitir un informe con los hallazgos y recomendaciones del auditor según su criterio profesional. Para muchos la auditoría de TI es una herramienta que permite realizar una evaluación completa y concreta del sistema de control interno de una compañía, para así garantizar la mejora continua en los principios de la seguridad de la información confidencial, integridad y disponibilidad (Auditoria superior, 2010).

La seguridad en TI está enfocada en la protección de datos, la información, es uno de los activos más importantes de las organizaciones, al igual que la infraestructura tecnológica. La auditoría de TI consiste evaluar controles, políticas y procedimientos que permitan

minimizar el riesgo que corre la compañía y va de la mano con la seguridad de la información para verificar si los controles están implementados o cuales podrían implementarse según el core de negocio de cada organización.

Desde que se aplica auditoría TI en las compañías, se han presenciado las falencias más fácilmente como:

- La corrupción: Esta categoría de fraude encuadra todas aquellas actividades en donde los empleados de una empresa utilizan indebidamente sus influencias para obtener un beneficio (AUDITORIA, 2014).
- El fraude de EECC: Son aquellos eventos de fraude en donde se ejecutan maniobras con el propósito de generar estados financieros que no reflejan adecuadamente la realidad económica de la compañía (AUDITORIA, 2014).
- La apropiación indebida de activos: Son aquellos esquemas de fraude en los cuales la persona que lleva a cabo la acción de fraude realiza sustracciones de activos o utiliza tales activos u otros recursos de la compañía para su beneficio propio (AUDITORIA, 2014).

Por lo anterior es necesario desarrollar metodologías y marcos de trabajo para su ejecución, así como la aplicación (CAAT'S) que gestiona la auditoría de sistemas (Villa, 2016).

2.6.2. Análisis de las Metodologías

Este proyecto tiene como base de estudio la metodología Magerit V.3 cuyo fuerte es el análisis y gestión de los riesgos, así como también la norma ISO 27002 que se enfoca en establecer y verificar controles en el sistema de control interno de las compañías.

2.6.2.1.Magerit V3

La gestión de los riesgos es uno de los contratiempos de las compañías, un buen gobierno, público o privado, donde el principio esencial en las decisiones del gobierno se fundamente en la comprensión de los riesgos de la compañía para tener beneficios, costos, riesgos y oportunidades.

La gestión de los riesgos de TI establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información dentro de esta norma. Garantizando que las organizaciones siguen los principios para equilibrar riesgos y oportunidades derivados del uso de la tecnología (PAE, 2014).

Magerit v3 pone la confianza como un valor a tener en cuenta en las organizaciones y para su implementación es por eso que alrededor de unas 500000 empresas españolas han acogido esta metodología para gestionar los riesgos, las empresas en 2016 han empezado a usar Magerit en un 42% con relación al 32% de 2016 (Economista, 2017) y así garantizar el cumplimiento de objetivos estratégicos y misionales de la organización, donde en la siguiente imagen muestra el ciclo den tratamiento de la gestión de riesgos que plantea Magerit (Barroso, 2012).

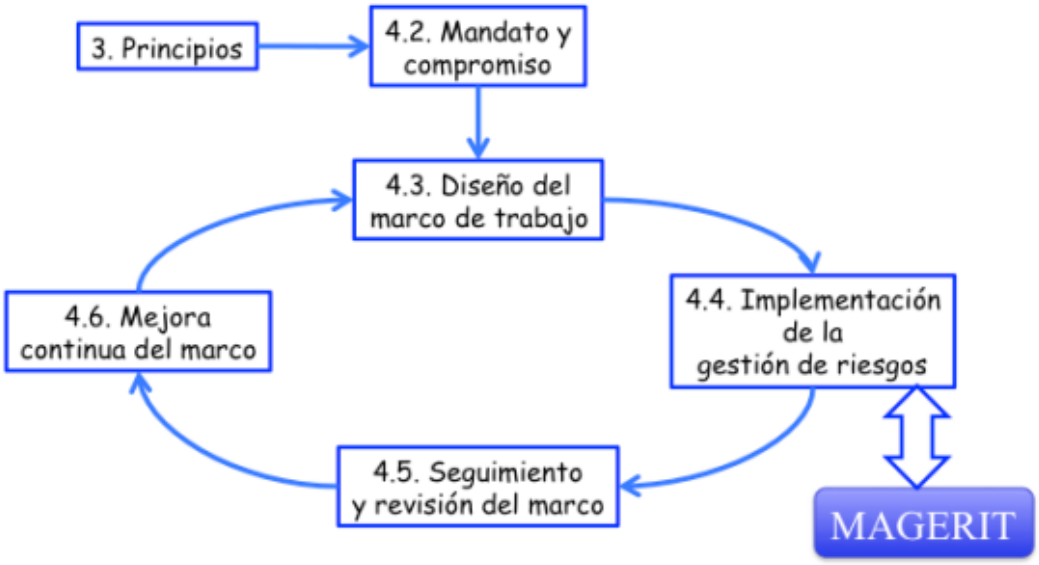


Figura 7: modelo de Magerit. "Tomada de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wb209bLyjIU"

2.6.2.2.ISO 31000

ISO 31000 ha permitido a las empresas incorporar estándares y procesos de alto nivel para evaluar y limitar los riesgos en todas sus operaciones (Icintec, 2011).

ISO 31000 ofrece principios y directrices genéricas sobre gestión de riesgos. La norma no es específica de ninguna industria o sector y puede ser utilizada por cualquier organización pública o privada y aplicarse a cualquier tipo de riesgo en una amplia serie de actividades y operaciones. ISO 31000 es la referencia mundial en sistemas de gestión de riesgos, y elegirla le pondrá a la vanguardia del mercado; además sus clientes confiarán en su toma de decisiones estratégicas (Icintec, 2011)..

Nuestros equipos de especialistas en SGS le ofrecen formación en ISO 31000, y evaluaciones de sistemas de gestión de riesgos según ISO 31000. Nuestra experiencia mundial y nuestros conocimientos técnicos garantizan la disponibilidad de expertos en su

industria o sector en cualquier parte del mundo. Obtenga más información sobre ISO 31000 (Gonzalez, 2016).

Técnicas de apreciación del riesgo las técnicas descritas en la norma ISO 31000:2009 son las siguientes (Gonzalez, 2016):

- Tormenta de ideas
- Entrevistas estructuradas o semiestructuradas
- Delphi
- Listas de ejemplo
- Análisis de riesgos preliminar (PHA)
- Estudio de Peligros y Operabilidad – HAZOP
- Análisis de peligros y puntos críticos de control (HACCP)
- Evaluación del riesgo ambiental
- Análisis de causas y consecuencias
- Análisis de casa y efecto
- Análisis de Capas de Protección (LOPA)
- Árboles de decisión
- Análisis de la fiabilidad humana
- Árbol de fallos y sucesos iniciadores
- Mantenimiento Centrado en la Fiabilidad
- Análisis de circuitos de fugas
- Análisis de cadenas de Markov
- Análisis Qué pasa si
- Análisis de escenarios
- Análisis de Impacto de negocio
- Análisis de Causa Raíz
- Análisis de modo y efecto de la falla
- Análisis de árbol de fallos
- Análisis de árbol de eventos
- Simulación de Monte Carlo
- Análisis Bayesiano
- Curvas FN
- Índices de riesgo
- Matrices de probabilidad y consecuencia
- Análisis costo beneficio
- Análisis de decisión multicriterio

Para realizar el proceso de riesgo en esta norma conviene trabajar según el modelo de la siguiente figura.

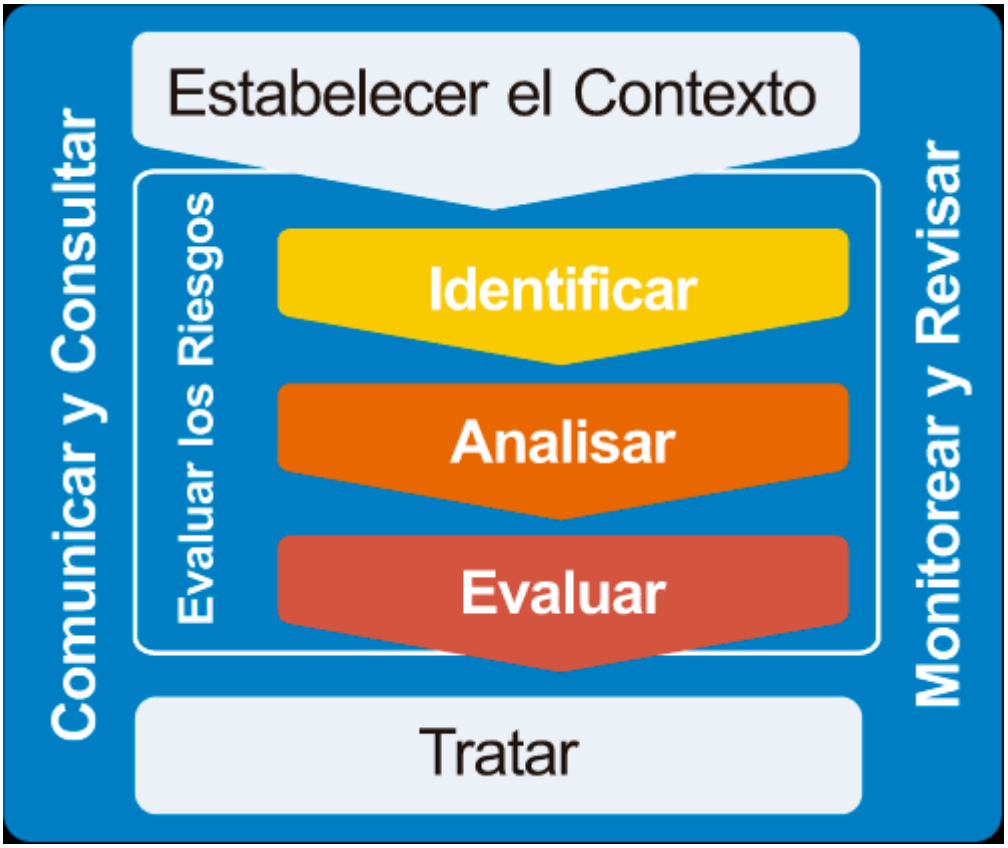


Figura 8: ISO 31000 "Tomada de https://www.softexpert.es/solucao/iso-31000/"

2.6.2.3.ISO 27002

Es un estándar o norma que evalúa los controles específicos que plantea los anexos de la ISO 27001. La disponibilidad, integridad y confidencialidad de la información son características para garantizar en los procesos y aplicaciones de software de las compañías.

Los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlos y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente y garantizar la seguridad en estos medios, esto implica también la prevención de ataques y errores (Ortiz, 2015).

Así mismo las ventajas que se debe tener en cuenta que la seguridad al 100% no existe. La norma establece una metodología y una serie de medidas que al menos busca una mejora continua y que, sin lugar a dudas, aumentará el porcentaje de seguridad actual de cualquier empresa (Corletti, 2008).

A continuación, el listado de los temas que gestiona la norma (ISO EN ESPAÑOL, 2012):

- Exactitud: La información ha de ser precisa y libre de errores.
- Completitud: La información debe contener todos aquellos hechos que pudieran ser importantes.
- Economicidad: El costo en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por ésta la organización.
- Confianza: Para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes de información.
- Relevancia: La información ha de ser útil para la toma de decisiones.
- Verificabilidad: La información ha de poder ser contrastada y comprobada en todo momento.

La norma ISO es acogida en Colombia por Icontec y según datos de MinTic es una de las metodologías más usadas por las medinas empresas en el país con alrededor de 31.52% (MinTic, 2016).

2.6.3. Análisis de las herramientas CAAT´s

El desarrollo de la auditoría se basa en la aplicación de normas, técnicas y procedimientos. Enfocadas a la Revisión del Control Interno. El auditor **de TI** desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad.

Una de las ventajas más notorias de las CAACT's es la versatilidad que estas presentan para la realización del trabajo de campo de la auditoría (se pueden utilizar sin importar el tipo de organización, su tamaño, sus operaciones y sector del mercado). Para ello el auditor debe tener el suficiente juicio y experiencia profesional para establecer la técnica o herramienta a utilizar (PAE, 2014).

Estas herramientas requieren mayor experiencia ya que suelen ser más complejas respecto a la aplicación de una auditoria tradicional, pues se orientan hacia la evaluación del funcionamiento interno de las aplicaciones en producción y la forma en que estos procesan la información y garantizan la trazabilidad que indica donde y cuando se toma la evidencia y el mapeo donde se muestra la localización y fecha la prueba (Villa, 2016).

Ventajas del uso de las CAAT's

- Incrementan o amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente.
- Incrementan el alcance y calidad de los muestreos, verificando un gran número de elementos. - Elevan la calidad y fiabilidad de las verificaciones a realizar.
- Reducen el período de las pruebas.
- Realizan un plan a priori sobre los puntos con potencial violación del Control Interno.
- Disminuyen considerablemente del riesgo de no-detección de los problemas.
- Posibilitan que los auditores puedan centrar su atención en aquellos indicadores que muestren saldos inusuales o variaciones significativas, que precisan de ser revisados como parte de la auditoría.
- Elevan la productividad y de la profundidad de los análisis realizados en la auditoría.

Tipos de herramientas y técnicas

- Técnicas administrativas: Son las apoderadas de concretar y ofrecer al auditor las áreas de interés, la metodología a emplearse para la ejecución del análisis y el alcance de la revisión (Quesada, 2013).
- Técnicas para evaluar los controles: Técnicas que verifican cálculos en aplicaciones complejas y comprueban la exactitud del procesamiento en forma global (Quesada, 2013).
- Técnicas para análisis de transacciones: Su principal objetivo es de seleccionar y analizar transacciones significativas de forma permanente, utilizando procedimientos analíticos y técnicas de muestreos (Quesada, 2013).
- Técnicas para el Análisis de Datos: Están orientadas hacia el uso de programas informáticos especializados que le permiten al auditor, de forma eficiente y flexible, examinar la información que ha sido procesada electrónicamente a través de los sistemas de información (Quesada, 2013).

3. METODOLOGÍA

La metodología contiene las siguientes fases: fase de inicio, fase de planeación, fase de ejecución y fase de cierre. En la primera fase se plantean objetivos y se busca la definición de los conceptos principales para el proyecto, la segunda fase se establecen tiempos temas a trabajar y desarrollar, para la tercera fase en la que se consolida en el desarrollo de las actividades para cumplir con los objetivos, se indagara sobre las metodologías para gestionar las auditorias, una categorización de la herramienta CAATS con el fin de realizar un diseño en UML del prototipo funcional y el desarrollo del mismo. La fase final correspondiente al cierre donde se analizan los resultados obtenidos para la creación del prototipo funcional.

3.1.Método

La investigación realizada se enfoca en un métodos cualitativo-descriptivos tiene como finalidad definir, clasificar, catalogar y categorizar el objeto de estudio. El principal método de investigación descriptiva son las encuestas aplicadas en un caso de estudio.

Esta investigación está alineada al proceso de la toma de evidencias documentales en las pruebas de cumplimiento de auditoría de TI, empleada a la evaluación el proceso tener los requisitos que deberán adoptarse para tomar las evidencias de las pruebas de cumplimiento.

3.2.Técnicas e instrumentos

3.2.1. Entrevista

La Entrevista es una indagación de información en la que el entrevistador pregunta a los entrevistados sobre los datos que hay que obtener, y posteriormente se analizan los datos

individuales para que mediante un análisis cualitativo obtener los datos de interés. El proyecto utiliza el instrumento de la entrevista enfocada a personal especializado en la auditoria de TI, con el objetivo de analizar el proceso de la toma de las evidencias en pruebas de auditorías de sistemas, para identificar cual son las observaciones, sugerencias al proceso y usarla como herramienta para darle un valor agregado al proyecto propuesto.

La Entrevista será tipo personal o vía telefónica y tendrá la siguiente información del entrevistado donde el nombre está oculto por el tratamiento de los datos.

- Empresa
- Cargo o perfil de Auditoria.
- Tiempo de experiencia en auditoria de TI.
- Nivel de escolaridad y/o Certificaciones.
- Genero

3.2.2. Procedimiento

Estas entrevistas tendrán unas preguntas pre definidas que están enmarcadas en la auditoria de TI y se enfocan en la toma de las evidencias documentales en las pruebas de cumplimiento de auditoria de TI. Se realizan presencialmente, por video llamadas o llamada telefónica para tener contacto directo con los especialistas en el tema. Esto nos ayuda a determinar la eficiencia, fortalezas y debilidades, para construir de forma integral el prototipo funcional.

3.2.3. Elección de muestra

Las técnicas de recolección de datos como las entrevistas usan un análisis cualitativo que se valora sobre datos estimados según la congruencia de las respuestas de los entrevistados, experiencia de los entrevistadores y lo que se busque con el objetivo de la entrevista, para

detectar y clasificación la información en los formatos definidos de la entrevista. (Definiciones.es, 2015)

Se toma las entrevistas realizadas para analizar el valor que ellas aportan al proyecto se agruparán las opiniones de cada uno de los puntos importantes en cuanto a la eficacia, eficiencia, fortalezas y debilidades de cada uno de los ítems relevantes para nuestro proyecto y así implantarlo en nuestro prototipo para que sea una herramienta útil.

3.2.4. Recolección de Datos

Durante la recolección de información para para analizar el proceso de Toma de evidencia documentales en las pruebas de auditoria de TI se tomó la siguiente información:

- Normas o metodologías de auditoria: Se consulta que metodologías usan los entrevistados en los procesos de auditoria de TI.
- Proceso de toma de evidencias documentales en las pruebas de cumplimiento de TI: Se consulta que pasos o métodos se usan actualmente en la auditoria.

3.2.5. Tipos de Datos

Los tipos de datos serán agrupados en las características más relevantes asociadas a las variables del problema, y son descritos en la tabla 5 Tipo de datos.

Variable	Descripción	Tipo de Variables
Pruebas de cumplimientos	Pruebas a sistemas de control.	Cualitativa Nominal
Evidencias	Certeza de las pruebas.	Cualitativa Nominal
Hallazgos	Oportunidades en sistema de control.	Cualitativa Nominal
Recomendaciones	Instrumento emitido.	Cualitativa Nominal
Activos	Bienes o derechos	Cualitativa Nominal

Tabla 2: Tipos de datos "Fuente: los autores"

3.2.6. Selección de Participantes

La selección de los participantes se realizó de acuerdo con la experiencia de las personas en la gestión de las auditorias de TI, tratando de buscar personal experto. En la siguiente tabla se relacionan las características que debe tener el personal experto para la realización de las entrevistas.

Escolaridad	Carrera	Área de las ciencias de la computación en la que se desempeña	Departamento	Conocimiento	Años de experiencia
Profesional especialista en auditoria de TI	Ingeniería de sistemas (Auditor)	Auditoria de TI	Tecnología	Gestión de las auditorias	Más de 5 años

Tabla 3: características de los entrevistados "fuente: lo autores"

4. ANÁLISIS DE RIESGOS

El siguiente capítulo trata los riegos del proyecto diseño de un modelo de automatización para la toma de evidencias documentales de las pruebas de cumplimiento en la auditoría de TI, se identificarán las principales actividades, activos, eventos y riegos para su posterior valoración, implementar los controles y el tratamiento de sus riesgos.

4.1.Identificación de riesgos

A continuación, se realiza la identificación de los riesgos en el proyecto prototipo para la toma de evidencias en pruebas de auditorías de T.I.

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
Definición de alcance	Gerente del proyecto	Mal selección del gerente del proyecto	Mala definición del alcance por mala elección del gerente del proyecto
		Falta de conocimiento	Mala definición del alcance por falta de conocimientos del gerente de proyecto
		Falta de experiencia	Mala definición del alcance por falta de experiencia del gerente del proyecto
	Equipos de computo	Fallo en el equipo de computo	Perdidas en la definición del alcance por fallos en el equipo de computo
		Daño en el equipo de computo	Perdida en la definición del alcance por daño en el equipo de computo
	Información	Mala recolección	Mala definición del alcance ocasionada por mala recolección de la información
		Recolección incompleta	Mala definición del alcance ocasionada por recolección incompleta de la información
		Falta de recolección	Mala definición del alcance ocasionada por no recolectar información

Tabla 4: análisis de riesgos del alcance Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
levantamiento de información	Información	Mala recolección	Fallas en el levantamiento de información por mala recolección de información
		Recolección incompleta	Fallas en el levantamiento de información por recolección incompleta de la información
		Falta de recolección	Mal levantamiento de información por no recolectar información
	Equipos de computo	Fallo en el equipo de computo	Perdida de información por fallos en el equipo de computo
		Daño en el equipo de computo	Perdida de información por daños en el equipo de computo
	Líder funcional	Mal selección del líder funcional	Fallas en el levantamiento debido a la mala elección del líder funcional
		Falta de conocimiento	Fallas en el levantamiento de información debido a la falta de conocimientos del líder funcional
		Falta de experiencia	Fallas en el levantamiento de información debido a la falta de experiencia del líder funcional
	Recursos financieros	Falta de recursos financieros	Fallas en el levantamiento de información ocasionada por falta de recursos financieros
		Mal manejo de los recursos financieros	Fallas en el levantamiento de información ocasionado por mal manejo de los recursos financieros
		Robo de los recursos financieros	Fallas en el levantamiento de información ocasionado por robo de los recursos financieros

Tabla 5: análisis de riesgos del levantamiento de información Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
Definición de recursos	Información	Mal levantamiento	Mala definición de recursos ocasionado por errores en la información
		Mala planeación	Mala definición de recursos ocasionado por mala planeación
	Equipos de computo	Fallo en el equipo de computo	Errores en la definición de los recursos por fallos en los equipos de computo
		Daño en el equipo de computo	Perdida de información de los recursos por daño en los equipos de computo
	Gerente del proyecto	Mal selección del gerente del proyecto	Fallas en la definición de los recursos por mala selección del gerente de proyecto
		Falta de conocimiento	Fallas en la definición de los recursos por falta de conocimiento del gerente de proyecto

Tabla 6: análisis de riesgos de la definición de recursos Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
Definición de requerimientos	Información	Falta de experiencia	Fallas en la definición de los recursos por falta de experiencia del gerente de proyecto
		Mala definición	Errores en la definición de los requerimientos ocasionado por mal levantamiento en la información
		Definición incompleta	Mala definición de los requerimientos ocasionado información incompleta
		Mal levantamiento	Mala definición de los requerimientos por mal levantamiento de información
	Software	Mal funcionamiento	Mala definición de los requerimientos por mal funcionamiento en el software
		Bloqueo del software	Errores en la definición de los requerimientos por bloqueo en el software
		fallo en el software	Errores en la definición de los requerimientos por fallos del software
	Equipos de computo	Fallo en el equipo de computo	Errores en la definición de los requerimientos por fallo en los equipos de computo
		Daño en el equipo de computo	Errores en la definición de los requerimientos por daño en el equipo de computo

	Líder funcional	Mal selección del líder funcional	Errores en la definición de los requerimientos por mala elección del líder funcional
		Falta de conocimiento	Errores en la definición de los requerimientos por falta de conocimientos del líder funcional
		falta de experiencia	Errores en la definición de los requerimientos por falta de experiencia del líder funcional

Tabla 7: análisis de riesgos de la definición de requerimientos Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
Seleccionar metodologías aplicables para la toma de evidencias de auditoria ti	Información	Falla en el levantamiento	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallas en el levantamiento de información
		Falta de recolección	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallas en la recolección de la información
		Selección incompleta	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por recopilación incompleta de la información
	Equipo lideres	Mal selección del equipo	Mala selección de las metodologías aplicables para la toma de evidencias

			de auditorías ti por mala selección del equipo líder
		Falta de conocimiento	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de conocimiento del equipo líder
		Falta de experiencia	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de experiencia del equipo líder
	Recursos financieros	Falta de recursos financieros	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de recursos financieros
		Mal manejo de los recursos financieros	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por mal manejo de los recursos financieros
		Robo de los recursos financieros	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por robo de los recursos financieros

Tabla 8: análisis de riesgos de la selección de metodologías Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
Categorización de aplicaciones	Equipos de computo	Fallo en el equipo de computo	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallos en los equipos de computo
		Daño en el equipo de computo	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por daños en los equipos de computo
	Software	Mal funcionamiento	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por mal funcionamiento del software
		Bloqueo del software	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por bloqueo del software
		Fallo en el software	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallo en el software

	Información	Mala categorización	Mala categorización de las aplicaciones ocasionada por mal levantamiento de la información
		Categorización incompleta	Mala categorización de las aplicaciones ocasionada por información incompleta en el levantamiento
		Falta de categorización	Mala categorización de las aplicaciones ocasionada por no realizar previamente el levantamiento de información

Tabla 9: análisis de riesgos de la categorización de aplicaciones Fuente: los autores

ACTIVIDADES	ACTIVOS	EVENTOS	RIESGOS
	Equipo lideres	Mal selección del equipo	Mala categorización de las aplicaciones ocasionada por mal selección del equipo líder
		Falta de conocimiento	Mala categorización de las aplicaciones ocasionada por mal falta de conocimiento del equipo líder
		Falta de experiencia	Mala categorización de las aplicaciones ocasionada por mal falta de experiencia del equipo líder

Análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti	Recursos financieros	Falta de recursos financieros	Errores en la categorización de las aplicaciones ocasionada por falta de recursos financieros
		Mal manejo de los recursos financieros	Errores en la categorización de las aplicaciones ocasionada por mal manejo de recursos financieros
		Robo de los recursos financieros	Errores en la categorización de las aplicaciones ocasionada por robo de los recursos financieros
	Equipos de computo	Fallo en el equipo de computo	Errores en la categorización de las aplicaciones ocasionada por fallo en los equipos de computo
		Daño en el equipo de computo	Perdida de información de las aplicaciones ocasionada por daño en los equipos de computo
	Software	Mal funcionamiento	Perdida de información de las aplicaciones ocasionada por mal funcionamiento del software
		Bloqueo del software	Perdida de información de las aplicaciones ocasionada por bloqueo del software
		Fallo en el software	Perdida de información de las aplicaciones ocasionada por mal fallo en el software

	Información	Mal levantamiento	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal levantamiento de información
		Análisis incompleto	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por análisis incompleto

Tabla 10: análisis de riesgos del análisis de resultados Fuente: los autores

ACTIVIDADES	**ACTIVOS**	**EVENTOS**	**RIESGOS**
Desarrollo del prototipo enfocado a la toma de evidencias a las auditorias	Equipo lideres	Falta de análisis	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de un análisis previo
		Mal selección del equipo	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mala elección del equipo líder
		Falta de conocimiento	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de conocimiento del equipo líder

		falta de experiencia	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de experiencia del equipo líder
	Recursos financieros	Falta de recursos financieros	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de recursos financieros
		Mal manejo de los recursos financieros	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal manejo de los recursos financieros
		Robo de los recursos financieros	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por robo de los recursos financieros
	Equipos de computo	Fallo en el equipo de computo	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por fallos en los equipos de computo
		Daño en el equipo de computo	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las

			pruebas de auditorías ti por daños en los equipos de computo
	Software	Mal funcionamiento	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal funcionamiento del software
		Bloqueo del software	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por bloqueo en el software
		Fallo en el software	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por fallos en el software
	Líder de desarrollo	Mal selección del líder de desarrollo	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por mal selección del líder de desarrollo
		Falta de conocimiento	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de conocimiento del líder de desarrollo
		Falta de experiencia	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de experiencia del

			líder de desarrollo
	Recursos Financieros	Falta de recursos financieros	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de recursos financieros
		Mal manejo de los recursos financieros	Malas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por mal manejo de los recursos financieros
		Robo de los recursos financieros	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por robo de los recursos financieros
	Equipos de computo	Fallo en el equipo de computo	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por fallo en los equipos de computo
		Daño en el equipo de computo	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por daño en los equipos de computo
	Software bd	No tener licenciamiento	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por no tener licenciamiento en el software de la bd

		Licenciamiento ilegal	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por licenciamiento ilegal en el software de la bd
		Falta de presupuesto para el licenciamiento de la bd	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de presupuesto para el licenciamiento del sw de la bd
		No tener licenciamiento	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por no tener licenciamiento en el software de la app
	Software app	Licenciamiento ilegal	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por licenciamiento ilegal en el software de la app
		Falta de presupuesto para el licenciamiento de la bd	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de presupuesto para el licenciamiento del sw de la app

Tabla 11: análisis de riesgos del desarrollo del prototipo Fuente: los autores

4.2.valoración del riesgo

Se listarán los riesgos del proyecto y junto a los interesados se realizará y se dará el puntaje en cada uno de los riesgos para su valoración. Se manejará una escala de 1 a 5 para el impacto siendo 1 insignificante y 5 catastrófico.

IMPACTO	
CATEGORIA	**PESO**
CATASTROFICA	5
MAYOR	4
MODERADA	3
MENOR	2
INSIGNIFICANTE	1

Tabla 12: impacto del riesgo.

Se manejará una escala de 1 a 5 para la probabilidad siendo 1 casi nunca y 5 siempre.

PROBALILIDAD	
CATEGORIA	**PESO**
SIEMPRE	5
MUY PROBABLE	4
MODERADA	3
IMPROBABLE	2
CASI NUNCA	1

Tabla 13: probabilidad del riesgo

Con el peso que les den los interesados y dueños de cada proceso a cada riesgo se realizará la valoración con las siguientes tablas.

ALTO	19 A 25
MEDIO	7 A 18
BAJO	0 A 6

Tabla 14: valor del riesgo

Por lo que a continuación se realiza la valoración de cada riesgo encontrado para las actividades que se realizan en el proyecto

	Riesgos	Impacto	Probabilidad	Valorización
1	Mala definición del alcance por mala elección del gerente del proyecto	4	3	12
2	Mala definición del alcance por falta de conocimientos del gerente de proyecto	5	4	20
3	Mala definición del alcance por falta de experiencia del gerente del proyecto	4	3	12
4	Perdidas en la definición del alcance por fallos en el equipo de computo	4	2	8
5	Perdida en la definición del alcance por daño en el equipo de computo	4	2	8
6	Mala definición del alcance ocasionada por mala recolección de la información	4	2	8
7	Mala definición del alcance ocasionada por recolección incompleta de la información	4	2	8
8	Mala definición del alcance ocasionada por no recolectar información	3	2	6
9	Fallas en el levantamiento de información por mala recolección de información	3	2	6
10	Fallas en el levantamiento de información por recolección incompleta de la información	3	3	9
11	Mal levantamiento de información por no recolectar información	4	2	8
12	Perdida de información por fallos en el equipo de computo	4	2	8

13	Perdida de información por daños en el equipo de computo	4	2	8
14	Fallas en el levantamiento debido a la mala elección del líder funcional	4	2	8
15	Fallas en el levantamiento de información debido a la falta de conocimientos del líder funcional	4	2	8
16	Fallas en el levantamiento de información debido a la falta de experiencia del líder funcional	3	2	6
17	Fallas en el levantamiento de información ocasionada por falta de recursos financieros	3	2	6
18	Fallas en el levantamiento de información ocasionado por mal manejo de los recursos financieros	3	3	9
19	Fallas en el levantamiento de información ocasionado por robo de los recursos financieros	4	1	4
20	Mala definición de recursos ocasionado por errores en la información	4	1	4
21	Mala definición de recursos ocasionado por mala planeación	3	1	3
22	Errores en la definición de los recursos por fallos en los equipos de computo	3	2	6
23	Perdida de información de los recursos por daño en los equipos de computo	4	3	12
24	Fallas en la definición de los recursos por mala selección del gerente de proyecto	3	1	3
25	Fallas en la definición de los recursos por falta de conocimiento del gerente de proyecto	4	1	4
26	Fallas en la definición de los recursos por falta de experiencia del gerente de proyecto	4	4	16

27	Errores en la definición de los requerimientos ocasionado por mal levantamiento en la información	4	3	12
28	Mala definición de los requerimientos ocasionado información incompleta	4	3	12
29	Mala definición de los requerimientos por mal levantamiento de información	5	4	20
30	Mala definición de los requerimientos por mal funcionamiento en el software	4	4	16
31	Errores en la definición de los requerimientos por bloqueo en el software	5	3	15
32	Errores en la definición de los requerimientos por fallos del software	4	2	8
33	Errores en la definición de los requerimientos por fallo en los equipos de computo	4	2	8
34	Errores en la definición de los requerimientos por daño en el equipo de computo	4	2	8
35	Errores en la definición de los requerimientos por mala elección del líder funcional	4	2	8
36	Errores en la definición de los requerimientos por falta de conocimientos del líder funcional	4	2	8
37	Errores en la definición de los requerimientos por falta de experiencia del líder funcional	3	4	12
38	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallas en el levantamiento de información	5	3	15
39	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallas en la recolección de la información	4	2	8
40	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por recopilación incompleta de la información	3	2	6

41	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por mala selección del equipo líder	4	1	4
42	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de conocimiento del equipo líder	3	3	9
43	Mala selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de experiencia del equipo líder	3	3	9
44	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por falta de recursos financieros	3	3	9
45	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por mal manejo de los recursos financieros	3	3	9
46	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por robo de los recursos financieros	4	2	8
47	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallos en los equipos de computo	4	2	8
48	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por daños en los equipos de computo	5	1	5
49	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por mal funcionamiento del software	4	4	16
50	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por bloqueo del software	4	3	12

51	Errores en la selección de las metodologías aplicables para la toma de evidencias de auditorías ti por fallo en el software	4	2	8
52	Mala categorización de las aplicaciones ocasionada por mal levantamiento de la información	4	2	8
53	Mala categorización de las aplicaciones ocasionada por información incompleta en el levantamiento	4	2	8
54	Mala categorización de las aplicaciones ocasionada por no realizar previamente el levantamiento de información	4	2	8
55	Mala categorización de las aplicaciones ocasionada por mal selección del equipo líder	4	2	8
56	Mala categorización de las aplicaciones ocasionada por mal falta de conocimiento del equipo líder	4	2	8
57	Mala categorización de las aplicaciones ocasionada por mal falta de experiencia del equipo líder	4	2	8
58	Errores en la categorización de las aplicaciones ocasionada por falta de recursos financieros	4	2	8
59	Errores en la categorización de las aplicaciones ocasionada por mal manejo de recursos financieros	5	2	10
60	Errores en la categorización de las aplicaciones ocasionada por robo de los recursos financieros	4	4	16
61	Errores en la categorización de las aplicaciones ocasionada por fallo en los equipos de computo	4	1	4
62	Perdida de información de las aplicaciones ocasionada por daño en los equipos de computo	3	3	9

63	Perdida de información de las aplicaciones ocasionada por mal funcionamiento del software	3	3	9
64	Perdida de información de las aplicaciones ocasionada por bloqueo del software	3	3	9
65	Perdida de información de las aplicaciones ocasionada por mal fallo en el software	3	3	9
66	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal levantamiento de información	4	3	12
67	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por análisis incompleto	4	3	12
68	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de un análisis previo	4	3	12
69	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mala elección del equipo líder	4	3	12
70	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de conocimiento del equipo líder	4	3	12
71	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de experiencia del equipo líder	4	3	12
72	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por falta de recursos financieros	3	3	9
73	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal manejo de los recursos financieros	3	3	9

74	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por robo de los recursos financieros	3	3	9
75	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por fallos en los equipos de computo	3	3	9
76	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por daños en los equipos de computo	3	3	9
77	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por mal funcionamiento del software	3	3	9
78	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por bloqueo en el software	3	3	9
79	Fallas en el análisis de resultados de las metodologías de las aplicaciones en las pruebas de auditorías ti por fallos en el software	3	3	9
80	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por mal selección del líder de desarrollo	3	3	9
81	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de conocimiento del líder de desarrollo	5	4	20
82	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de experiencia del líder de desarrollo	4	2	8

83	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de recursos financieros	4	2	8
84	Malas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por mal manejo de los recursos financieros	4	2	8
85	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por robo de los recursos financieros	4	2	8
86	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por fallo en los equipos de computo	4	2	8
87	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por daño en los equipos de computo	4	1	4
88	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por no tener licenciamiento en el software de la bd	4	3	12
89	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por licenciamiento ilegal en el software de la bd	4	3	12
90	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de presupuesto para el licenciamiento del sw de la bd	4	3	12
91	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por no tener licenciamiento en el software de la app	4	3	12

92	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por licenciamiento ilegal en el software de la app	4	3	12
93	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de presupuesto para el licenciamiento del sw de la app	4	2	8

Tabla 15: valoración del riesgo Fuente: los autores.

Posteriormente de realizar la valoración del riesgo los resultados son que 3 riegos son de valoración alta, 77 riesgos son de valoración media y por último 13 riesgos son de valoración baja.

4.3.Controles

En el apartado anterior se valoraron los riesgos por lo que esta sección se realiza el tratamiento de los riesgos con valoración alta. A cada riego se le identificaron controles para su tratamiento tanto preventivos, defectivos y correctivos. Se realiza la valoración de los controles con la siguiente tabla.

CLASE DEL CONTROL CALIFICACIÓN	
Control	**Valor**
Automático	3
Anual y no discrecional	2
Manual y discrecional	1

Tabla 16: calificación del control

Donde si el análisis de los controles es mayor a 2 es aprobado y si es menor a 2 es inapropiado, a continuación, se describen los controles para para los riesgos de valoración alta.

R2	MALA DEFINICION DEL ALCANCE POR FALTA DE CONOCIMIENTOS DEL GERENTE DE PROYECTO								
CODIGO	NOMBRE	PREVENTIVO	DETECTIVO	CORRECTIVO	AUTOMATICO	MANUAL	DISCRECIONAL	NO DISCRECIONAL	VALORACION DEL CONTROL
CTL 1	Evaluar las capacidades y conocimientos del gerente del proyecto antes de su nombramiento	X				X		X	2
CTL 2	Realizar la evaluacion y revision del alcance con los interesados antes de su aprobacion		X			X		X	2
CTL 3	Convocar reunion extraordinaria con los interesados del proyecto para realizar las correcciones necesarias			X		X		X	2
								PROMEDIO	2

R29	MALA DEFINICION DE LOS REQUERIMIENTOS POR MAL LEVANTAMIENTO DE INFORMACION								
CODIGO	NOMBRE	PREVENTIVO	DETECTIVO	CORRECTIVO	AUTOMATICO	MANUAL	DISCRECIONAL	NO DISCRECIONAL	VALORACION DEL CONTROL
CTL 4	Evaluar las capacidades y conocimientos del analista funcional antes de su nombramiento	X				X		X	2
CTL 5	Verificar periodicamente por el lider funcional los procesos realizados por el analista funcional		X			X		X	2
CTL 6	Realizar el levantamiento de informacion del proceso mal definido en el menor tiempo			X		X		X	2
								PROMEDIO	2

R81	FALLAS EN EL DESARROLLO DEL PROTOTIPO ENFOCADO A LA TOMA DE EVIDENCIAS A LAS AUDITORIAS OCASIONADO POR FALTA DE CONOCIMIENTO DEL LIDER DE DESARROLLO								
CODIGO	NOMBRE	PREVENTIVO	DETECTIVO	CORRECTIVO	AUTOMATICO	MANUAL	DISCRECIONAL	NO DISCRECIONAL	VALORACION DEL CONTROL
CTL 7	Evaluar las capacidades y conocimientos del lider de desarrollo antes de su nombramiento	X				X		X	2
CTL 8	Realizar test de pruebas del software antes de su puesta en marcha		X			X		X	2
CTL 9	Realizar la correccion de la falla en el software en el menor tiempo			X		X		X	2
								PROMEDIO	2

Figura 9: Controles del Proyecto

Para el tratamiento de riesgos ubicamos en la matriz de riesgo la zona donde se encuentran los riesgos con la valoración más alta.

RIESGO INHERENTE						
		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5				R2, R29,R81	
	4					
	3					
	2					
	1					

Tabla 17: riesgo inherente

Luego de valorar los controles a aplicar para cada riesgo realizamos nuevamente la valoración para ver su reducción.

TRATAMIENTO DEL RIESGO	
Promedio Puntaje Controles	**Descripción**
1	No se reduce la probabilidad
1.3	No se reduce la probabilidad
1.6	No se reduce la probabilidad
2	Se reduce la probabilidad en 1 punto
2.3	Se reduce la probabilidad en 2 puntos
2.6	Se reduce la probabilidad en 3 puntos
3	Se reduce la probabilidad en 4 puntos

Tabla 18: tratamiento de riesgos

Finalmente en la matriz de riesgos vemos el riesgo inherente.

RIEGOS TRATADOS Y RIESGO RESIDUAL				
		IMPACTO	**PROBABILIDAD**	**PUNTAJE**
R2	Mala definición del alcance por falta de conocimientos del gerente de proyecto	5	3	15
R29	Mala definición de los requerimientos por mal levantamiento de información	5	3	15
R81	Fallas en el desarrollo del prototipo enfocado a la toma de evidencias a las auditorias ocasionado por falta de conocimiento del líder de desarrollo	5	3	15

Tabla 19tratamiento de riesgo

RIESGO RESIDUAL						
		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5					
	4				**R2, R29, R81**	
	3					
	2					
	1					

Tabla 20: Riesgo residual

5. DESARROLLO DE LA PROPUESTA

5.1.Diagnóstico de las metodologías.

Para la ejecución de esta sección se realiza una matriz de diagnóstico de las metodologías estipuladas en el marco teórico del presente trabajo.

El primer paso para iniciar una auditoría de sistemas es la planeación donde se define cómo se va a ejecutar la auditoria, se establecen los objetivos, la metodología a usar, técnicas y procedimientos necesarios para gestionar la auditoria de TI.

Para la planeación de la auditoria de sistemas se siguen los siguientes pasos (Solarte, 2015):

- Elaborar el plan de auditoría
- Seleccionar los estándares a utilizar de acuerdo al objetivo (COBIT, MAGERIT, ISO/IEC 27001, ISO/IEC 27002, otro)
- De acuerdo con el estándar elegido, seleccionar los ítems que serán evaluados que estén en relación directa con el objetivo y alcances definidos en el plan.
- Seleccionar el equipo de trabajo y asignar tareas específicas.
- Determinar las actividades que se llevarán a cabo y los tiempos en que serán llevadas a cabo en cada ítem evaluado. (Programa de auditoría)
- Diseñar instrumentos para recolección de información (formatos de entrevistas, formatos de listas de chequeo, formatos de cuestionarios)
- Diseñar el plan de pruebas.

5.1.1. Descripción de las características de las metodologías

Gestión de riesgos: Es la acción integral para el abordaje de una situación de desastre. Permite determinar los riesgos, intervenir para modificarlos, disminuirlos, eliminarlos o lograr la preparación pertinente para responder ante los daños que, sin duda, causará un determinado desastre (Huerta, 2017).

Consideración de alta gerencia: Es la gestión que hace la alta gerencia para ayudar al trámite de la gestión de los riesgos (Huerta, 2017).

Aplicación de controles: Relaciona lo que la norma tiene con respecto a la gestión de los controles que se aplican para mitigar los riesgos (Huerta, 2017).

Gestión de activos: se refiere a los que la norma busca para gestionar todo el ciclo de vida de los activos de una organización con el fin de maximizar su valor (Huerta, 2017).

Tipo de compañías: Indica las compañías en las que las normas pueden aplicarse o desarrollarse (Huerta, 2017).

A continuación, se discriminan las características de las metodologías para la gestión de las auditorias de TI.

Características	ISO 27002	Magerit V3	ISO 31000
Gestión de riesgos	Identifica amenazas. Directrices para el análisis de riesgos. Análisis de la gestión de riesgos en SGSI. Tiene enfoque de gestión de riesgos.	Promueve la identificación de amenazas. Método sistemático para el análisis de los riesgos. Descubrir y planificar riesgo. Estimación de impacto de los riesgos. Brinda una herramienta (PILAR) para análisis de riesgos. Realiza el análisis de riesgo cualitativo y cuantitativo.	Genera una etapa para identifica amenazas. Plantea unas reglas para el análisis de los riesgos. Evalúa el sistema de control interno.
Consideración de alta gerencia	Su aplicación desmitifica que la seguridad de la información en un tema técnico.	Considerar a los responsables de la organización. Preparar a la organización para la aplicación de auditorías.	Su aplicación ayuda a la gerencia para controlar los riesgos.
Aplicación de controles	Establecer controles predeterminado para su aplicación. Divide los controles por clases como lo son: seguridad lógica, pistas de auditoria, integridad, continuidad y seguridad física.	Planifica la implementación de controles. Categoriza los controles para gestionar los riesgos.	Establecer guías para el establecimiento de controles.

Gestión de activos	Administra los activos por medio de un inventario. Establece los propietarios de cada activo. Gestiona directrices para el uso aceptable de los activos. Establece directrices de clasificación de los activos. Promueve el etiquetado y manejo de la información	Orienta la clasificación de los activos. Divide los activos en varios grupos con el fin de identificar más claramente los riesgos. Gestiona la descripción de los activos para identificar los riesgos. Promueve el etiquetado y manejo de la información	Realiza la clasificación de los activos. Gestiona criterios para el uso aceptable de los activos. Promueve el etiquetado y manejo de la información
Tipo de compañías	Está orientada a todo tipo de compañías.	Organizaciones publicas Pyme. Organizaciones sin ánimo de lucro.	Está orientada a todo tipo de compañías.
Ventajas	Aborda los riesgos de forma oportuna y en cada sector de la organización.	Soporta herramientas comerciales y no comerciales. Soporta ISO 27001, 15408 y 17799. Brinda una herramienta sistematizada para gestionar riesgos.	Soporta herramientas comerciales Aborda los riesgos de forma oportuna y en cada sector de la organización.

Desventajas	No soporta otras metodologías. No contiene una herramienta que ayude a la implementar la norma.	No gestiona el análisis de las vulnerabilidades. No incluye las recomendaciones dentro del análisis e los riesgos.	No soporta otras metodologías.

Tabla 21: características de las metodologías.

5.1.2. Conclusiones del diagnóstico

Teniendo en cuenta que la gestión de riesgos es uno de los fuertes en la auditoria de sistemas, se identifican que la norma ISO 27002 establece controles específicos para cada área de las organizaciones mientras que Magerit V3 establece la gestión de riesgos como prioridad en su desarrollo.

En el análisis de elementos que incorporan el riesgo es necesario para tener en cuenta aquellos que pueden incrementar la probabilidad de que un riesgo ocurra. Inclusive, es posible generar riesgos nuevos como la integridad de la información, la conducta de las personas involucradas, la complejidad de las transacciones involucradas en el proceso, así como, los cambios en los sistemas o en el personal clave; adicionalmente se debe tener en cuenta los factores de carácter externo que pudieran llegar a afectar la Organización como son los económicos, sociales, legales o de cambio tecnológico (Camelo, 2010).

5.2.Categorización de las CAAT's.

Las técnicas de auditoria asistidas por computadora CAAT´s son importantes para los auditores de TI, porque mediante su uso facilitan la gestión de la auditoria, destacando la confianza del análisis realizado por el auditor y la confianza de las entidades (Quesada, 2013). Donde algunas

de las principales herramientas usadas en Colombia según la Asociación Colombiana de Ingenieros de Sistemas (ACCIS, 2015) son las siguientes:

IDEA: Esta herramienta puede disminuir costos de análisis, mejorar la calidad del trabajo, con esta herramienta se puede leer, visualizar, analizar y manipular datos, también se puede hacer muestreos y extraer archivos (AUDIT, 2011). Así mismo y se usa en ambientes de:

- Auditoría externa de estados financieros.
- Auditoría interna.
- Detección de fraudes.
- Informes y análisis de gestión.
- Transferencias de archivos.
- Bancos e instituciones financieras.
- Industrias.
- Organizaciones de ventas al por menor.
- Entes gubernamentales (prestadores de ayudas y beneficios).

Valorando la usabilidad de la aplicación se identifica que tiene facilidad de uso, donde se puede hacer la creación de proyectos y asignar personal para la auditoria como se muestra en la figura 8.

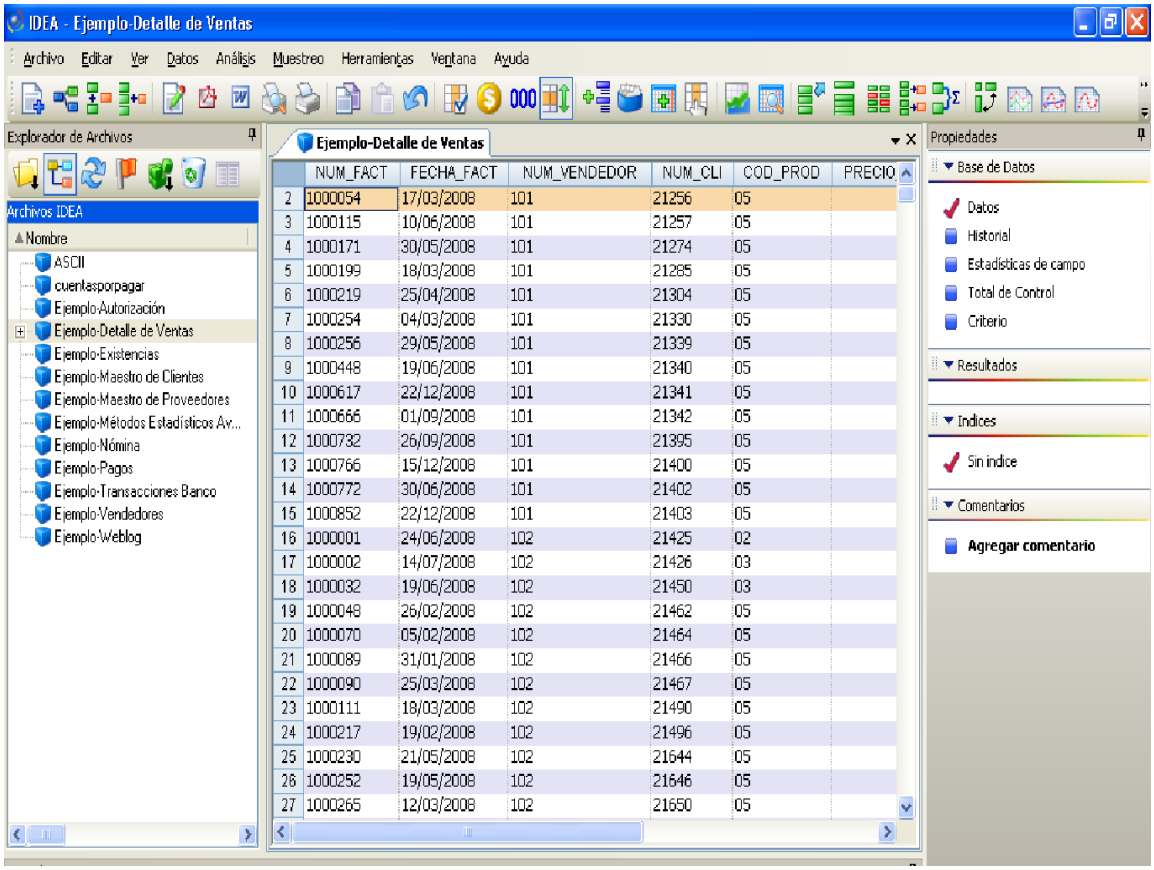


Figura 10: proyecto en CAAT´s "Fuente los autores"

Así mismo las auditorias muestras gráficas y consolidadas de la información recolectada como se ve en la figura 9.

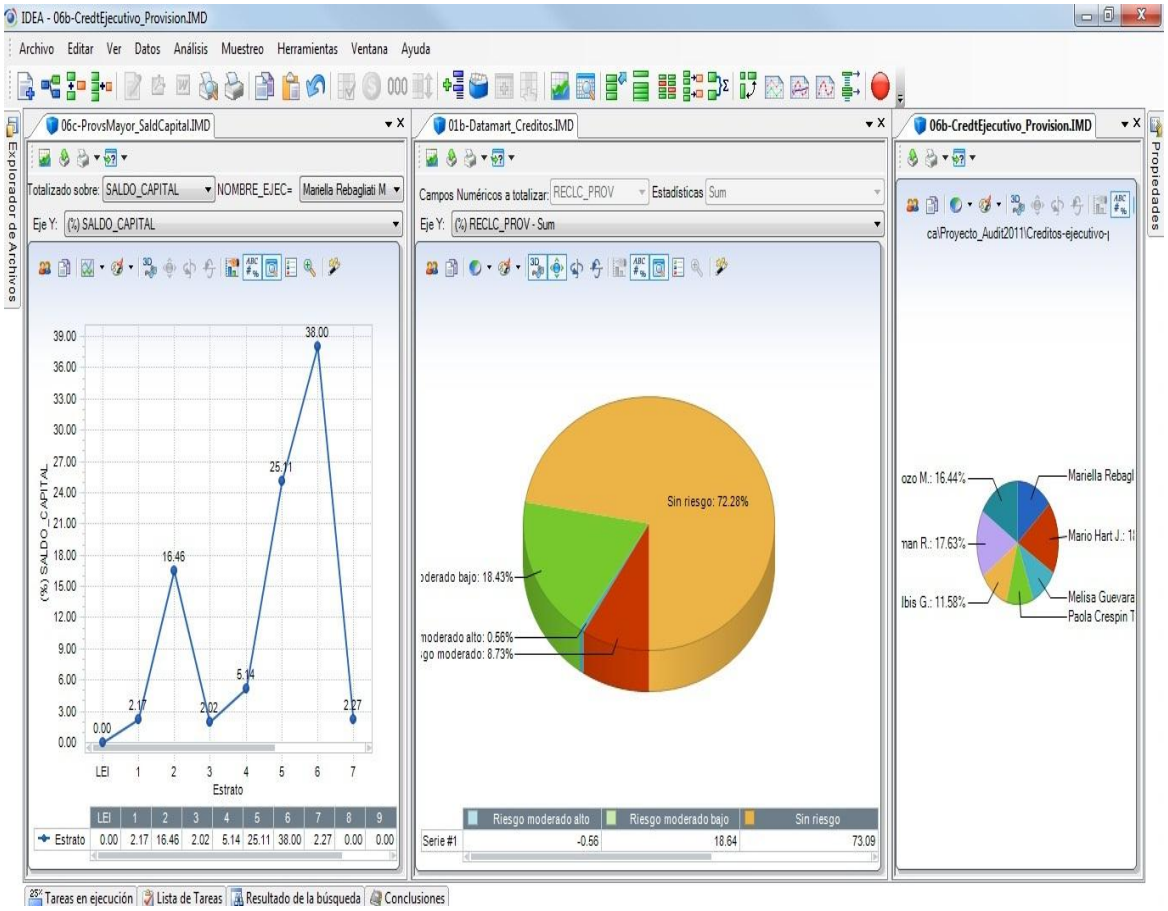


Figura 11: proyecto en CAAT´s "Fuente los autores"

Idea es una herramienta enfocada en la ejecución de pruebas y la generación de reportes.

ACL: Es una herramienta CAAT enfocada al acceso de datos, análisis y reportes para auditores y profesionales financieros (AUDIT, 2011), como también una de las más usadas en la gestión de auditorías de sistemas y permite:

- Análisis de datos para un completo aseguramiento.
- Localiza errores y fraudes potenciales.
- Identifica errores y los controla.
- Limpia y normaliza los datos para incrementar la consistencia de los resultados.
- Realiza un test analítico automático y manda una notificación vía e-mail con el resultado.

ACL es una herramienta intuitiva y genérica donde permite gestionar la auditoria de TI y evaluar los aspectos mencionados anteriormente y genera proyectos para asignar responsables a tareas como se ve en la figura 10.

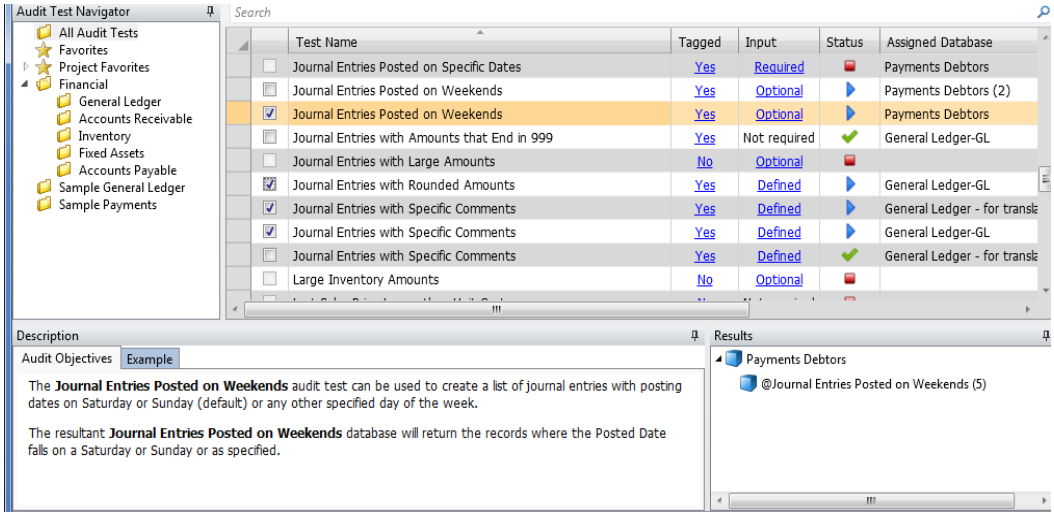


Figura 12: generación de proyecto "fuente: los autores"

ACL proporciona varias persona en un proyecto por lo que se puede asignar por usuarios roles y responsabilidades como se ve en la figura 11.

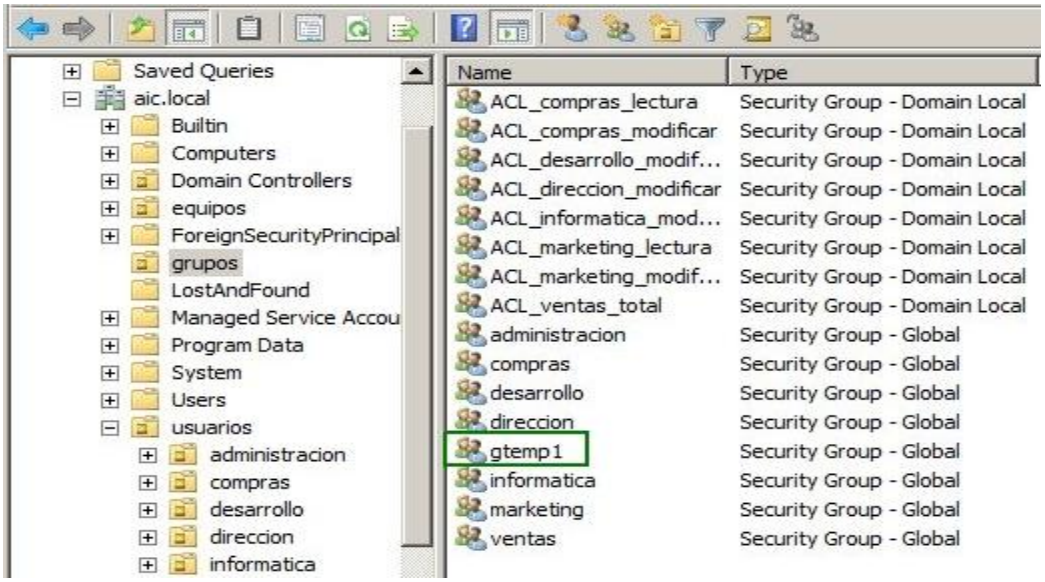


Figura 13: generación de encargados de la ejecución de la auditoria: "fuente los autores"

Por otro lado, permite la inclusión de pruebas que se hagan según cada proyecto como muestra la figura 12.

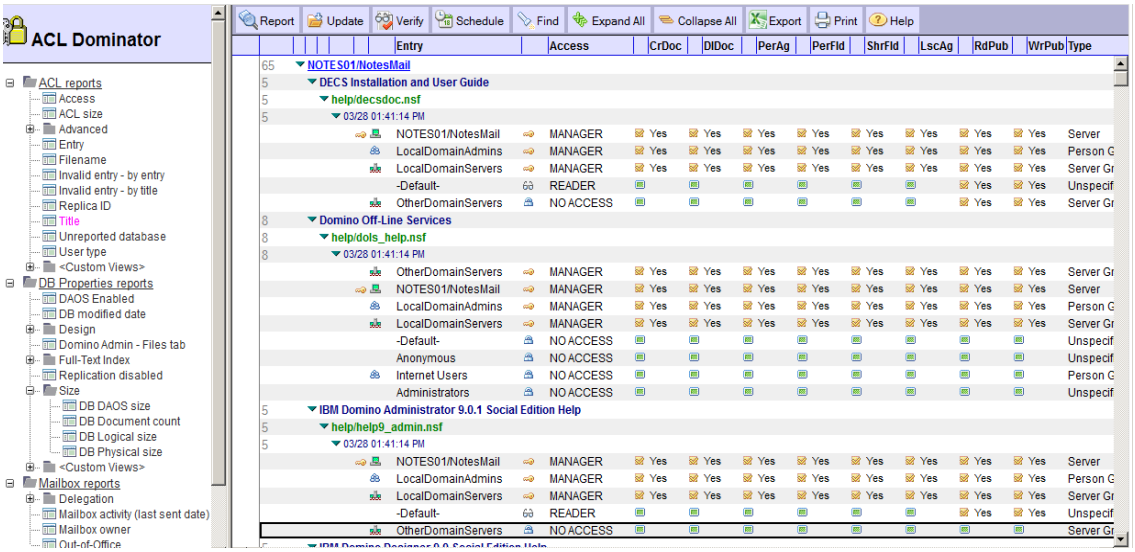


Figura 14: ejecución de pruebas en ACL "fuente: los autores"

Win Audit: Es un sistema completo para la automatización de la función de Auditoría, soportando todo el proceso y flujo de trabajo, desde la fase de planificación, pasando por el trabajo de campo, hasta la preparación del informe final (Quesada, 2013). Sus Beneficios son:

- Eficiencia en el trabajo
- Base de conocimiento
- Flexibilidad
- Estandarización y control
- Adaptabilidad
- Comunicación
- Reducción de costos y aprovechamiento del recurso más valioso (el auditor):
- Seguridad y confidencialidad
- Facilidad de uso
- Integración con ACL

Esta CAAT es una herramienta adaptable y permite la ejecución de los proyectos por lo que tiene en su módulo incluido la creación de proyectos como se muestra en la siguiente figura.

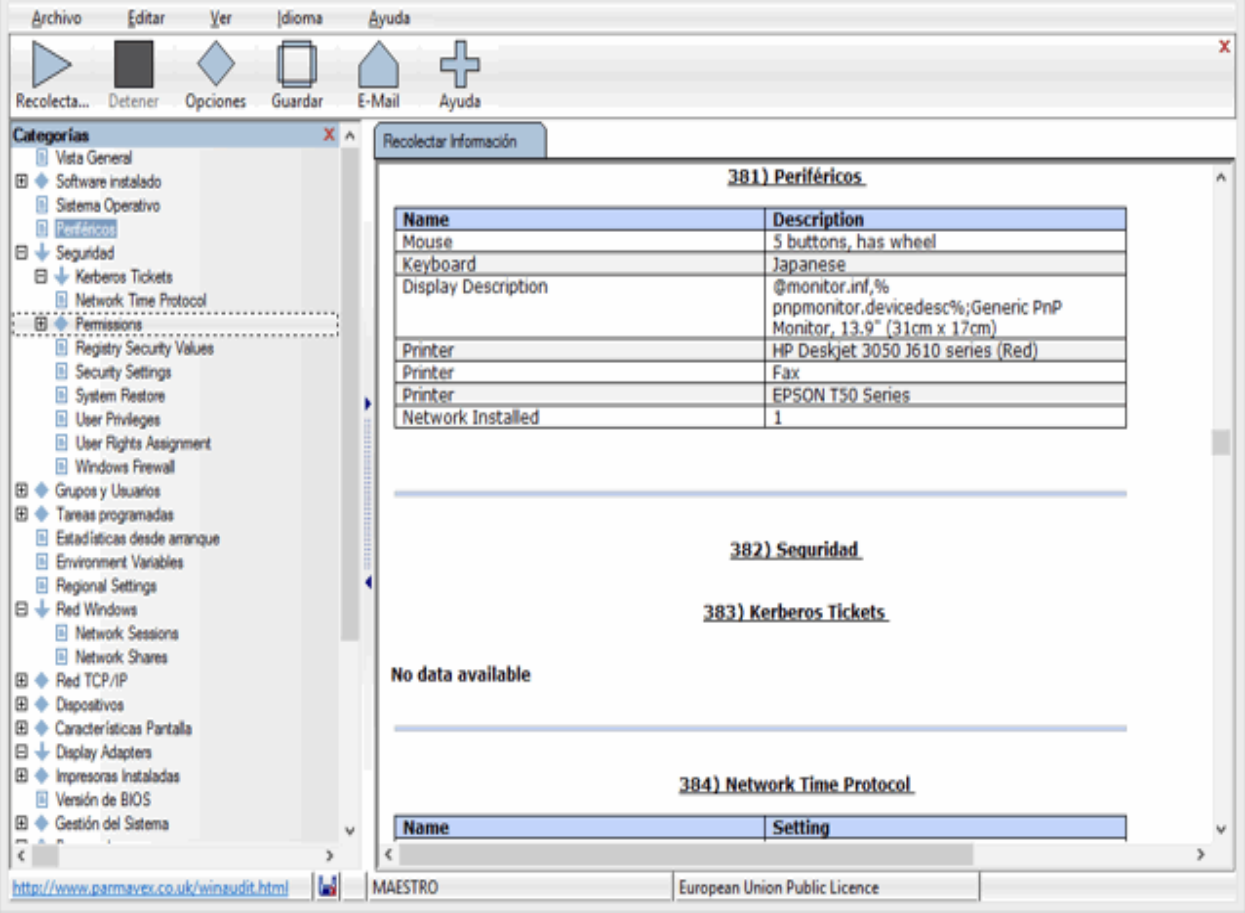


Figura 15: creación de proyecto "Fuente los autores"

En la siguiente figura y como se plantea en las demás CAAT´s la generación de pruebas es indispensable y permite realizarla con el fin de generar un informe posterior.

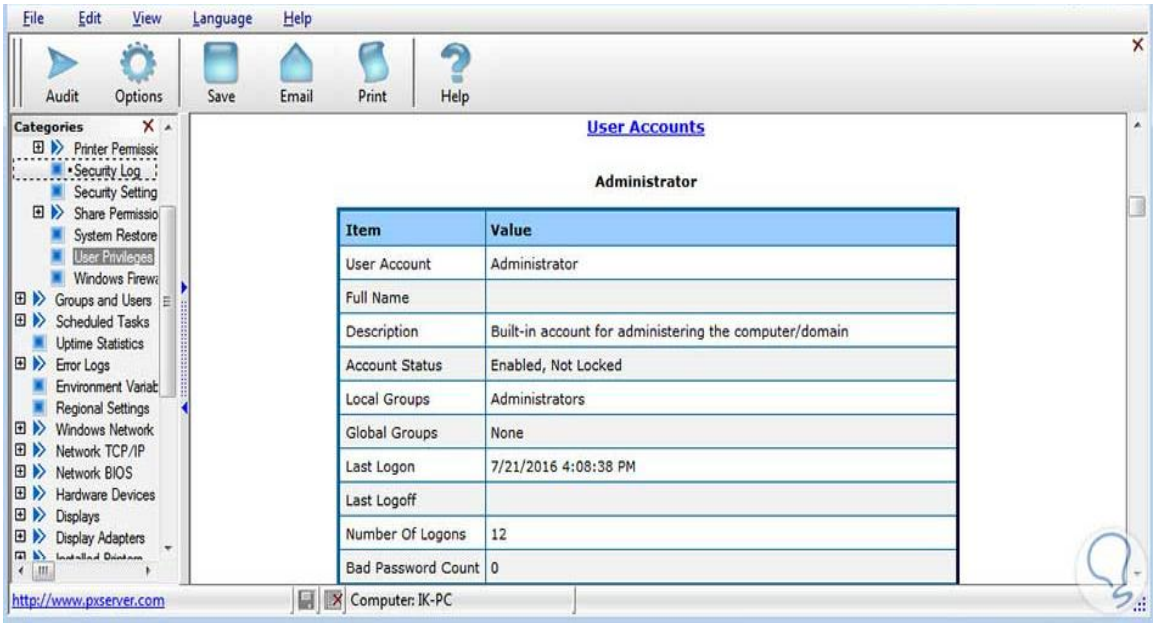


Figura 16: creación de pruebas "fuente: los autores"

Así como también la herramienta permite definir cada prueba para documentar la evidencia tomada.

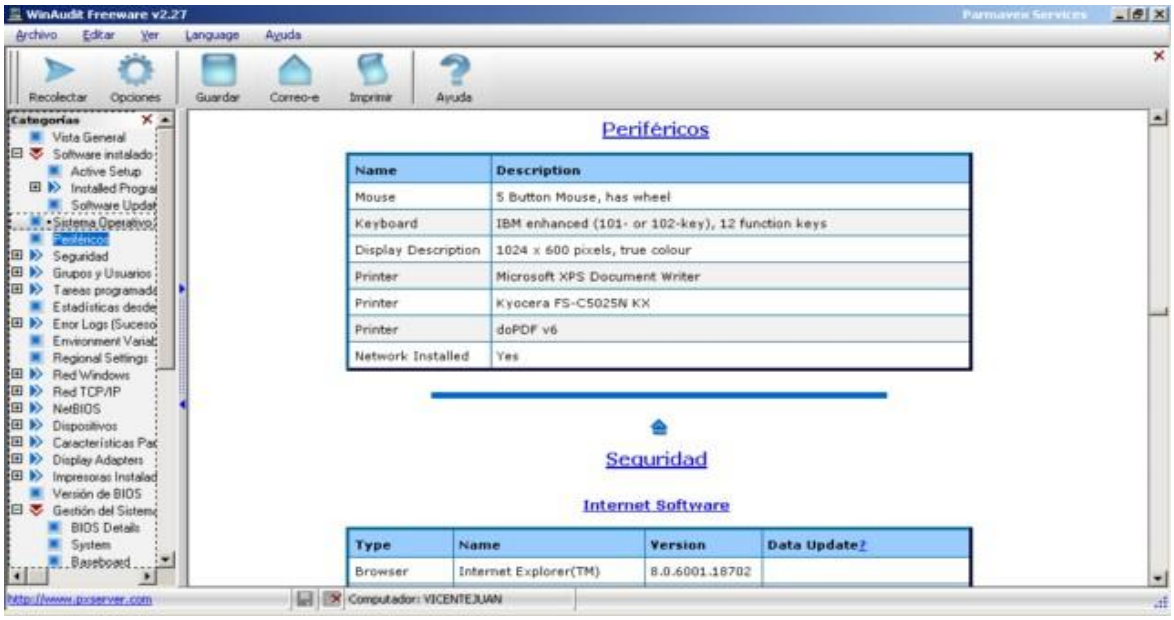


Figura 17: definición de la prueba "Fuente: los autores"

La siguiente tabla contiene la categorización de las herramientas de auditoria más usadas, donde los valores contenidos se dan en una escala de uno a cinco (1-5) donde 1 es más bajo y 5 e mas alto o eficiente.

CAAT's	Metodología	Toma de evidencias	usabilidad	Tipo de Plataforma	Gestión de riesgos	Informe
Idea	Soporta Cobit	No	4	stand alone	2	Informe Gerencial de la auditoria
ACL	Soporta ISO 27000, 9000, Cobit	SI	3	stand alone	2.5	Informe detallado y gerencial de la auditoria
Win Audit:	Soporta ISO 27000	SI	3	Móvil	3	Informe detallado de la auditoria

Tabla 22: categorización de las herramientas CAAT´S.

Como conclusión de la categorización se identifica que es indispensable que las herramientas CAAT´S soporte al menos una metodología para la gestión de la auditoría ya que estas ayudan a la aplicación de buenas prácticas y procedimientos en la auditoria. Así mismo es importante que la herramienta genere una optimización de tiempos en la gestión de las auditorias.

Por otra parte, la usabilidad como requerimiento en las herramientas asistidas por computadora para la gestión de auditorías es una ayuda para así garantizar la facilidad de uso y lo intuitivas que estas pueden llegar a ser en su manejo, para optimizar los tiempos de gestión de generación de informes con sus recomendaciones y hallazgos.

5.3.Análisis de resultados

El desarrollo de esta sección se centra en el análisis de los resultados obtenidos del diagnóstico realizado a las metodologías y la categorización de las CAAT´S, después de recolectar la información a través de la consulta sobre las metodologías y las herramientas CAAT´S.

En el diagnóstico de las metodologías se identificó que ISO 27002 da controles específicos para una organización mientras que ISO 31000 y Magerit se enfocan en la gestión de riesgo y aplicación de controles como principal característica. Sin embargo, Magerit proporciona unos estándares como el mapa de riesgos y los controles a los que se les hace pruebas para generar un informe con aceptaciones y rechazo según cada prueba. Por lo que se identifica el diseño de las pruebas de auditoria como un punto principal para el desarrollo del prototipo para almacenar cada evidencia documental obtenida en el proceso de la auditoria.

En la categorización de las herramientas CAAT´S se identificó que la mayor parte de las herramientas soportan una o más metodologías para la gestión de auditorías ya que son ayudas para optimización de tiempos en su ejecución, así como cambien la gestión de las pruebas más sin embargo de las herramientas analizadas no tiene un sistema de recolección de evidencias por lo que se ve como un ítem a incluir en el desarrollo del prototipo funcional y que cumple con la idea central del proyecto. Mas sin embargo existen algunas herramientas para la toma de evidencias como ACL GRC de recolección de pruebas, iAuditor, nimonik audit entre otras pero estas herramientas no gestionan la auditoria solamente permiten tomar evidencias y asociarles un cometario y generar un informe rápido y limitado.

Así como se realiza el diagnóstico de las metodologías y la categorización de las herramientas CAATs, se realiza como actividad completaría una serie de entrevistas a expertos enfocados en un caso de pruebas en la empresa Mac Center de Bogotá, con el fin de validar las metodologías usadas en auditoria y sobre cómo se realiza el proceso de toma de evidencias en las pruebas de cumplimiento.

para poder verificar la importancia de la toma de evidencias documentales en las pruebas de auditoria de TI, se presenta en el capítulo de metodología una entrevista que se usara como herramienta en este proceso se realizaron un total de 5 entrevistas donde los resultados se plasmaron en el Anexo C, los entrevistados tienen un promedio de edad de 35 años, tienen experiencia certificable en auditoria de TI de 5 a 15 años, así como también suman un total de 5 certificaciones y 3 especializaciones en auditoria y una en seguridad informática. Se contempló a través de un análisis cualitativo que la información levantada era muy similar por lo que muestra quedo en 5 entrevistas.

Metodologías usadas en auditoria: en el siguiente grafico se muestra las metodologías que alguna vez fueron usadas para auditoria por el personal entrevistado por lo que cada uno sabia más de una metodología. Así mismo se puede analizar que la mayor parte conocen ISO 27001 y en segundo lugar ISO 27002 y Magerit por lo que se identifican como las principales metodologías y teniendo en cuenta que ISO 27002 es un extracto detallado de los controles de la ISO 27001 toma mayor relevancia esta norma junto con Magerit. Juntas establecer criterios y controles específicos para la auditoria por lo que se seleccionan estas dos metodologías para que el prototipo funcional que se está desarrollando soporte dichas metodologías.

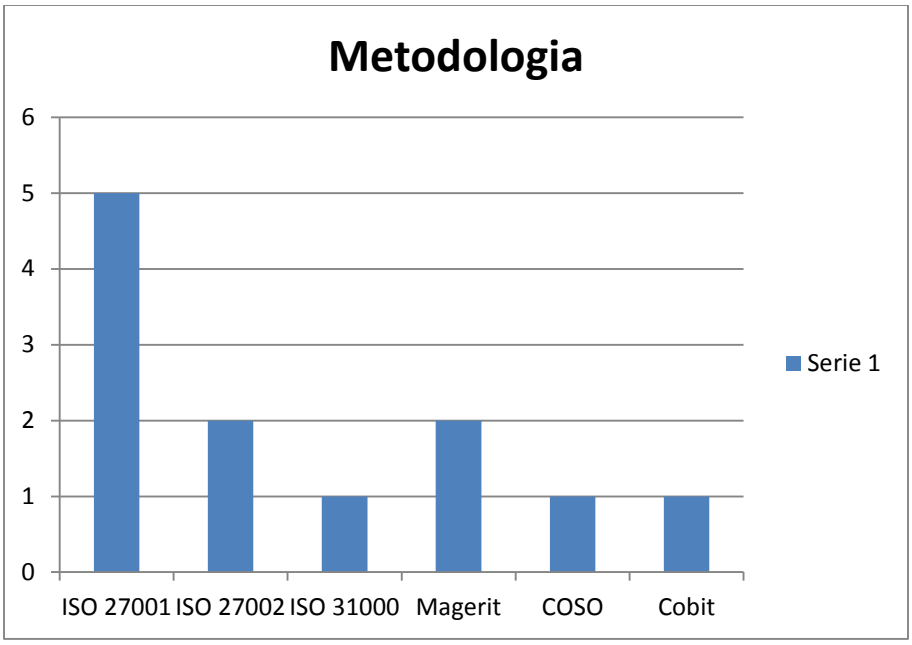


Figura 18: análisis de las metodologías Fuente: los autores

En cuanto a cómo se realiza el proceso de la toma de evidencias se pudo concluir que todos usan la recolección de las evidencias por medio de fotografías, archivos digitales, físicos y testimonios de los usuarios o auditados. Así mismo 3 de los entrevistados concluyeron que sería bueno incluir una herramienta CAAT en este proceso y 2 que reducir tiempos por lo que al analizar se puede ver que el reducir tiempos en la gestión de las pruebas va de la mano con las herramientas usadas.

Para finalizar se tiene que los entrevistados han usado o conocen herramientas CAATs en sus auditorías según se ve en la siguiente figura.

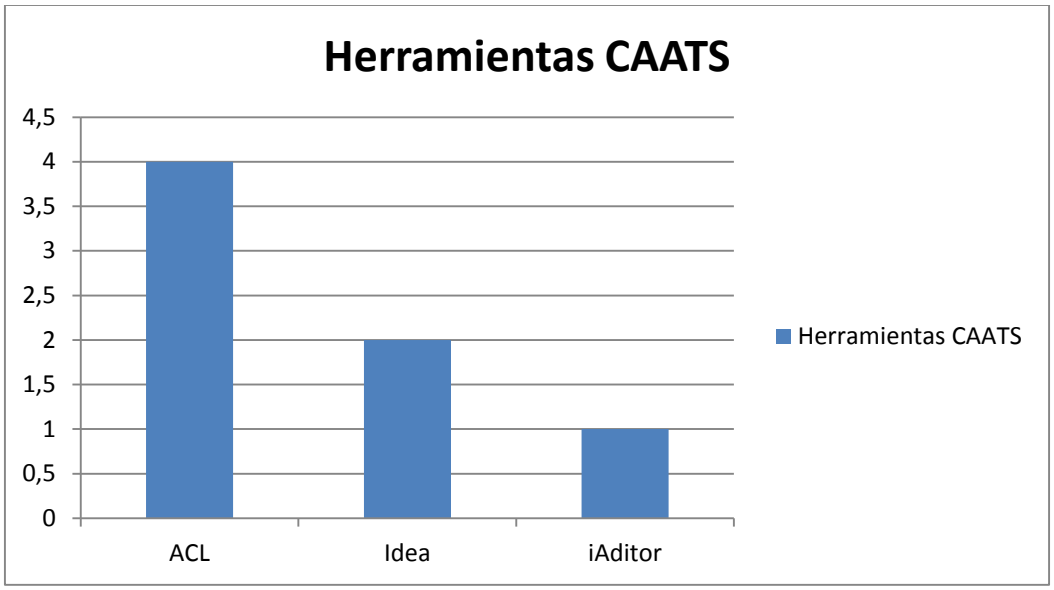


Figura 19: Análisis de las herramientas CAATS

Según lo identificado se concluye que las metodologías a tener en cuenta son ISO 27002 y Magerit, por su enfoque en riesgos y controles ya que las pruebas que un auditor hace y lo que verifica son que los controles funcionen o si están o no están implementados.

Así mismo se observa que se debe optimizar el proceso de la toma de evidencias de las pruebas de auditoria por medio de una herramienta o método.

Para finalizar ACL es la herramienta automatizada para la gestión de auditoria de la que los auditores más conocen.

5.4.Desarrollo del prototipo funcional

El aplicativo a desarrollar es de funcionamiento web debe cumplir los requerimientos especificados en este documento.

5.4.1. Propósito

El aplicativo es realizado para el seguimiento y registro de las evidencias documentales en las pruebas de auditoria de TI.

5.4.2. Alcance

El prototipo funcional incluirá los requerimientos y reglas del negocio que involucren el de las evidencias documentales en las pruebas de auditoria de TI ya que se priorizaron como de vital importancia.

5.4.3. Perspectiva del producto

El sistema a desarrollar es para poder gestionar la toma de evidencias documentales en las pruebas de cumplimiento de auditoria de, debe almacenar información de los usuarios, evidencias y pruebas realizadas en las auditorías.

5.4.4. Funcionalidad del producto

El sistema debe almacenar la información de los auditores que gestionaran las pruebas, como también los temas relacionados con las evidencias documentales dentro de un proyecto específico, el sistema debe almacenar la información de los lideres e auditoria, auditores sénior, auditorios junior y validadores que la persona registrada sea un auditor de TI mediante él envió de los soportes necesarios.

5.4.5. Análisis de Requerimientos

CÓD	TIPO	DESCRIPCIÓN	SUSTENTO DE SU INCLUSIÓN	PROPIETARIO	FUENTE	PRIORIDAD
1	Funcional	Registrar datos de usuario	se debe registrar datos principales de usuario para validar que se ingrese sesión	auditores, dueños de la APP	Estudio de seguridad de la información	ALTA
2	Funcional	Validar usuario si es auditor	para evitar que la herramienta la usen personas no idóneas se requiere un registro de un documento que lo certifique como auditor	auditores, dueños de la APP	Estudio de las aplicaciones de auditoria	ALTA
3	Funcional	Validar certificado del auditor	con el fin de validar si el certificado que el auditor sube el valido se requiere que la certificación llegue a un usuario administrador de la herramienta	dueños de la APP	consulta en Internet	MEDIA

4	Funcional	Iniciar sesión de usuario	se requiere para validar cuando el usuario entre al sistema	dueños de la APP	consulta en Internet	ALTA
5	Funcional	Registrar proyecto	con el paso del tiempo se requiere que un auditor tenga varios proyectos	auditores, dueños de la APP	Estudio de las aplicaciones de auditoria	ALTA
6	Funcional	Asignar auditores a proyecto	es necesario tener varios auditores por lo que se quiere asignar personal	auditores, dueños de la APP	Estudio de las aplicaciones de auditoria	ALTA
7	Funcional	Asignar roles de auditoria	en un proyecto es necesario tener varios auditores por lo que se quiere asignar roles en la auditoria	auditores, dueños de la APP	Estudio de proceso de las auditorias	ALTA
8	Funcional	Asignar tareas a un auditor	por los roles cada auditor tiene responsabilidades por lo que el líder le debe asignar una o más tareas dentro de la auditoria	auditores, dueños de la APP	Estudio de proceso de las auditorias	MEDIA
9	Funcional	Registrar formato para ficha técnica de TI a auditar	por buenas prácticas se debe registrar la ficha técnica	auditores, dueños de la APP	Estudio de metodologías en el proceso	ALTA

			del aplicativo o herramienta que se está auditando		de la auditoria	
10	Funcional	Registrar Prueba	por buenas prácticas se debe registrar la el formato de las pruebas	auditores, dueños de la APP	Estudio de metodologías en el proceso de la auditoria	ALTA
11	Funcional	Registrar formato de pruebas de auditoria	para fomentar las buenas prácticas se debe registrar la el formato de las pruebas de auditoria	auditores, dueños de la APP	Estudio de buenas prácticas en el proceso de la auditoria	ALTA
12	Funcional	Seleccionar controles para prueba	por buenas prácticas la prueba se hace para ver si los controles están funcionando	auditores, dueños de la APP	Estudio de metodologías en el proceso de la auditoria	MEDIA
13	funcional	Almacenar evidencia fotos tomadas por cámara de dispositivo y posicionamiento geográfico de estas	para sustentar la prueba se requiere acceso a la cámara para tomar evidencias	Dueños de la APP	Estudio de metodologías de la auditoria	ALTA
14	funcional	Almacenar documentos o archivos de evidencias de la	para sustentar la prueba se requiere	Dueños de la APP	Estudio de metodologías de la	MEDIA

		auditoria	adjuntar evidencias		auditoria	
15	funcional	Aprobar reporte	por buenas prácticas el informe de la auditoria debe ser aprobado por un líder	Auditores, Dueños de la APP	Estudio de aplicaciones de auditoria	ALTA
16	funcional	Generar reporte	para visualizar las pruebas se debe generar un informe	Dueños de la APP	Estudio de aplicaciones de auditoria	ALTA
17	restricciones	Garantizar que solamente los miembros del proyecto puedan hacer CRUD en la información del Proyecto	para sustentar la integridad de los datos no cualquiera puede acceder o modificar	Dueños de la APP	estudio de seguridad de la información	ALTA
18	restricciones	Validar que una prueba tenga varias evidencias	para garantizar que la prueba se haga correctamente se debe validar que tenga una o muchas evidencias	Dueños de la APP	estudio de seguridad de la información	ALTA
19	restricciones	Validar que varios auditores puedan estar asociados a un proyecto	garantizar que en un proyecto se tengan varios auditores	Auditores, Dueños de la APP	estudio de seguridad de la información	ALTA

20	restricciones	Validar certificación del auditor para finalizar creación de usuario	para garantizar que los usuarios del APP sean personas idóneas se requiere pedir un certificado de auditor	Auditores, Dueños de la APP	estudio de seguridad de la información	MEDIA
21	restricciones	Establecer que un control pueda mitigar varios riesgos	para establecer la matriz de riesgos se requiere asociar los controles a los riesgos	Auditores, Dueños de la APP	estudio de seguridad de la información	ALTA
22	restricciones	Establecer que un riesgo pueda tener asociados varios controles	para establecer la matriz de riesgos se requiere asociar los riesgos a los controles	Auditores, Dueños de la APP	estudio de seguridad de la información	ALTA
23	restricciones	Validar que un auditor pueda crear varias pruebas	establecer buenas prácticas para la ejecución de pruebas	Dueños de la APP	estudio de seguridad de la información	ALTA
24	restricciones	Validar que los auditores con tarea de pruebas puedan crear varias pruebas y solo consultar las que no crearon	garantizar que las pruebas sean integras y no erradas	Dueños de la APP	estudio de seguridad de la información	MEDIA
25	restricciones	Validar que si un control se repite en una prueba le genere	establecer comunicación entre los roles del	Dueños de la APP	estudio de seguridad	MEDIA

		un aviso al auditor de que el control fue asignado a otra prueba	sistema		de la informac ión	
26	restriccio nes	Validar que el auditor líder sea el único que apruebe el reporte	garantizar un reporte idóneo	Auditores, Dueños de la APP	estudio de segurida d de la informac ión	ALTA

Tabla 23: listado de requerimientos

La priorización de los requerimientos se da por la información recolectada en la categorización de la CAATs, las respectivas pruebas de las herramientas y en las entrevistas recolectadas a especialistas.

5.4.6. Diseño UML del Prototipo

5.4.6.1.Diagramas de casos de uso

En primer lugar, se establecen los actores que son los principales usuarios de la aplicación web:

ACTOR ACT1	Administrador
DESCRIPCIÓN	Es el encargado de gestionar la configuración, cambios y seguridad de la aplicación web.
PERMISOS	Gestionar (Crear, actualizar, eliminar), Administrar Usuarios, Visualizar.

Tabla 24: actor 1 en casos de uso "Fuente: El autor".

ACTOR ACT2	Usuario(Auditor)
DESCRIPCIÓN	Puede visualizar todo el contenido de la aplicación web, también pueden realizar carga de documentación y gestionar las pruebas de cumplimiento en una auditoria TI.
PERMISOS	Visualizar el contenido de la Aplicación web. Realizar las pruebas de cumplimiento en una auditoria de TI.

Tabla 25: actor 1 en casos de uso "Fuente: El autor".

ACTOR ACT3	Usuario(Auditor líder)
DESCRIPCIÓN	Puede visualizar todo el contenido de la aplicación web, también pueden realizar aprobaciones.
PERMISOS	Visualizar el contenido de la Aplicación web. Realizar aprobación del informe y la auditoria

Tabla 26: actor 3 en casos de uso "Fuente: El autor".

Caso de uso 1: inicio sesión administrador. Para el diseño del sistema, conceptualmente se realizó el siguiente diagrama de caso de uso, véase Figura 15, que permite observar el comportamiento del actor 1 en este caso concreto el administrador, en el inicio de sesión para poder ingresar a gestionar los contenidos de la aplicación web. Este comportamiento sirve de esquema para los sistemas web enfocados a la realización de auditorías de TI.

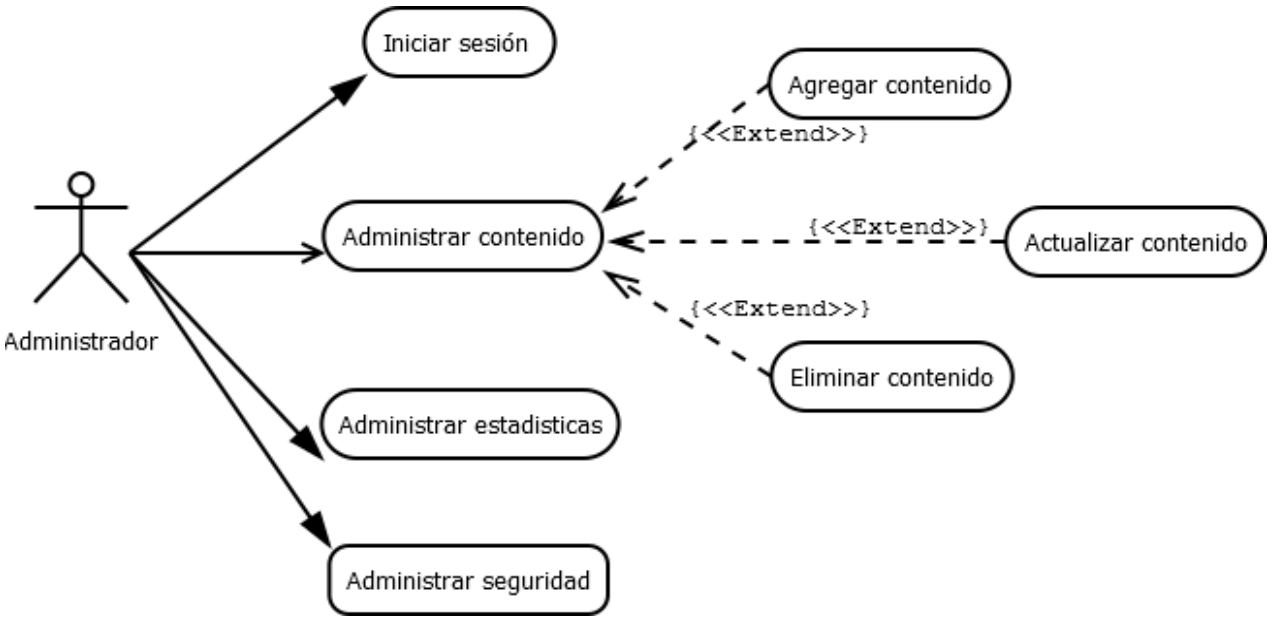


Figura 20 Caso de uso: Inicio sesión administrador Fuente: El Autor.

Caso de uso 2: Gestionar estructura organizacional de pruebas de cumplimiento. Este diagrama de caso de uso muestra el comportamiento del sistema luego que permite el acceso al administrador para la gestión del contenido, véase Figura 16. Este comportamiento sirve de esquema para los sistemas web enfocados a la realización de auditorías de TI.

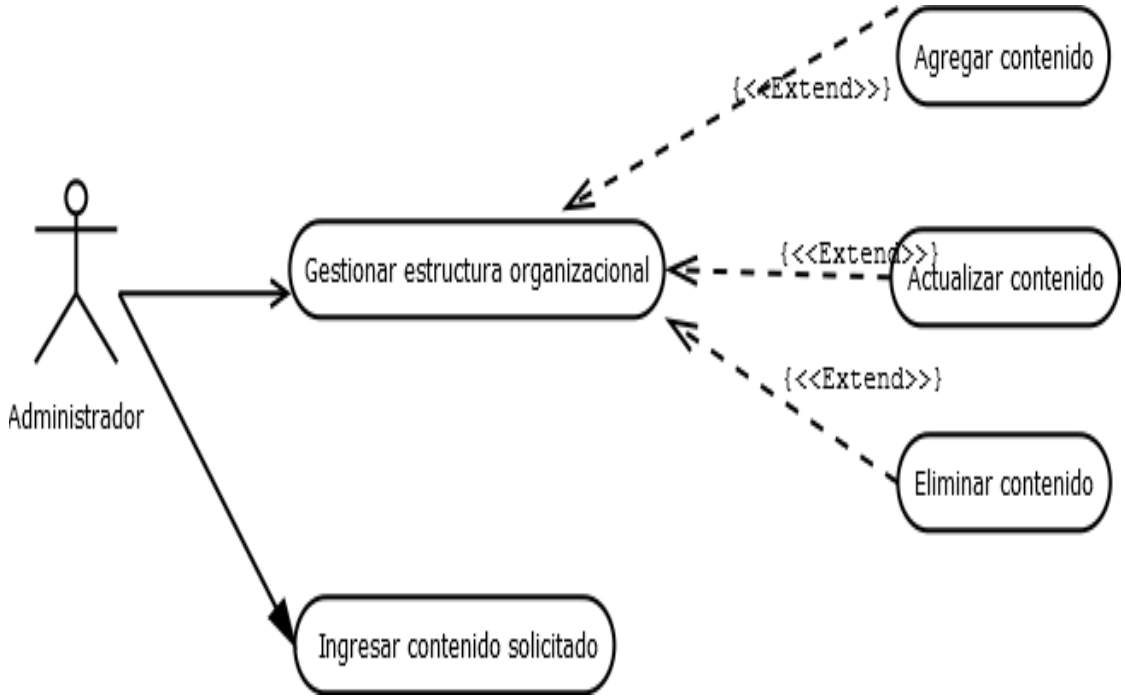


Figura 21: Caso de uso: gestionar estructura organizacional de pruebas de cumplimiento "Fuente: El autor"

Caso de uso 3: Menú de usuarios. Este caso de uso muestra el comportamiento del menú frente al usuario final de la aplicación web, véase Figura 17. Este comportamiento sirve de esquema para los sistemas web enfocados a la realización de auditorías de TI.

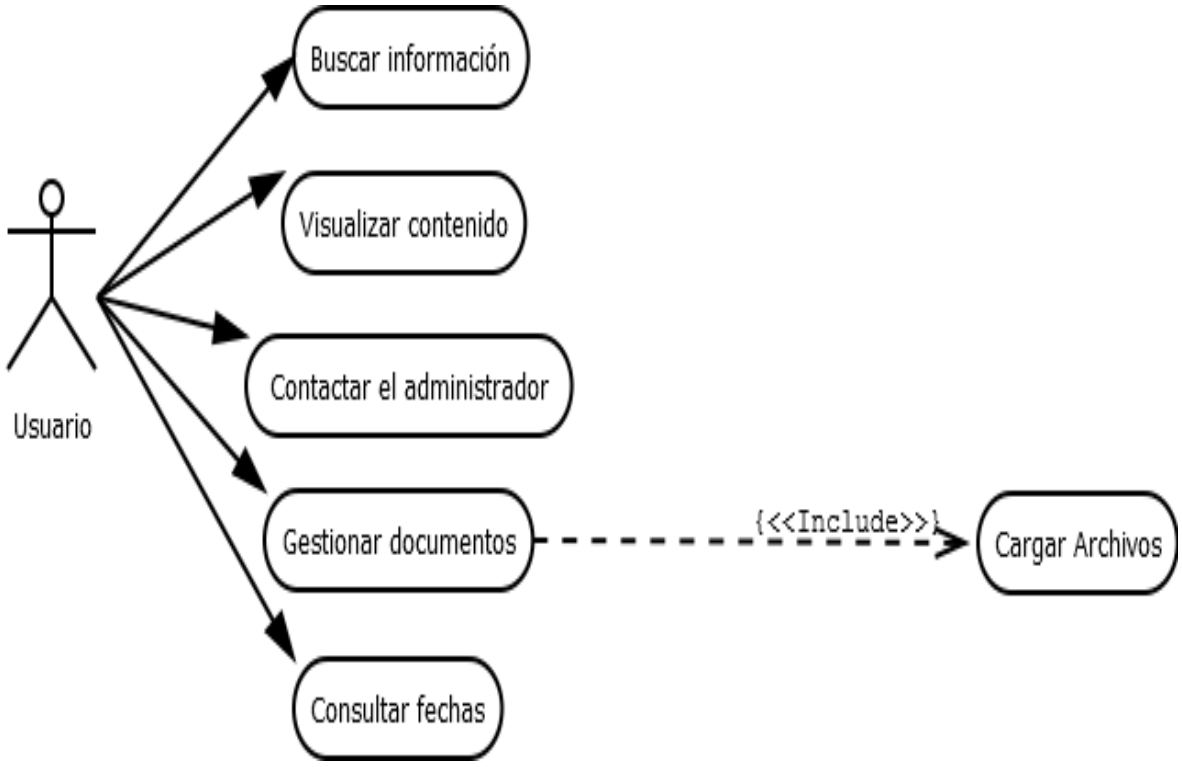


Figura 22: Caso de uso: menú de usuarios "Fuente: El autor"

4.4.4.2 DIAGRAMAS DE SECUENCIA

Cu1. Inicio de sesión administrador. En el diagrama de secuencias de inicio de sesión del administrador, se muestran las interacciones de los objetos del sistema para el anterior procedimiento, véase figura 18. Este comportamiento sirve de esquema para los sistemas web enfocados a la realización de auditorías de TI.

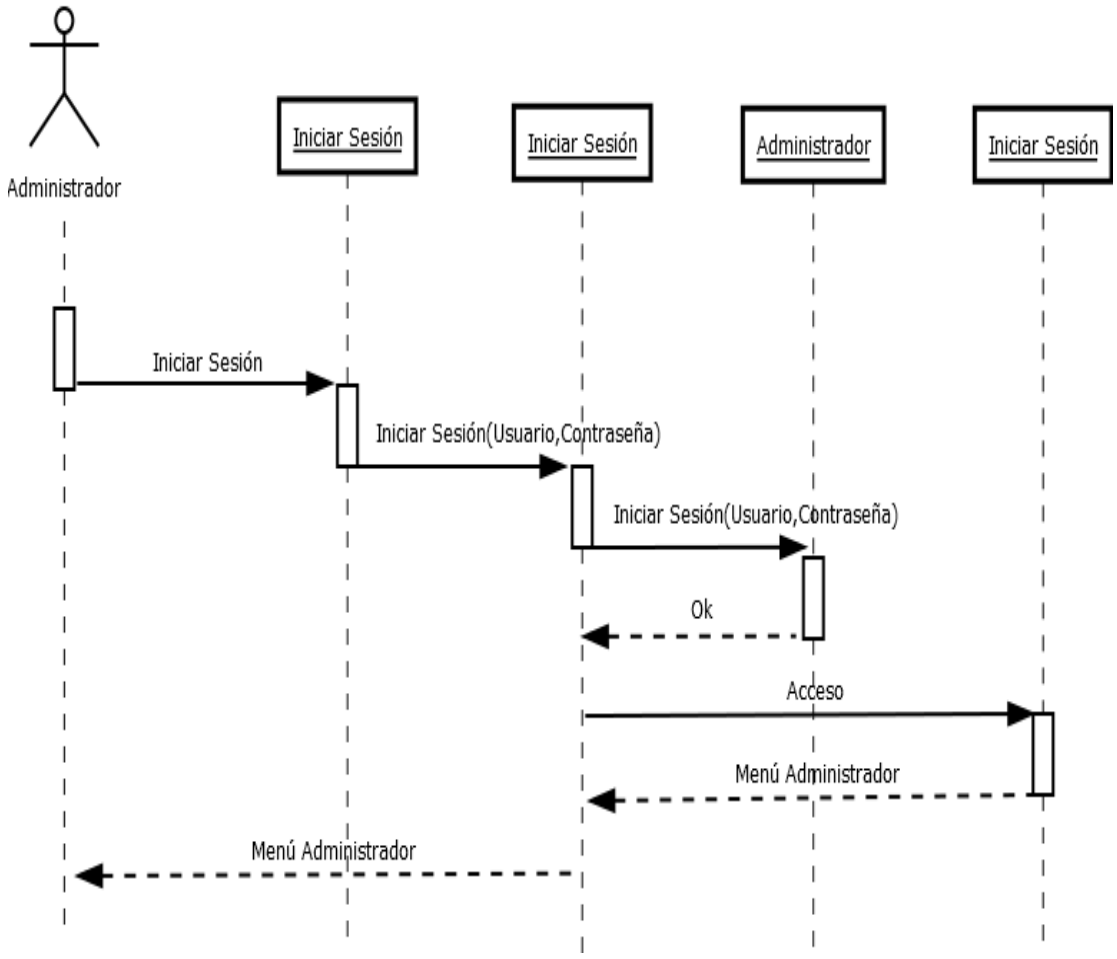


Figura 23: Diagrama de secuencia: inicio sesión administrador "Fuente: El autor"

Cu2. Gestionar estructura organizacional de las pruebas de cumplimiento. El siguiente diagrama de secuencias es el que muestra las interacciones del proceso de la gestión de la estructura organizacional, véase Figura 19, aquí se puede observar los módulos que se activan en este proceso y además las relaciones entre ellos. Este comportamiento sirve de esquema para los sistemas web enfocados a la realización de auditorías de TI.

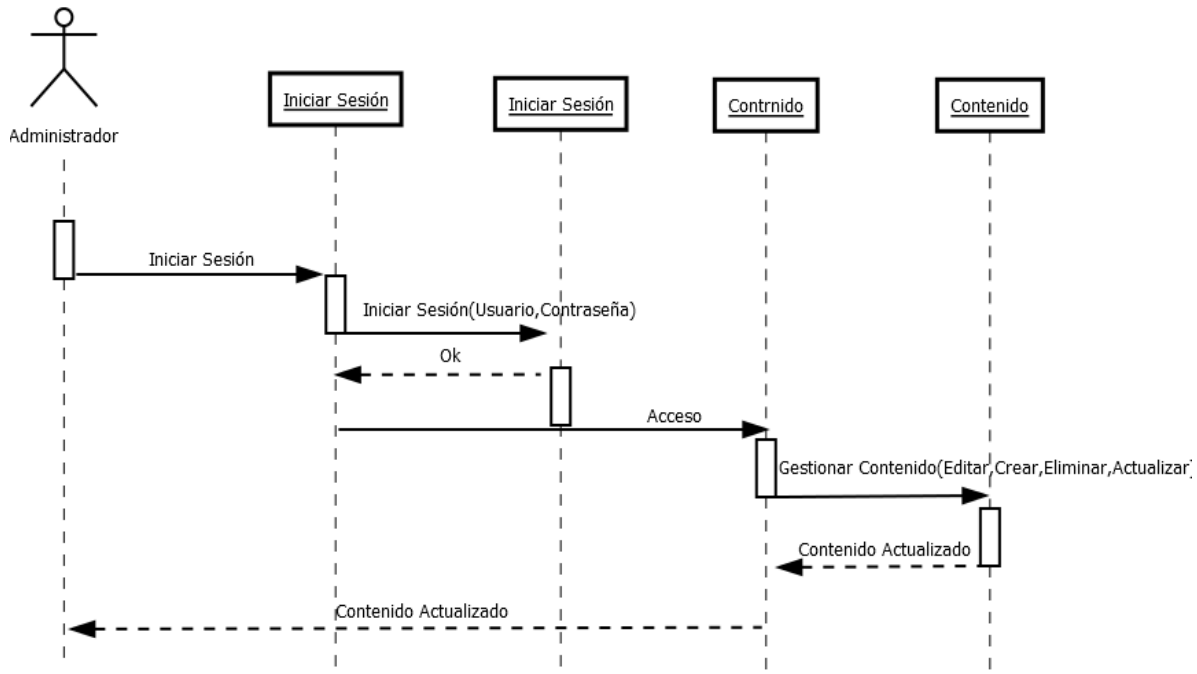


Figura 24: Diagrama de secuencia: gestionar estructura organizacional de pruebas de cumplimiento "Fuente: El autor."

Cu3. Menú de usuarios. Por último, se muestra el diagrama de secuencias que permite observar las interacciones de los objetos en el menú para los usuarios, véase Figura 20.

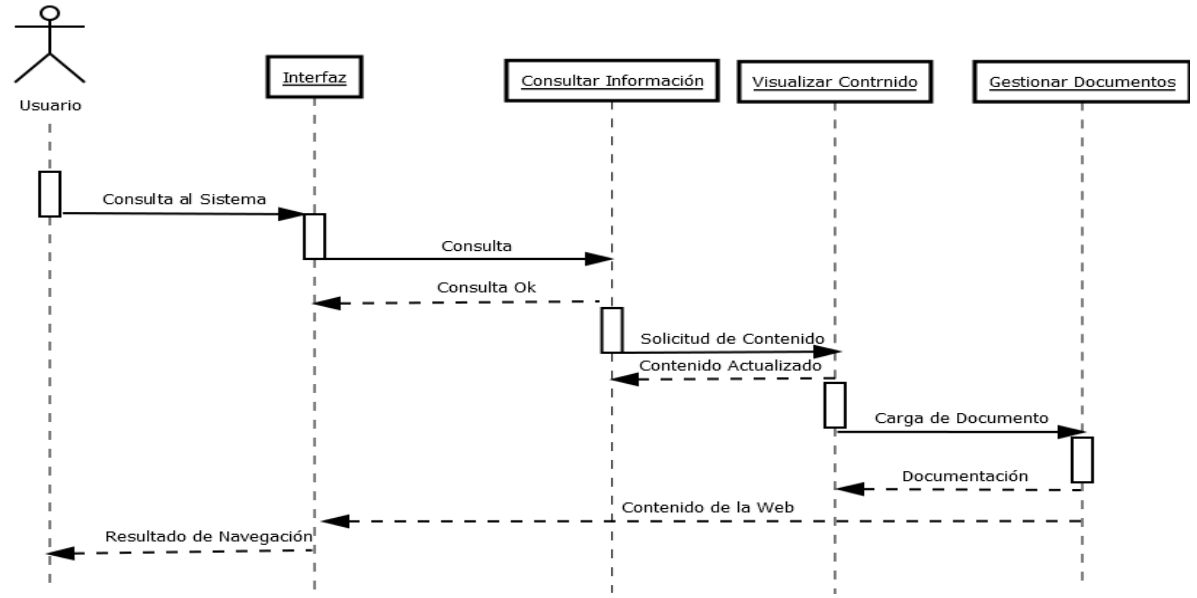


Figura 25: Diagrama de secuencia: menú de usuarios "Fuente: El autor."

A continuación, se establecer el Modelo de bases de datos que se diseñó para el prototipo funcional

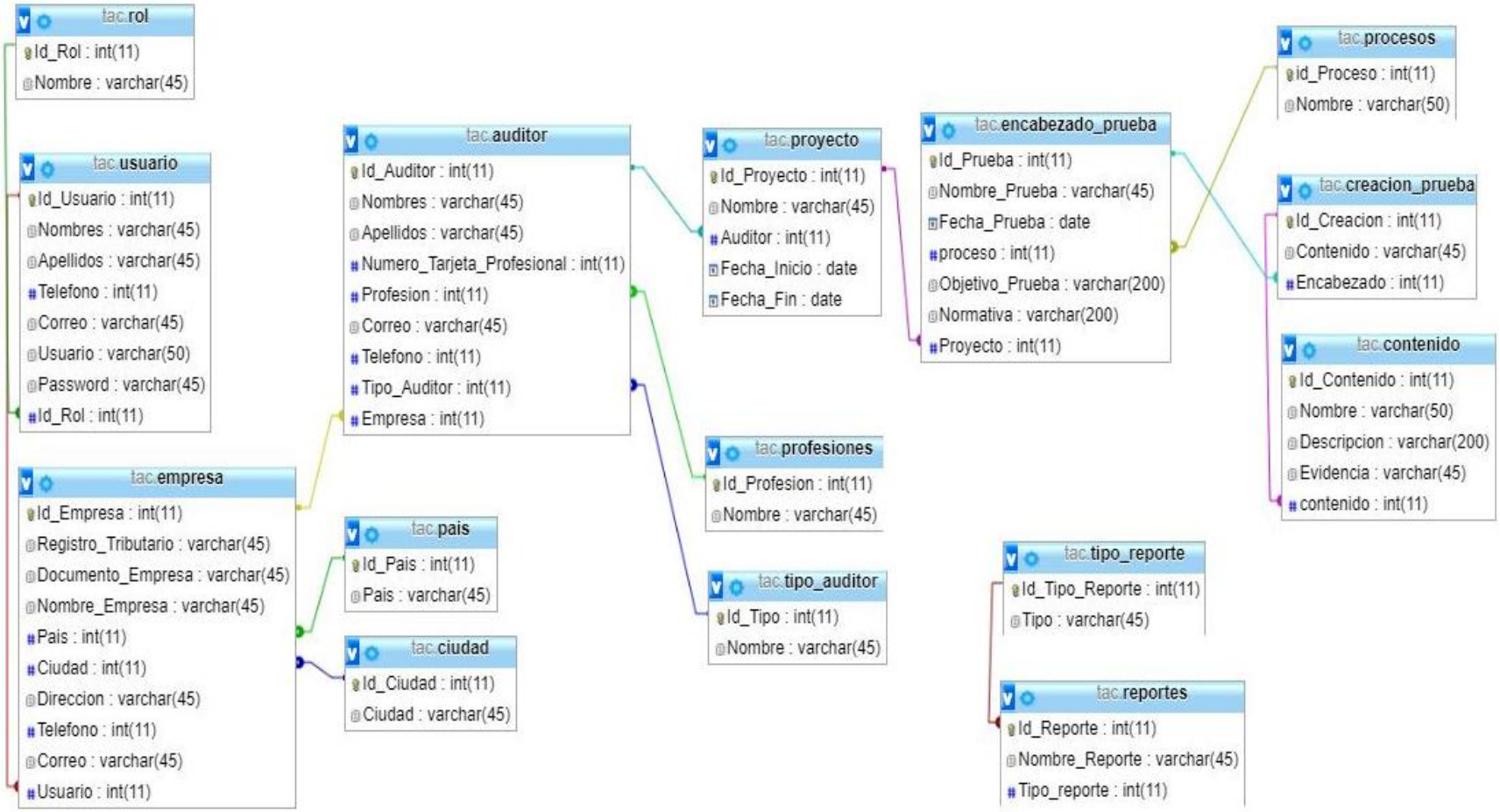


Figura 26: Diagrama de entidad relación "fuente los autores"

Así mismo el diccionario de datos se podrá ver en el Anexo C

5.4.7. Desarrollo del Prototipo

Siguiendo las metodologías de ingeniería de software para el correcto desarrollo del proyecto, empezando por el cronograma de actividades y estimando el tiempo en el que se puede realizar el proyecto.

En la etapa de diseño se establecieron responsabilidades y distribución de trabajo, se plateo los posibles diseños y soluciones para realizar las entregas correspondientes

El aplicativo será distribuido debe garantizar heterogeneidad y ser un aplicativo web.

La etapa de diseño se realizara en Visio herramientas que permiten el manejo de uml y en Netbeans para desarrollar la lógica y en MySql como motor de base de datos.

Ítem	Elemento
Herramienta	Net beans 7.0
Lenguaje	Java Server Faces
Jdk	1.7
Servidor de conexión	Web service

Tabla 27: características a usar en el desarrollo

5.4.8. Pruebas Funcionales del Prototipo

Tipo de prueba	Definiciones
Unitarias	**Unitarias:** permite verificar la funcionalidad y estructura de cada componente individualmente del sistema una vez que ha sido codificado.
Sistema	**Sistema:** estas pruebas buscan diferencias entre la solución desarrollada y los requerimientos, con el fin de identificar errores que se puedan generar entre la especificación funcional y el diseño del sistema. **Interfaz de usuario**: ppermite verificar que la navegación a través de los elementos que se están probando, reflejen las funciones del negocio y los requerimientos funcionales. **Integridad de las bases de datos:** consiste en asegurar que los métodos y procesos de acceso a la base de datos funcionan correctamente y sin corromper datos.
Funcionales	**Funcional:** la prueba funcional es un proceso para procurar encontrar discrepancias entre el programa y la especificación funcional.
Aceptación	Es la prueba final basada en las especificaciones del usuario o basada en el uso del programa por el usuario final luego de un periodo de tiempo

Tabla 28: tipos de pruebas: fuente los autores

5.4.9. Casos de Prueba

Las pruebas se hacen para identificar que el prototipo funcional haga en cada función lo que tenga que hacer y que no haya errores ni falencias en el desarrollo.

Casos de Prueba	
Código	Cp001
Nombre	Inicio de sesión
Precondiciones	• Datos en blanco • Usuario sin iniciar sesión • Usuario no registrado
Pasos de la Prueba	**Resultados**
Escoger un nombre de usuario iniciar sesión	Usuario (admin1) no registrado
Registrar ese usuario	Ingresar Usuario (admin1)
Llenar formulario	Diligenciar formulario de usuario
Guardar formulario	Guardado correctamente
Registrar contraseña	Se registra una contraseña de 4 caracteres
Enviar solicitud para autorizar	Solicitud de aceptación en proceso el usuario administrador del sistema valida los datos y da visto bueno
Ingresar con usuario creado	Usuario (admin1) contraseña (****)

Tabla 29: caso de prueba 1 Fuente los autores

Casos de Prueba	
Código	Cp002
Nombre	Administrar contenidos
Precondiciones	• Usuario administrador o líder
Pasos de la Prueba	**Resultados**
Agregar prueba	Prueba agregada satisfactoriamente
Diligenciar datos de la prueba	Llenar formulario de la prueba
Guardar prueba	Guardar datos de la prueba
Diligencias contenido de la prueba	Agregar paso de la prueba Se agrega prueba de existencias de extintores Se agrega prueba de fecha de vencimiento de extintores en
Guardar datos de cada contenido de la prueba	Almacenada correctamente
Agregar evidencia de la prueba	Prueba agregada
Diligenciar formulario de la evidencia	Nombre de la prueba y evidencia
Guardar evidencia	Evidencia guardada

Tabla 30: coso de prueba 2 Fuente los autores

Casos de Prueba	
Código	Cp003
Nombre	Gestionar estructura organizacional
Precondiciones	• Usuario administrador o líder • Crear proyectos
Pasos de la Prueba	**Resultados**
Agregar usuarios	Crear usuarios para varios auditores • UserPrue1 • UserPrue2 • UserPrue3 Validar datos de los auditores
Agregar usuarios a proyecto	Asignar usuarios a un proyecto
Agregar responsabilidades a usuarios	Agregar roles y responsabilidades a cada usuario • UserPrue1 Auditor senior • UserPrue2 Auditor junior • UserPrue3Auxiliar
Eliminar usuarios de proyecto	Eliminar UserPrue2 Auditor junior
Eliminar responsabilidades del proyecto	Eliminar auxiliar del proyecto

Tabla 31: coso de prueba 3 Fuente los autores

Casos de Prueba	
Código	CPNF001
Nombre	Validar usabilidad
Precondiciones	Líder Desarrollador
Pasos de la Prueba	**Resultados**
Se creó un usuario para pruebas de usabilidad	Usuario creado
Se seleccionó un auditor se le enseño como usar el prototipo funcional	
El auditor agrego un proyecto y realizo la gestión de la prueba con sus evidencias	Usuario satisfecho un 90 % Su opinión es que el prototipo es fácil de usar e intuitivo, pero así mismo hay que hacerle mejoras en cuanto al contenido de los estilos

Tabla 32 coso de prueba no funcional 1 Fuente los autores

6. PRODUCTOS POR ENTREGAR

Dentro de este capítulo se describe, los productos a entregar alineados con nuestro objetivo principal y nuestros objetivos específicos de nuestro proyecto a continuación se detallan cada paso de los entregables. Se comenzó con diagnóstico de las metodologías para la gestión de auditoría TI, donde se analizaron las metodologías para gestionar auditoria de TI según el contexto de gestión de riesgos y de controles, siguiendo con la categorización de las aplicaciones para gestionar auditorias de TI para así analizar los puntos a resaltar de cada aplicación, también se realizó un análisis selectivo de la categorización, metodologías de auditoria de TI y un análisis de las entrevistas realizadas para concluir lo que se debe incluir en el prototipo funcional, se diseñó el prototipo funcional en UML así como se desarrolló el prototipo en Java server faces y se realizaron los respectivos cosos de prueba del prototipo para validar su funcionalidad y correcta ejecución de pruebas funcionales.

7. RESULTADOS

Para cumplir los objetivos del este proyecto se realizo el diagnóstico para la elección de las metodologías aplicables y relacionadas para la toma de evidencias de auditoria TI, se evidenció que se tienen metodologías enfocadas a procesos específicos en los cuales se desempeñan muy bien y que se enfocan en la revisión de controles, el resultado que obtuvimos en el diagnostico fueron ISO 27002 y Magerit.

Se realizó la identificación de las características de las aplicaciones utilizadas en la gestión de pruebas de auditoria TI y se encontró que algunas son más eficientes y agiles para reducir tiempos y que una falencia en la principal herramienta analizada es el campo de la toma de evidencias documentales, con esto tomamos lo que se acoplaba a nuestro proyecto para mejorar el proceso de toma de evidencias en las pruebas de cumplimiento de TI. El trabajo se enfocó en las herramientas con mayor puntaje y sacamos de ellas los lineamientos para así alinear el proyecto.

Con el fin de fortalecer el trabajo se realizó una serie de entrevistas a expertos de auditoria de TI, enfocadas en la toma de evidencias para las prueba de cumplimiento y así validar donde se obtuvo que ISO 27001 en compañía de la ISO 27002 son las metodologías más usadas y conocidas, en segundo lugar esta magerit, por lo que los resultados están acordes con el diagnostico hecho de las metodologías

Teniendo en cuenta lo anterior se desarrolló un prototipo funcional enfocado a la toma de evidencias documentales en las pruebas de cumplimiento en las auditorias de TI, obteniendo los resultados esperados, para el avance de la auditoria y para el beneficio de los auditores con la ayuda de la tecnología.

8. CONCLUSIONES

- El trabajo de grado presento una alternativa para gestionar la toma de evidencias en las auditorias de TI para los auditores de sistemas. La implementación de un prototipo funcional que gestiones las evidencias que se toman en las pruebas de cumplimiento en auditorías de, en este sentido, permite que un auditor pueda optimizar el proceso de las pruebas.
- Se logró acoplar una metodología con las características funcionales de una herramienta CAAT, de esta manera se toma ventaja de las características de una herramienta CAAT, permitiendo mejoras al momento de tomar evidencias en la toma de evidencias documentales en las pruebas de cumplimiento.
- El resultado final del trabajo de grado es la creación de un prototipo funcional que genera un informe de hallazgos y recomendaciones según Iso 27002 y Magerit V3.
- En el desarrollo de este proyecto, se detectó que el impacto que podría llegar a tener la implementación del Prototipo funcional para la toma de evidencias documentales en las pruebas de cumplimiento de auditorías de TI es bastante positivo para futuros desarrollos más específicos y se observa que la puesta en marcha de este proyecto es un pequeño paso para mejorar la ejecución de una auditoria de TI.
- Posteriormente de obtener los resultados se pudo concluir que la utilización del prototipo funcional para un proceso especifico en la empresa MacCenter, minimiza el tiempo de ejecución de las pruebas y la recolección de las evidencias análisis en comparación a la herramienta de análisis estático.

- Durante el tiempo que se desarrolló el proyecto se puso en práctica lo aprendido en las diferentes materias de la especialización de auditoria de sistemas de información de la universidad católica de Colombia, como también se vio necesario la consulta de muchas fuentes de conocimiento para la terminación del proyecto.

9. RECOMENDACIONES

El proyecto se enfocó sobre un prototipo funcional en la toma de evidencias en pruebas de auditoria TI, el cual se debe ir mejorando y ser una aplicación con la cual cualquier auditor pueda desempeñar su trabajo sin problemas y obteniendo una trazabilidad en la recolección de pruebas y para agilidad de sus informes, con los cuales contribuyan a las organizaciones en la toma de decisiones y en la mejora continua de sus procesos.

10. TRABAJOS FUTUROS

Se debe tener presente que es un prototipo funcional se debe mejorar en su interface gráfica y su diseño para en un futuro tener un software desarrollado y tener una funcionalidad al 100% tiendo en cuenta que el prototipo se enfatizó en la toma de evidencias, pero para soportar las metodologías se tendrá en cuenta los desarrollos respectivos para incluir la gestión de riesgos y los controles.

Tomar este software como base, porque no ampliar su alcance a otros capítulos de la auditoria como puede ser las auditorias TI basándose en los riesgos de los procesos y así ser un software más integral y de mayor utilidad y ser una herramienta de primera mano para los auditores Ti.

11. ESTRATEGIAS DE COMUNICACIÓN

Este proyecto posterior a su terminación se divulgará mediante diferentes tipos de comunicación para que los interesados ya sean a nivel educativo, profesional o especialistas en el campo de la auditoria lo conozcan. Como estrategia se adoptará en primer lugar la sustentación del proyecto a nivel universitario, en segundo lugar, se continuará con el desarrollo del proyecto para que mediante la participación activa en comunidades y asociaciones para adquirir el reconocimiento para lo que se usaran los siguientes medios:

- Correo electrónico: Es necesario que cada integrante tenga el listado de los correos electrónicos de cada compañero o miembro del equipo de trabajo para pasar información dialogar dudas etc.
- Teléfono celular: cada integrante debe tener en su agenda de teléfonos el número de celular de su equipo de trabajo para poder hacer consultas, dar información y acordar pautas etc.
- Realizar conferencias: para la comunicación con los interesados especial mente el cliente, es necesario la realización de unas entrevistas para recolección de datos.
- Realización de encuestas: es una herramienta para poder definir ciertos criterios dentro del proyecto solo si es necesario.

REFERENCIAS

ACCIS. (2015). *Programas de Especialización o Maestría en Auditoria de Tecnologías de Información y Seguridad Informática* . Obtenido de Programas de Especialización o Maestría en Auditoria de Tecnologías de Información y Seguridad Informática : http://acis.org.co/portal/content/listado-de-programas-de-especializaci%C3%B3n-o-maestr%C3%ADa-en-auditor%C3%ADa-de-tecnolog%C3%ADas-de

Amaya, C. (08 de 01 de 2015). *Welivesecurity*. Obtenido de Welivesecurity: http://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion

Areatecnología. (s.f.). *www.areatecnología.com.* Recuperado el 29 de 04 de 2016, de www.areatecnología.com: http://www.areatecnologia.com/que-es-tecnologia.html

AUDIT. (03 de 06 de 2011). *Técnicas de auditoría asistida por computadora*. Recuperado el 10 de 09 de 2017, de Técnicas de auditoría asistida por computadora: http://carlos-auditoria.blogspot.com.co/2011/06/tecnicas-de-auditoria-asistida-por.html

Auditoria. (12 de 11 de 2014). *Tecnicas de fraude*. Obtenido de Tecnicas de fraude: https://prezi.com/nvtgvcywalxw/tecnicas-de-fraude-informatico/

Auditoria superior. (12 de 09 de 2010). *GUÍA DE LA AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN*. Recuperado el 27 de 07 de 2017, de AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN: http://www.auditoriachihuahua.gob.mx/portal/wp-content/uploads/2013/08/GUIA_DE_AUDITORIA_DE_TI.pdf

auditoría, M. d. (08 de 10 de 2016). *Reporte de transparencia*. Obtenido de Reporte de transparencia: http://www.grantthornton.com.ar/servicios/auditoria/metodologia-de-auditoria/

Australiano, E. (07 de 06 de 2000). *Administración de riesgos*. Obtenido de Administración de riesgos: http://www.edesaesp.com.co/wp-content/uploads/2013/05/ASNZ-4360-de-1999.pdf

Ballestas, P. (27 de 05 de 2016). *Análisis de Riesgos Magerit*. Obtenido de Análisis de Riesgos Magerit: https://prezi.com/ukh_2gzmboss/comparacion-iso-27002-analisis-de-riesgos-magerit-y-octave/

Barroso, J. G. (2012). *MAGERIT – versión 3.0.* madrid: Dirección General de Modernización Administrativa. Obtenido de MAGERIT – versión 3.0.

Camelo, L. (12 de 05 de 2010). *Gestión de Riesgos*. Obtenido de Gestión de Riesgos: http://seguridadinformacioncolombia.blogspot.com.co/2010/05/gestion-de-riesgos.html

CAMPAGNAT. (05 de 25 de 2017). *tecnologia e innovacion*. Obtenido de tecnologia e innovacion: http://www.champagnat.org/000.php?p=36

Cobit. (12 de 06 de 2014). *Guias de auditoria*. Obtenido de Guias de auditoria: https://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2202_gui_Spa_0415.pdf

Computer. (2014). *Tecnicas de aduitoria asistidas por computadora*. Recuperado el 05 de 09 de 2017, de Tecnicas de aduitoria asistidas por computadora: https://es.scribd.com/doc/49852466/TECNICAS-DE-AUDITORIAS-ASISTIDAS-POR-COMPUTADORAS

Consultoría, A. &. (17 de 02 de 2017). *CONOCES QUÉ ES LA AUDITORIA DE TECNOLOGÍAS DE INFORMACIÓN*. Obtenido de CONOCES QUÉ ES LA AUDITORIA DE TECNOLOGÍAS DE INFORMACIÓN: https://www.cynthus.com.mx/blog/auditoria-y-consultoria/auditoria-en-ti/

Corletti, A. (10 de 06 de 2008). *Iso 27002 ventajas y desventajas*. Recuperado el 30 de 08 de 2017, de Iso 27002 ventajas y desventajas: http://www.criptored.upm.es/guiateoria/gt_m292n.htm

Definiciones.es. (12 de 04 de 2015). *Analisis cualitativos*. Obtenido de Analisis cualitativos: https://definicion.de/cualitativo/

Dinero.com. (22 de 06 de 2016). *Bogotá está en auge de crecimiento empresarial*. Obtenido de Bogotá está en auge de crecimiento empresarial: http://www.dinero.com/empresas/articulo/cuantas-empresas-estan-registradas-en-bogota-a-2016/224854

Economista. (01 de 09 de 2017). *MAGERIT DE ASESORAMIENTO SL*. Obtenido de MAGERIT DE ASESORAMIENTO SL: http://ranking-empresas.eleconomista.es/MAGERIT-ASESORAMIENTO.html

El TIEMPO. (23 de 10 de 1995). *DERECHOS DE AUTOR PARA CREADORES DE SOFTWARE*. Recuperado el 01 de 09 de 2017, de DERECHOS DE AUTOR PARA CREADORES DE SOFTWARE: http://www.eltiempo.com/archivo/documento/MAM-431727

España, D. (24 de 02 de 2017). *Definiciones habeas data*. Obtenido de Definiciones habeas data: https://definicion.de/habeas-data/

Gonzalez, H. (28 de 10 de 2016). *GESTION DEL RIESGO – ISO 31000*. Obtenido de GESTION DEL RIESGO – ISO 31000: https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

Historia de la Auditoria. (17 de 03 de 2015). Recuperado el 08 de 07 de 2017, de Historia de la Auditoria: https://chaui201511701024029.wordpress.com/2015/03/17/historia-de-la-auditoria/

Huerta, A. (25 de 06 de 2017). *segurity work*. Obtenido de segurity work: http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

Icintec. (11 de 02 de 2011). *Gestion de riesgo*. Obtenido de Gestion de riesgo: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

infysis. (09 de 11 de 2009). *AUDITORIA DE SISTEMAS*. Recuperado el 15 de 07 de 2017, de AUDITORIA DE SISTEMAS: http://msucreseccion29infysis.blogspot.es/1257696600/auditoria-de-sistemas/

International, i. (16 de 05 de 2015). *Soluciones de auditoria*. Obtenido de Soluciones de auditoria: http://www.iaudit.info/solutions

ISO EN ESPAÑOL. (05 de 09 de 2012). *El portal de ISO 27002*. Recuperado el 29 de 08 de 2017, de El portal de ISO 27002: http://www.iso27000.es/iso27002.html

IsoTools. (27 de 07 de 2016). *Software ISO Riesgos y Seguridad*. Obtenido de Software ISO Riesgos y Seguridad: https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000

itmplatform. (22 de 11 de 2015). *gestión de riesgos*. Obtenido de gestión de riesgos: http://www.itmplatform.com/es/blog/que-es-la-gestion-de-riesgos/

Matriz de Riesgos . (08 de 11 de 2016). Recuperado el 28 de 08 de 2017, de Matriz de Riesgos : http://www.ceolevel.com/como-crear-una-efectiva-matriz-de-riesgos-en-tan-solo-3-pasos

MinTic. (2014 de 03 de 2016). *Seguridad y rpivacidad de la informacion*. Obtenido de Seguridad y rpivacidad de la informacion: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Moyano. (21 de 07 de 2017). *segu-info*. Obtenido de segu-info: http://blog.segu-info.com.ar/2013/04/auditoria_ti.html

Ortiz, A. (15 de 06 de 2015). *Iso 27002*. Recuperado el 05 de 09 de 2017, de Iso 27002: Autenticación o autentificación

PAE. (08 de 07 de 2014). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Recuperado el 15 de 08 de 2017, de MAGERIT v.3: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WbVtBrLyjIV

Protafolio. (25 de 12 de 2016). *El tercer trimestre fue bueno para la creación de empresas en Colombia*. Obtenido de El tercer trimestre fue bueno para la creación de empresas en Colombia: http://www.portafolio.co/negocios/empresas/creacion-de-empresas-en-colombia-crece-este-2016-501270

Quesada, H. (01 de 12 de 2013). *TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT´s)*. Recuperado el 10 de 09 de 2017, de TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT´s): http://hdquezadal.blogspot.com.co/2013/12/tecnicas-de-auditoria-asistidas-por.html

Rodriguez, L. (2011). *AUDITORIA Y SISTEMAS DE INFORMACION*. Recuperado el 20 de 07 de 2017, de AUDITORIA Y SISTEMAS DE INFORMACION: http://systemsofinformation.blogspot.com.co/2008/09/la-auditoria-de-sistemas-de-informacion.html

Rodríguez, S. V. (23 de 08 de 2015). *Diseño de pruebas de auditoria de cumplimiento y sustantivas*. Obtenido de Diseño de pruebas de auditoria de cumplimiento y sustantivas: https://prezi.com/c2qz68_usg6y/diseno-de-pruebas-de-auditoria-de-cumplimiento-y-sustantivas/

Salcedo, M. R. (13 de 10 de 2013). *INFORMÁTICA JURÍDICA- META DOCUMENTAL*. Recuperado el 01 de 09 de 2017, de INFORMÁTICA JURÍDICA- META DOCUMENTAL: http://rebecainformaticajuridica.weebly.com/proteccioacuten-a-datos-personales-y-software.html

Salgado, H. S. (2012). *Introduccion a la Auditoria*. Recuperado el 30 de 08 de 2017, de Introduccion a la Auditoria: http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf

Sama, A. (17 de 06 de 2011). *Seguridad de la informacion y auditoria de sistemas*. Recuperado el 12 de 08 de 2017, de matriz de riesgos: http://12302154.blogspot.com.co/2011/06/matriz-de-riesgos-ii.html

Solarte, F. (2015). *METODOLOGÍA PARA REALIZAR AUDITORÍA*. Recuperado el 08 de 09 de 2017, de METODOLOGÍA PARA REALIZAR AUDITORÍA: http://auditordesistemas.blogspot.com.co/2011/11/metodologia-para-realizar-auditoria.html

Tecnologia, A. (20 de 06 de 2017). *La Tecnologia*. Obtenido de La Tecnologia: http://www.areatecnologia.com/que-es-tecnologia.html

tecnologicas, D. (15 de 08 de 2008). *Ingenieria de Software*. Obtenido de Ingenieria de Software: https://definicion.de/ingenieria-de-software/

Tools, I. (30 de 08 de 2016). *Iso y riesgos*. Obtenido de Iso y riesgos: http://www.isotools.com.co/etapas-del-proceso-gestion-del-riesgo-correspondencia-ntc-iso-31000-meci-saro/

UCatabria. (04 de 08 de 2017). *Metodo hipotetico*. Obtenido de Metodo hipotetico: http://ocw.unican.es/ciencias-de-la-salud/ciencias-psicosociales-i/materiales/bloque-i/tema-

Villa, C. (28 de 02 de 2016). *USO DE HERRAMIENTAS CAAT´S EN LAS REVISIONES DE CONTROL INTERNO IT*. Recuperado el 26 de 08 de 2017, de COORDENADAS BDO: https://www.bdo.es/es-es/blogs/coordenadas/febrero-2016/uso-de-herramientas-caats-por-el-auditor-interno

voigtmann. (25 de 03 de 2016). *Características de un desarrollo de software moderno*. Obtenido de Características de un desarrollo de software moderno: http://www.voigtmann.de/es/desarrollo-de-software/

WinAudit. (04 de 02 de 2015). *WinAudit*. Recuperado el 06 de 06 de 2017, de WinAudit: https://www.maestrodelacomputacion.net/winaudit-software-gratuito-para-auditoria-informatica/

ANEXOS

Anexo A- cronograma

Nombre de tarea	Duración	Comienzo	Fin
INICIO			
Levantamiento de Información	30 días	jue 01/06/17	mié 12/07/17
Definir título	2 días	jue 13/07/17	vie 14/07/17
Definir Pregunta de Investigación	5 días	vie 14/07/17	jue 20/07/17
Definir Objetivos	3 días	mar 18/07/17	jue 20/07/17
Definir justificación	10 días	jue 20/07/17	jue 03/08/17
Definir Alcance	10 días	vie 04/08/17	jue 17/08/17
PLANEACIÓN			
Definir Gestión de Tiempo	6 días	vie 18/08/17	vie 25/08/17
Definir Gestión de Recursos	6 días	mar 22/08/17	mar 29/08/17
Definir Gestión de Costos	6 días	mié 23/08/17	mié 30/08/17
Realizar Estado del Arte	10 días	jue 24/08/17	mié 06/09/17
Definir SRS	10 días	vie 01/09/17	jue 14/09/17
EJECUCIÓN			
Realizar Desarrollo	25 días	lun 13/03/17	vie 14/04/17
Realizar Diseño UML	5 días	vie 15/09/17	jue 21/09/17
Realizar diagnóstico de las metodologías	5 días	mar 19/09/17	lun 25/09/17
Identificar CAATs mas usadas	5 días	vie 22/09/17	jue 28/09/17
Realizar Pruebas Funcionales	5 días	vie 29/09/17	jue 05/10/17
Realizar manuales de la herramienta	2 días	vie 06/10/17	lun 09/10/17
Realizar Validación de la Herramienta por medio de una auditoría	10 días	mar 10/10/17	lun 23/10/17
Seguimiento de proyecto con el tutor			
CIERRE			
Análisis de resultados	2 sem.	mar 24/10/17	lun 06/11/17
Realizar artículo de investigación	1 sem	mar 07/11/17	lun 13/11/17
Sustentación de Proyecto	1 día?	vie 01/12/17	vie 01/12/17
seguimiento de proyecto con el tutor			

Anexo B-Presupuesto

RUBROS	VALOR UNITARIO	VALOR TOTAL
PERSONAL	$ 115.000	$15.785.700
EQUIPOS	$100.000	$100.000
SOFTWARE	$250.000	$250.000
MATERIALES	$200.000	$200.000
SALIDAS DE CAMPO	$0.00	$0.00
MATERIAL BIBLIOGRÁFICO	$120.000	$120.000
PUBLICACIONES Y PATENTES	$0.00	$0.00
SERVICIOS TÉCNICOS	$100.000	$100.000
VIAJES	$0.00	$0.00
CONSTRUCCIONES	$0.00	$0.00
MANTENIMIENTO	$0.00	$0.00
ADMINISTRACIÓN	$15.500	$15.500
TOTAL	**$900.500**	**$$15.785.700**

INVESTIGADOR / EXPERTO/ AUXILIAR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN Horas/semana	VALOR
Gerente Proyecto	Especialista de Seguridad e la Información	Liderar el proyecto	15	$20.000
Líder Funcional	Ingeniero de sistemas	Liderar el equipo funcional	10	$15.000
Líder de Desarrollo	Ingeniero de sistemas Ingeniero de sistemas	Liderar el equipo de desarrollo	10	$15.000
Líder de QA	Ingeniero de sistemas	Liderar el equipo de pruebas	10	$15.000
Líder Auditor	Especialista en Auditoria TI	Liderar el equipo de auditores	10	$16.000
TOTAL				**$81.000**

EQUIPO	JUSTIFICACIÓN	VALOR TOTAL
Analista de gerencia	Apoyo en las labores de gerencia	$7.000
Analista Funcional	Realizar labores Funcionales del Proyecto	$6.500

Analista de Desarrollo	Realizar desarrollos del Proyecto	$6.500
Analista de QA	Realizar la pruebas de los desarrollos	$6.500
Analista de Auditoria	Realizar una auditoría a la Aplicación	$8.000
TOTAL		$34.500

.

EQUIPO	VALOR TOTAL
Computador portátil Equipo Funcional	$22.500
Computador portátil Equipo Desarrollo	$30.000
Computador portátil Equipo QA	$22.500
Computador portátil Equipo Auditoria	$25.000
TOTAL	$100.000

SOFTWARE	JUSTIFICACIÓN	VALOR TOTAL
Host	Espacio para alojar la aplicación	$80.000
Librerías de Interfaz	Librerías para garantizar la usabilidad de la aplicación	$30.000
Microsoft Office	Compra de Project para cronograma	$60.000
Licencias de UML	Compra de Visio para diseño UML	$60.000
Licencias de QA	Software para administrar pruebas	$20.000
Licencias de Software de auditoría	Herramienta de análisis de vulnerabilidades	$0.00
TOTAL		$250.000

LUGAR / NO. DE VIAJES	**JUSTIFICACIÓN**	**PASAJES ($)**	**ESTADÍA ($)**	**TOTAL DÍAS**	**TOTAL**
N/A	N/A	N/A	N/A	N/A	$0.00
TOTAL					$0.00

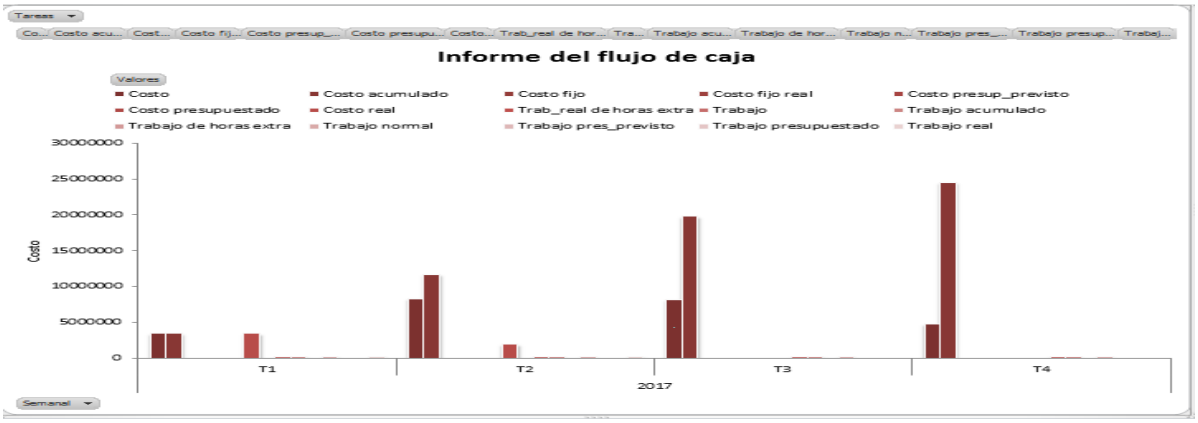
ITEM	COSTO UNITARIO	#	TOTAL
N/A	N/A	N/A	$0.00
TOTAL			$0.00

MATERIALES	JUSTIFICACIÓN	VALOR TOTAL
Acceso a Bases de datos		$40.000
TOTAL		$40.000

ÍTEM	JUSTIFICACIÓN	VALOR TOTAL
Acceso a Internet		$80.000
TOTAL		$80.000

TIPO DE SERVICIOS	JUSTIFICACIÓN	VALOR TOTAL
Servicios públicos		$100.000
Servicios Técnicos		$50.000
Otros		$50.000
TOTAL		$200.000

La siguiente imagen muestra el flujo de caja según el cronograma diseñado y el presupuesto gastado.



Anexo C. Entrevistas a expertos

Entrevista a Expertos 1

Objetivo: Adquirir información de los entrevistados sobre el proceso de la toma de evidencias documentales en las pruebas de auditoria de TI.

Empresa: Mac Center

Cargo o perfil de Auditoria: Gerente de Auditoria

Tiempo de experiencia en auditoria de TI: 15 años

Nivel de escolaridad y/o Certificaciones: certificación de CISA, Itil y especialización en auditoria de TI.

Género: Masculino

Edad: 47 Años

Preguntas

1. **¿Cuéntenos a que se dedica actualmente?**

   Buenas tardes, tengo el cargo de gerente de auditoría de TI hace 5 años en esta empresa, lidero los procesos de auditoria interna asociados a toda la tecnología que se encuentra en la compañía.

2. **¿Qué metodologías para gestionar las auditorias de TI ha utilizado en su experiencia auditando?**

   En mi experiencia como auditor he realizado auditoria en varias empresas, donde me he desempeñado como auditor junior, auditor senior y gerente he usado las normas que dicta isaca (cobit), auditorias bajo la norma ISO 27001 específicamente la ISO 27002 y en una ocasión realice Magerit para establecer la gestión de riesgos.

3. **¿De acuerdo con su experiencia cuéntenos como realiza el proceso de la toma de evidencias en las pruebas de cumplimiento auditorias TI?**

   En la toma de evidencias la he realizado específicamente para auditar los controles y recolecto las evidencias con fotográficas, recolección de documentos físicos y digitales.

4. **¿Le cambiaria algo al proceso de toma de evidencias en las pruebas de cumplimiento ¿Qué y Por qué?**

   Si. Porque cuando en la empresa no tiene presupuesto para herramientas TAACs donde se facilita un poco el realizar los papeles de Trabajo, el proceso es un poco largo y complicado.me gustaría poder reducir el tiempo al tomar las evidencias.

5. **¿Ha interactuado con herramientas automatizadas para la gestión e auditoria de TI? Si su respuesta es afirmativa ¿cuáles?**

   Si. Pero no para la toma de evidencias he manejado ACL e Idea.

Entrevista a Expertos 2

Objetivo: Adquirir información de los entrevistados sobre el proceso de la toma de evidencias documentales en las pruebas de auditoria de TI.

Empresa: Mac Center

Cargo o perfil de Auditoria: auditor senior

Tiempo de experiencia en auditoria de TI: 6 años

Nivel de escolaridad y/o Certificaciones: especialización en auditoria y seguridad informática.

Género: Femenino

Edad: 31 años

Preguntas

1. **¿Cuéntenos a que se dedica actualmente?**
   Soy auditor de Mac center empecé como auditor junior y luego logre un acenso a auditor senior.
2. **¿Qué metodologías para gestionar las auditorias de TI ha utilizado en su experiencia auditando?**
   Mi experiencia ha sido solo en Mac center por lo que solamente he realizado ISO 27001 dentro de la empresa.
3. **¿De acuerdo con su experiencia cuéntenos como realiza el proceso de la toma de evidencias en las pruebas de cumplimiento auditorias TI?**
   En la empresa quienes realizan ese proceso son los auditores junior por protocolo pero la estructuración de las pruebas las hacemos los senior por lo que si he realizado el proceso y lo he supervisado, se toman fotos se recolectan los documentos físicos, archivos en pdf y testimonios de usuarios.
4. **¿Le cambiaria algo al proceso de toma de evidencias en las pruebas de cumplimiento ¿Qué y Por qué?**
   Personalmente creo que no sin embargo sería bueno poder reducir tiempos

5. **¿Ha interactuado con herramientas automatizadas para la gestión e auditoria de TI? Si su respuesta es afirmativa ¿cuáles?**

   Si solamente he interactuado con ACL y en algunas ocasiones herramientas gratuitas como iAuditor para toma de evidencias.

Entrevista a Expertos 3

Objetivo: Adquirir información de los entrevistados sobre el proceso de la toma de evidencias documentales en las pruebas de auditoria de TI.

Empresa: Mac Center

Cargo o perfil de Auditoria: auditor Senior

Tiempo de experiencia en auditoria de TI: 5 Años

Nivel de escolaridad y/o Certificaciones: certificaciones en ISO27001, COBIT, PMP y CISA

Género: Masculino

Edad: 40

Preguntas

1. **¿Cuéntenos a que se dedica actualmente?**

   Soy auditor senior en Mac center por tercerización soy contratado por una empresa temporal y realizo auditoría y consultoría.

2. **¿Qué metodologías para gestionar las auditorias de TI ha utilizado en su experiencia auditando?**

   He trabajado con normas coso, iso 31000 y 27001

3. **¿De acuerdo con su experiencia cuéntenos como realiza el proceso de la toma de evidencias en las pruebas de cumplimiento auditorias TI?**

   He realizado el proceso de las pruebas y sus evidencias enfocándolos como anexo en los papeles de auditoria generando imágenes con marcas de auditoria y documentación necesaria que pruebe que el proceso auditado cumple o no.

4. **¿Le cambiaria algo al proceso de toma de evidencias en las pruebas de cumplimiento ¿Qué y Por qué?**

   Si. Creo que es un proceso demorado nuca lo he ejecutado con herramientas CAATs creo que el uso de una herramienta podría ayudar a gestionar eso más fácilmente, sin embargo no conozco ninguna herramienta que gestione la totalidad de la auditoria

5. **¿Ha interactuado con herramientas automatizadas para la gestión e auditoria de TI? Si su respuesta es afirmativa ¿cuáles?**

   No nunca he realizado auditoria con esas herramientas, pero si conozco IDEA.

Entrevista a Expertos 4

Objetivo: Adquirir información de los entrevistados sobre el proceso de la toma de evidencias documentales en las pruebas de auditoria de TI.

Empresa: Mac Center

Cargo o perfil de Auditoria: auditor Junior

Tiempo de experiencia en auditoria de TI: 5 años

Nivel de escolaridad y/o Certificaciones: ingeniero de sistemas con énfasis en auditoria

Género: Masculino

Edad: 29 Años

Preguntas

1. **¿Cuéntenos a que se dedica actualmente?**
   Soy auditor junior realizo tareas de realización de pruebas y estructuración de los papeles de trabajo.
2. **¿Qué metodologías para gestionar las auditorias de TI ha utilizado en su experiencia auditando?**
   Solamente he usado ISO 27001.
3. **¿De acuerdo con su experiencia cuéntenos como realiza el proceso de la toma de evidencias en las pruebas de cumplimiento auditorias TI?**
   Yo realizo la recolección de evidencias, tomo las evidencias con fotos de los lugares y de cada prueba que necesite evidencias físicas y lógicas.
4. **¿Le cambiaria algo al proceso de toma de evidencias en las pruebas de cumplimiento ¿Qué y Por qué?**
   Si sería bueno poder automatizar el proceso de las evidencias con alguna TAACs
5. **¿Ha interactuado con herramientas automatizadas para la gestión e auditoria de TI? Si su respuesta es afirmativa ¿cuáles?**
   Si, no las he usado para proceso de auditoría, pero si he interactuado con ACL

Entrevista a Expertos 5

Objetivo: Adquirir información de los entrevistados sobre el proceso de la toma de evidencias documentales en las pruebas de auditoria de TI.

Empresa: Mac Center

Cargo o perfil de Auditoria: Asesor de Auditoria

Tiempo de experiencia en auditoria de TI: 6 años

Nivel de escolaridad y/o Certificaciones: especialización en auditoria de sistemas de información

Género: Femenino

Edad: 28

Preguntas

1. **¿Cuéntenos a que se dedica actualmente?**
   Soy asesora de tecnología con el fin de mejorar los procesos dentro del área de tecnología
2. **¿Qué metodologías para gestionar las auditorias de TI ha utilizado en su experiencia auditando?**
   ISO 27001
3. **¿De acuerdo con su experiencia cuéntenos como realiza el proceso de la toma de evidencias en las pruebas de cumplimiento auditorias TI?**
   Recolectaba las evidencias físicas y digitales para realizar las marcas de auditoria e incluirlas en un informe particular de las labores que yo realizaba en la auditoria.
4. **¿Le cambiaria algo al proceso de toma de evidencias en las pruebas de cumplimiento ¿Qué y Por qué?**
   Si creo que es un proceso complicado y tedioso por lo que es demorado y complicado incluiría una herramienta para ayudar a mejorar los tiempos de ejecución.
5. **¿Ha interactuado con herramientas automatizadas para la gestión e auditoria de TI? Si su respuesta es afirmativa ¿cuáles?**
   Si he interactuado con Idea y ACL

Anexo D. Diccionario de Datos

1 auditor

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Auditor	int(11)		No		auto_increment			
Nombres	varchar(45)		No					
Apellidos	varchar(45)		No					
Numero_Tarjeta _Profesional	int(11)		No					
Profesion	int(11)		No			-> profesiones.Id_Profesion ON UPDATE CASCADE ON DELETE NO_ACTION		
Correo	varchar(45)		No					
Telefono	int(11)		No					
Tipo_Auditor	int(11)		No			-> tipo_auditor.Id_Tipo ON UPDATE CASCADE ON DELETE NO_ACTION		
Empresa	int(11)		No			-> empresa.Id_Empresa ON UPDATE CASCADE ON DELETE NO_ACTION		

2 ciudad

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Ciudad	int(11)		No		auto_increment			
Ciudad	varchar(45)		No					

3 contenido

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Contenido	int(11)		No		auto_increment			
Nombre	varchar(50)		No					
Descripcion	varchar(200)		No					
Evidencia	varchar(45)		No					
contenido	int(11)		No			-> creacion_prueba.Id_Creacion ON UPDATE CASCADE ON DELETE NO_ACTION		

4 creacion_prueba

Columna	Tipo	Atributos	Nulo	Predetermina do	Extra	Enlaces a	Comentarios	MIME
Id_Creacion	int(11)		No		auto_increment			
Contenido	varchar(45)		No					
Encabezado	int(11)		No			-> encabezado_prueba.Id_Prueb a ON UPDATE CASCADE ON DELETE NO_ACTION		

5 empresa

Columna	Tipo	Atributos	Nulo	Predetermina do	Extra	Enlaces a	Comentarios	MIME
Id_Empresa	int(11)		No		auto_increment			
Registro_Tributario	varchar(45)		No					
Documento_Empresa	varchar(45)		No					
Nombre_Empre sa	varchar(45)		No					
Pais	int(11)		No			-> pais.Id_Pais ON UPDATE CASCADE ON DELETE NO_ACTION		
Ciudad	int(11)		No			-> ciudad.Id_Ciudad ON UPDATE CASCADE ON DELETENO_ACTION		
Direccion	varchar(45)		No					
Telefono	int(11)		No					
Correo	varchar(45)		No					
Usuario	int(11)		No			-> usuario.Id_Usuario ON UPDATE CASCADE ON DELETE CASCADE		

6
encabezado_prueba

Columna	Tipo	Atributos	Nulo	Predetermina lo	Extra	Enlaces a	Comentarios	MIME
Id_Prueba	int(11)		No		auto_increment			
Nombre_Prueba	varchar(45)		No					
Fecha_Prueba	date		No					
proceso	int(11)		No			-> procesos.id_Proceso ON UPDATE CASCADE ON DELETE NO_ACTION		
Objetivo_Prueb a	varchar(200)		No					
Normativa	varchar(200)		No					
Proyecto	int(11)		No			-> proyecto.Id_Proyecto ON UPDATE CASCADE ON DELETE NO_ACTION		

7 pais

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Pais	int(11)		No		auto_increment			
Pais	varchar(45)		No					

8 procesos

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
id_Proceso	int(11)		No		auto_increment			
Nombre	varchar(50)		No					

9 profesiones

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Profesion	int(11)		No		auto_increment			
Nombre	varchar(45)		No					

10 proyecto

Columna	Tipo	Atributos	Nulo	Predeterminado	Extra	Enlaces a	Comentarios	MIME
Id_Proyecto	int(11)		No		auto_increment			
Nombre	varchar(45)		No					
Auditor	int(11)		No			-> auditor.Id_Auditor ON UPDATE CASCADE ON DELETENO_ACTION		
Fecha_Inicio	date		No					
Fecha_Fin	date		No					

11 reportes

Columna	Tipo	Atributos	Nulo	Predeterminado	Extra	Enlaces a	Comentarios	MIME
Id_Reporte	int(11)		No		auto_increment	-> tipo_reporte.Id_Tipo_Reporte ON UPDATE NO_ACTION ON DELETE NO_ACTION		
Nombre_Report e	varchar(45)		No					
Tipo_reporte	int(11)		No					

12 rol

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Rol	int(11)		No		auto_increment			
Nombre	varchar(45)		No					

13 tipo_auditor

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Tipo	int(11)		No		auto_increment			
Nombre	varchar(45)		No					

14 tipo_reporte

Columna	Tipo	Atributos	Nulo	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Tipo_Reporte	int(11)		No		auto_increment			
Tipo	varchar(45)		No					

15 usuario

Columna	Tipo	Atributos	Null	Predetermina	Extra	Enlaces a	Comentarios	MIME
Id_Usuario	int(11)		No		auto_increment			
Nombres	varchar(45)		No					
Apellidos	varchar(45)		No					
Telefono	int(11)		No					
Correo	varchar(45)		No					
Usuario	varchar(50)		No					
Password	varchar(45)		No					
Id_Rol	int(11)		No			-> rol.Id_Rol ON UPDATE CASCADE ON DELETE NO_ACTION		