SINF-27: SOFTWARE DE APOYO PARA AUDITORÍA A LA SEGURIDAD INFORMATICA Y DE LA INFORMACION BASADO EN LA NORMA ISO 27001 E ISO 27002.

JAMES FERNANDO CAIVIO NASNER
DARIO ALEJANDRO MERA ARAUJO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO NARIÑO
2016

SINF27 – SOFTWARE DE APOYO A LA SEGURIDAD INFORMATICA Y DE LA INFORMACION BASADO EN LA NORMA ISO 27001 E ISO 27002

JAMES FERNANDO CAIVIO NASNER
DARIO ALEJANDRO MERA ARAUJO

Trabajo de grado presentado como requisito parcial para optar al título de ingeniero de Sistemas

Director:
FRANCISCO NICOLAS SOLARTE SOLARTE
Ingeniero de Sistemas Especialista
Profesor Universidad de Nariño

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO NARIÑO
2016

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010, emanado del Honorable Consejo Académico.

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

San Juan de Pasto, 5 de Abril de 2016.

DEDICATORIA

A mi familia, mi apoyo, mi ejemplo, mi soporte y quienes me han dado la fuerza y toda la ayuda que han podido en todos los momentos, especialmente para mis padres Roberto Mera y Yenit Araujo, mi abuela Margarita Mora y mi tía Pastora Rosero quienes me han dado la bendición de tener tres madres, haciéndome uno de los seres más afortunados del mundo.

A mi hermano Camilo Mera y a mis primos Juan Andrés, Jared y Natalia quienes me han recordado que la familia es lo más importante y me inspiran a ser cada día mejor persona para poder enseñarles algo de la mejor manera que se puede, con el ejemplo, y de igual manera me han permitido crecer junto a ellos desde siempre y aprender de sus grandes cualidades

A todos mis tíos y tías, les dedico este paso con inmensa esperanza de que nuestra familia sea como siempre igual de unida y nos alegremos todos de los logros de los demás miembros y suframos con los problemas ajenos y apoyemos a quienes lo necesitan como siempre lo hemos hecho.

A la memoria de mi abuelo Alfredo Araujo, un excelente ser humano y profesor quien extendía su vida de docente a su quehacer diario, quien amaba enseñar cualquier cosa y hacer a todos quienes estuvimos a su alrededor y bajo su protección mejores personas con el solo hecho de estar a su lado, quien me enseñó tantas cosas desde a hacer un dibujo, manejar bicicleta o tocar guitarra hasta a ser un ser humano digno, honesto y trabajador.

A mis buenos amigos que me acompañaron en el camino universitario quienes al estar lejos de mi familia se convirtieron en mis hermanos, compañeros de anécdotas, estudios, aventuras y culpables de hacer de la vida más llevadera y amable, son tantas y tan buenas personas las que me he encontrado en el recorrer de la carrera pero principalmente a Carlos Muñoz, William Cuatin, Andrés Benavides, Johana Lagos y Luisa Ramírez.

A todos mis profesores, les dedico este grado por su dedicación exigencia, disciplina y ejemplo que despertaron en mí, sentimientos de admiración y deseos de no defraudar sus esfuerzos y convertirme en un gran profesional.

A mi compañero y amigo James Caivio con quien tuve el honor de trabajar y desarrollar este trabajo.

Dario Alejandro Mera Araujo

DEDICATORIA

A mi madre Lucia Nasner, por todo su cariño y amor, demostrado a través de sus preocupaciones y su ejemplo de una mujer verraca y luchadora.

A mi padre Carlos Caivio, por siempre estar ahí preocuparse por el bienestar de toda la familia.

A mi abuela, Dolores Caipe, por ser mi segunda madre, y brindarme ese cariño incondicional, a quien le debo la mitad de lo que hoy en día soy.

A mis Hermanas Carolina y Sindy Caivio, y mi hermano Carlos, por ser tres seres realmente especiales en mi vida, que siempre quieren lo mejor para mí.

A mis tios Efren y Brayan Nasner, y tias Betti y Consuelo Nasner por estar presentes en gran parte de mi carrera, brindándome su apoyo incondicional y llenando de alegría mi vida.

A los amigos que llegaron en esta etapa de mi vida, Christian Ordoñez, Juan Carlos Narváez, Yamid Pantoja, y en especial a mi compañero de proyecto de grado Dario Mera. Por su buena compañía.

A todos los profesores del programa de Ingeniería de Sistemas que tuve la oportunidad de conocer, por medio de su enseñanza.

A toda mi familia y personas en general, que demostraron sus buenos deseos de que saliera adelante.

James Caivio

AGRADECIMIENTOS

Los autores expresan agradecimientos a:
A nuestros padres, hermanos, tíos, primos y todos los familiares quienes nos han acompañado, guiado y se enorgullecen de cada pequeño logro, es un honor decirles que este es de todos ellos, y que cada cosa que han hecho por nosotros han forjado el camino que nos ha llevado a estudiar, progresar y alcanzar esta meta.

Al ingeniero Francisco Nicolás Solarte por su compromiso entrega y labor constante de enseñanza, guía y asesoría, y sobre todo a su buena disposición y amabilidad en cada momento del desarrollo de este proyecto.

Al Ingeniero Nelson Jaramillo Decano de la Facultad de Ingeniería y al Ingeniero Manuel Bolaños Director del Departamento de Sistemas, por su dedicación y colaboración para culminar este proyecto.

Cabe dar un agradecimiento especial y denotar al ingeniero Manuel Bolaños quien fue la primera persona en recomendarnos y guiarnos en este proyecto por primera vez.

A los ingenieros Delio Gómez y Javier Villalba, por colaborarnos en la elaboración de los requisitos funcionales del software con su experiencia en el área y por tener la amabilidad de transmitirla y compartirla.

Al señor Guerlin Alfredo Araujo, gerente y propietario de la empresa Araujo y asociados, en donde realizamos algunas pruebas para el sistema.

A todos los amigos, compañeros, profesores y otras personas que nos acompañaron en el camino universitario quienes con su trabajo, compañía, amistad y apoyo fueron la familia que nos rodeó en estos más de 5 años y a quienes siempre recordaremos con especial aprecio y cariño.

RESUMEN

El área de auditoría es primordial en todas las empresas, instituciones, cooperativas, etc. Por lo cual se han formulado normas globales para dicha acción, entre las cuales están la norma ISO 27001 e ISO 27002 en ellas su eje central es la seguridad de sistemas informáticos y de información.

Para realizar una buena auditoría se debe conocer muy bien las normas en toda su extensión, para así poder obtener los mejores resultados posibles. Pero ya qué estos textos son muy extensos y con muchos sub temas dentro de otros mayores existe la necesidad de desarrollar un sistema software que facilite en gran medida este laborioso trabajo reduciendo el tiempo y los esfuerzos. Para aprovecharlos mejor en el análisis de los resultados para presentar un buen informe de tal auditoría.

Este trabajo de grado presenta el desarrollo de un software de apoyo al área de auditoría. Para el manejo de las normas ISO 27001 e ISO 27002.

ABSTRACT

Audit area is central to all enterprises, institutions, cooperatives, etc. Therefore global standards have been formulated for such action, among which are the ISO 27001 and ISO 27002 in which its central axis is the security of computer systems and information.

To make a good audit should be very familiar with the rules from top to bottom, in order to obtain the best possible results. But since these texts are very large and with many sub themes within larger ones we feel the need to develop a software system that facilitates us greatly this laborious work by reducing the time and effort. To make better use in the analysis of the results to present a good report of such audit.

This degree work presents the development of software to support the audit area. For the management of the ISO 27001 and ISO 27002 standards.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Anexo 1: Carpeta Software

- Sinf27.rar

Anexo 2: Carpeta Bases de datos

- Bases.bagkup
- Vacia.backup
- Araujoasociados.Backup

Anexo 3: Carpeta Reportes Araujo y Asociados

- ReporteAuditotia.pdf
- ReporteActivos.pdf
- ReporteControles.pdf
- ReporteCuestionarios.pdf
- ReporteMatrizRiesgo.pdf
- ReporteDalvaguardas.pdf

Anexo 4: Rut Organización Araujo Y asociados

Anexo 5: Video Tutorial Instalación base de datos y software

Anexo 6: Manual de usuario

GLOSARIO

Amenaza: según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgo: según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativos: consiste en evaluar cuál es el impacto y la probabilidad de ocurrencia de cada uno de los riesgos identificados.

Análisis de riesgos cuantitativos: análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Auditor: persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad de una organización.

Autenticación: proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Backup: acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales.

Bases de datos: colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella.

Centro de informática: Ci, Es un área de trabajo cuya función es la de concentrar, almacenar y procesar datos y funciones operativas de una entidad de manera sistematizada.

Contraseña: se refiere al conjunto de caracteres que le permiten el acceso a un usuario a utilizar cierta proporción de un sistema o a una red.

Cliente: persona o personas encargadas de describir las historias de usuario, es decir, lo que necesita que el aplicativo software haga.

Datos: término general para la información procesada por un ordenador.

Hardware: conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, mouse, unidades de disco y monitor.

Infraestructura: la tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

Interfaz: es el diseño de pantallas. Zona de comunicación, en la que se realiza la interacción entre el usuario y el programa.

Inventario de activos: lista de todos aquellos recursos (físicos de información, software, documentos, servicios, personas, etc.), que tengan un valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en él; ámbito de la seguridad de la Información.

ISO: (international organization for standarization), Organización Internacional para la Normalización, creadora de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

Mantenimiento correctivo: medida de tipo reactivo orientada a eliminar la causa de una no-conformidad, con el fin de prevenir su repetición.

Mantenimiento preventivo: medida de tipo pro-activo orientada a prevenir potenciales de una no-conformidad.

Módulos: hace referencia a cada uno de las grandes divisiones de un programa de aplicación.

Reportes: documento impreso o digital de una acción realizada por una persona o máquina.

Objetivo: declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Política de seguridad: Intención y dirección general expresada formalmente por la dirección, Documentos que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de seguridad de información.

Proceso: conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Riesgo: según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Servidor: ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin.

Sistema: conjunto estructurado de elementos (objetos) que interactúan ordenadamente para lograr un fin común.

Sistema de Información: conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: componentes inmateriales del ordenador: programas, sistemas operativos, etc.

TI: tecnologías de información.

Usuarios: personas que hacen uso de los recursos de cómputo que les son suministrados por el Centro de Informática.

Vulnerabilidad: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

INTRODUCCIÓN

Existen normas elaboradas por la ISO y la IEC como son la ISO 27001 y la ISO 27002 en las cuales se encuentran los procesos y tópicos a verificar o evaluar, contienen controles, objetivos, riesgos y criterios de aceptación, y todos los conceptos y bases fundamentales para realizar una buena auditoría a la seguridad de sistemas informáticos y de información.

Es el objetivo primordial de este trabajo elaborar un soporte de tipo software para esta teoría, y para apoyar los procesos de auditoría, en especial la seguridad, es decir una clasificación y organización de los temas y subtemas de las normas para que la realización de las verificaciones y de las pruebas de validación de la auditoría y la organización, cálculo y análisis de la gestión de riesgos se realicen de manera general a cualquier sistema de información de una forma fácil, simple y muy estructurada, con reportes claros y fácilmente documentables.

El programa realizara procesamiento de información a través de formularios de entrada, siendo el primero el que reciba la información de la auditoría tal, como encargado, director, colaboradores, nombre de la empresa auditada, responsables de cada área, nombre del grupo auditor y de más opciones necesarias, luego se brindara otro formulario en el cual se registran todos los activos y sus características clasificándolos principalmente por el tipo de activo del catálogo presente en Magerit, lo que permitirá establecer su valor para la empresa y saber que amenazas lo afectan.

Después de estos registros se inicia el proceso de verificación, luego de los respectivos log in, y verificaciones de usuario, el primer menú muestra el listado de los dominios de la norma ISO 27001 de los cuales el auditor deberá escoger los que va a verificar, hecho esto aparece un listado con los subjetivos y el proceso se repite hasta encontrar los cuestionarios correspondientes a áreas específicas de la auditoría, denominadas en la norma ISO 27001 como objetivos de control, el auditor deberá verificar y responder las preguntas, para lo cual el software sugiere herramientas para algunos cuestionarios, y el programa automáticamente procesara esta información resultando en una relación con las amenazas que se activen por cada objetivo de control que de un resultado negativo en la verificación, una vez se tengan las amenazas, estas se relacionaran con los activos a quienes afectan y se mostrará la matriz de probabilidad e impacto de la auditoría, también el programa mostrará más informes estadísticos como cumplimiento de la auditoría general, por objetivos de control, hallazgos en preguntas clave, y listado de posibles controles aplicables según Magerit o ISO 27002 según escoja el auditor, quien de este listado podrá escoger la mejor opción.

Este trabajo se realiza para satisfacer la necesidad de una estructura clara que sirva de guión y de soporte para la gestión de la información recolectada en los inicios de una auditoría, el sistema contendrá una base de datos contenedora de dominios y procesos, de los cuales de cada uno se clasificaran y organizaran las pruebas, verificaciones y herramientas necesarias para llevar a cabo la auditoría general empezando por las unidades más pequeñas como lo son los procesos hasta llegar a una integración completa de todos los dominios y producir una documentación clara de los hallazgos y las recomendaciones.

IDENTIFICACION DEL PROBLEMA

Título del proyecto

SINF-27: SOFTWARE DE APOYO PARA AUDITORÍA A LA SEGURIDAD INFORMATICA Y DE LA INFORMACION BASADO EN LA NORMA ISO 27001 E ISO 27002.

Tema

Desarrollo de software de apoyo a auditoría a la seguridad informática y de la información estructurando en un aplicativo la esencia y organización de la norma ISO 27001 e ISO 27002, para generar reportes de probabilidad e impacto de amenazas, usando metodología de gestión de riesgos Magerit.

Área de investigación

Este trabajo corresponde al área de auditoría a sistemas informáticos y de información, aplicando conocimientos de programación, diseño de software y bases de datos, para lograr un producto investigativo que proponga una solución viable de tipo software.

Línea de investigación

Gestión de seguridad y control: esta línea tiene como objetivo, planificar, analizar, diseñar, implantar sistemas de control de información, con el propósito de brindar soporte a auditorías y sistemas de control y verificación.

DEFINICION DEL PROBLEMA

Planteamiento del problema

Es de gran complejidad y dificultad realizar procesos de auditoría en especial en la seguridad informática sin contar con herramientas CAATS. Los problemas que esto ocasiona y sus efectos en el tiempo y elaboración de instrumentos se dan por falta de estructuración, organización, planeación y automatización.

En la actualidad se carece de un sistema integral que permita realizar un proceso de auditoría a la seguridad de la información y que al tiempo sugiera y clasifique las herramientas de software que se usan para verificar los aspectos que se prueban, sobre los sistemas informáticos que deben ser evaluados.

El problema en este ámbito es la necesidad de gastar una cantidad de esfuerzos y recursos para la realización de auditorías, de precisar contratar personal para la sola interpretación de las normas y bases teóricas y más esfuerzos aun en la puesta en marcha de la auditoría, y la elaboración de reportes

El problema de la realización de estas auditorías radica en la complejidad y poca estructuración del proceso que abarca conocer, aprender y aplicar la norma de seguridad ISO/IEC 27001 y sus normas anexas, aplicar un software para realizar el proceso de análisis y evaluación de riesgos o hacerlo manualmente o con el uso de una herramienta de software, verificar la lista de controles existentes aplicando la norma ISO/IEC 27002, realizar las pruebas definidas y diseñadas para la auditoría con el uso de otras herramientas específicas de software, y finalmente proponer controles de manera manual y de acuerdo a los hallazgos que han sido encontrados, entre otras tareas.

Como es un proceso extenso, se requiere de una herramienta de software que permita gestionar la auditoría de manera integral, de tal manera que pueda realizar el proceso de análisis y evaluación de riesgos, las pruebas y usar las normas sin tener que salir del mismo.

Formulación del problema

¿Cómo facilitar el proceso de auditoría a la seguridad informática e información alineado con las normas ISO/IEC 27001 E ISO/IEC 27002 de manera integral través del desarrollo una herramienta software?

Sistematización del problema

- ¿Cómo conocer y entender los fundamentos teóricos de la norma ISO 27001 e ISO 27002 aplicables en la auditoría a la seguridad informática y de la información para poder aplicarlos?

- ¿Cómo diseñar e implementar la estructura del nuevo sistema para que sea de fácil manejo para los usuarios auditores en un lenguaje orientado a objetos apropiado?

- ¿Cómo hacer el diseño e implementación del sistema para que satisfaga las necesidades de los auditores y el cumplimiento de las etapas de la auditoría?

- ¿Cómo integrar y generar los reportes de manera simple y fácil de entender para los auditores?

- ¿Cómo poner a prueba el software integral aplicándolo a un caso específico para realizar los ajustes necesarios?

- ¿Cómo difundir los resultados de la aplicación del software para hacer conocer la herramienta y que pueda ser usada por los auditores?

OBJETIVOS

Objetivo general

Facilitar el proceso de auditoría a la seguridad informática basado en ISO 27001 y 27002 mediante el desarrollo de un software que satisfaga las necesidades de los usuarios auditores.

Objetivos específicos

- Identificar la estructura de la norma ISO 27001 e ISO 27002, objetivos y sus procesos, que permitan tener en claro las bases teóricas que soportan a esta área de la auditoría.

- Definir una arquitectura del software basada en un lenguaje orientado a objetos, clasificando las clases más importantes del sistema como dominios, procesos, riesgos, criterios de aceptación, pruebas entre otras para tener clara la clasificación de tareas y de áreas de trabajo.

- Modelar espacios de verificación para los procesos y dominios de las normas basados en pruebas, uso de diferentes aplicaciones, listas de verificación y otras herramientas de evaluación encaminados hacia satisfacer las necesidades de los auditores y cumplir las etapas de auditoría.

- Modelar e implementar un sistema de reportes unificado e integral que contenga todas las salidas de las diferentes aplicaciones usadas.

- Evaluar el software desarrollado en un sistema de información real, en una organización o empresa, a través de pruebas en los campos de verificación y cuestionarios que ofrece el programa con información real de este sistema de información, para poder verificar las salidas y reportes que el software ofrece.

- Implementar la documentación del proceso de elaboración del software y las salidas y los reportes del software para proceder a hacer un análisis, clasificación, conclusiones y recomendaciones para el sistema de información

auditado y para que estos documentos sirvan de guía y herramienta de difusión del software para usos futuros.

JUSTIFICACIÓN

La información es uno de los activos más importantes de una organización y su seguridad es un asunto de vital impacto en la misma, dicha seguridad se encuentra teóricamente especificada y estructurada dentro de diversas normas y sería muy útil incluir dicha estructuración teórica en un sistema practico que haga más fácil todo el proceso desde la apropiación de las normas hasta la aplicación y verificación de los procesos es por eso que la herramienta que se pretende desarrollar encamina sus aportes hacia la realización de un proceso de auditoría a la seguridad informática y de la información basándose en las normas existentes para tal fin.

El sistema software hará aportes en la estructuración de la auditoría, ya que contendrá las acciones a realizar ante cualquier área que se quiera evaluar, las pruebas, los riesgos criterios de aceptación y en general cualquier toma de decisiones relevantes dentro del proceso estará acotada y comprendida y la planeación de la auditoría estará hecha ya que el software desagregara funcionalidades de manera cronológica acorde a las actividades que deberían hacerse en una auditoría, dándole al usuario el orden lógico y temporal para la información que debe ingresar y generara a su vez los reportes en orden.

La herramienta es importante porque integrara no solo las etapas de la auditoría sino también enlazara las herramientas software necesarias para la auditoría a la seguridad informática y de la información, útil para llevar a cabo pruebas y testeos en áreas específicas dentro de la auditoría.

En el desarrollo y puesta en marcha del sistema se usaran aplicaciones existentes pero que están aisladas, lo que presenta dificultad en el análisis general de resultados y posibles errores a causa de la no integración y consolidación de hallazgos, el sistema será de gran importancia ya que unificara estas herramientas.

En el ámbito económico será muy útil e importante para la universidad ya que se llevara a cabo una prueba del software en un sistema de información en uso y se entregaran los hallazgos y recomendaciones correspondientes para mejora en el sistema.

Con el desarrollo de este trabajo se beneficiaran:

- Los usuarios del software que en este caso serán los auditores ya que van a tener a su disposición las listas de chequeo, cuestionarios estructura y orientación de la auditoría.

- Se beneficiaran también directivos de una organización que no sean auditores pero que quieran llevar a cabo una auditoría interna, que la podrán hacer teniendo el software, para mejorar la seguridad dentro de la organización.

- La Universidad de Nariño ya que será quien tenga los derechos del mismo por ser desarrollado como proyecto de graduación, también se beneficiaran los desarrolladores ya que esto permitirá la obtención del título y se beneficiara la comunidad estudiantil, en general ya que este trabajo servirá como base de investigación y consulta para el crecimiento académico en el área de soporte a auditoría de seguridad informática y de información.

1. MARCO TEORICO

1.1 ANTECEDENTES

Existen muchas especialidades de auditoría en la actualidad, están de igual manera relacionadas al gran número de tipos de auditorías muchas normas, incluso más de una en algunos casos para un tipo específico de auditoría, es en ese orden de ideas una fundamentación teórica y estructura guía para la auditoría a sistemas informáticos y de la información, la norma ISO 27001 e ISO 27002. En este tipo de auditoría se debe evaluar cada aspecto, de los sistemas de procesamiento de información, y los procesos y tareas más pequeñas relacionados con estos aspectos.

El proceso natural y tradicional de realización de una auditoría es bastante complejo y necesita de conocimientos en diversas áreas como planeación y gestión de proyectos, elaboración y puesta en marcha de instrumentos de recolección de información, gestión de riesgos, análisis de resultados y elaboración de informes entre otros, además de un conocimiento y manejo de la estructura de la norma de auditoría que se esté siguiendo. Para responder a este reto y acorde a los rápidos avances que tienen en este tiempo todas las áreas del conocimiento se hace necesario también cambiar la forma en que se realizan las auditorías, por ejemplo con la ayuda de un software que estructure y guie todo el proceso basándose siempre en tres fundamentos teóricos: ISO 27002, ISO 27002 y Magerit.

Los siguientes trabajos a diferentes niveles, regional, nacional e internacional se toman como base para el desarrollo de este trabajo.

1.1.1 Regionales. El proyecto “DIAGNÓSTICO DEL ESTADO DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), CON LA APLICACIÓN DE UN SOFTWARE, EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DE SAN JUAN DE PASTO”, presentado por los estudiantes JOSE DANIEL GUERRA ERASO y RAFAEL LLERENA RIASCOS, en la INSTITUCIÓN UNIVERSITARIA CESMAG de la ciudad de SAN JUAN DE PASTO en el año 2009 donde ellos crearon una herramienta de software que permite determinar el estado de madurez en que esta una organización, mediante la aplicación de listas de chequeo en cada uno de los dominios.

De este trabajo es de gran utilidad la forma como se hacen los diagnósticos de sistemas de información con la aplicación de un software, permite un análisis de la forma en que se evalúa la información por dominios y un entendimiento de la

importancia y utilidad de la aplicación de listas de chequeo organizadas en cuestionarios que verifican o validan un tema común, esta herramienta daba como salidas el estado de madures de los sistemas de gestión de la seguridad de la información en una organización mientras que la herramienta que se pretende desarrollar desemboca en reportes del estado de riesgo que tiene la organización en cuanto a la seguridad de su información, es por esto que brinda una base y punto de partida de los criterios de aceptación o diagnóstico de la seguridad de la información.

1.1.2 Nacionales. FUNDAMENTOS DE ISO 27001 y su aplicación a empresas articulo elaborado por: MARTHA ISASBEL LADINO A; PAULA ANDREA VILLAS; ANA MARIA LOPEZ. SCIENTIA ET TECHNICA 2011. UNIVERSIDAD TECNOLÓGICA DE PEREIRA COLOMBIA. Que busca describir los fundamentos de la norma ISO 27001 y su aplicación en organizaciones. Adicionalmente, indica cómo implementar estas buenas prácticas en pequeñas empresas que no pueden realizar su certificación.[1]

De este artículo es de gran utilidad el resumen de los fundamentos de ISO 27001 y la forma práctica como son aplicados a las empresas, esto servirá para una mejor apropiación y entendimiento de la estructura de la norma y su implementación en pequeñas empresas.

1.1.3 Internacionales. SISTEMA DE GESTIÓN INTEGRADO SEGÚN LAS NORMAS ISO 9001, ISO/IEC 20000 E ISO/IEC 27001. articulo elaborado por ANTONI LLUIS MESQUIDA, ANTONIA MAS, ESPERANCA AMENGUAL, IGNACIO CABESTRERO DEPARTAMENTO DE MATEMATICAS E INFORMATICA, UNIVERSIDAD DE LAS ISLAS BALEARES, ESPAÑA 2010. Que realizan un análisis de la situación actual de los estándares de sistemas de gestión más comúnmente demandados por las organizaciones TI para identificar los elementos comunes entre estas normas para crear un nuevo sistema de gestión integrado. [2].

De este sistema se toma la integración de diferentes bases teóricas y la forma como toma elementos comunes y los pone en práctica en un solo sistema, se observa entendimiento de metodologías de trabajo que incluyen diferentes marcos teóricos para diferentes aplicaciones como por ejemplo estructurar una auditoría y gestionar sus riesgos.

LA NORMA ISO 27001. SEGURIDAD DE LA INFORMACION. GARANTIA DE LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACION. Elaborado por Carlos Manuel Fernández Sánchez. Calidad: Revista de la Asociación Española para la Calidad: La norma UNE ISO/IEC 27001:2007 del "Sistema de Gestión de la Seguridad de la Información" permite

evaluar los riesgos físicos y lógicos, y establecer las estrategias y controles adecuados que aseguren la protección de la información. [3]

Aporta fundamentos teóricos que garantizan que la aplicación de la norma ISO 27001 da las luces de como evaluar los riesgos físicos y lógicos, y establecer las estrategias y controles adecuados que aseguren la protección de la información.

1.2 NORMAS Y DOCUMENTOS USADOS

1.2.1 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.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. [4]

1.2.1.1 Alcance. Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). También se especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.[5]

1.2.1.2 Sistema de gestión de seguridad de la información

- **Requerimientos generales**

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan.

- **Establecer y manejar el SGSI**

- **Establecer el SGSI**

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.
b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología.
c) Definir el enfoque de valuación del riesgo de la organización
d) Identificar los riesgos.
e) Analizar y evaluar el riesgo.
f) Identificar y evaluar las opciones para el tratamiento de los riesgos.
g) Seleccionar objetivos de control y controles para el tratamiento de riesgos. Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos
h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.
i) Obtener la autorización de la gerencia para implementar y operar el SGSI.
j) Preparar un Enunciado de aplicabilidad.

- **Implementar y operar el S.G.S.I**

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.
c) Implementar los controles seleccionados para satisfacer los objetivos de control.
d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones
e) para evaluar la efectividad del control para producir resultados comparables y reproducibles.

NOTA: La medición de la efectividad de los controles permite a los gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

f) Implementar los programas de capacitación y conocimiento.
g) Manejar las operaciones del SGSI.
h) Manejar recursos para el SGSI.
i) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de errores y respuesta a incidentes de seguridad.

- **Monitorear y revisar el SGSI**

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de revisión, monitoreo y otros controles.
b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.
c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios.
e) Realizar auditorías SGSI internas a intervalos planeados.

NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.
g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

- **Mantener y mejorar el SGSI**

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.
b) Tomar las acciones correctivas y preventivas apropiadas. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.
c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea

relevante, acordar cómo proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

- **Mejoramiento del SGSI**
- **Mejoramiento continuo**

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoría, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

- **Acción correctiva**

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

- identificar las no-conformidades;
- determinar las causas de las no-conformidades;
- evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
- determinar e implementar la acción correctiva necesaria;
- registrar los resultados de la acción tomada; y
- revisar la acción correctiva tomada.

- **Acción preventiva**

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

- identificar las no-conformidades potenciales y sus causas;
- evaluar la necesidad para la acción para evitar la ocurrencia de no conformidades;
- determinar e implementar la acción preventiva necesaria;
- registrar los resultados de la acción tomada; y
- revisar la acción preventiva tomada.

NOTA**:** La acción para evitar las no-conformidades con frecuencia es una acción más efectiva en costo que la acción correctiva.

La organización debe identificar los riesgos cambiados e identificar los

requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo. [4]

1.2.1.3 Dominios y subdominios

- **A.5 Políticas de seguridad**
  A.5.1 Política de seguridad de información
- **A.6 Organización de la seguridad de la información**
  A.6.1 Organización interna
  A.6.2 Entidades externas
- **A.7 Gestión de activos**
  A.7.1 Responsabilidad por los activos
  A.7.2 Clasificación de la información
- **A.8 Seguridad de los recursos humanos**
  A.8.1 Antes del empleo
  A.8.2 Durante el empleo
  A.8.3 Terminación o cambio de empleo
- **A.9 Seguridad física y ambiental**
  A.9.1 Áreas seguras
  A.9.2 Seguridad del equipo
- **A.10 Gestión de las comunicaciones y operaciones**
  A.10.1 Procedimientos y responsabilidades operacionales
  A.10.2 Gestión de la entrega del servicio de terceros
  A.10.3 Planeación y aceptación del sistema
  A.10.4 Protección contra software malicioso y código móvil
  A.10.5 Respaldo (back-up)
  A.10.6 Gestión de seguridad de redes
  A.10.7 Gestión de medios
  A.10.8 Intercambio de información
  A.10.9 Servicios de comercio electrónico
  A.10.10 Monitoreo
- **A.11 Control de acceso**
  A.11.1 Requerimiento comercial para el control del acceso
  A.11.2 Gestión del acceso del usuario
  A.11.3 Responsabilidades del usuario
  A.11.4 Control de acceso a redes
  A.11.5 Control de acceso al sistema de operación
  A.11.6 Control de acceso a la aplicación e información
  A.11.7 Computación móvil y tele-trabajo

- **A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información**
  A.12.1 Requerimientos de seguridad de los sistemas
  A.12.2 Procesamiento correcto en las aplicaciones
  A.12.3 Controles criptográficos
  A.12.4 Seguridad de los archivos del sistema
  A.12.5 Seguridad en los procesos de desarrollo y soporte
  A.12.6 Gestión de vulnerabilidad técnica
- **A. 13 Gestión de incidentes en la seguridad de la información**
  A.13.1 Reporte de eventos y debilidades en la seguridad de la información
  A.13.2 Gestión de incidentes y mejoras en la seguridad de la información
- **A.14 Gestión de la continuidad comercial**
  A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial
- **A.15 Cumplimiento**
  A.15.1 Cumplimiento con requerimientos legales
  A.15.2 Cumplimiento con las políticas y estándares de seguridad y normativa técnica
  A.15.3 Consideraciones de auditoría de los sistemas de información [4]

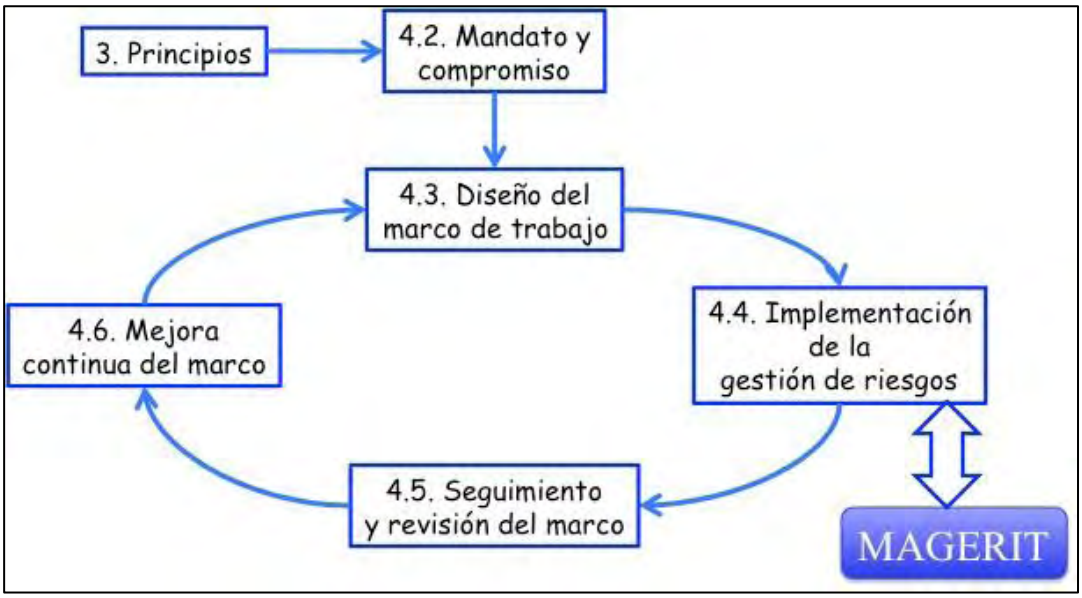
1.2.2 Magerit. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. [6]

1.2.2.1 Proceso. MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. [5]. (ver figura 1)

Figura 1. Proceso de gestión de riesgos de Magerit



Fuente: Magerit

1.2.2.2 Objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

1.2.2.3 Dimensiones de la seguridad. El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad: disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información se puede tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, se puede tener suplantación de identidad.

Trazabilidad: aseguramiento de que en toda etapa del proceso se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

1.2.2.4 Definiciones ligadas a gestión de riesgos:

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Tratamiento de los riesgos: proceso destinado a modificar el riesgo.

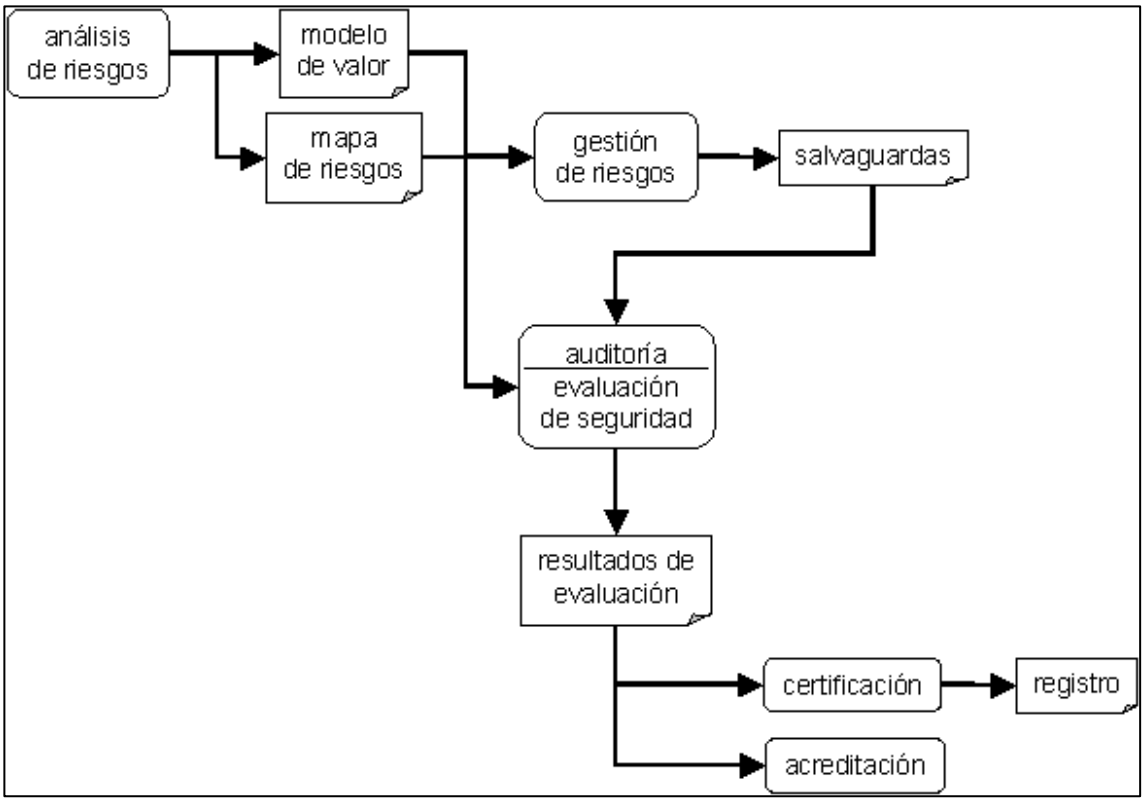
Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces se aceptan riesgos operacionales para acometer actividades que pueden reportar un beneficio que supera al riesgo, o que se tiene la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo.

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.[5]

1.2.2.5 Evaluación, certificación, auditoría y acreditación. El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. El análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema. (ver figura 2)

Figura 2. Evaluación, certificación, auditoría y acreditación

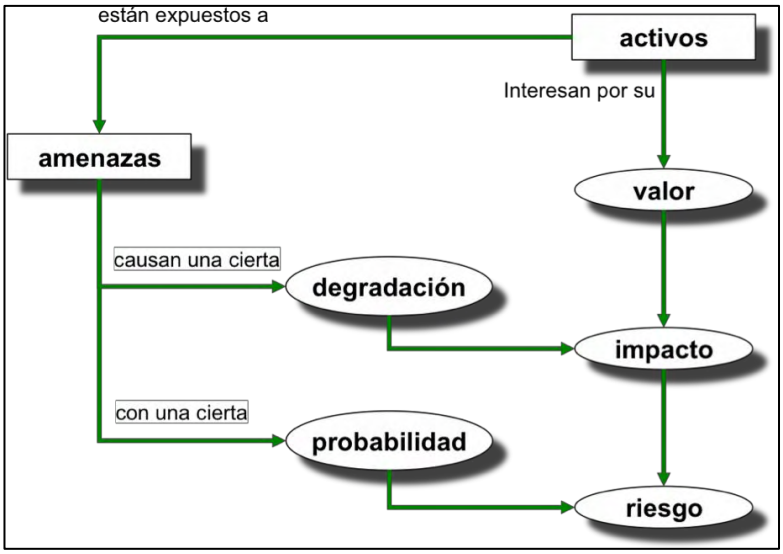


Fuente: Magerit

1.2.2.6 Método de análisis de riesgos. El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza. (ver figura 3)

Figura 3. Método de análisis de riesgos



Fuente: Magerit

- **Paso 1: Activos**

En un sistema de información hay 2 cosas esenciales:

- La información que maneja
- y los servicios que presta.

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

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas *(software)* que permiten manejar los datos.
- Los equipos informáticos *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

- **Valoración**

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección se requiere en la dimensión (o dimensiones) de seguridad que sean pertinentes.

- **Paso 2: Amenazas**

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

- **Identificación de las amenazas**

- De origen natural
- Del entorno (de origen industrial)
- Defectos de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

- **Valoración de las amenazas**

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.
Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- **Degradación:** cuán perjudicado resultaría el valor del activo
- **Probabilidad:** cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal. (ver tabla 1)

Tabla 1. Probabilidad escala cualitativa

Abreviación	**Ocurrencia/t**	**Expectativa de ocurrencia**	**Dificultad de ocurrencia**
MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy posible	Factible
M	Media	posible	Media
B	Baja	Poco posible	Difícil
MB	Muy baja	Muy raro	Muy difícil

Fuente: Magerit

En la anterior tabla se muestran algunos de los criterios para determinar la probabilidad de ocurrencia de una amenaza.

- **Ocurrencia sobre tiempo:** determina en un nivel cuantitativo el número de tipificaciones de una amenaza en un periodo de tiempo por ejemplo un año.
- **Expectativa de ocurrencia**: basada en las sensaciones del personal cercano al contexto de ocurrencia o en análisis de expertos de lo que se esperaría que ocurra.
- **Dificultad de ocurrencia**: se basa en el análisis de variable como salvaguardas o nivel de riesgos para determinar qué tan factible es la tipificación de una amenaza.

Tabla 2. Probabilidad escala cuantitativa

Abreviación	probabilidad	Nivel	% ocurrencia
MA	100	5	100
A	10	4	80
M	1	3	60
B	1/10	2	40
MB	1/100	1	20

Fuente: Magerit

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Los anteriores son valores típicos.

- **Determinación del impacto potencial**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

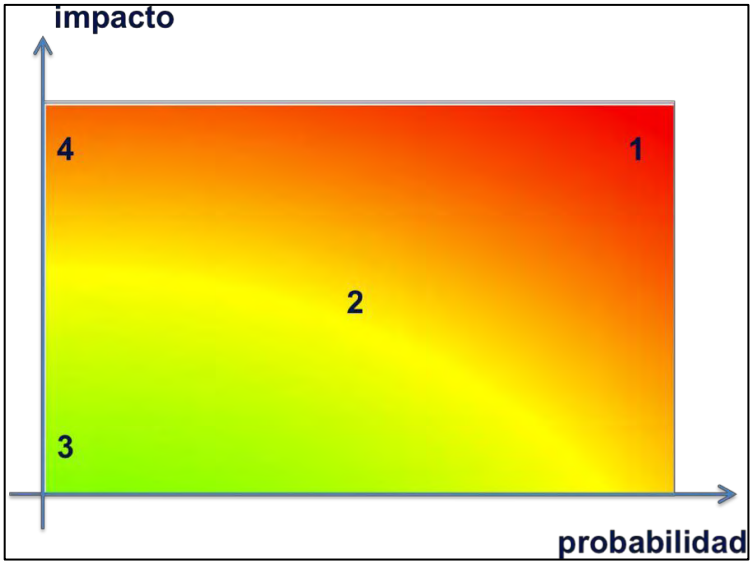
- **Determinación del riesgo potencial**

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo:

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables pero de muy alto impacto. (ver figura 4)

Figura 4. Zonas de riesgos, impacto vs probabilidad



Fuente: Magerit

- **Paso 3: Salvaguardas**

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal.

- **Selección de salvaguardas**

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas.

- **Efecto de las salvaguardas**

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- **Reduciendo la probabilidad de las amenazas.**

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

- **Limitando el daño causado.**

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

- **Vulnerabilidades**

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor sobre un activo. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

- **Paso 4: impacto residual**

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

- **Paso 5: riesgo residual**

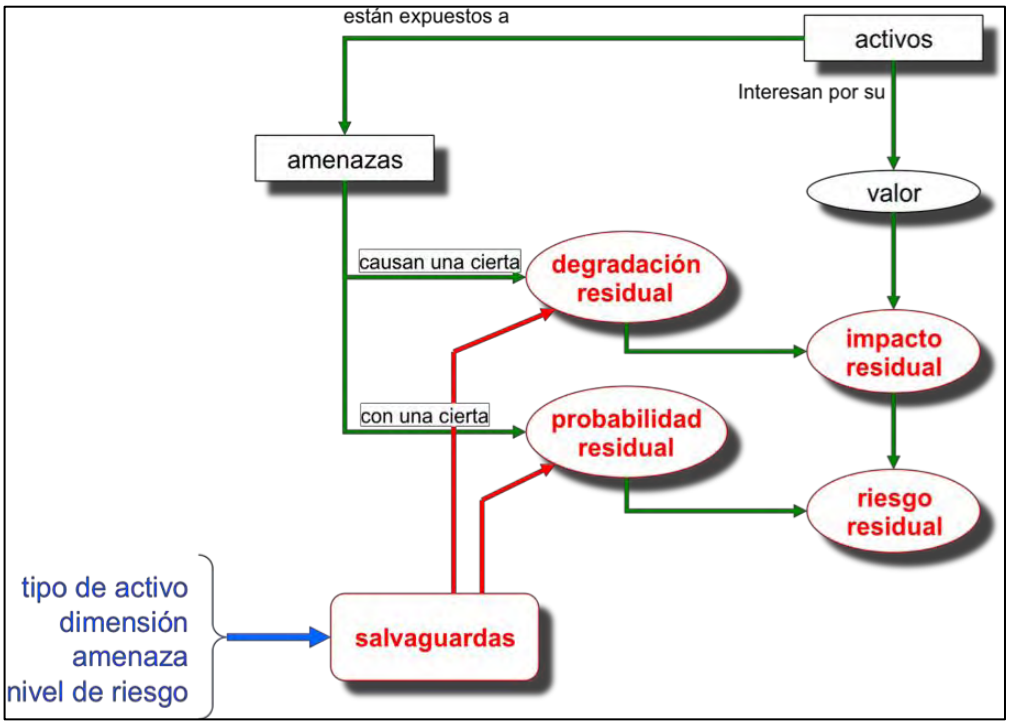
Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. [5] (ver figura 5)

Figura 5. Elementos de análisis del riesgo residual



Fuente: Magerit

2. METODOLOGÍA

2.1 TIPO DE INVESTIGACIÓN

Descriptivo aplicativo: investigación aplicativa es la clase de investigación que también recibe el nombre de práctica o empírica. Se caracteriza porque busca la aplicación o utilización de los conocimientos que se adquieren. La investigación aplicada se encuentra estrechamente vinculada con la investigación básica, que requiere de un marco teórico. En la investigación aplicada o empírica, lo que le interesa al investigador, primordialmente, son las consecuencias prácticas. [6] Es la intención plasmada en este proyecto aplicar los conocimientos y la investigación en programación, bases de datos, auditoría, y seguridad informática en el desarrollo de un aplicativo software.

El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas [7], en este caso de la norma mencionada y el proceso de realización de auditoría con ella, Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables, como por ejemplo las relaciones de dependencia y jerarquías entre los subniveles de evaluación de las normas ISO 27001 y 27002.

Para este trabajo se plantea la recolección de datos sobre la base y objetivo de facilitar el proceso de auditoría con ayuda de un software, el procesamiento de estos datos para convertirlos en información útil, para luego analizar minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

2.2 PARADIGMA Y ENFOQUE

2.2.1 Paradigma. El producto de una investigación de corte cuantitativo será un informe en el que se muestre una serie de datos clasificados, sin ningún tipo de información adicional que le dé una explicación, más allá de la que en sí mismos conllevan. Para que estos datos no sean arbitrarios y den una idea clara del análisis de resultados es necesario que estén organizados bajo criterios de clasificación para facilitar su interpretación. [8]

Además de lo antes expuesto, vale decir que la investigación cuantitativa estudia la asociación o relación entre las variables que han sido cuantificadas, lo que ayuda aún más en la interpretación de los resultados.

El objetivo de esta investigación se centra en lo medible, tal como lo es una auditoría, es por eso que se busca cuantificar objetivamente las variables involucradas en ella, por ejemplo los activos, nivel de satisfacción de listas de verificación y de sus dependientes subdominios y dominios, y el nivel en cuanto afectarán a la organización y a los activos, este es un modelo pensado para explicar, controlar y predecir fenómenos.

2.2.2 Enfoque. El Método analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías. [9]

A partir de la observación de la experiencia, es posible establecer deducciones al analizar los datos recogidos mediante la observación. El método empírico-analítico aborda la realidad de los hechos que son observables, cuantificables y medibles. Es un método que contrasta sus hipótesis de una forma rigurosa a través de la demostración científica que determina si dicha hipótesis es verdadera o falsa. Para verificar la hipótesis o refutarla se llevan a cabo diferentes experimentos. [10]

En este caso se pretende desmembrar el proceso de auditoría a través de los componentes de la estructura teórica es decir dominios subdominios, controles y cuestionarios, también se separara la parte que hace referencia a la gestión de riesgos, y los componentes vitales de la auditoría como son activos, amenazas, riesgos, probabilidades , impactos etc. A través de la observación de estos hechos y verificaciones que componen los cuestionarios que hacen referencia a los dominios y subdominios de la norma se pretende verificar la auditoría en general y decir si el sistema auditado cumple o no con los requerimientos necesarios

2.3 POBLACION Y MUESTRA

2.3.1 Población. La población objeto de estudio es muy amplia y comprende a los auditores en seguridad informática en primer lugar, pero al pretender ser el proyecto el desarrollo de una herramienta de uso fácil que sirva para hacer controles y auditorías internas de cualquier nivel, también incluye a jefes de

sistemas, gerentes y auditores internos. Es útil mencionar que los resultados sin embargo pueden ser aplicados a otro tipo de auditoría ya que la aplicación de las diferentes normas es común en cuanto a su implementación.

2.3.2 Muestra. En primer lugar la muestra será el uso de los mismos desarrolladores del software como testers de el mismo en un sistema de información en una organización o empresa, siendo los encargados de llevar a cabo las pruebas de verificación y de responder todas las listas de verificación del software, además de esto se recogerá información de profesores de la universidad con amplia experiencia en todo tipo de auditorías, tanto para a la elaboración de los requisitos iniciales del software en el caso de los ingenieros Delio Gómez, Javier Villalba, y Francisco Solarte, como para un apoyo continuo en el caso Francisco Solarte quien además es asesor del trabajo. En última instancia la muestra contendrá también al Gerente de la organización Araujo y asociados Guerlin Alfredo Araujo Mora quien será el encargado de llevar a cabo las recomendaciones y poner en marcha los controles sugeridos.

2.4 FUENTES DE INFORMACION

2.4.1 Fuentes primarias

- **Observación directa:** método de acercamiento a la información a través de la información en primera persona del objeto estudio en este caso servirá para verificar las respuestas que se darán a las pruebas del software en la etapa de pruebas del mismo.

- **Entrevistas:** son principalmente cuestionarios de respuestas abiertas que se diseñan especialmente para una persona especifica quien tiene un rango o acceso especial a la información relevante, en este caso servirán para acercarse a los profesores expertos en auditoría de la universidad, y establecer los requisitos del software a desarrollar, también servirán para acercarse a áreas específicas en el desarrollo de la etapa de pruebas del software.

- **Listas de verificación**: son preguntas con opciones de respuesta cerradas en rangos numéricos o cualitativos, en el proyecto serán un método de entrada del software que recibirá la información de verificación de cada cuestionario correspondiente a los objetivos de control.

- **Formularios:** los formularios son formatos de entrada de información que están diseñados para que el usuario introduzca datos estructurados que serán procesados o almacenados después. Este trabajo contara con formularios que recibirán toda la información necesaria en cuanto a los activos, este formulario

contara con los espacio para recibir el nombre, tipo y valor de cada activo, principalmente, entre otras opciones, también se ingresara mediante un formulario toda la información concerniente a la auditoría como nombre del grupo auditor, empresa auditada, encargado, director, colaboradores, áreas auditadas, auditores encargados de cada área etc.

2.4.2 Fuentes secundarias. Normas de auditoría (ISO 27001 Y 27002): 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. ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. [11]

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)". [12]

Estos dos documentos serán la columna vertebral del trabajo ya que serán la base teórica sobre la cual se desarrollara la estructura del software, ya que el mismo contendrá todos los dominios, subdominios y objetivos de control que tiene la norma ISO 27001 y permitirá su verificación, en cuanto a la norma ISO 27002 el software se valdrá de los controles y políticas de mejores prácticas que están en ella para elaborar el plan de recomendaciones y mejoramiento de la auditoría.

Normas de gestión de riesgos (Magerit): MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. [13]

Este método compuesto por tres libros será la guía del diseño de la forma en como el software tiene que operar y procesar la información, en primera medida el software clasificara los activos de la empresa auditada según los tipos de activos existentes en Magerit, luego se verificara las amenazas presentes para la organización y se evaluara la probabilidad y el impacto para la empresa evaluando variables como la cantidad de activos afectados y el valor para la organización de los mismos, finalmente el usuario del software podrá elegir que controles

implementar, sean los presentes en el catálogo de Magerit o los que se encuentran en la norma ISO 27002.

- **Internet:** se apoyara el trabajo con información presente en internet, tanto para la elaboración del anteproyecto como del documento final, y en cuanto al proceso de elaboración software será de gran utilidad el uso de esta herramienta para consultas prácticas en áreas de programación, bases de datos, y en general las dudas que se puedan presentar.

3. DESARROLLO DEL TRABAJO

3.1 ETAPA DE RECOLECCIÓN DE INFORMACIÓN

3.1.1 Requerimientos. Los requerimientos para el software se hicieron basándose en las opiniones y recomendaciones del asesor y director de trabajo Francisco Solarte quien es un auditor con amplia experiencia, además de entrevistas realizadas a los ingenieros Javier Villalba y Delio Gómez, se adjuntaran copias de estas entrevistas.

Se realizó una síntesis que recopila los resultados de las tres entrevistas en el siguiente informe de requerimientos:

- El software deberá permitir ingresar y organizar la información correspondiente a cada auditoría que realice, como lo son los datos de nombre del grupo auditor, de los colaboradores, las áreas auditadas, la empresa auditada, la fecha de inicio de la auditoría y los dominio y o aspectos que se evaluaran.
- El software deberá facilitar en todo momento de la auditoría una consulta a los tiempos y al cronograma proporcionado basándose en los dominios escogidos por el auditor.
- El software deberá permitir restringir y registrar diferentes tipos de acceso de acuerdo a los colaboradores que se registren y a las áreas de la auditoría en las que puedan y deban trabajar.
- El software deberá organizar las preguntas y cuestionarios en los ítems en los cuales están definidos por la norma.
- Una vez ingresado un usuario el software deberá restringir y organizar la información a la que este tenga acceso y en la que pueda trabajar, de acuerdo a los dominios que se le asignaron o a las áreas de la seguridad que él deba evaluar.
- El software deberá mostrar una lista organizada y clasificada según la norma con las preguntas que deba evaluar.
- Se mostrara un formulario de datos de activos de acuerdo a Magerit en el cual el usuario deberá ingresar toda la información de los activos de la empresa, incluyendo su valor, el cual se determinara automáticamente mediante las fórmulas de Magerit, y su tipo, el cual servirá para determinar que amenazas lo afectan y así poder determinar el impacto de su afectación.
- El software deberá permitir navegar mediante la estructura hasta llegar a las preguntas y responderlas.
- Una vez gestionado los cuestionarios se procederán a evaluar los dominios que aprueben o no la evaluación, los que no aprueben deberán activar una lista de amenazas y estas a su vez los activos a quienes afectan, así se

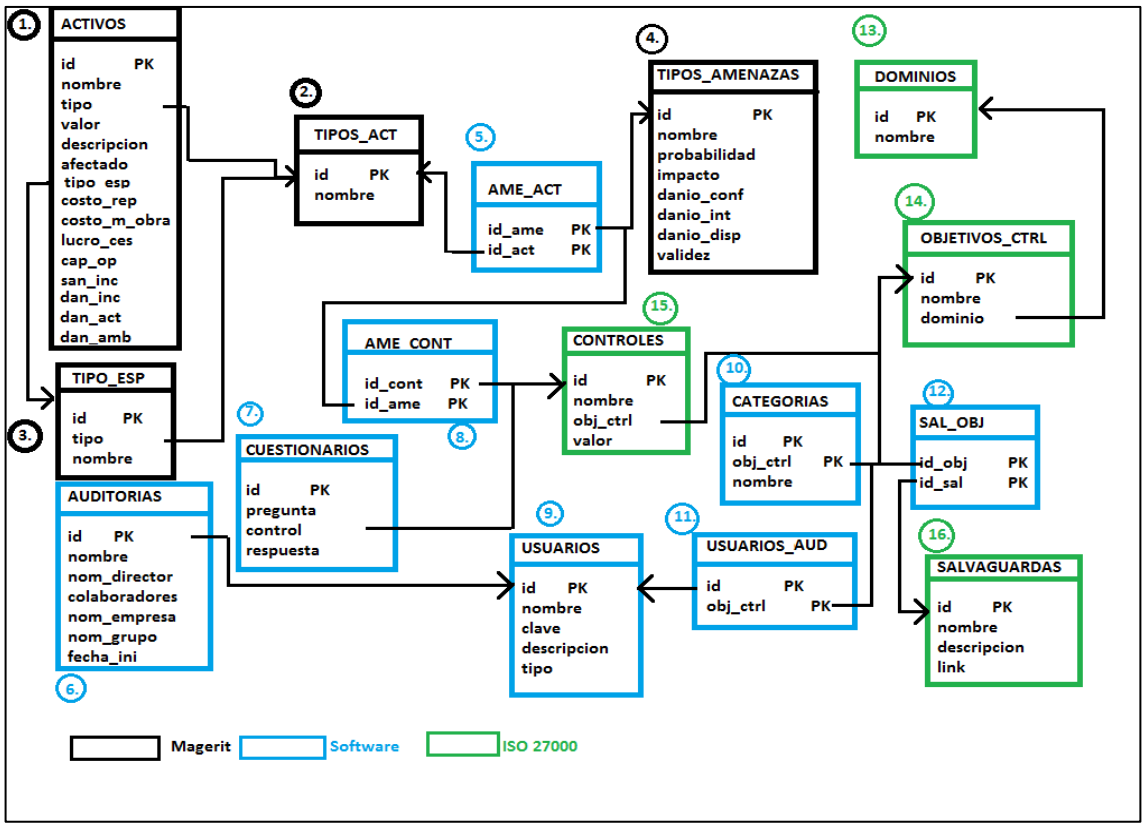
obtendrá el impacto de cada amenaza.

- Se deberá gestionar un formulario de probabilidad de ocurrencia de las amenazas y con esto ya se podrá obtener la matriz de riesgos.
- Se deberá relacionar las amenazas activadas con los controles apropiados.
- Se deberá proporcionar un conjunto de reportes que faciliten la tarea de elaboración de hallazgos y conclusiones del auditor.

3.2 ETAPA DE DISEÑO

3.2.1 Diseño de la base de datos. En esta base de datos se organizaran, clasificaran y contendrán todos los datos necesarios para el funcionamiento de un proyecto individual del software, es decir cada proyecto nuevo que se abra usará una copia de esta base de datos vacía. (ver figura 6)

Figura 6. Esquema relacional de la base de datos



La base de datos del software está conformada por 16 tablas, para su mejor entendimiento y uso se clasificaron en tres grupos: las que hacen referencia a los elementos de Magerit, y que los agrupan y organizan, en diferentes clases para su uso lógico dentro de la programación y de lo que el software necesita.

El segundo grupo lo conforman las tablas estructurales del software, necesarias para relacionar otros elementos o para agrupar y ordenar elementos lógicos de una auditoría como lo son los datos de las auditorías o los usuarios por ejemplo, también se contempla en este ítem el banco de preguntas de evaluación de cada objetivo de control.

El tercer grupo lo conforma la estructura de la norma ISO 27000, agrupando a los dominios, los subdominios los objetivos y las salvaguardas, esto permite navegar a través de la norma desagregando ítems desde lo general a lo específico.

3.2.1.1 Tablas de magerit:

[1] Activos:

Conformación:

- **Id:** identificador numérico llave primaria.
- **Nombre:** campo tipo char que almacena el nombre del activo
- **Descripción:** breve descripción tipo char del activo.
- **Afectado:** campo boleano que indica si el activo está siendo o no afectado según la evaluación realizada a los objetivos de control.
- **Tipo:** campo referenciado a la tabla tipos de activo, clasificada en los tipos de activos de Magerit.
- **Tipo_esp:** especificación del tipo, tomada de Magerit, referenciado a tabla tipo_esp.
- **Campos de dimensiones del valor:** campos numéricos que almacenan diferentes aspectos del valor de un activo presentes en Magertit.
- **Valor:** campo numérico en donde se almacena el valor total obtenido de las dimensiones de valor.
- **Objetivo:** almacenar toda la información correspondiente a los activos de la organización, permitir su fácil relación y operación con otros componentes del sistema y facilitar la obtención y elaboración de reportes
- **Fuente de los datos:** los datos almacenados en esta tabla se obtienen de formularios que el usuario debe diligenciar, excepto los campos **afectado**, que se obtiene de la evaluación de los objetivos de control, y **valor** que se obtiene del promedio de las dimensiones de valor. (ver figura 7)

Figura 7. SQL creación de la tabla activos

SQL pane

```
4
5   CREATE TABLE activos
6   (
7     id serial NOT NULL,
8     nombre text,
9     tipo integer,
10    valor double precision,
11    descripcion text,
12    afectado character(1),
13    costo_mano_obra integer,
14    lucro_cesante integer,
15    capacidad_operar integer,
16    sanciones_incumplimiento integer,
17    danios_otros_activos integer,
18    danio_personas integer,
19    danio_ambiental integer,
20    costo_reposicion integer,
21    tipo_esp integer,
22    CONSTRAINT activos_pkey PRIMARY KEY (id),
23    CONSTRAINT activos_tipo_esp_fkey FOREIGN KEY (tipo_esp)
24        REFERENCES tipo_esp (id) MATCH SIMPLE
25        ON UPDATE NO ACTION ON DELETE NO ACTION,
26    CONSTRAINT activos_tipo_fkey FOREIGN KEY (tipo)
27        REFERENCES tipos_act (id) MATCH SIMPLE
28        ON UPDATE NO ACTION ON DELETE NO ACTION
29  )
30  WITH (
31    OIDS=FALSE
32  );
33  ALTER TABLE activos
34    OWNER TO postgres;
```

Figura 8. Tabla activos en pgadmin

id [PK] serial	nombre text	tipo integer	valor double precis	descripcion text	afectado character(1)	costo_mano_ integer	lucro_cesant integer	capacidad_o integer	sanciones_in integer	danios_otros integer	danio_perso integer	danio_ambie integer	costo_reposi integer	tipo_esp integer

[2] Tabla tipos de activos:

Conformación:

- **Id**: identificador, campo numérico, llave primaria
- **Nombre:** nombre del tipo del activo, once tipos tomados de Magerit

- **Objetivo:** clasificar y ordenar a los activos dentro de las categorías presentes en Magerit, tabla referenciada por activos y por tipo_esp, permitir al usuario una fácil clasificación e ingreso de los activos, facilitar la elaboración de reportes.
- **Fuente:** los datos para esta tabla serán ingresados por los desarrolladores del software tomados de Magerit. (ver figura 9)

Figura 9. SQL creación tabla tipos_act

SQL pane

```
1   -- Table: tipos_act
2
3   -- DROP TABLE tipos_act;
4
5   CREATE TABLE tipos_act
6   (
7     nombre text,
8     id integer NOT NULL,
9     CONSTRAINT tipos_act_pkey PRIMARY KEY (id)
10  )
11  WITH (
12    OIDS=FALSE
13  );
14  ALTER TABLE tipos_act
15    OWNER TO postgres;
16
```

- **SQL inserción de datos:**

```
insert into "tipos_act"("id","nombre")
values
(1,'1. Informacion'),
(2,'2. Servicios '),
(3,'3. Datos'),
(4,'4. Llaves criptograficas'),
(5,'5. Software'),
(6,'6. Hardware '),
(7,'7. Redes de comunicación '),
(8,'8. Medidas de soporte '),
(9,'9. Equipamiento auxiliar '),
(10,'10. Instalaciones '),
(11,'11. Personal ')
```

Figura 10. Tabla tipos_act en pgadmin

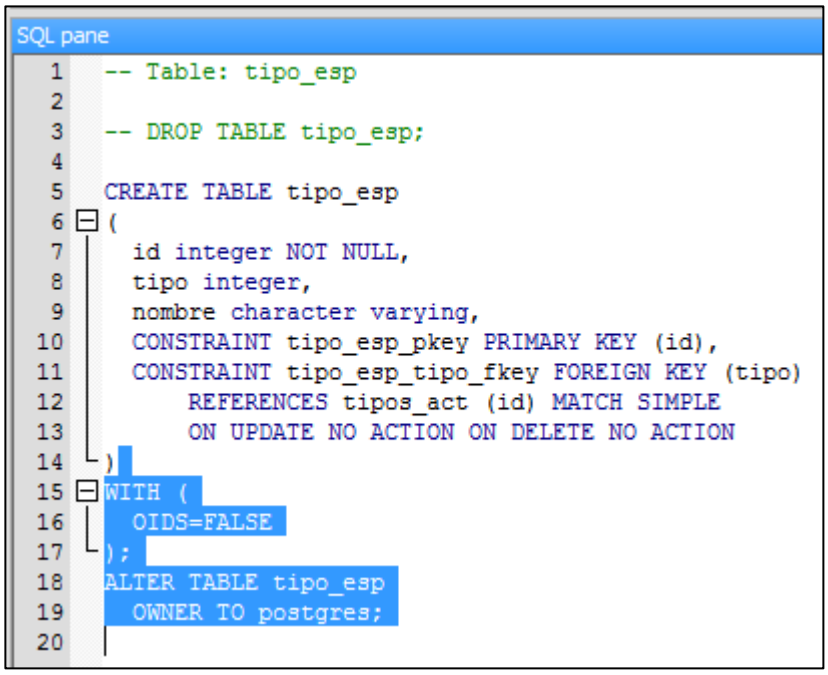
	nombre text	id [PK] integer
1	1. Informacion	1
2	2. Servicios	2
3	3. Datos	3
4	4. Llaves criptograficas	4
5	5. Software	5
6	6. Hardware	6
7	7. Redes de comunicación	7
8	8. Medidas de soporte	8
9	9. Equipamiento auxiliar	9
10	10. Instalaciones	10
11	11. Personal	11
*		

[3] Tabla de tipo específico de activos tipo_esp:

Conformación:

- **Id:** identificador numérico, llave primaria
- **Tipo:** campo numérico referenciado a tipo_act, almacena 130 tipos específicos de activo spresentes en Magerit
- **Nombre:** campo char,almacena los nombres de los tipos específicos de activos
- **Objetivo:** clasificar y ordenar a los activos dentro de las categorías presentes en Magerit, tabla que referencia tipos_activos, permitir al usuario una fácil clasificación e ingreso de los activos, permitir la desagregación de tipos de activos de general a especifico, facilitar la elaboración de reportes.
- **Fuente de los datos**: los datos para esta tabla serán ingresados por los desarrolladores del software tomados de Magerit (ver figura 11-14)

Figura 11. SQL creación de tabla tipo_esp



- **Inserción de datos:**

```
INSERT INTO "tipo_esp" ("id","tipo","nombre")
VALUES

--1. INFORMACION
(11,1,' 1.1 Datos vitales: registros de la organización o de
interes para la administracion de la organización'),

--2. SERVICIOS
(21,2,' 2.1 Anonimo: sin requerir identificación de usuario'),
(22,2,' 2.2 Al público en general: sin relación contractual'),
(23,2,' 2.3 A usuarios externos: bajo relación contractual'),
(24,2,' 2.4 Interno: dentro de la misma organización'),
(25,2,' 2.5 World wide web'),
(26,2,' 2.6 Acceso remoto a cuenta local'),
(27,2,' 2.7 Correo electrónico'),
(28,2,' 2.8 Almacenamiento de ficheros'),
(29,2,' 2.9 Transferencia de ficheros'),
(210,2,' 2.10 Intecambio electrónico de datos'),
(211,2,' 2.11 Servicio de directorio'),
(212,2,' 2.12 Gestión de identidades'),
(213,2,' 2.13 Gestión de privilegios'),
(214,2,' 2.14 Infraestructura de clave pública'),

--3. DATOS...
```

Figura 12. Fragmento de la tabla tipo_esp en pgadmin

	id [PK] integer	tipo integer	nombre character varying
1	11	1	1.1 Datos vitales: registros de la organización o de interes
2	21	2	2.1 Anonimo: sin requerir identificación de usuario
3	22	2	2.2 Al público en general: sin relación contractual
4	23	2	2.3 A usuarios externos: bajo relación contractual
5	24	2	2.4 Interno: dentro de la misma organización
6	25	2	2.5 World wide web
7	26	2	2.6 Acceso remoto a cuenta local
8	27	2	2.7 Correo electrónico
9	28	2	2.8 Almacenamiento de ficheros
10	29	2	2.9 Transferencia de ficheros

[4] Tabla tipos_amenazas

Conformación:

- **Id:** identificador de la tabla, tipo numérico, llave primaria
- **Nombre:** tipo char, almacena los nombres de 57 tipos de amenazas presentes en Magerit
- **Probabilidad:** entero que almacena la probabilidad de ocurrencia de cada amenaza, en tres diferentes categorías
- **Impacto:** entero que almacena el impacto de la ocurrencia de cada amenaza, en tres diferentes categorías.
- **Danio_conf:** boleano que registra si cada amenaza hace daño o no en la dimensión de seguridad confiabilidad
- **Danio_disp:** boleano que registra si cada amenaza hace daño o no en la dimensión de seguridad disponibilidad
- **Danio_int:** boleano que registra si cada amenaza hace daño o no en la dimensión de seguridad confiabilidad
- **Validez:** boleano que registra si cada amenaza es activada o no luego de la evaluación de los objetivos de control
- **Objetivo:** clasificar y ordenar los tipos de amenazas que están presentes en Magerit, almacenar el impacto y la probabilidad de ocurrencia de cada amenaza, almacenar el daño que cada amenaza hace en cada dimensión de seguridad, información tomada de Magerit, determinar y almacenar si una amenaza es activada o no luego de la evaluación de los objetivos de control
- **Fuente de los datos:** algunos datos de esta tabla son tomados de Magerit e ingresados por los desarrolladores de software, el campo probabilidad es ingresado por el usuario, y los campos impacto y validez son calculados de otros datos del sistema

Figura 13. SQL creación tabla tipos_ame

SQL pane

```
-- Table: tipos_ame

-- DROP TABLE tipos_ame;

CREATE TABLE tipos_ame
(
  id integer NOT NULL,
  nombre text,
  probabilidad integer,
  impacto integer,
  danio_conf integer,
  danio_int integer,
  danio_dis integer,
  validez integer,
  CONSTRAINT amenazas_pkey PRIMARY KEY (id)
)
WITH (
  OIDS=FALSE
);
ALTER TABLE tipos_ame
  OWNER TO postgres;

```

- **Inserción SQL:**

```
INSERT INTO "tipos_ame"
("id","nombre","danio_conf","danio_int","danio_dis")
VALUES

---1. desastres naturales


(11,'1.1 Fuego',0,0,1),
(12,'1.1 Daños por agua',0,0,1),
(13,'1.3 Desastres Naturales',0,0,1),

-----------------------------------------

---2. De origen industrial

(21,'2.1 Fuego',0,0,1),
(22,'2.2 Daños por agua ',0,0,1),
(23,'2.3 Desastres industriales ',0,0,1),
(24,'2.4 Contaminación mecánica ',0,0,1),
(25,'2.5 contaminacion electromagnetica ',0,0,1),
(26,'2.6 Avería de origen físico o lógico ',0,0,1),
(27,'2.7 Corte del suministro eléctrico ',0,0,1),
(28,'2.8 Condiciones inadecuadas de temperatura o
humedad',0,0,1),
```

Figura 14. Fragmento de la tabla tipos_ame en pgadmin

	id [PK] integer	nombre text	probabilidad integer	impacto integer	danio_conf integer	danio_int integer	danio_dis integer	validez integer
1	11	1.1 Fuego			0	0	1	
2	12	1.1 Daños por agua			0	0	1	
3	13	1.3 Desastres Naturales			0	0	1	
4	21	2.1 Fuego			0	0	1	
5	22	2.2 Daños por agua			0	0	1	
6	23	2.3 Desastres industriales			0	0	1	
7	24	2.4 Contaminación mecánica			0	0	1	
8	25	2.5 contaminacion electromagnetica			0	0	1	
9	26	2.6 Avería de origen físico o lógico			0	0	1	
10	27	2.7 Corte del suministro eléctrico			0	0	1	
11	28	2.8 Condiciones inadecuadas de temperat			0	0	1	
12	29	2.9 Fallo de servicios de comunicacione			0	0	1	
13	31	3.1 Errores de los usuarios	2	3	1	1	1	1
14	32	3.2 Errores del administrador	2	3	1	1	1	1
15	33	3.3 Errores de monitorización	2	3	0	1	0	1
16	34	3.4 Errores de configuración	2	3	0	1	0	1
17	35	3.5 Deficiencias en la organización	2	3	0	0	1	1
18	36	3.6 Difusión de software dañino		3	1	1	1	1
19	37	3.7 Errores de reencaminamiento		3	1	0	0	1
20	38	38. Errores de secuencia			0	1	0	
21	39	3.9 Escapes de información	2	3	1	0	0	1

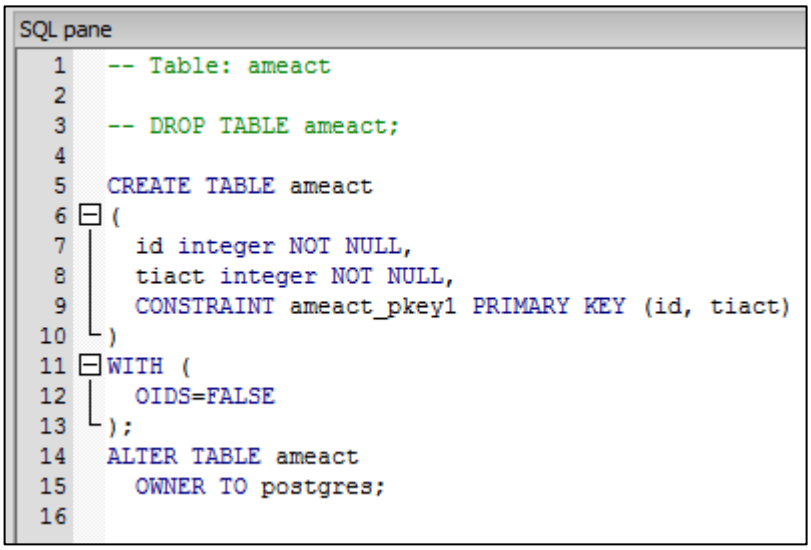
3.2.1.2 Tablas Propias del software:

[1] Tabla que relaciona amenazas y activos ame_act:

Conformación:

- **Id_ame:** identificador numérico parte de la llave primaria y llave foránea hacia tipos_ame.
- **Id_act:** identificador numérico parte de la llave primaria y llave foránea hacia Tipos_act
- **Objetivo:** establecer la relación muchos a muchos entre las tablas tipos_act y tipos_ame, y permitir saber a qué tipos de activos afecta cada amenaza activada.
- **Fuente de los datos:** los datos de esta tabla son insertados por los desarrolladores del software y la relación de cada amenaza con los activos afectados está presente en Magerit. (ver figura 15-18)

Figura 15. SQL creación de tabla ame_act



- **Inserción SQL:**

```
INSERT INTO "ameact" ("idame","idact")
VALUES


(1,33),(1,34),(1,41),(1,42),(1,411), 1---

(2,31),(2,32),(2,37),(2,38),(2,310),(2,311),(2,312),(2,316),(2,43
),(2,44),(2,45),(2,47),(2,48),(2,49),(2,411),(2,413),(2,414),(2,4
15),(2,418), 2---

(3,31),(3,32),(3,39),(3,310),(3,311),(3,312),(3,43),(3,44),(3,49)
,(3,413),(3,414),(3,415), 3---

(4,31),(4,32),(4,310),(4,311),(4,312),(4,43),(4,44),(4,49),(4,413
),(4,414),(4,415), 4---
...
```

Figura 16. Fragmento de tabla ameact en pgadmin

	id [PK] integer	tiact [PK] integer
1	1	33
2	1	34
3	1	41
4	1	42
5	1	411
6	2	31
7	2	32
8	2	37
9	2	38
10	2	43
11	2	44
12	2	45
13	2	47
14	2	48
15	2	49

[2] Tabla auditorías:

Conformación:

- **Id:** identificador numérico, llave primaria
- **Nombre:** tipo char, almacena el nombre o título de la auditoría.
- **Nom_director:** tipo char, almacena el nombre del director de la auditoría, llave foránea a usuarios
- **Colaboradores:** tipo char, almacena el nombre de los colaboradores de la auditoría, llave foránea a usuarios.
- **Nom_empresa:** tipo char, nombre de la empresa u organización auditada.
- **Nom_grupo:** tipo char, nombre del grupo auditor
- **Fecha:** tipo date, almacena la fecha de inicio de la auditoría.
- **Categoría:** tipo entero, llave foránea a dominios, sirve para determinar a qué áreas se aplicara la auditoría
- **Objetivo:** almacenar los datos de auditoría para cada nuevo proyecto, crear un nuevo proyecto, gestionar los usuarios que tendrán acceso al proyecto, establecer la categoría de la auditoría
- **Fuente de los datos:** todos los datos de esta tabla son ingresados mediante formulario por el usuario.

Figura 17. SQL de creación tabla auditorías

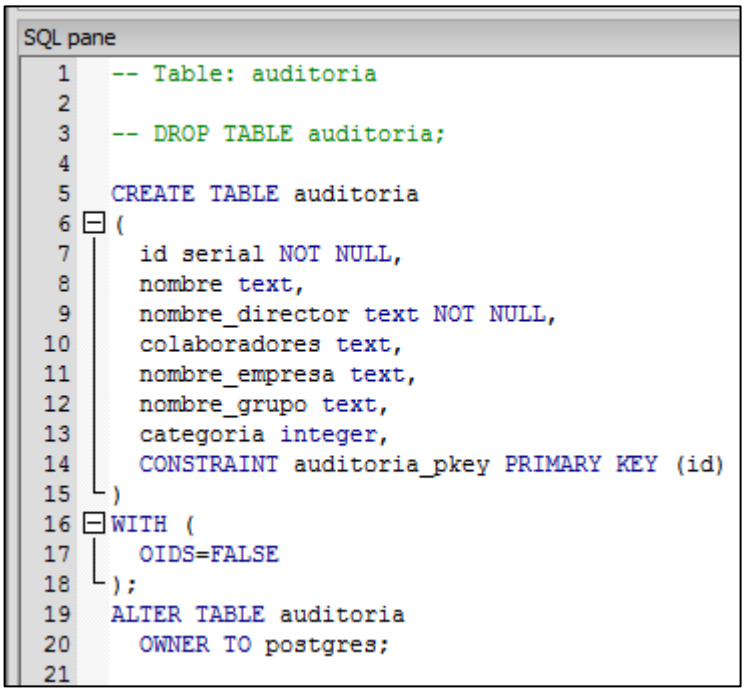
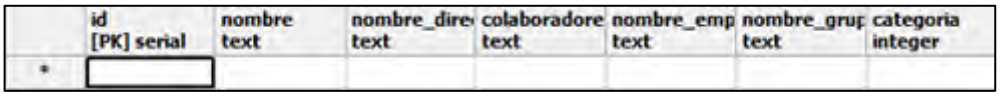


Figura 18. Tabla auditoría en pgadmin



[3] Tabla cuestionarios

Conformación:

- **Id:** identificador numérico llave primaria.
- **Pregunta:** tipo char, almacena cada una de las preguntas.
- **Control:** tipo numérico, se referencia a la tabla controles para saber a qué cuestionario pertenece cada pregunta
- **Respuesta:** campo numérico, almacena de uno a cinco el nivel de satisfacción de la evaluación de una pregunta.
- **Objetivo:** almacenar las preguntas y respuestas que evalúan cada control, permitir el cálculo del valor de la evaluación de cada control, facilitar el almacenamiento y elaboración de reportes.
- **Fuente de los datos:** las preguntas son ingresadas por los desarrolladores del software, luego de un análisis de lo que debe evaluar cada control de ISO 27001, de la misma forma se ingresa el id, y se relaciona con la tabla controles

en la tupla correspondiente, mientras que la respuesta debe ser ingresada por el auditor mediante un formulario. (ver figura 19-22)

Figura 19. SQL de creación de tabla cuestionarios

SQL pane

```
-- Table: cuestionarios

-- DROP TABLE cuestionarios;

CREATE TABLE cuestionarios
(
  pregunta text,
  control integer,
  id integer NOT NULL,
  respuesta integer,
  valor integer,
  CONSTRAINT cuestionarios_pkey PRIMARY KEY (id),
  CONSTRAINT cuestionarios_control_fkey FOREIGN KEY (control)
      REFERENCES controles (id) MATCH SIMPLE
      ON UPDATE NO ACTION ON DELETE NO ACTION
)
WITH (
  OIDS=FALSE
);
ALTER TABLE cuestionarios
  OWNER TO postgres;

```

- **Inserción SQL:**

```
INSERT INTO "cuestionarios" ("id","pregunta","control")
VALUES

(5111,'¿La política de seguridad de la información cuenta con
una definición de seguridad de la información, sus objetivos
generales y el alcance e importancia de la seguridad como
mecanismo que permite compartir la información?
',511),


(5112,'¿La política de seguridad de la información cuenta con
una declaración de la intención de la dirección, que apoye las
metas y los principios de seguridad de la información, de acuerdo
con la estrategia y los objetivos del negocio?
',511),


(5113,'¿La política de seguridad de la información cuenta con
una estructura para establecer los objetivos de control y los
controles, incluyendo la estructura de la evaluación de riesgos y
de la gestión del riesgo? ',511),

(5114,'¿La política de seguridad de la información cuenta con
 el cumplimiento de los requisitos legales, reglamentarios y
contractuales? ',511),
(5115,'¿La política de seguridad de la información cuenta con
 los requisitos de educación, formación y concientización sobre
seguridad',511),


(5116,'¿La política de seguridad de la información cuenta con
 La gestión de continuidad del negocio? ',511),
...
```

Figura 20. Fragmento de la tabla cuestionarios en pgadmin

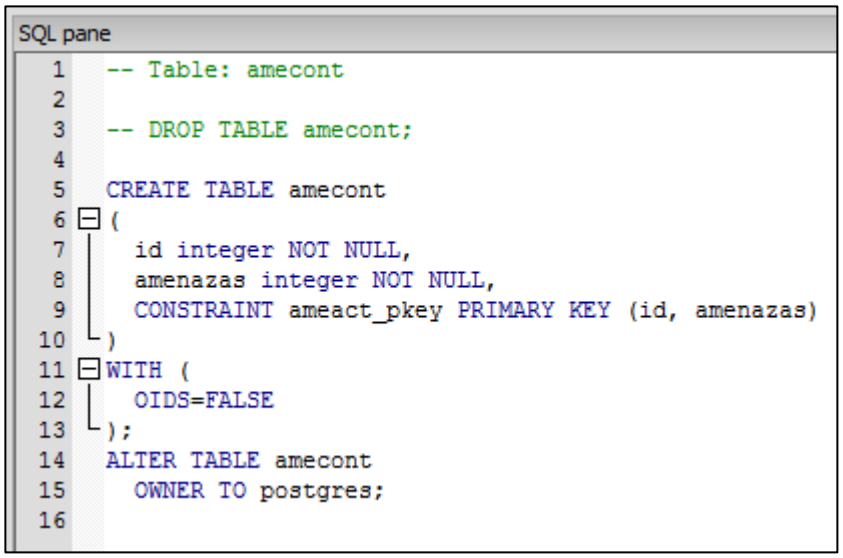
	pregunta text	control integer	id [PK] integer	valor integer
1	Se cuenta con Una verificación de los detalles adiciona	812	812	
2	¿La política de seguridad de la información cuenta con	511	5111	5
3	¿La política de seguridad de la información cuenta con	511	5112	5
4	¿La política de seguridad de la información cuenta con	511	5113	4
5	¿La política de seguridad de la información cuenta con	511	5114	3
6	¿La política de seguridad de la información cuenta con	511	5115	3
7	¿La política de seguridad de la información cuenta con	511	5116	3
8	¿Las entradas para la revisión por la dirección cuenta c	512	5121	5
9	¿Las entradas para la revisión por la dirección cuenta c	512	5122	2
10	¿Las entradas para la revisión por la dirección cuenta c	512	5123	2
11	¿Las entradas para la revisión por la dirección cuenta c	512	5124	2
12	¿Las entradas para la revisión por la dirección cuenta c	512	5125	2
13	¿Las entradas para la revisión por la dirección cuenta c	512	5126	2
14	¿Las entradas para la revisión por la dirección cuenta c	512	5127	2
15	¿Las entradas para la revisión por la dirección cuenta c	512	5128	2
16	¿Las entradas para la revisión por la dirección cuenta c	512	5129	2

[4] Tabla que relaciona amenazas con controles ame_cont

Conformación:

- **Idcont:** identificador numérico, parte de la llave primaria, referencia a controles
- **Idame:** identificador numérico, parte de la llave primaria, referencia a tipos_ame
- **Objetivo:** establecer la relación muchos a muchos entre las tablas controles y tipos_ame, y permitir saber a qué tipos de amenaza activa cada objetivo de control.
- **Fuente de los datos:** los datos de esta tabla son ingresados por los desarrolladores del software, luego de analizar los riesgos de la reprobación de la evaluación de cada objetivo de control.

Figura 21. SQL creación tabla ame_cont



- **Inserción SQL:**

```
insert into "amecont" values
(511,32),(511,33),(511,34),(511,35), ---511

(512,32),(512,33),(512,34), ---512

(611,32),(611,33),(611,34), ---611

(612,33),(612,34),(612,35), ---612

(613,32),(613,33),(613,34),(613,35), ---613

(614,39),(614,31),(614,33),(614,34) ---614

(615,39),(615,31),(615,32),(615,33),(615,34),(615,423),(615,424),
 ---615

...
```

Figura 22. Fragmento de la tabla ame_cont en pgadmin

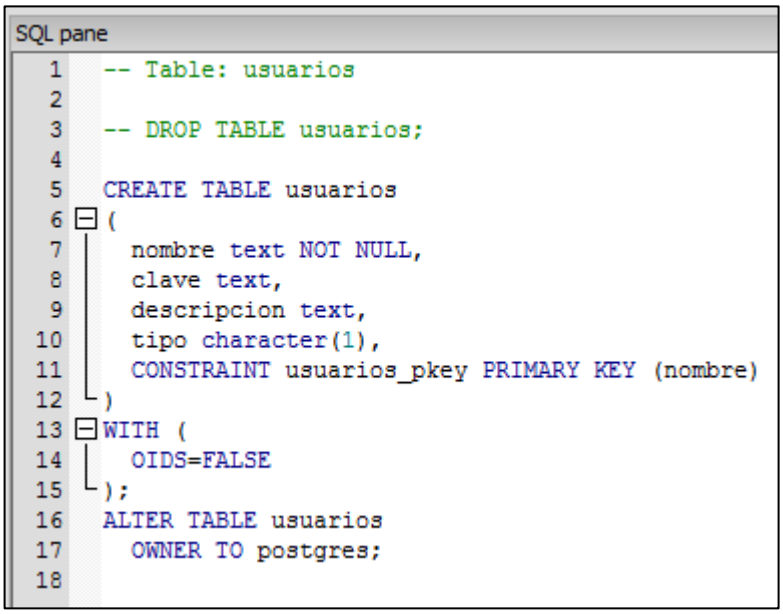
	id [PK] integer	amenazas [PK] integer
1	511	32
2	511	33
3	511	34
4	511	35
5	512	32
6	512	33
7	512	34
8	512	35
9	611	32
10	611	33
11	611	34
12	611	35
13	612	32
14	612	33
15	612	34
16	612	35

[5] Tabla usuarios

Conformación:

- **Id: i**dentificador numérico, llave primaria
- **Nombre:** nombre del usuario tipo char, sirve como nombre de inicio de sesión
- **Clave:** tipo char, clave de inicio de sesión de un usuario.
- **Descripción:** tipo char, descripción del usuario
- **Tipo:** boleano, indica si el usuario es directo de la auditoría o es un usuario común, por defecto se ingresa usuario común a menos que se indique lo contrario.
- **Objetivo:** permitir la creación de usuarios, el inicio de sesión, las restricciones de ingreso, gestionar claves, distinguir si el usuario es administrador o colaborador, es referenciada desde usuarios_obj y auditorías.
- **Fuente de los datos:** los datos de esta tabla son ingresados por el usuario al inscribir un usuario del software. (ver figura 23-26)

Figura 23. SQL para creación de tabla usuarios



SQL pane

```
1   -- Table: usuarios
2
3   -- DROP TABLE usuarios;
4
5   CREATE TABLE usuarios
6   (
7     nombre text NOT NULL,
8     clave text,
9     descripcion text,
10    tipo character(1),
11    CONSTRAINT usuarios_pkey PRIMARY KEY (nombre)
12  )
13  WITH (
14    OIDS=FALSE
15  );
16  ALTER TABLE usuarios
17    OWNER TO postgres;
18
```

Figura 24. Tabla usuarios en pgadmin

	nombre [PK] text	clave text	descripcion text	tipo character(1)
1	dario	123	Ingeniro	1
2	Dario Mera	1234	Desarrollad	1
3	james	123	Ingeniero	1
4	James Caivi	4321	Desarrollad	1
5	Usuario	0000	Usuario de	0
*				

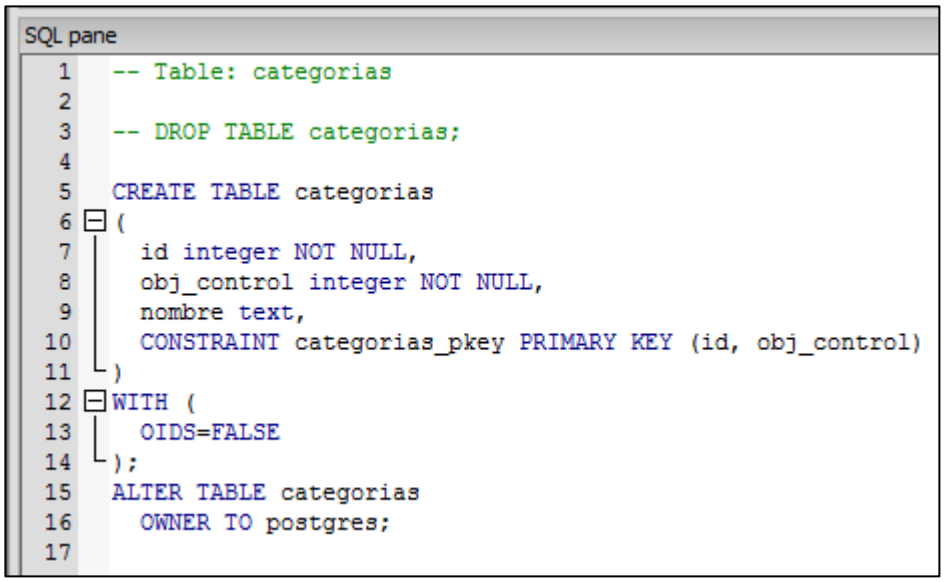
[6] Tabla categorías

Conformación:

- **Id:** identificador numérico, parte de llave primaria compuesta.
- **Id_obj_ctrl:** identificador numérico, parte de llave primaria compuesta, se referencia a obj_ctrl.
- **Nombre:** tipo char almacena el nombre de las categorías.
- **Objetivo:** establecer la relación entre categorías y objetivos de control para permitir al usuario escoger una, por ejemplo redes o sistemas operativos, y así poder trabajar con los objetivos de control correspondientes.

- **Fuente de los datos:** los datos de esta tabla son ingresados por los desarrolladores del software, luego de clasificar a los objetivos de control en las categorías correspondientes.

Figura 25. SQL para creación de tabla categorías



- **Inserción SQL:**

```
INSERT INTO "categorias" ("id","obj_control","nombre")
VALUES

(1,,106,"redes"),
(1,,108,"redes"),
(1,,109,"redes"),
(1,,114,"redes"),
...
```

Figura 26. Fragmento de tabla categorías en pgadmin

	id [PK] integer	obj_control [PK] integer	nombre text
1	1	106	redes
2	1	108	redes
3	1	109	redes
4	1	114	redes
5	1	117	redes
6	2	103	sistemas op
7	2	104	sistemas op
8	2	105	sistemas op

[7] Tabla usuarios_auditoría

Conformación:

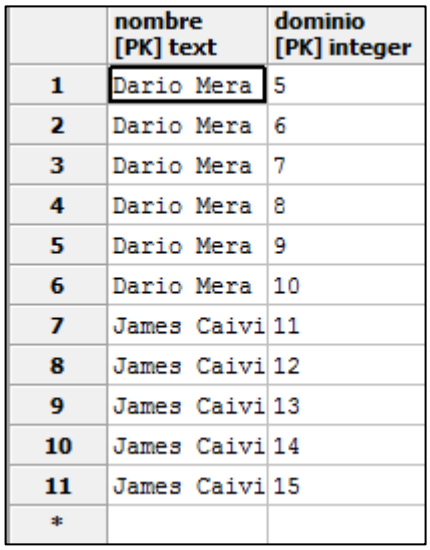
- **Id:** identificador numérico, parte de llave primaria compuesta, se referencia a usuarios.
- **Obj_ctrl:** identificador numérico, parte de llave primaria compuesta, se referencia a objetivos_ctrl.
- **Objetivo:** establecer la relación muchos a muchos entre usuarios, y objetivos de control, delimitar las áreas a las que cada usuario tiene acceso.
- **Fuente de los datos:** el usuario director deberá elegir las áreas a las que cada colaborador tiene acceso mediante un formulario. (ver figura 27-30)

Figura 27. SQL para creación de la tabla usuarios auditoría

SQL pane

```
1   -- Table: usuarios_auditoria
2
3   -- DROP TABLE usuarios_auditoria;
4
5   CREATE TABLE usuarios_auditoria
6   (
7     nombre text NOT NULL,
8     dominio integer NOT NULL,
9     CONSTRAINT usuarios_auditoria_pkey PRIMARY KEY (nombre, dominio)
10  )
11  WITH (
12    OIDS=FALSE
13  );
14  ALTER TABLE usuarios_auditoria
15    OWNER TO postgres;
16
```

Figura 28. tabla usuarios_obj



	nombre [PK] text	dominio [PK] integer
1	Dario Mera	5
2	Dario Mera	6
3	Dario Mera	7
4	Dario Mera	8
5	Dario Mera	9
6	Dario Mera	10
7	James Caivi	11
8	James Caivi	12
9	James Caivi	13
10	James Caivi	14
11	James Caivi	15
*		

[8] Tabla que relaciona salvaguardas con objetivos de control sal_obj

Conformación:

- **Id_obj:** identificador numérico, parte de llave primaria compuesta, se referencia a objetivos_ctrl.
- **Id_sal:** identificador numérico, parte de llave primaria compuesta, se referencia a salvaguardas.
- **Objetivo:** establecer la relación muchos a muchos entre objetivos de control y salvaguardas, permite determinar que salvaguardas se activan con cada objetivo de control evaluado.
- **Fuente de los datos:** los datos de esta tabla los ingresan los desarrolladores del software, tomados de la norma ISO 27002.

Figura 29. SQL para creación de tabla sal_obj

SQL pane

```
1   -- Table: sal_obj
2
3   -- DROP TABLE sal_obj;
4
5   CREATE TABLE sal_obj
6   (
7     idsal integer NOT NULL,
8     idobj integer NOT NULL,
9     CONSTRAINT sal_obj_pkey PRIMARY KEY (idobj, idsal),
10    CONSTRAINT sal_obj_idobj_fkey FOREIGN KEY (idobj)
11        REFERENCES objetivos_ctrl (id) MATCH SIMPLE
12        ON UPDATE NO ACTION ON DELETE NO ACTION,
13    CONSTRAINT sal_obj_idsal_fkey FOREIGN KEY (idsal)
14        REFERENCES salvaguardas (id) MATCH SIMPLE
15        ON UPDATE NO ACTION ON DELETE NO ACTION
16  )
17  WITH (
18    OIDS=FALSE
19  );
20  ALTER TABLE sal_obj
21    OWNER TO postgres;
22
```

- **Inserción SQL:**

```
INSERT INTO "sal_obj" ("idobj","idsal")
VALUES



(51,1),
(51,2),
(51,3),
(51,4),
(51,5),
(51,6),
(51,7),
(51,8),
(51,9),
(51,10),
(51,11),
(51,12),
(51,13),
(51,14),
(51,15),
(51,16),
(51,17),
...
```

Figura 30: Fragmento de tabla sal_obj

	idsal integer	idobj [PK] integer
1	1	51
2	2	51
3	3	51
4	4	51
5	5	51
6	6	51
7	7	51
8	8	51
9	9	51
10	10	51
11	11	51
12	12	51
13	13	51
14	14	51
15	15	51
16	16	51
17	17	51

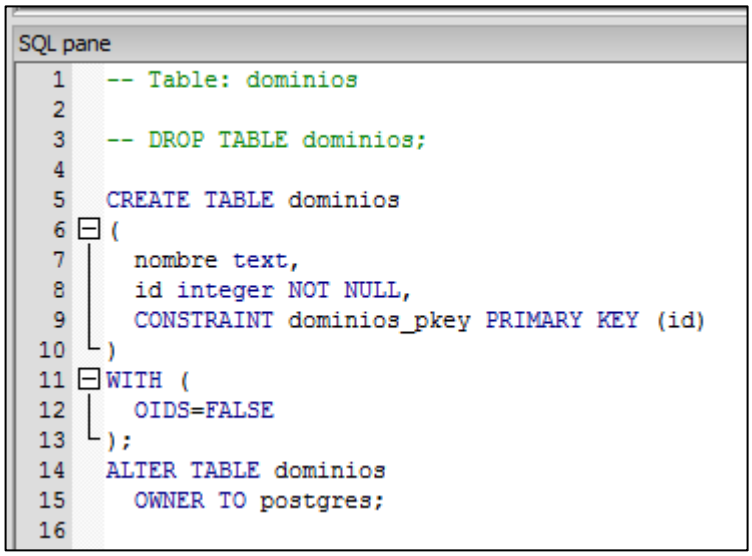
3.2.1.3 Tablas de las normas ISO 27000:

[1] Tabla de Dominios

- **Conformación:**

- **Id:** identificador numérico, llave primaria.
- **Dominios:** tipo char, almacena los nombres de los once dominios de la norma.
- **Objetivo:** almacenar la primera categoría de la norma ISO 27001 contener a la siguiente categoría, permitir elegir los dominios sobre los cuales se trabajara.
- **Fuente de los datos:** los datos para esta tabla se ingresan por los desarrolladores tomados de la norma ISO 27001. (ver figura 31-34)

Figura 31. SQL para creación de tabla dominios



- **Inserción de datos SQL:**

```
INSERT INTO "dominios" ("id","nombre")
VALUES
(5,'Politica de seguridad'),

(6,'Organizacion de la seguridad de la informacion'),

(7,'Gestion de activos');

(8,'Seguidad de los recusos humanos'),

(9,'Seguridad física y ambiental'),


(10,'Gestion de las comunicaciones y las operaciones'),

(11,'Control de acceso'),

(12,'Adquisicion , desarrollo y mantenimiento de los sistemas de
informacion'),

(13,'Gestion de los incidentes de seguridad de la informacion'),

(14,'Gestion de la continuidad comercial'),

(15,'Cumplimiento');
```

Figura 32. Tabla dominios

	nombre text	id [PK] integer
1	Politica de seguridad	5
2	Organizacion de la seguridad de la informacion	6
3	Gestion de activos	7
4	Seguidad de los recusos humanos	8
5	Seguridad física y ambiental	9
6	Gestion de las comunicaciones y las operaciones	10
7	Control de acceso	11
8	Adquisicion , desarrollo y mantenimiento de los sistemas de informacion	12
9	Gestion de los incidentes de seguridad de la informacion	13
10	Gestion de la continuidad comercial	14
11	Cumplimiento	15
*		

[2] Tabla objetivos de control objetivos_ctrl

Conformación:

- **Id:** identificador numérico, llave primaria
- **Nombre:** tipo char almacena los nombres de los objetivos de control
- **Dominio:** tipo numérico, se referencia a dominios
- **Objetivo:** almacenar la segunda categoría de la norma ISO 27001 contener a la siguiente categoría, permitir elegir los objetivos de control sobre los cuales se trabajara, es referenciada por categorías para determinar las áreas a trabajar por categoría, es referenciada por usuarios_auditoría para determinar a qué áreas tienen acceso los usuarios, es referenciada por salvaguardas para determinar las salvaguardas correspondientes a cada objetivo de control.
- **Fuente de los datos:** los datos para esta tabla se ingresan por los desarrolladores tomados de la norma ISO 27001.

Figura 33. SQL para creación de tabla objetivos_ctrl

SQL pane

```sql
-- Table: objetivos_ctrl

-- DROP TABLE objetivos_ctrl;

CREATE TABLE objetivos_ctrl
(
    nombre text,
    dominio integer,
    id integer NOT NULL,
    CONSTRAINT objetivos_crtl_pkey PRIMARY KEY (id),
    CONSTRAINT objetivos_crtl_control_fkey FOREIGN KEY (dominio)
        REFERENCES dominios (id) MATCH SIMPLE
        ON UPDATE NO ACTION ON DELETE NO ACTION
)
WITH (
    OIDS=FALSE
);
ALTER TABLE objetivos_ctrl
    OWNER TO postgres;
```

- **Inserción SQL:**

```sql
INSERT INTO "objetivos_ctrl" ("id","nombre","dominio")
VALUES

--- 5 politica de seguridad
(51,'politica de seguridad de informacion',5),

--- 6 organizacion de la s eguridad de la informacion
(61,'organizacion interna',6),
(62,'entidades externas',6),

---7 gestion de activos
(71,'responsabilidad por los activos',7),
(72,'clasificacion d e la informacion',7),

---8 seguridad de los recursos humanos
(81,'antes del empleo',8),
(82,'durante el empleo',8),
(83,'terminacion o cambio de empleo',8),

---9 seguridad fisica y ambiental
(91,'areas seguras',9),
(92,'seguridad del equipo',9),
....
```

Figura 34. Fragmento de la tabla objetivos_ctrl

	nombre text	dominio integer	id [PK] integer
1	politica de seguridad de informaci	5	51
2	organizacion interna	6	61
3	entidades externas	6	62
4	responsabilidad por los activos	7	71
5	clasificacion d e la informacion	7	72
6	antes del empleo	8	81
7	durante el empleo	8	82
8	terminacion o cambio de empleo	8	83
9	areas seguras	9	91
10	seguridad del equipo	9	92
11	procedimientos y responsabilidades c	10	101
12	gestion de la entrega de servicios	10	102
13	planeacion y aceptacion del sistema	10	103
14	proteccion contra software maliciosc	10	104
15	respaldo backup	10	105

[3] Tabla controles

Conformación:

- **Id:** identificador numérico, llave primaria
- **Nombre:** tipo char almacena los nombres de los controles
- **Dominio:** tipo numérico, se referencia a objetivos_ctrl
- **Valor:** tipo numérico, almacena el valor del porcentaje de cumplimiento luego de la evaluación del cuestionario correspondiente al control
- **Objetivo:** almacenar la tercera categoría de la norma ISO 27001 contener a los cuestionarios correspondientes a cada control, calcular el valor de satisfacción de cada control y activar las amenazas correspondientes, permitir elegir los controles sobre los cuales se trabajara, es referenciada por ame_cont para determinar las amenazas que activa cada control, es referenciada por cuestionarios para determinar a qué control pertenece cada pregunta
- **Fuente de los datos:** los datos para esta tabla se ingresan por los desarrolladores tomados de la norma ISO 27001 excepto el campo valor que se obtiene de la evaluación de cada cuestionario. (ver figura 35-39)

Figura 35. Creación SQL tabla controles

SQL pane

```
1   -- Table: controles
2
3   -- DROP TABLE controles;
4
5   CREATE TABLE controles
6   (
7     nombre text,
8     obj_ctrl integer,
9     id integer NOT NULL,
10    herr_sw text,
11    valor double precision,
12    amenazas_act text,
13    CONSTRAINT controles_pkey PRIMARY KEY (id),
14    CONSTRAINT controles_obj_ctrl_fkey FOREIGN KEY (obj_ctrl)
15        REFERENCES objetivos_ctrl (id) MATCH SIMPLE
16        ON UPDATE NO ACTION ON DELETE NO ACTION
17  )
18  WITH (
19    OIDS=FALSE
20  );
21  ALTER TABLE controles
22    OWNER TO postgres;
23
```

- **Inserción SQL:**

```
INSERT INTO "controles" ("id","nombre","obj_ctrl")
VALUES
--- 5 Politicas de seguridad
---     5.1 Politica  de  seguridad de informacion

(511,'Documentar pollitica de la seguridad de la
informacion',51),

(512,'Revision de la politica de seguridad de la
informacion',51),

--- 6 Organización de la seguridad de la información
---      6.1  Organizacion interna

(611,'Compromiso de la gerencia con la seguridad de la
informacion',61),

(612,'Coordinacion de la seguridad de información',61),

(613,'Asignación de responsabilidades de seguridad de
informacion',61),

(614,'proceso de atorización para los medios de procesamiento de
información',61),
...
```

Figura 36. Fragmento de tabla controles

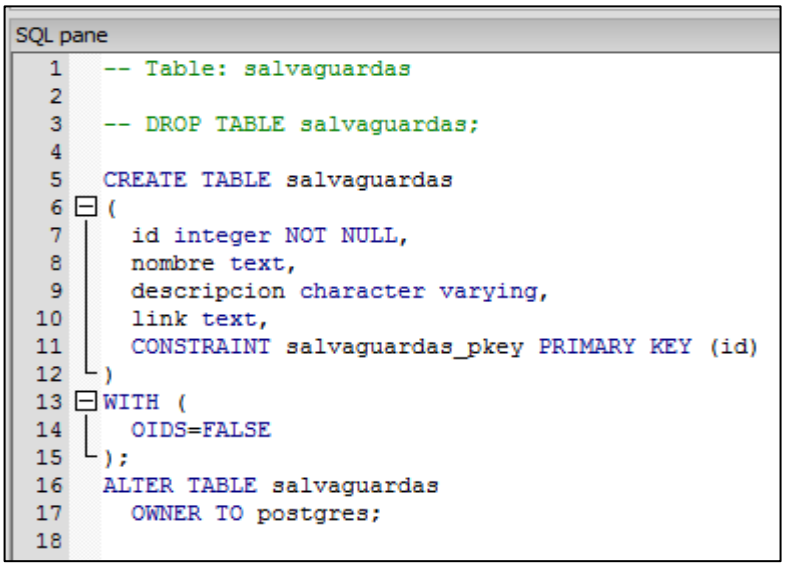
	nombre text	obj_ctrl integer	id [PK] integer	valor double precis
1	Documentar	51	511	76.66666666
2	Revision de	51	512	56.92307692
3	Compromiso	61	611	0
4	Coordinacio	61	612	0
5	Asignación	61	613	0
6	proceso de	61	614	0
7	Acuerdos de	61	615	0
8	Contacto co	61	616	0
9	Contacto co	61	617	0
10	Revision in	61	618	0
11	Identificac	62	621	68.33333333
12	Tratamiento	62	622	85.33333333
13	Tratamiento	62	623	66.66666666
14	Inventarios	71	711	71.42857142
15	Propiedad d	71	712	0
16	Uso aceptab	71	713	90
17	Lineamiento	72	721	0

[4] Tabla Salvaguardas

- **Conformación:**

- **Id:** identificador numérico, llave primaria
- **Nombre:** tipo char, almacena los nombres de las salvaguardas
- **Descripción:** tipo char, almacena la descripción presente en la norma.
- **Link:** tipo char, almacena el URL de cada salvaguarda.
- **Objetivo:** almacenar las salvaguardas de la norma ISO 27002, contener las URL's de las soluciones recomendadas.
- **Fuente de los datos:** los datos de esta tabla son ingresados por los desarrolladores del software, tomados de la norma ISO 27002. (ver figura 37-38)

Figura 37. SQL para creación de la tabla salvaguardas



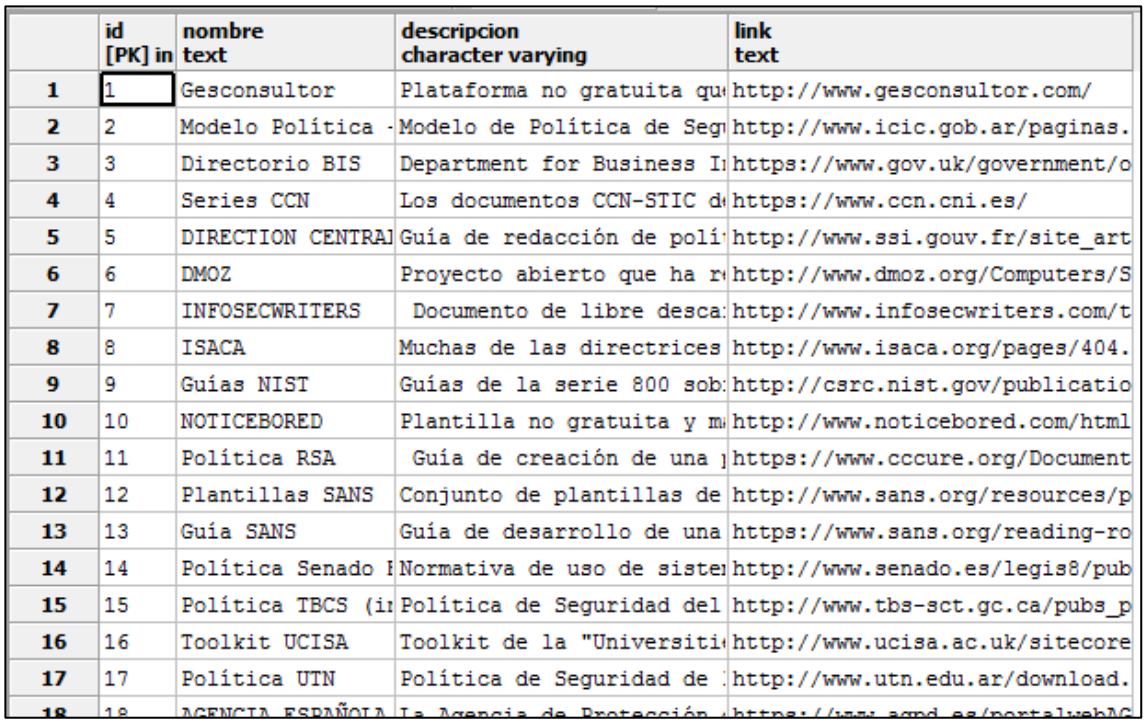
- **Inserción SQL:**

```
INSERT INTO "salvaguardas" ("id","nombre","descripcion","link")
VALUES

(1,'Gesconsultor','Plataforma no gratuita que integra todos los
elementos necesarios para la implantación y gestión completa del
ciclo de vida de un SGSI, así como otros requisitos de
cumplimiento de aspectos legales, normativos, contractuales y con
terceras partes que sean de aplicación al Alcance del Sistema de
Gestión. El portal web aporta información de libre disposición
sobre SGSI, Esquema Nacional de Seguridad y otros marcos y
políticas relevantes y cómo deben ser
tratados.','http://www.gesconsultor.com/'),
---
(2,'Modelo Política - ICIC','Modelo de Política de Seguridad de
la Información para la Administración pública de Argentina,
basado en ISO 27002. Establece directrices para cada uno de los
controles.','http://www.icic.gob.ar/paginas.dhtml?pagina=195'),
---
(3,'Directorio BIS','Department for Business Innovation and
Skills (apoyado por el Departamento de Industria y Comercio del
Reino Unido) dispone de diversos documentos relacionados con la
seguridad de la información, incluídas guías de desarrollo de
políticas de seguridad y diversos checklists (inglés) con el
objetivo de lograr la protección y desarrollo económico de las
empresas.','https://www.gov.uk/government/organisations/departmen
t-for-business-innovation-skills'),
---

....
```

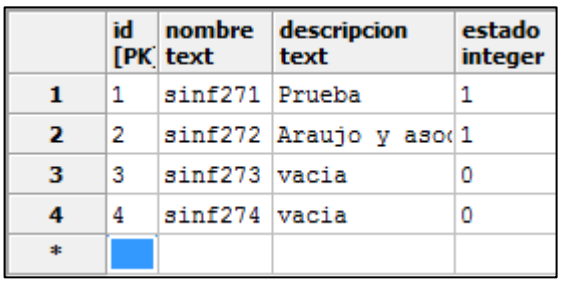
Figura 38. Fragmento de la tabla salvaguardas



	id [PK] in	nombre text	descripcion character varying	link text
1	1	Gesconsultor	Plataforma no gratuita qu	http://www.gesconsultor.com/
2	2	Modelo Política -	Modelo de Política de Seg	http://www.icic.gob.ar/paginas.
3	3	Directorio BIS	Department for Business I	https://www.gov.uk/government/o
4	4	Series CCN	Los documentos CCN-STIC d	https://www.ccn.cni.es/
5	5	DIRECTION CENTRAI	Guía de redacción de polí	http://www.ssi.gouv.fr/site_art
6	6	DMOZ	Proyecto abierto que ha r	http://www.dmoz.org/Computers/S
7	7	INFOSECWRITERS	Documento de libre desca	http://www.infosecwriters.com/t
8	8	ISACA	Muchas de las directrices	http://www.isaca.org/pages/404.
9	9	Guías NIST	Guías de la serie 800 sob	http://csrc.nist.gov/publicatio
10	10	NOTICEBORED	Plantilla no gratuita y m	http://www.noticebored.com/html
11	11	Política RSA	Guía de creación de una	https://www.cccure.org/Document
12	12	Plantillas SANS	Conjunto de plantillas de	http://www.sans.org/resources/p
13	13	Guía SANS	Guía de desarrollo de una	https://www.sans.org/reading-ro
14	14	Política Senado E	Normativa de uso de siste	http://www.senado.es/legis8/pub
15	15	Política TBCS (ir	Política de Seguridad del	http://www.tbs-sct.gc.ca/pubs_p
16	16	Toolkit UCISA	Toolkit de la "Universiti	http://www.ucisa.ac.uk/sitecore
17	17	Política UTN	Política de Seguridad de	http://www.utn.edu.ar/download.
18	18	AGENCIA ESPAÑOLA	La Agencia de Protección	https://www.agpd.es/portalwebAG

3.2.2 Base de datos para diferentes proyectos. Se creó una base de datos con una sola tabla que agrupa los datos de los diferentes proyectos que se manejen en el software, en la columna nombre va el nombre de una base de datos con la estructura explicada anteriormente, para crear un nuevo proyecto se usa un base de datos con esta estructura más, sin datos de auditoría, usuarios, activos, o evaluaciones realizadas, es decir solo las tablas y datos de Magerit y de la norma ISO 27000, en este caso una base de datos tiene el estado 0, pero al ser usada e insertarle datos el estado se pone en 1. (ver figura 39)

Figura 39. Base de datos administradora de proyectos

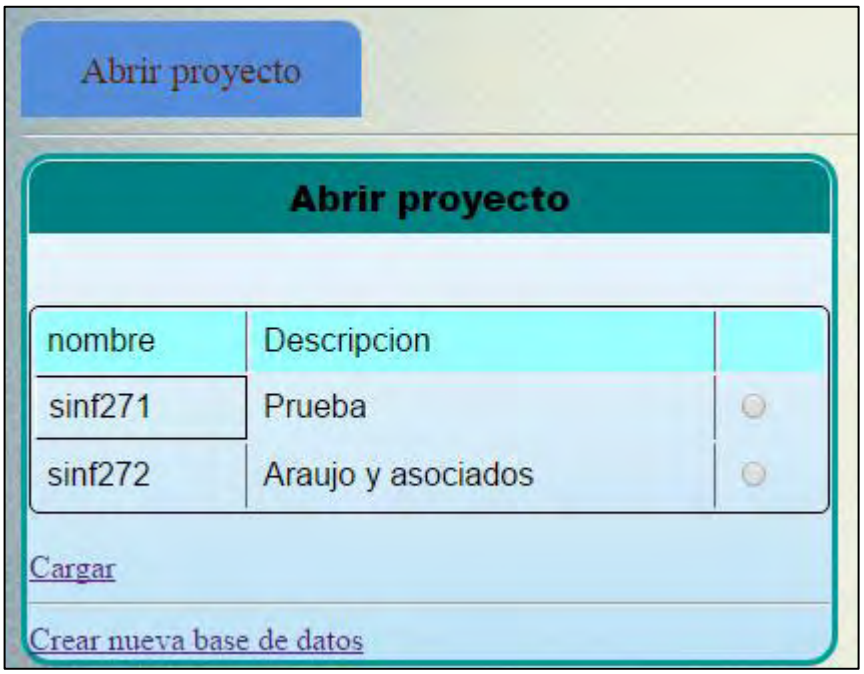


	id [PK	nombre text	descripcion text	estado integer
1	1	sinf271	Prueba	1
2	2	sinf272	Araujo y aso	1
3	3	sinf273	vacia	0
4	4	sinf274	vacia	0
*				

3.2.3 Diseño de interfaces:

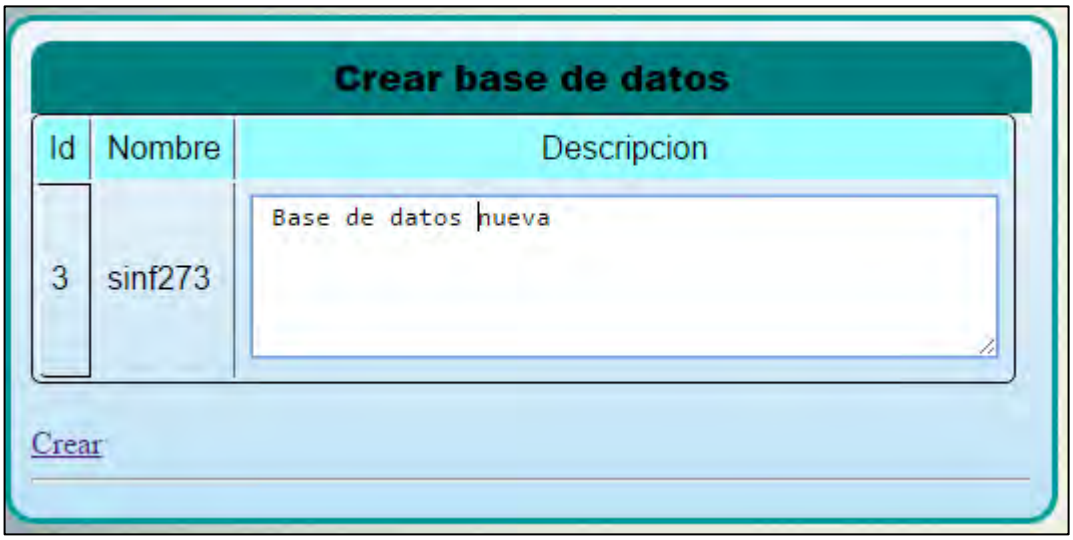
Cargar nuevo proyecto. La primera acción a realizar en el software es abrir un proyecto, esto se puede hacer de dos maneras diferentes, en la primera interfaz se muestran los proyectos que se están trabajando en el momento. (ver figura 40)

Figura 40. Interfaz con proyectos en proceso



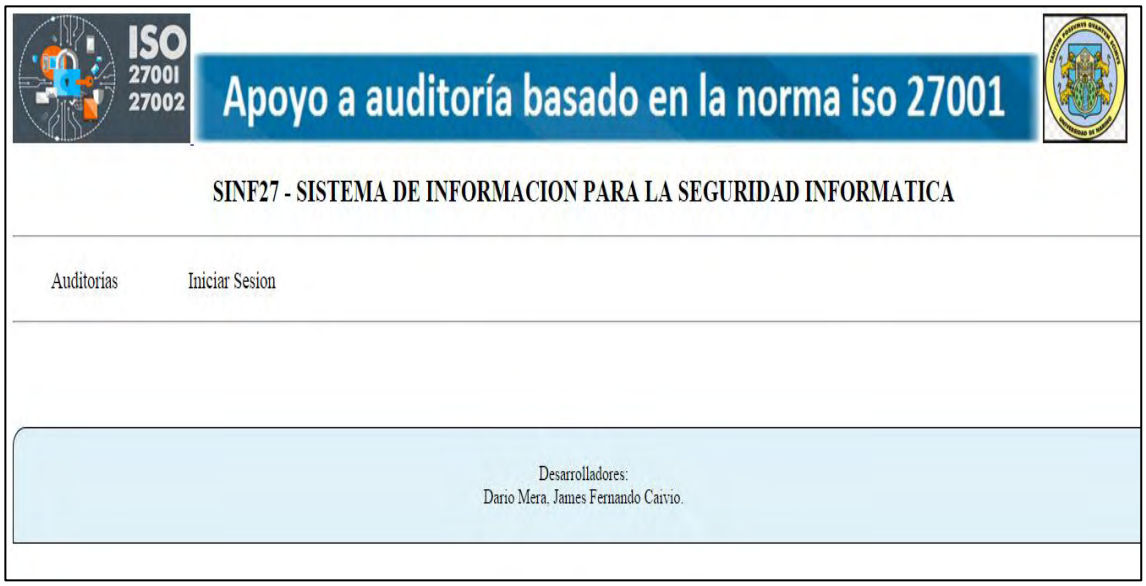
En caso de precisar crear un nuevo proyecto hay que crear una nueva base de datos, y poner una descripción de ella. (ver figura 41)

Figura 41. Crear base de datos nueva



Interfaces pantalla de inicio para un proyecto creado. En este aparte se muestra el diseño de las interfaces necesarias para ingresar los datos de una auditoría, de los colaboradores, para crear y registrar usuarios y asignarles a estos usuarios las áreas a las cuales tendrán acceso en el sistema. (ver figura 42)

Figura 42. Pantalla de inicio

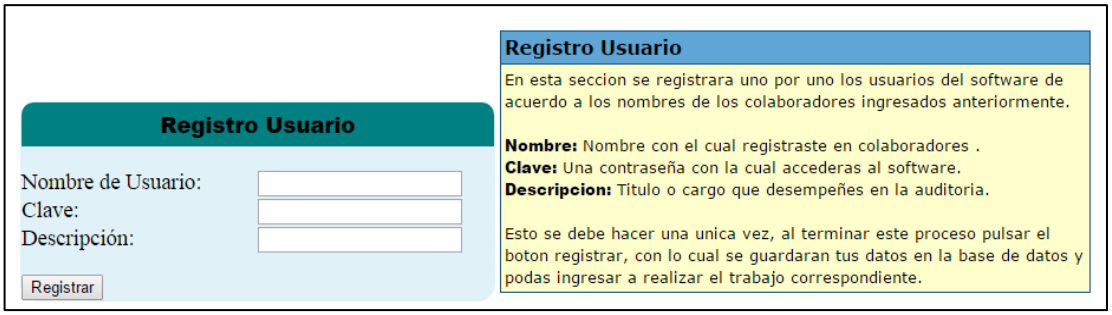


Este primer contacto con el software debe dar acceso a dos formularios iniciales:

Formulario iniciar sesión: esta sección contiene dos subformularios los cuales permiten registrar un nuevo usuario o ingresar con uno existente.

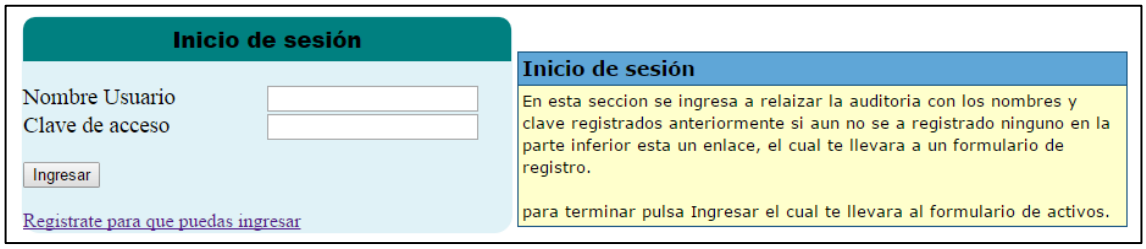
Registrar usuario nuevo: los datos ingresados en este formulario se recogen en la tabla usuarios, y se usaran posteriormente para validar o denegar un ingreso, esta sección no da ingreso al software, solo registra el usuario, para ello es necesario acceder a la siguiente sección. (ver figura 43)

Figura 43. Formulario registrar usuario



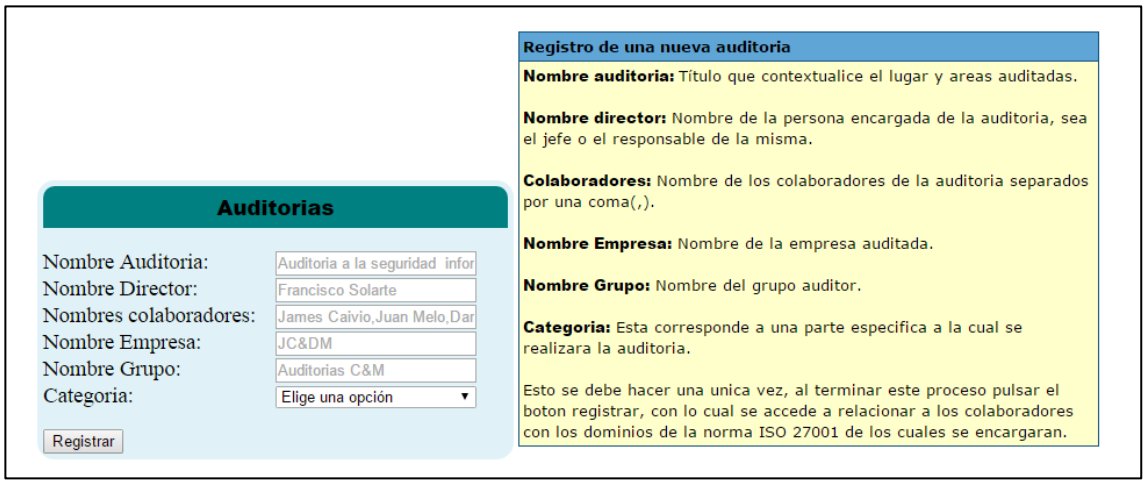
Inicio de sesión: verificar datos ingresados anteriormente para permitir ingresar a un usuario. (ver figura 44)

Figura 44. Inicio de sesión



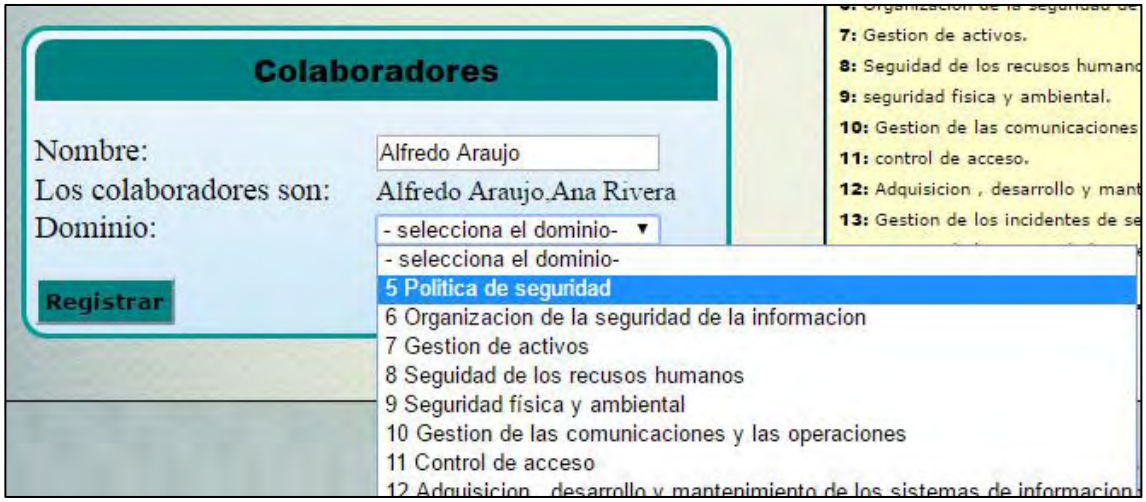
Formulario auditorías: la principal función de este formulario debe ser gestionar los datos generales de la auditoría, y guardarlos en una tabla, las columnas colaboradores y director crean los usuarios que podrán acceder a una auditoría en particular. (ver figura 45)

Figura 45. Formulario auditorías



Formulario colaboradores: posterior al registro de la auditoría es necesario asignar y delimitar las áreas a las que los usuarios tendrán acceso, para este fin está el formulario de colaboradores en el cual se debe elegir uno a uno los colaboradores y asignarles su área de trabajo. Estos colaboradores se listaran acorde a lo ingresado anteriormente y se listaran para guiar al usuario. (ver figura 46)

Figura 46. Formulario colaboradores



Diseño de la interfaz de gestión de activos:

Clasificación de los activos: obtenido del modelo de activos de Magerit el diseño de la gestión de los mismos para este software se basa en la categorización de cada uno dentro de alguno de los tipos presentes en Magerit, lo cual permite establecer la importancia y el valor de cada activo para la organización

Activos esenciales

Información:

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos.

Servicios:

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

Activos comunes

Datos:

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Claves criptográficas:

La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

Aplicaciones informáticas:

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

Equipamiento informático hardware:

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Redes de comunicación:

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

Soportes de información:

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

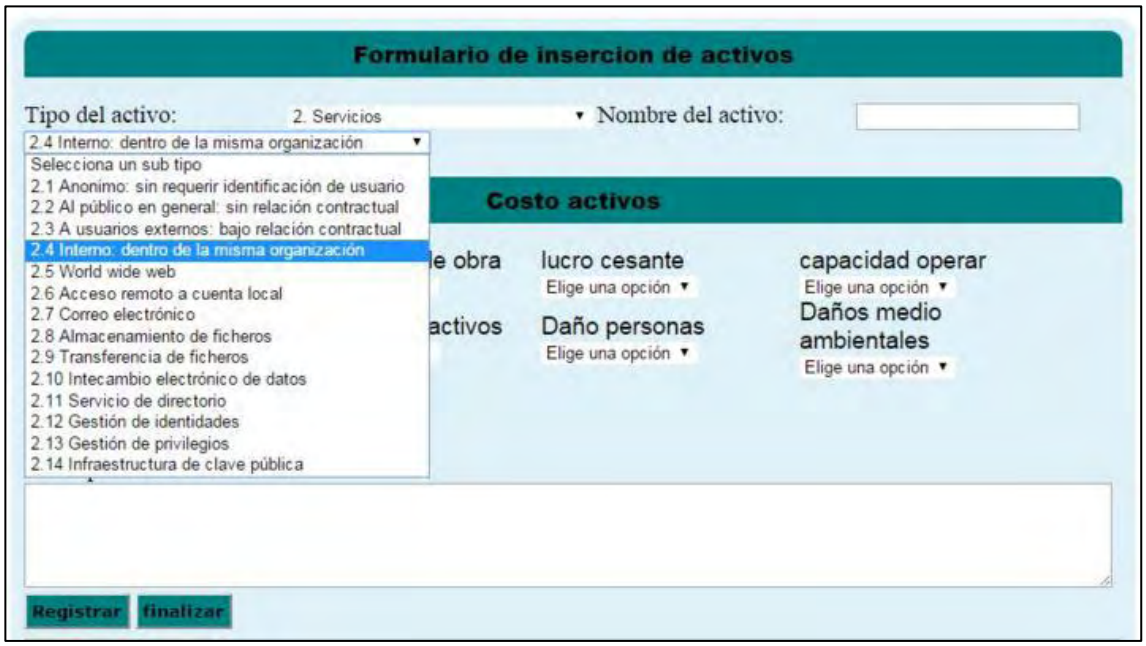
Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Instalaciones: en este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

Personal: en este epígrafe aparecen las personas relacionadas con los sistemas de información. [5] (ver figura 47)

Figura 47. Formulario de gestion de activos



- **Valor de los activos**

En este formulario también es importante obtener del usuario el valor de un activo, este valor es obtenido en Magerit de la aplicación de un algoritmo que contempla varias dimensiones del costo de un activo y a partir de ahí calcula el costo total, para cada dimensión el usuario podrá escoger un nivel de uno a cinco y el software automáticamente calculara el valor total.

Las dimensiones del costo del activo son:

- Costo de reposición: adquisición e instalación
- Costo mano de obra: (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos

- Capacidad de operar : confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento: sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos: propios a ajenos traducido en el costo de ellos
- Daño a personas
- Daños medio ambientales [5]

Diligenciamiento de las dimensiones de valor de activos

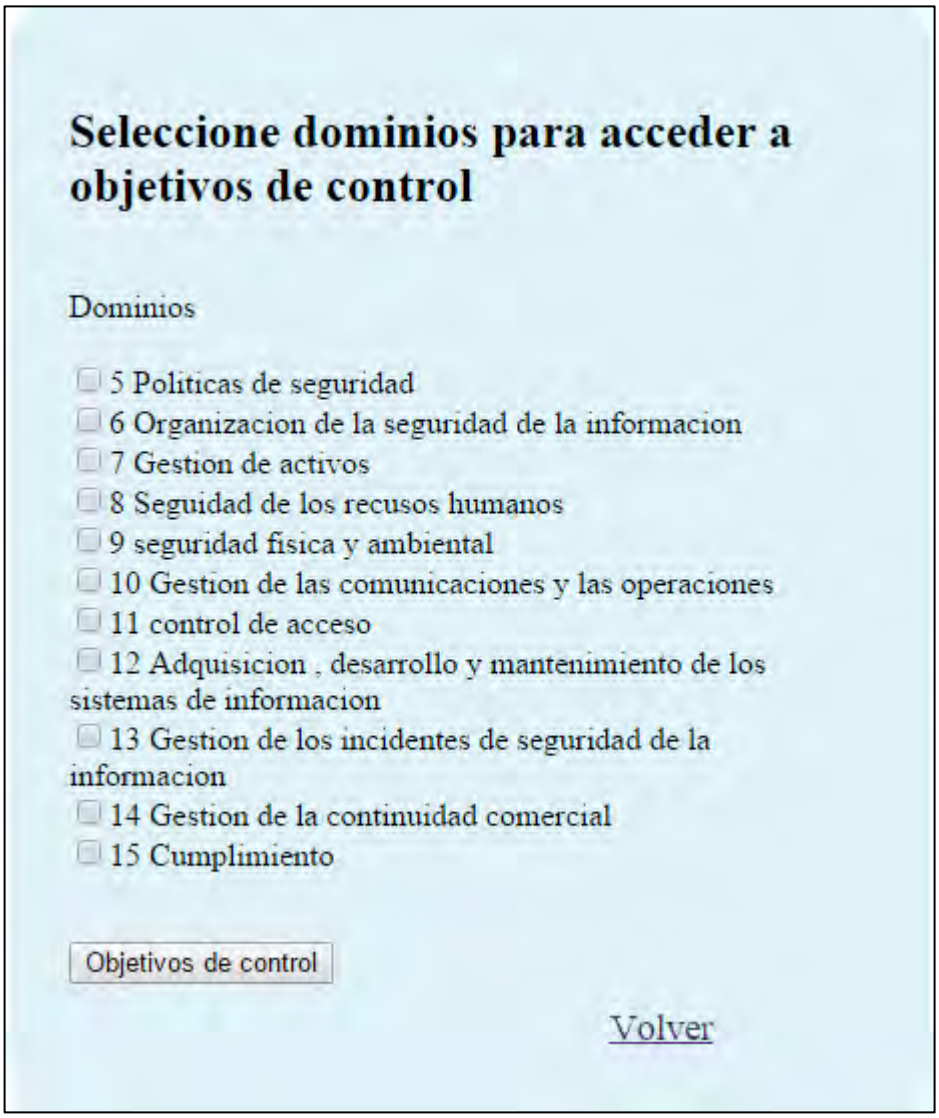
Para elegir la categoría que tenga cada dimensión en cuanto a su valor se debe tener en cuenta que el valor de cada activo es relativo al tamaño o valor total de los activos de la organización, es decir, no se puede establecer una escala numérica en la cual un valor absoluto sea suficiente para categorizar el valor dentro de un nivel ya que, por ejemplo un activo de un costo de veinte millones tendrá una categoría de valor cinco para una empresa pequeña y puede que sea dos o incluso uno dependiendo de lo grande de la organización.

También es importante denotar que dentro de la metodología de Magerit este valor se usa para determinar el impacto del daño de un activo según lo que tenga este en las 8 dimensiones de valor, en este orden de ideas es importante pensar en el impacto de cada dimensión según el activo para la organización.

Diseño de las interfaces de la norma Iso27001. Para mostrar fácil e intuitiva mente la norma al usuario auditor se agrupa el diseño de esta en los niveles de la norma de tal forma que se puedan ir desagregando una a una hasta llegar a los cuestionarios con ayuda del uso de casillas de verificación.

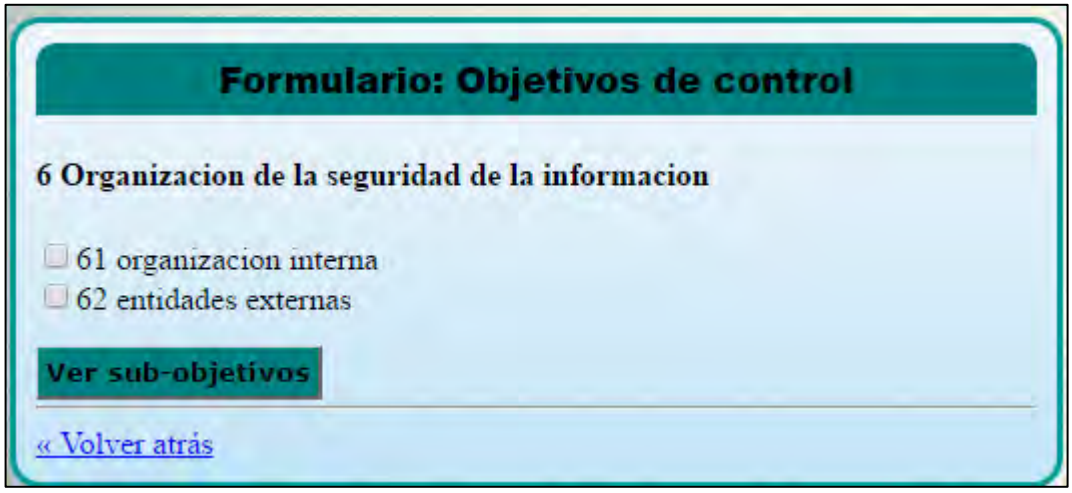
Dominios: se presenta una lista con los once dominios de la norma. (ver figura 48)

Figura 48. Diseño de la lista de dominios



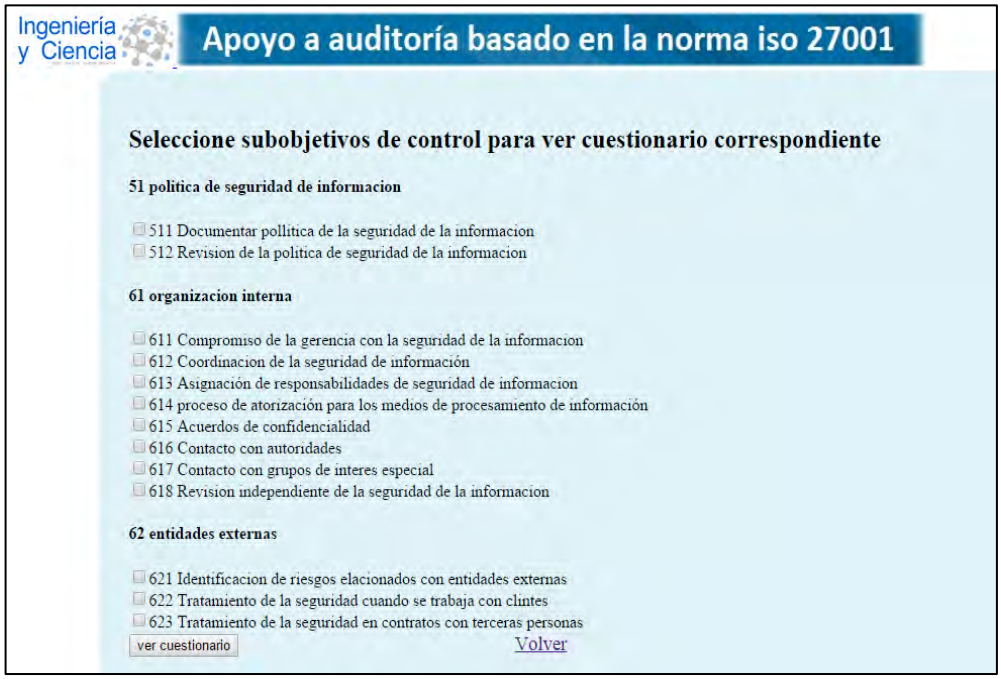
Objetivos de control: se presenta una lista con los objetivos de control. (ver figura 49)

Figura 49: Objetivos de control en el software



Sub objetivos de control: se presenta una lista con los sub objetivos de control. (ver figura 50)

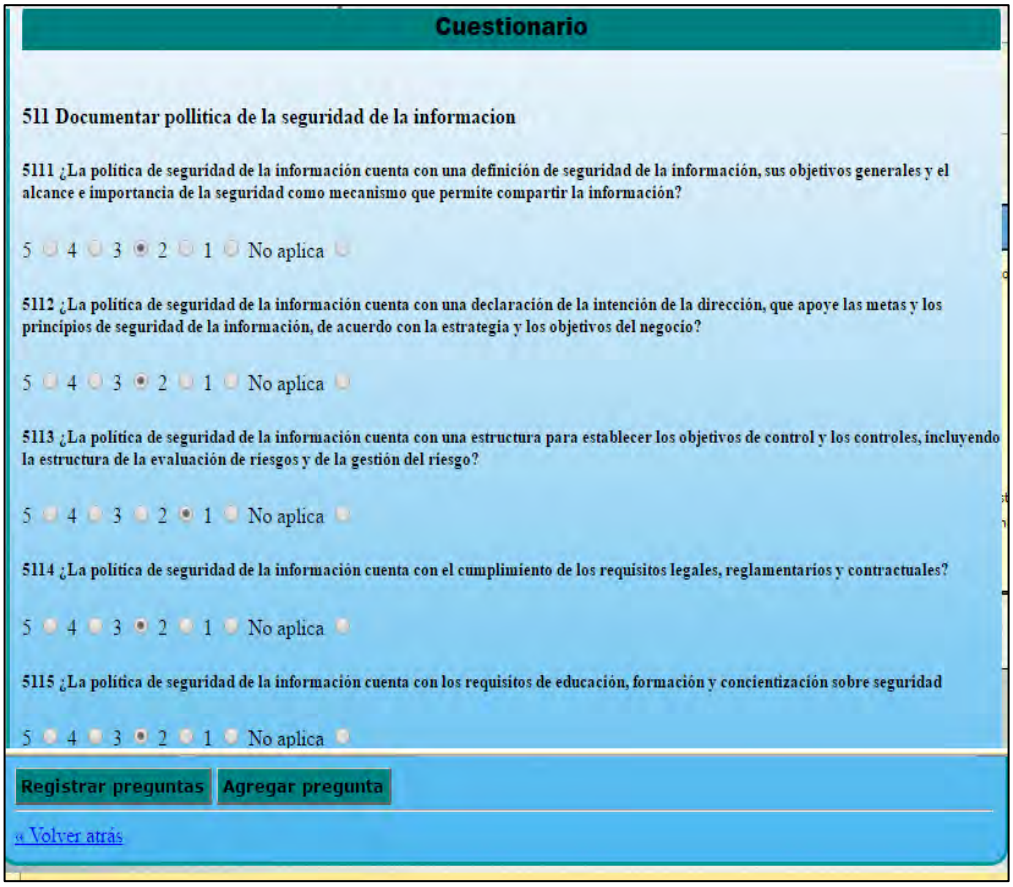
Figura 50. Diseño de lista de sub objetivos de control



Cuestionarios: los cuestionarios dan la facilidad al usuario de ser diligenciados en niveles de 1 a 5, lo que permite al auditor acomodarse de una manera flexible a cualquier tipo de herramienta para responderlos, sea entrevista, checklist, preguntas cerradas o abiertas etc. Y ubicar su respuesta dentro el nivel apropiado el cual será el valor que se registre en la base de datos.

También se podrá responder un ítem con la opción no aplica, lo que anula la pregunta, y se puede agregar más preguntas al banco de preguntas que tiene el software. (ver figura 51)

Figura 51. Diseño de lista de respuesta de cuestionarios



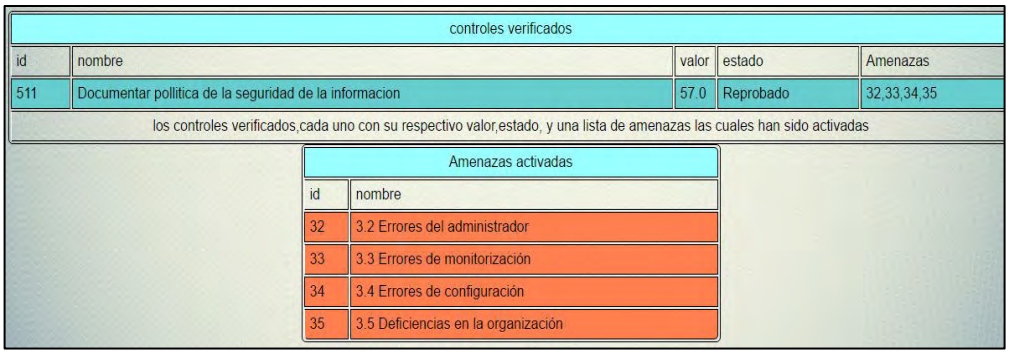
Diseño de las interfaces de gestión de riesgos. El diseño de la gestión de riesgos busca automatizar dentro del software la forma como maneja los riesgos Magerit, lo primero que se hizo para la gestión de riesgos está contemplado en el diseño de gestión de activos ya que el valor e importancia de estos es un criterio importante en Magerit para determinar el impacto de la activación de una amenaza.

Luego de ello hay que seguir la estructura de la norma ISO, hasta responder los cuestionarios de evaluación.

Una vez se han respondido los cuestionarios se sigue este algoritmo:

- Obtención de valor de cumplimiento de cada cuestionario relacionado con su sub objetivo de control correspondiente
- Verificación de cada control, si es mayor a setenta es aprobado de lo contrario es reprobado
- Verificación y activación de las amenazas para cada control en caso de ser reprobado. (ver figura 52)

Figura 52. Controles evaluados y amenazas activadas



Ingreso de la probabilidad para cada amenaza activada. El usuario deberá elegir a probabilidad de ocurrencia de entre tres categorías, siendo tres la máxima probabilidad, y uno la mínima, para ello se deberá establecer una escala de eventos en un tiempo determinado o en caso de existir, acudir a los registros de la organización. (ver figura 53)

Figura 53. Formulario de ingreso de probabilidades

Cálculo del impacto: luego de contar con la lista de amenazas activadas por un control, se evalúan los activos de la empresa que se afectan con cada amenaza, y se procede a aplicar los siguientes criterios:

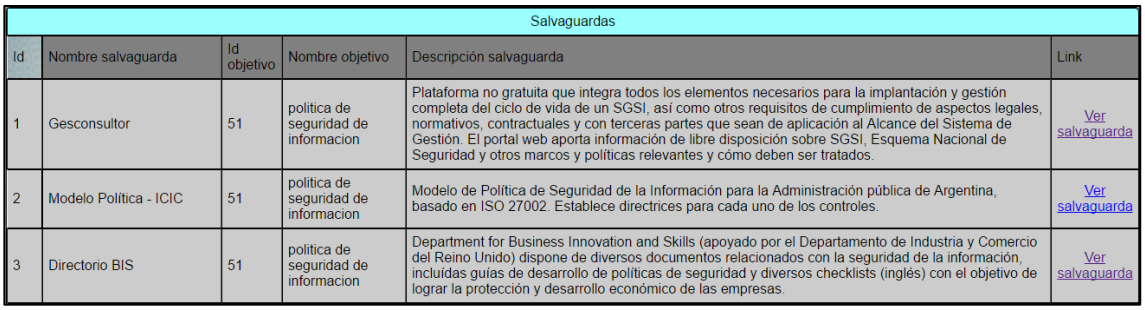
- El porcentaje de activos afectados por una amenaza sobre la totalidad de los activos
- El valor promedio de los activos afectados
- El porcentaje de activos esenciales, es decir de información o servicios, afectados sobre el total de activos afectados. (ver figura 54)

Figura 54. Matriz de riesgo

nombre	Probabilidad	Impacto
3.2 Errores del administrador	2	2
3.3 Errores de monitorización	2	3
3.4 Errores de configuración	2	3
3.5 Deficiencias en la organización	2	1

Determinar las salvaguardas correspondientes según los objetivos de control correspondientes. Cada salvaguarda fue tomada de la norma de salvaguardas anexa a la ISO 27001, llamada ISO 27002, y tiene un link que lleva a la solución propuesta. (ver figura 55)

Figura 55. Formulario para elección de salvaguardas



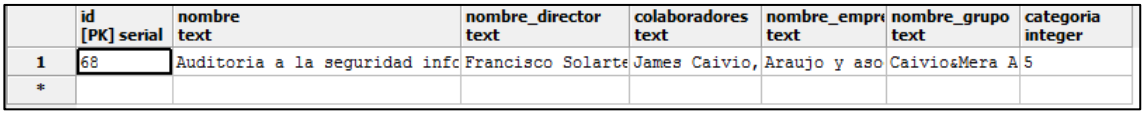
Salvaguardas

Id	Nombre salvaguarda	Id objetivo	Nombre objetivo	Descripción salvaguarda	Link
1	Gesconsultor	51	politica de seguridad de informacion	Plataforma no gratuita que integra todos los elementos necesarios para la implantación y gestión completa del ciclo de vida de un SGSI, así como otros requisitos de cumplimiento de aspectos legales, normativos, contractuales y con terceras partes que sean de aplicación al Alcance del Sistema de Gestión. El portal web aporta información de libre disposición sobre SGSI, Esquema Nacional de Seguridad y otros marcos y políticas relevantes y cómo deben ser tratados.	Ver salvaguarda
2	Modelo Política - ICIC	51	politica de seguridad de informacion	Modelo de Política de Seguridad de la Información para la Administración pública de Argentina, basado en ISO 27002. Establece directrices para cada uno de los controles.	Ver salvaguarda
3	Directorio BIS	51	politica de seguridad de informacion	Department for Business Innovation and Skills (apoyado por el Departamento de Industria y Comercio del Reino Unido) dispone de diversos documentos relacionados con la seguridad de la información, incluídas guías de desarrollo de políticas de seguridad y diversos checklists (inglés) con el objetivo de lograr la protección y desarrollo económico de las empresas.	Ver salvaguarda

3.2.4 Diseño de reportes. El diseño los reportes se basa en la organización de la información de las bases de datos, se hacen consultas de tablas específicas para mostrar datos que el software ha calculado y se han insertado en él, además se implementará para cada reporte la funcionalidad de exportarlo a formato PDF.

Diseño de reporte de datos de auditoría. En este reporte se conjugaran los datos de la tabla auditoría y de la tabla usuarios_auditorías, para que el usuario pueda tener la información general de cada auditoría que trabaje. (ver figura 56)

Figura 56. Datos de tabla auditorías para reporte



	id [PK] serial	nombre text	nombre_director text	colaboradores text	nombre_empr text	nombre_grupo text	categoria integer
1	68	Auditoria a la seguridad infc	Francisco Solarte	James Caivio,	Araujo y aso	Caivio&Mera A	5
*							

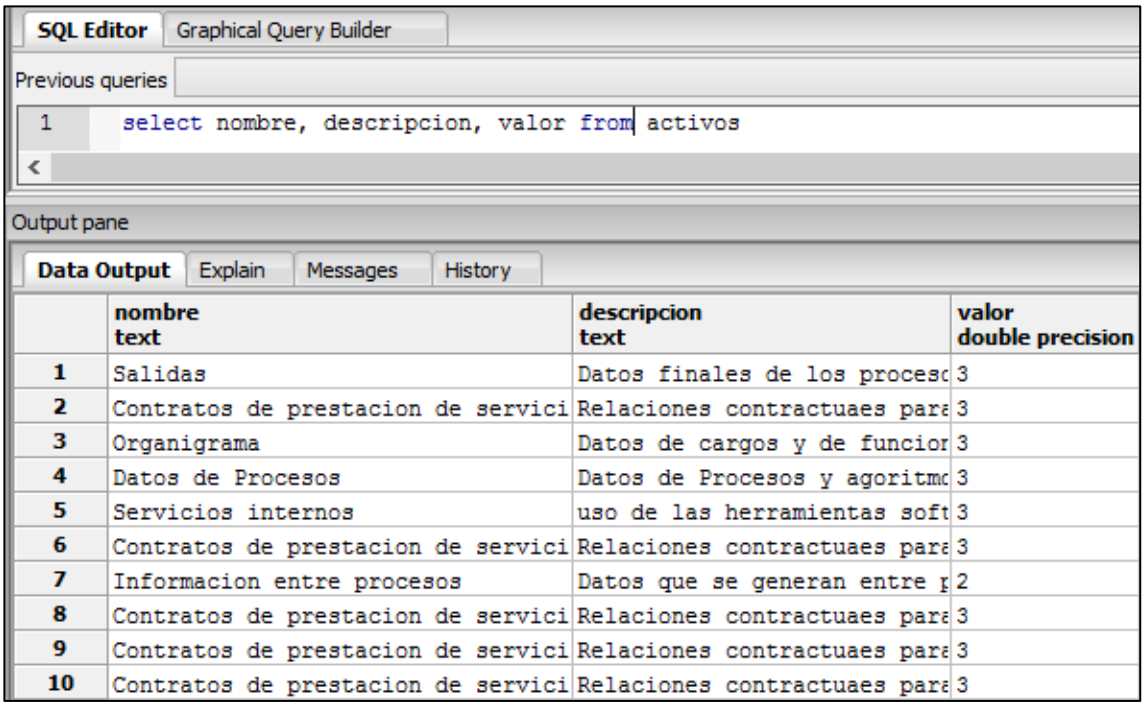
Figura 57. Datos de tabla usuarios auditoría para reporte

	nombre [PK] text	dominio [PK] integer
1	Dario Mera	5
2	Dario Mera	6
3	Dario Mera	7
4	Dario Mera	8
5	Dario Mera	9
6	Dario Mera	10
7	James Caivio	11
8	James Caivio	12
9	James Caivio	13
10	James Caivio	14
11	James Caivio	15
*		

Se ejecutarán select de las dos tablas anteriores y se organizarán para ser mostrados en el software.

Diseño de reporte de datos de activos. Consulta de la tabla activos para ser organizada y mostrada en el software. (ver figura 58)

Figura 58. Selección de la tabla activos en pgadmin para el reporte



SQL Editor | Graphical Query Builder

Previous queries

```
1   select nombre, descripcion, valor from activos
```

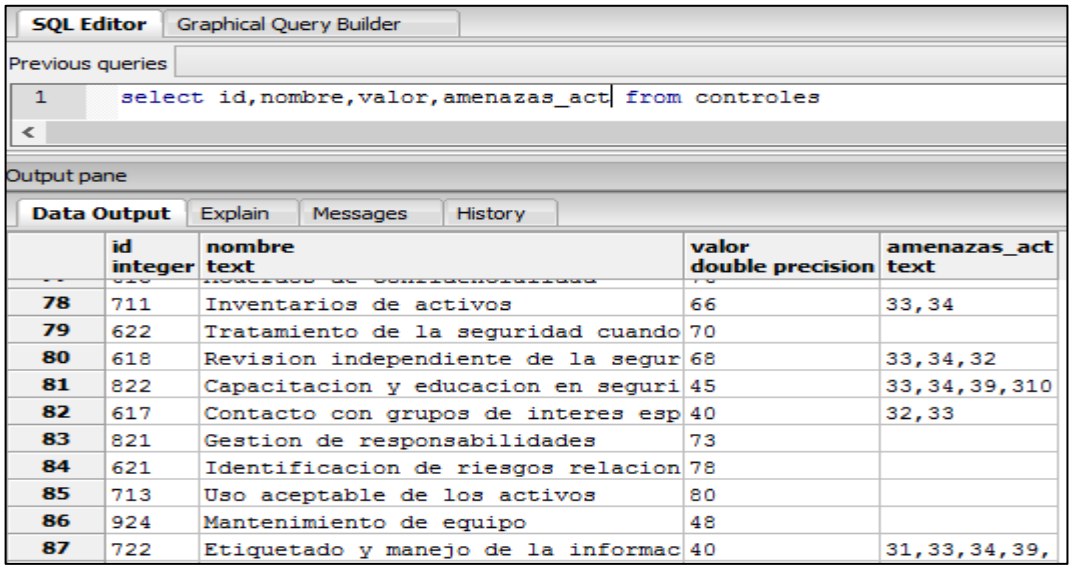
Output pane

Data Output | Explain | Messages | History

	nombre text	descripcion text	valor double precision
1	Salidas	Datos finales de los proces	3
2	Contratos de prestacion de servici	Relaciones contractuaes para	3
3	Organigrama	Datos de cargos y de funcior	3
4	Datos de Procesos	Datos de Procesos y agoritmc	3
5	Servicios internos	uso de las herramientas soft	3
6	Contratos de prestacion de servici	Relaciones contractuaes para	3
7	Informacion entre procesos	Datos que se generan entre p	2
8	Contratos de prestacion de servici	Relaciones contractuaes para	3
9	Contratos de prestacion de servici	Relaciones contractuaes para	3
10	Contratos de prestacion de servici	Relaciones contractuaes para	3

Diseño de reporte de datos de controles. Consulta en tabla controles para ser organizada y mostrada en el software. (ver figura 59)

Figura 59. Selección de tabla controles en pgadmin para el reporte



SQL Editor | Graphical Query Builder

Previous queries

```
1   select id,nombre,valor,amenazas_act from controles
```

Output pane

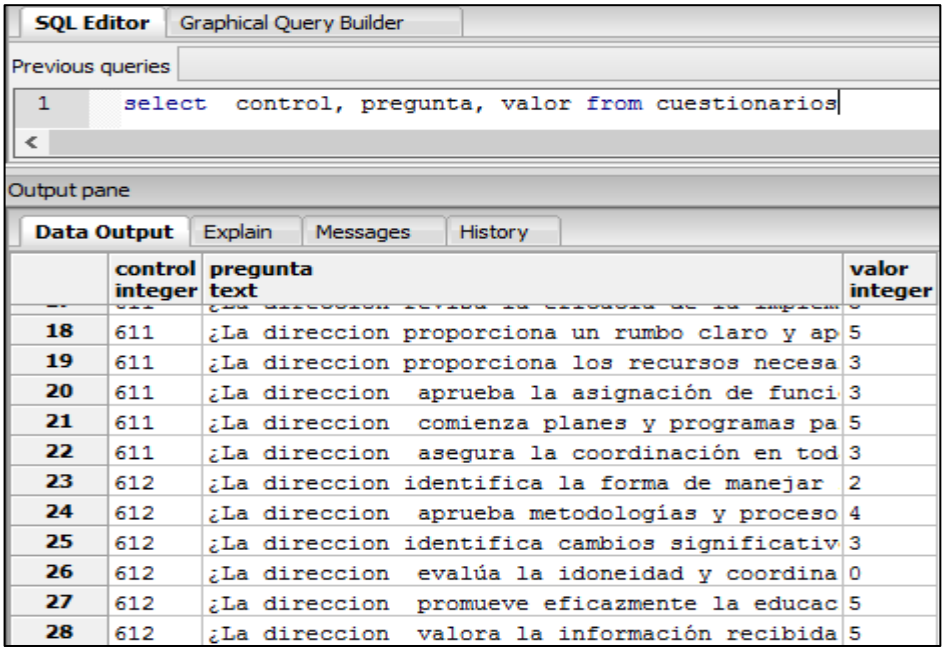
Data Output | Explain | Messages | History

	id integer	nombre text	valor double precision	amenazas_act text
78	711	Inventarios de activos	66	33,34
79	622	Tratamiento de la seguridad cuando	70	
80	618	Revision independiente de la segur	68	33,34,32
81	822	Capacitacion y educacion en seguri	45	33,34,39,310
82	617	Contacto con grupos de interes esp	40	32,33
83	821	Gestion de responsabilidades	73	
84	621	Identificacion de riesgos relacion	78	
85	713	Uso aceptable de los activos	80	
86	924	Mantenimiento de equipo	48	
87	722	Etiquetado y manejo de la informac	40	31,33,34,39,

Diseño de reporte de cuestionarios. Consulta en tabla controles para ser organizada y mostrada en el software

Se mostrara de cada control su respectivo cuestionario. (ver figura 60)

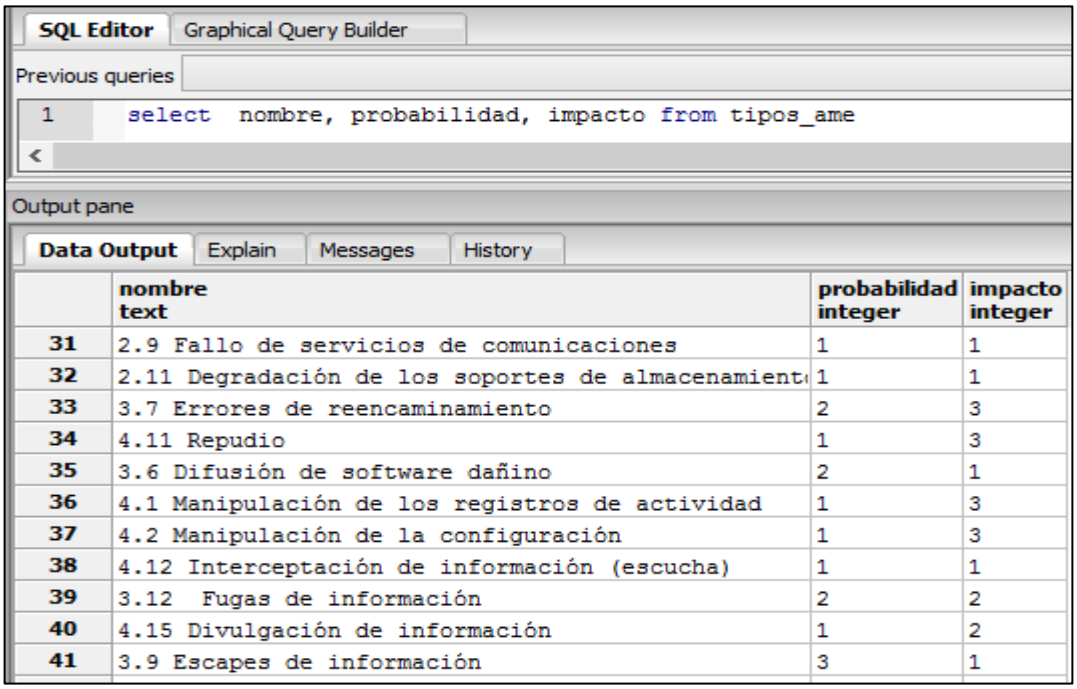
Figura 60. Selección de tabla cuestionarios en pgadmin para el reporte



	control integer	pregunta text	valor integer
18	611	¿La direccion proporciona un rumbo claro y ap	5
19	611	¿La direccion proporciona los recursos necesa	3
20	611	¿La direccion aprueba la asignación de funci	3
21	611	¿La direccion comienza planes y programas pa	5
22	611	¿La direccion asegura la coordinación en tod	3
23	612	¿La direccion identifica la forma de manejar	2
24	612	¿La direccion aprueba metodologías y proceso	4
25	612	¿La direccion identifica cambios significativ	3
26	612	¿La direccion evalúa la idoneidad y coordina	0
27	612	¿La direccion promueve eficazmente la educac	5
28	612	¿La direccion valora la información recibida	5

Diseño de reporte de matriz de riesgos. Consulta en tabla tipos-Ame luego de calcular impacto e ingresar probabilidad para ser organizada y mostrada en el software. (ver figura 61)

Figura 61. Selección de tabla tipos_ame en pgadmin para el reporte



SQL Editor | Graphical Query Builder

Previous queries

```
1   select  nombre, probabilidad, impacto from tipos_ame
```

Output pane

Data Output | Explain | Messages | History

	nombre text	probabilidad integer	impacto integer
31	2.9 Fallo de servicios de comunicaciones	1	1
32	2.11 Degradación de los soportes de almacenament	1	1
33	3.7 Errores de reencaminamiento	2	3
34	4.11 Repudio	1	3
35	3.6 Difusión de software dañino	2	1
36	4.1 Manipulación de los registros de actividad	1	3
37	4.2 Manipulación de la configuración	1	3
38	4.12 Interceptación de información (escucha)	1	1
39	3.12 Fugas de información	2	2
40	4.15 Divulgación de información	1	2
41	3.9 Escapes de información	3	1

Diseño de reporte de salvaguardas. Consulta en tabla salvaguardas para ser organizada y mostrada en el software. (ver figura 62)

Figura 62. Selección de tabla salvaguardas en pgadmin para el reporte

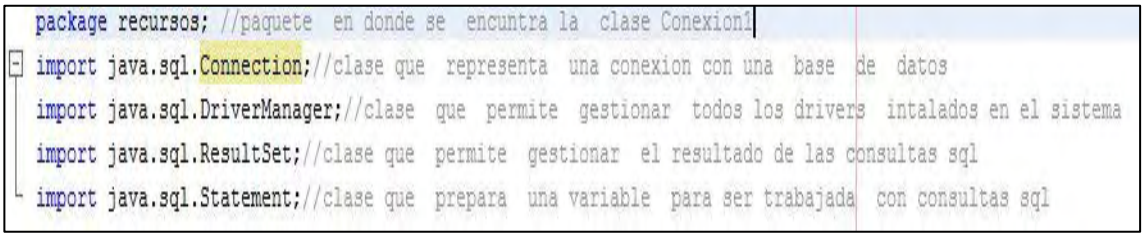
	id [PK] integ	nombre text	descripcion character varying	link text
1	1	Gesconsultor	Plataforma no gr	http://www.gesconsult
2	2	Modelo Política	Modelo de Políti	http://www.icic.gob.a
3	3	Directorio BIS	Department for E	https://www.gov.uk/go
4	4	Series CCN	Los documentos C	https://www.ccn.cni.e
5	5	DIRECTION CENTR	Guía de redacció	http://www.ssi.gouv.f
6	6	DMOZ	Proyecto abierto	http://www.dmoz.org/C
7	7	INFOSECWRITERS	Documento de li	http://www.infosecwri
8	8	ISACA	Muchas de las di	http://www.isaca.org/
9	9	Guías NIST	Guías de la seri	http://csrc.nist.gov/

3.3 ETAPA DE IMPLEMENTACIÓN

Luego de la creación de las tablas y la inserción de sus correspondientes datos, se implementó el código necesario para ingresar los datos de parte de los usuarios, para restringir o dar acceso a las áreas del sistema a los usuarios, y para realizar los cálculos correspondientes a la gestión de riesgos.

3.3.1 Conexión de bases de datos con el software. Esta conexión se realizó a través de una clase que se encuentra en el package java recursos. Usa las siguientes liberias: (ver figura 63)

Figura 63. Librerías usadas para la conexión



```
package recursos; //paquete en donde se encuntra la clase Conexion1
import java.sql.Connection;//clase que representa una conexion con una base de datos
import java.sql.DriverManager;//clase que permite gestionar todos los drivers intalados en el sistema
import java.sql.ResultSet;//clase que permite gestionar el resultado de las consultas sql
import java.sql.Statement;//clase que prepara una variable para ser trabajada con consultas sql
```

Conexión con base de datos "bases" Se utilizó la conexión con la base de datos "bases" la cual contiene los diferentes proyectos en proceso y también bases de datos vacías para crear nuevos. (ver figura 64)

Figura 64. Tabla bases

	id [PK] integer	nombre text	descripcion text	estado integer
1	1	sinf271	Prueba	1
2	2	sinf272	Araujo y as	1
3	3	sinf273	Base de da	1
4	4	sinf274	Araujo aso	1
5	5	sinf275	vacia	0
*				

En la columna estado se contienen los valores 1 y 0, siendo uno para una base de datos en proceso y cero para una nueva. (ver figura 65-68)

Figura 65. Lugar de la conexión en Netbeans

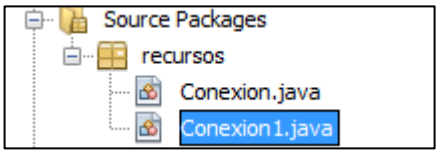


Figura 66. Clase conexion1

```
public class Conexion1 {  //clase Conexion1
        public static String bd="jdbc:postgresql://localhost:5432/bases";
        /*Variable para almacenar la URL de conexión a nuestra Base de Datos*/
        public static   String usr="postgres";//Tipo de usuario
        public static   String psw="123";//Password de posgresql
```

En la imagen anterior se puede apreciar la declaración de variables globales

Figura 67. Método abrir

```
public static Connection abrir(){
// metodo para abir  la conexion con la base d e  datos
    try {
        Class.forName("org.postgresql.Driver");
        //cargar  el controlador de la base de datos
        Connection con = DriverManager.getConnection(bd,usr,psw);
        //crea objeto con que conecta la base de datos enviandole
        //los parametros bd,usr,psw anteriormente descritos
        return con;
        //retorna el resultado de la conexion 0 o 1
    } catch (Exception e) {
        return null;
    }
}
```

El método abrir establece la comunicación con la base de datos.

Figura 68. Método consultar

```
public static ResultSet Consultar(String cad){
 //metodo para realizar consultas sql que recibe la variable cad
    try {
        Connection con = abrir();
        //llamamos al metodo abrir
        Statement sql;
        //creamos sql tipo Statement para realizar queries a la base de datos
        ResultSet datos=null;
        //creamos datos tipo ResultSet que almacena el resultado de las consultas
        if (con!=null){  // si  la conexion es exitosa
            sql = con.createStatement();
            //creamos sql tipo Statement para realizar queries a la base de datos
            datos = sql.executeQuery(cad);
            //en datos guardamos  el resultado del query que recibimos en la variable cad
        }
        return datos;  // retorna  el resultado de la consulta
    } catch (Exception e) {
        return null;
    }
}
```

El método consultar guarda una consulta en un string, por ejemplo aquí, se lama cad, luego usa el método abrir y realiza la consulta sql. Retorna el resultado de la consulta sql. (ver figura 69)

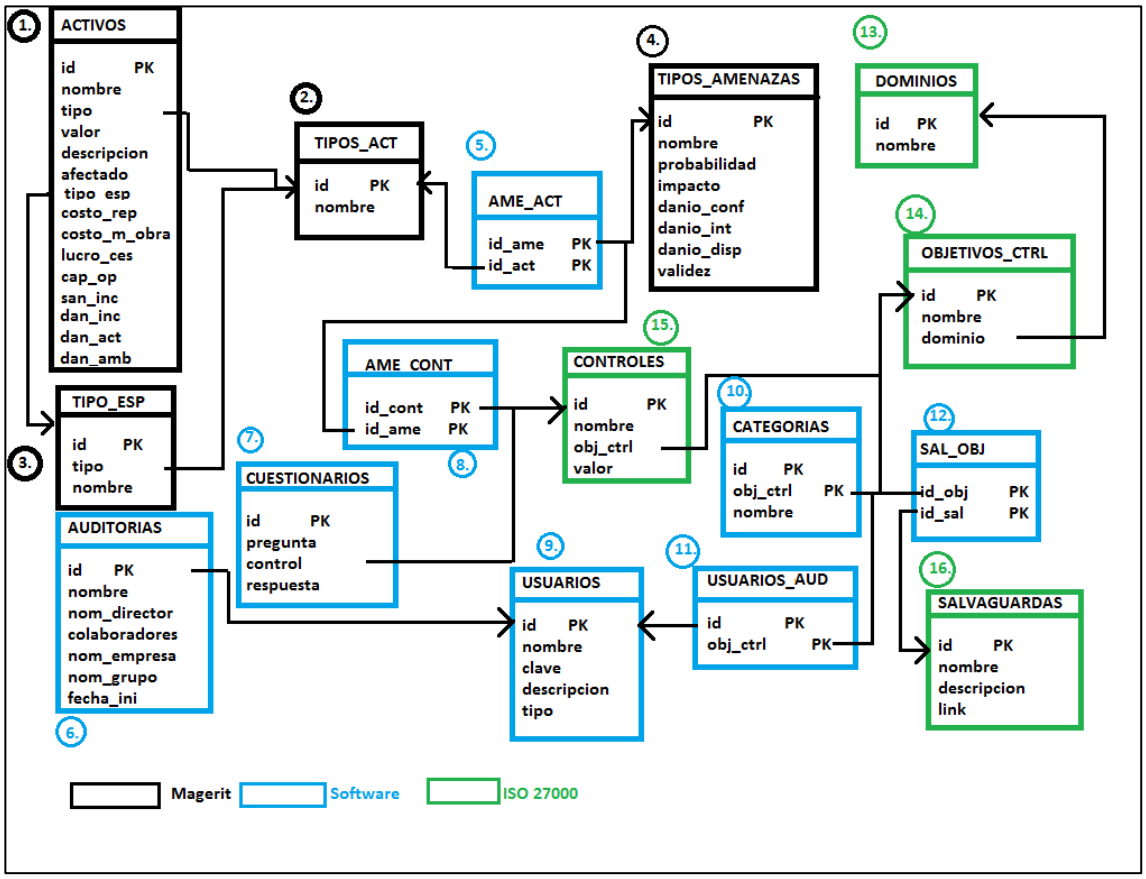
Figura 69. Método actualizar

```
public static int Actualizar(String cad){
//metodo para  insertar o actualizar tablas de la base de datos recibiendo la variable tip0 cad
    try {
        Connection con = abrir();
        //llamamos al metodo abrir
        Statement sql;
         //creamos sql tipo Statement para realizar queries a la base de datos
        int i=0;// variable  tipo  in para  guardar el resultado de la insercion o actualizacion
        if (con!=null){//si conexion exitosa
            sql = con.createStatement();
             //creamos sql tipo Statement para realizar queries a la base de datos
            i = sql.executeUpdate(cad);
            //ejecutamos la insercion o actualizacion y retorna 1 o 0
        }
        return i;//retornamos resultado 1
    } catch (Exception e) {
        return 0; //retorna 0 en caso de no haberse realizaso la actualizacion o insert
    }
}
```

El método actualizar guarda una actualización en un string, por ejemplo aquí, se lama cad, luego usa el método abrir y realiza la actualización sql. Retorna un 1 o un 0 dependiendo si se realizó la actualización.

Conexión a base de datos del proyecto a trabajar. Una vez establecida la conexión con una base de datos específica, se usa otra base de datos sinf27 la cual contiene la estructura del software y permite gestionar los datos para un proyecto específico. (ver figura 70)

Figura 70. Esquema relacional base de datos para un proyecto



Los métodos para esta conexión son los mismos que para la anterior además del método variables(String); que recibe el nombre de la base de datos a trabajar y lo guarda en una variable tipo String para que la conexión se establezca con este nombre a través del método abrir. (ver figura 71)

Figura 71. Método variable

```
public  static void   variables( String nombre){
//metodo que recibe el nombre  de la base de  datos a trabajar
        bd="jdbc:postgresql://localhost:5432/";
        //Variable para almacenar la URL de conexión a nuestra Base de Datos*/
        bd+=nombre;
        //le agregamos a la variable el nombre de la base de  datos


 }
```

Cargar una base de datos. Una vez creadas las conexiones podemos usar todos sus métodos y comunicación con la respectiva base de datos cargando una en el software. (ver figura 72)

Figura 72. Cargar_base.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%> <%-- importamos la leibreria sql y todas  sus clases --%>
<%@page import="recursos.Conexion1"%><%-- importamos la clase Conexion1--%>
<%@page import="recursos.Conexion"%><%-- importamos la clase Conexion--%>

<%
    String nom=request.getParameter("rbase");
    //recupera el parametro del radion button y lo guardo en  la variable nom
    ResultSet datos=Conexion1.Consultar("select * from bases where id="+nom+"");
     //hago la consulta de la base de datos con el id  igual a nom y lo guardo en  la variable datos";
    if(datos.next()){//ubicar en el resusltado de la consulta que se hizo
        String nombre=datos.getString(2);
        //recupero el nombre de la base de datos y lo almaceno el la variable nombre
        out.println("1");//imprimo 1 en caso de que la consulta no sea null
        Conexion.variables(nombre);
        // le  envio  el nombre de  la base de  datos  a trabajar a  travez del metodo variables(nombre)


    }
    else{
        out.println("0");//imprimo 0 si la consulta es vacia
    }
    datos.close();// cerrar la consulta sql

%>
```

En la cadena nom se recupera el valor del radiobutton para cargar la base de datos elegida. (ver figura 73)

Figura 73. Carga de una base de datos

Por ejemplo en este caso se eligió y cargo la base de datos sinf274

3.3.2 Creación de auditorías:

Guardar datos de auditoría. Interfaz y formulario que recibe datos de auditoría y los guarda en la base de datos en la tabla auditorías. (ver figura 74-77)

Figura 74. Guardar datos de auditoría

Figura 75. Auditoría.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>
<%@page import="recursos.Conexion"%>

<%
String naud = request.getParameter("nombreauditoria");//recupera  nombre auditoria
String ndir = request.getParameter("nombredirector");//recupera   nombre director
String ncol = request.getParameter("nomcolab");     //recupera  nombre colaboradores
String nempre = request.getParameter("nempre");    //recupera  en nombnre de  la empresa
String ngrupo = request.getParameter("ngrupo");   //recupera en nombre  del grupo
String cat = request.getParameter("categoria");  //recupera en tipo de categoria
int c= Integer.parseInt(cat);                   //convierto en tipo de categoria a  entero
if(c!=0){                                       //si  se  ha seleccionado  categoria
String actualizar = "INSERT INTO auditoria(nombre,nombre_director,colaboradores,nombre_empresa,nombre_grupo,categoria)";
//realizo una inserción de los datos en la tabla auditoria
actualizar+="VALUES ('"+naud+"','"+ndir+"','"+ncol+"','"+nempre+"','"+ngrupo+"',"+cat+")";
int i = Conexion.Actualizar(actualizar); //llamo  al metodo actualuzar(actualizar enviando la cadena de la inserción)
if(i==0)out.println("0");               //se la insercion es incorrecta imprimo 0
else out.println("1");                  //si la insercion es correcta imprimo 1
}
else out.println("falta seleccionar tipo de auditoria");
%>
```

Con el anterior código se guarda los datos de la interfaz en la base de datos

Guardar datos de colaboradores. En la base de datos en la tabla usuarios_auditoría se guardan los colaboradores y los dominios a los cuales ellos tienen acceso.

Figura 76. Interfaz colaboradores

Figura 77. Colaboradores.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>
<%@page import="recursos.Conexion"%>
<%
String nom = request.getParameter("col");//recupero el nombre  del colaborador
String id = request.getParameter("so");//recupero el id del dominio asignado
int dominio=Integer.parseInt(id);//convierto a  entero el dominio
ResultSet da=Conexion.Consultar("select colaboradores from auditoria where"
                            + "(colaboradores LIKE '%"+nom+"%'  or colaboradores LIKE '%"+nom+",%'  or  "
                            + "colaboradores LIKE  '%,"+nom+"%'  or  colaboradores LIKE  '%,"+nom+",%')");
// consulto el nombre del colaborador  a insertar
if(da.next()){//en caso de  que  si exista el nombre  del colaborador
 String actualizar = "insert into usuarios_auditoria values('"+nom+"','"+dominio+"')";
 //inserto en el nombre  y  el dominio  del colaborador en la tabla usuarios_auditoria
int i = Conexion.Actualizar(actualizar);//guardo el resultado del insert  en la variable i
if(i==0)out.println("Error en la Insercion");//en caso de  que no sea correcto imprimo error
else out.println("Usuario Adicionado!");//en caso de ser  correcto imprimo bien
}else{out.println("el usuario "+nom+" no se  encuentra");}
 //En caso de que la consulta de null imprimo que  el usuario no se  encuentra
%>
```

Figura 78. Tabla usuarios auditoría

	nombre [PK] text	dominio [PK] integer
1	Dario Mera	5
2	Dario Mera	6
3	Dario Mera	7
4	Dario Mera	8
5	Dario Mera	9
6	Dario Mera	10
7	James Caivio	11
8	James Caivio	12
9	James Caivio	13
10	James Caivio	14
11	James Caivio	15
*		

3.3.3 Creación de usuarios e inicio de sesión:

Creación de usuario nuevo. A continuación se presenta la creación de un nuevo usuario, y el resultado en la base de datos en la tabla usuarios. (ver figura 79-81)

Figura 79. Interfaz registro usuario

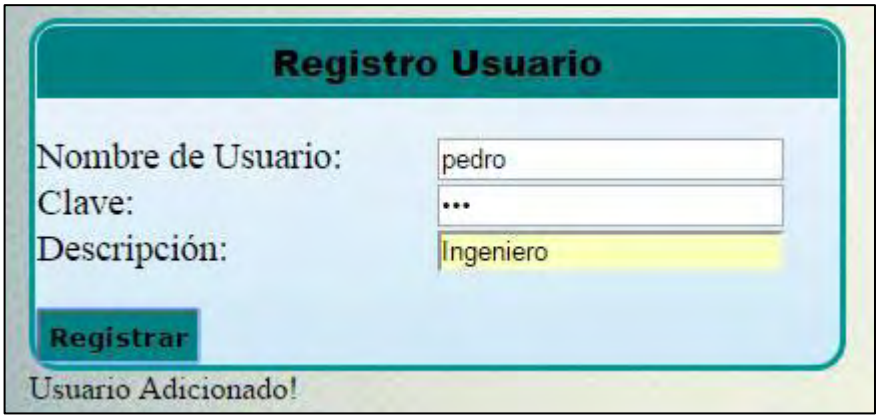


Figura 80. Registro.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%><%-- importo la libreria java.sql Docu--%>
<%@page import="recursos.Conexion"%><%-- importo la clase Conexion--%>
        <%
        String usuarios="";  //cadena para guardar usuarios
        String tipo="";//variable para  guardar tipo
        int cont=0;//contador para colocar  comas(,)
        String nom = request.getParameter("nombre");//recupero  el nombre del usuario
        String clave = request.getParameter("clave");//reupero la  clave  del usuario
        String desc = request.getParameter("desc");  //recupero la descripción del usuario
        ResultSet da1=Conexion.Consultar("select  distinct nombre from usuarios_auditoria");
        //consulto los nombres de los colaboradores de la auditoria
        while(da1.next()){//mientras  haya registros en la consulta
            String usu=da1.getString(1);//guardo el nombre  en una variable usu
            if(cont!=0) usuarios+=",";//los  separo por  una  coma
            else  cont++;usuarios+=usu;//hago una cadena con  los colaboradores registrados
        }
         ResultSet da=Conexion.Consultar("select distinct nombre from usuarios_auditoria where nombre ='"+nom+"'");
         //realizo la consulta con el nombre recuperado del registro si existe
        if(da.next()){//si existe  el nombre
            ResultSet datos=Conexion.Consultar("select  nombre_director from auditoria");
            //consulto el nombre  del director de  la  auditoria
            datos.next();
            String direc=datos.getString(1);//guardo el nombre  en la variable direc
            if(direc.equals(nom)) tipo="0";//si  el nombre  ingresado es igual al del director coloco tipo 0
            else          tipo="1";//si el nombre  es diferente  al del director coloco tipo 1
            String actualizar = "insert into usuarios values('"+nom+"','"+clave+"','"+desc+"','"+tipo+"')";
            //guardo el actualizar  la cadena de  insercion con el nombre,clave,descripcion y el tipo
            int i = Conexion.Actualizar(actualizar);//llamo al metodo actualizar y le  envio la cadena actualizar
            if(i==0)out.println("Error en la Insercion");//si  el resultado de la insercion es 0 error
            else out.println("Usuario Adicionado!");//si  el resultado de la insercion es 1 bien
         }else{out.println("Usuario "+nom+" no existe!");//si no existe  el nombre mensaje
              out.println("Los usuarios registrados son:  "+usuarios+".");//mensaje con los usuarios q  existen
              }
        da.close();//cierro cosnsulta
        da1.close();//cierro consulta
        %>
```

Figura 81. Tabla usuarios

	nombre [PK] text	clave text	descripcion text	tipo character(1)
1	luis	123	ingeniero	0
2	manuel	123	ingeniero	1
3	pedro	123	Ingeniero	1
*				

Verificación de usuario para inicio de sesión. Se verifican los campos nombre y clave en la anterior figura.

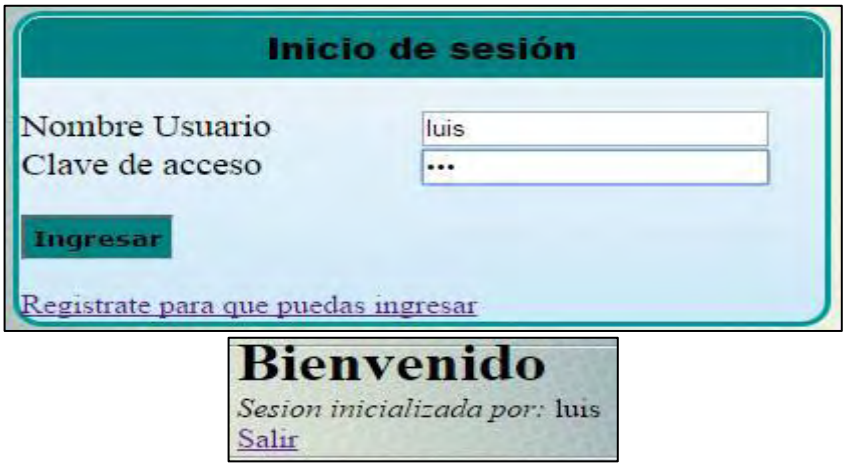
Figura 82. Verificacion_usuario.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
    <%@page import="java.sql.*"%><%-- importo la libreria java.sql Docu--%>
    <%@page import="recursos.Conexion"%><%-- importo la clase Conexion--%>

    <%
        String nom=request.getParameter("nombre");//recupera el parametro del campo de texto
        String cla=request.getParameter("clave");//recupera de clave
        String c="select * from usuarios where nombre='"+nom+"' and clave='"+cla+"'";
        //guardo en una variable c, la cadena de la consulta para buscar el nombre y la clave ingresados
        ResultSet datos=Conexion.Consultar(c);//llama al metodo consultar(c), enviandole la cadena c
        if(datos.next()){//ubicar en el resusltado de la consulta que se hizo
            out.println("1");//si la consulta el nombre y clave  son correctas imprimo 1
            HttpSession sesion=request.getSession();//recupera la sesion que esta activa ahora
            sesion.setAttribute("xusuario",datos.getString(1));
            //coloco el nombre  del usuario en la variable xusuario
        }
        else{//si no existe  el nombre o la clave
            out.println("0");//imprimo 0
        }
        datos.close();// cerrar la consulta sql

    %>
```

Figura 83. Inicio de sesión



3.3.4 Inserción, clasificación y valoración de activos. Al insertar un activo, se debe clasificar dentro de los tipos que están en las tablas consultando este listado de ellas, elegir el adecuado e ingresar en los datos del activo. (ver figura 84)

Figura 84. Activos.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>
<%@page import="recursos.Conexion"%>
<%
  String nom = request.getParameter("nact");//recupero el nombnre  del activo
  String tipact = request.getParameter("tipoact");  //recupero tipo de activo
  String subtipact = request.getParameter("subtipoact");//recupero sub-tipo activo
  int tipi=Integer.parseInt(tipact);//convierto el tipo activo a entero
  int subtipi=Integer.parseInt(subtipact);//convierto el sub-tipo activo a entero
  int vcosto= Integer.parseInt(request.getParameter("valcosto"));//recupero el valor costo y convierto a entero
  int cmobra=Integer.parseInt(request.getParameter("cmobra"));//recupero el valor costo mano de obra y convierto a entero
  int vallucro=Integer.parseInt(request.getParameter("vallucro"));//recupero el valor lucro y convierto a entero
  int vcapaci=Integer.parseInt(request.getParameter("valcapacidad"));//recupero el valor capacidad y convierto a entero
  int valsan=Integer.parseInt(request.getParameter("valsancion"));//recupero el valor sancion y convierto a entero
  int votros=Integer.parseInt(request.getParameter("dotros"));//recupero el valor daño a otros y convierto a entero
  int dpersonas=Integer.parseInt(request.getParameter("dpersonas"));//recupero el valor daño personas y convierto a entero
  int dambiente=Integer.parseInt(request.getParameter("dambiente"));//recupero el valor daño ambiente y convierto a entero
  String val = request.getParameter("vact");//recupero el valor total del activo
  Double vali=Double.parseDouble(val); //convierto el valor total activo a tipo double
  String desc = request.getParameter("desc");//recupero alñ descripcion del activo
  String actualizar= "INSERT INTO activos (nombre,tipo,valor,descripcion,costo_reposicion,costo_mano_obra,lucro_cesante,capacidad
  //realizo la insercion del activo conlos  datos reuperados y los meto en la variable actualizar
  actualizar+= "VALUES ('"+nom+"',"+tipi+","+vali+",'"+desc+"',"+vcosto+","+cmobra+","+vallucro+","+vcapaci+","+valsan+","+votros
  int i = Conexion.Actualizar(actualizar);//llamo al metodo actualizar  enviandole  al cadena con la consulta
  if(i==0)out.println("Error en la Insercion");//si el resultado es cero,imprimo error
  else out.println("Activo Adicionado!");//si  el resultado es 1 imprimo bien
%>
```

A continuación se muestra la interfaz que permite insertar datos. (ver figura 85)

Figura 85. Interfaz Activos

A continuación, se puede ver la tabla que contiene los datos de los activos.

Figura 86. Tabla activos

	id [PK] serial	nombre text	tipo integer	valor double pı	descripcion text	afectadc characte	costo_re integer	costo_r integer	lucro_ intege	capaci integer	sanc inte	danios intege	danio_p integer	danio_a integer	tipo_esp integer
1	226	Informacion	1	3	Datos de lo		1	3	5	5	5	3	1	1	11
2	227	Informacion	1	2	Datos que s		2	3	5	5	2	3	1	1	11
3	228	Salidas	1	3	Datos final		5	5	3	1	4	1	1	1	11
4	229	Organigrama	1	3	Datos de ca		2	3	4	5	3	3	3	2	12
5	230	Datos de Pr	1	3	Datos de Pr		3	3	5	5	3	2	2	1	12
6	231	Servicios i	2	3	uso de las		3	3	5	5	3	2	2	1	24
7	232	Contratos d	2	3	Relaciones		4	4	5	2	5	3	4	1	23
8	233	Contratos d	2	3	Relaciones		4	4	5	2	5	3	4	1	23
9	234	Contratos d	2	3	Relaciones		4	4	5	2	5	3	4	1	23
10	235	Contratos d	2	3	Relaciones		4	4	5	2	5	3	4	1	23
11	236	Contratos d	2	3	Relaciones		4	4	5	2	5	3	4	1	23
12	237	Prestacion	2	3	Relaciones		4	4	5	2	3	3	4	1	22
13	238	Ficheros	3	2	Organizador		2	3	3	3	2	2	2	1	31
14	239	Copias de r	3	2	Copias de r		2	5	3	3	2	2	2	1	32
15	240	Registros d	3	2	Bitacoras d		2	2	2	2	4	2	2	3	38
16	241	Claves crip	4	2	Claves para		1	3	3	3	2	4	4	1	41
17	242	Monica	5	2	Software a		3	2	3	3	3	2	2	1	52
18	243	Software co	5	2	Paquete de		3	3	3	3	3	2	2	1	53
19	244	Equipos med	6	2	conjunto de		3	4	4	4	3	2	2	1	62
20	245	Informatica	6	2	conjunto de		2	3	3	3	3	2	2	1	63
21	246	Informatica	6	1	conjunto de		2	3	2	2	1	1	1	1	64

También es necesario elegir el valor del activo, poniendo valores en las dimensiones de valor, el software se encarga de calcular el valor total.

3.3.5 Implementación de la estructura de la norma ISO 27001

Dominios. Se realiza un código que usa la conexión con la base de datos y una consulta SQL para listar los dominios que están en las tablas, luego el usuario elige los dominios que va a trabajar y avanza al siguiente nivel. (ver figura 87-88)

Figura 87. Formulario para elegir dominios

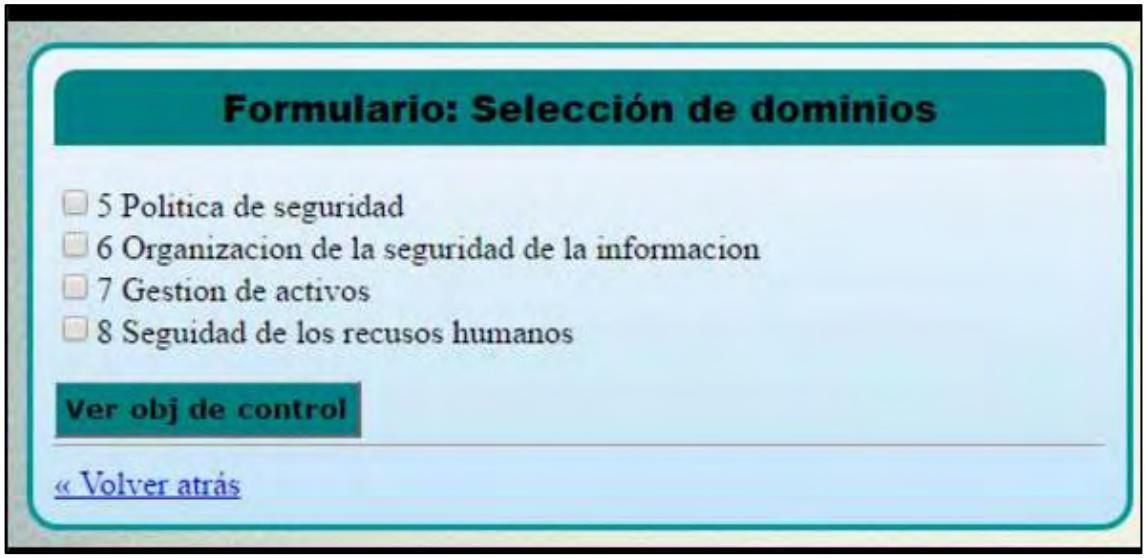


Figura 88. Ver Dominios .jsp

```
<%

ResultSet da=Conexion.Consultar("select dominios.nombre,id from dominios,usuarios_auditoria  where usuarios_auditoria.nombre='"+usu+"' and id=dominio
//realizo la consulta recuperando el nombre y id de los dominios que que le corresponden al usuario que inicion sesion
while(da.next()){//mientras haya datos
int id=Integer.parseInt(da.getString(2));//recupero el id de la consulta y lo guardo en la variable id
String nombre=da.getString(1);//recupero el nombre de la consulta y lo guardo en la variable nombre
out.println("<input type='checkbox' id='publicar"+id+"' name='publicar"+id+"' value='"+id+"' onClick='marcaruno(this)'>" +id+"  "+nombre+"<br>" );
//creo u checkbox con el id del resultado del id  de la consulta, y ademas imprimo el id y el nombre de los dominios
}
da.close(); //cierro la consulta sql
%>
```

Objetivos de control. De la misma forma que en el nivel anterior, se listan los objetivos de control, y se eligen los que se van a trabajar. (ver figura 89-90)

Figura 89. Formulario para elegir objetivos de control

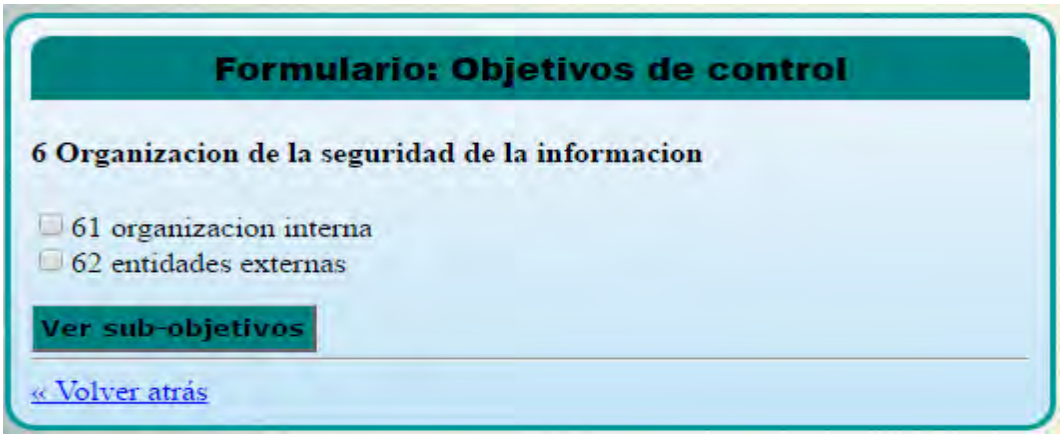


Figura 90. Ver_obj_ctrol.jsp

```
<%
   ResultSet datos=Conexion.Consultar("SELECT categoria FROM auditoria where id in(select max(id)from auditoria)");
   //consulta que recupera la categoria de la auditoria
   datos.next();
   int cat = Integer.parseInt(datos.getString(1));//guardo el resultado de la consulta en  la variable cat
   datos.close();
   ResultSet da=Conexion.Consultar("select count(*) from dominios ");
   //consulta que recupera el numero de dominios
   da.next();
   String cont=da.getString(1);//guardo el resultado de la consulta el la variable cont
   int con=Integer.parseInt(cont);//convierto el resultado de la consulta a  entero
  for(int j=1;j<=con+5;j++){//mientras que j sea menor  a contador mas 5 ya que  los dominios empiezan en 5
   String nom = request.getParameter("publicar"+j);//recupero el dominio seleccionado
   if(nom!=null){//si el dato de recupere el diferente de null
       String consul2 = "select *from dominios where id="+nom+" order by id asc";//consulto los datos del dominio
       ResultSet da1 = Conexion.Consultar(consul2);//llamo al metodo consultar enviandole la cadena consul2
       ResultSet da2 = Conexion.Consultar("select objetivos_ctrl.id,objetivos_ctrl.nombre from objetivos_ctrl,categorias "
       +"where objetivos_ctrl.dominio="+nom+" and objetivos_ctrl.id=categorias.obj_control  and categorias.id="+cat+" order by id asc ");
       //selecciono el id,nombre que corresponden al dominio seleccionado
       da1.next();
       int ide= Integer.parseInt(da1.getString(2));//guardo el id del resultado de la consulta
       String nom1=da1.getString(1);//guardo el nombre del resultado de  la consulta
       out.println("<div id='div"+ide+"'>");//creo un div(division) con id igual al ide del dominio
       out.println("<h4>"+ide+"  "+nom1+"</h4>");//imprimo el ide y nombre del dominio
       //out.println("<input type='checkbox' name='marcar"+ide+"' id='marcar"+ide+"'>");
       //out.println("marcar todo <br>");
       while(da2.next()){//mientras  haya objetivos de control
       int id=Integer.parseInt(da2.getString(1));//guardo id  de objetivo de control
       String nombre=da2.getString(2);  //guardo nombre de  objetivo de  control
        out.println("<input type='checkbox' id='dominios"+id+"' name='dominios"+id+"' value='"+id+"' onClick='marcaruno(this)'>"
        +"<h4>" +id+"  "+nombre+"</h4><br>" );  //creo un checkbox con el id del sub-objetivo, e imprimo el id y nombre del objetivo de control
       }
       da1.close();//cierro consulta 1
       da2.close();//cierro consulta 2
       out.println("</div>");//cierro division
   }
}
da.close();//cierro consulta
%>
```

Controles. De la misma forma que en el nivel anterior, se listan los controles, y se eligen los que se van a trabajar, estos contienen a los cuestionarios para evaluar cada control. (ver figura 91-92)

Figura 91. Formulario para elegir sub objetivos de control

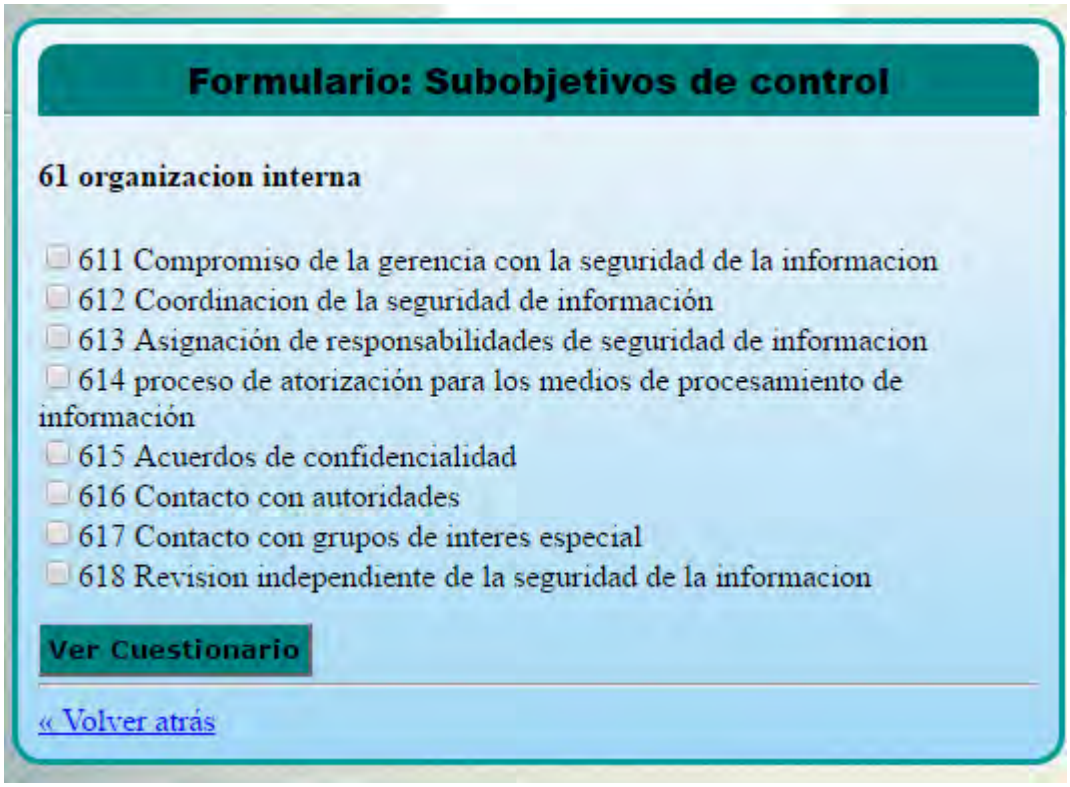


Figura 92. Ver_controles

```
<%
    ResultSet da=Conexion.Consultar("select max(id) from objetivos_ctrl");
    //seleciono el maxino id de la tabla objetivos_ctrl
    da.next();
    int cont=da.getInt(1);//guardo el resultado de la consulta el cont
    for(int j=51;j<=cont;j++){//mientras que j sea menor que cont
        String nom = request.getParameter("dominios"+j);//recupero el objetivo seleccionado
        if(nom!=null){//si el dato recuperado es diferente de null
            String consul2 = "select id,nombre from objetivos_ctrl where id="+nom;
            //guado el consul2 la consulta del id y nombre de los sub-objetivos con id igual al recuperado
            ResultSet da1 = Conexion.Consultar(consul2);//llamo al metodo consultar enviandole consul2
            da1.next();
            int ide= da1.getInt(1);//guardo el id del sub-objetivo de la consulta
            String nom1=da1.getString(2);//guardo el nombre del sub-objetivo de la consulta
            out.println("<div id='div"+ide+"'>");//creo un div(division)
            out.println("<h4>"+ide+"  "+nom1+"</h4>");//imprimo id y nombre del objetivo de control
            ResultSet da2 = Conexion.Consultar("select id,nombre from controles where obj_ctrl="+nom+" order by id asc");
            //consulto los sub-objetivos de control con el id del objetivo
            while(da2.next()){//mientras haya datos
            int id=da2.getInt(1);//guardo el id del sub-objetivo de control, de la consulta
            String nombre=da2.getString(2);  //guardo el nombre del sub-objetivo de control, de la consulta
            out.println("<input type='checkbox' id='control"+id+"' name='control"+id+"' value='"+id+"' onClick='marcaruno(this)'>"
            +"<h4'>" +id+"  "+nombre+"</h4><br>" ); // creo un checkbox para cada sub-objetivo de control,  imprimo id y nombr
        }
            da1.close();//cierro consulta 1
            da2.close();//cierro consulta 2
            out.println("</div>");//cierro division
        }
    }
```

Cuestionarios. De la misma forma que en el nivel anterior, se listan las preguntas de cada control, en este caso permite elegir las preguntas que harán parte del cuestionario, luego de ello las preguntas elegidas dan la opción de responderlas con un nivel de satisfacción de uno a cinco. (ver figura 93)

Figura 93. Formulario para elegir cuestionarios de control

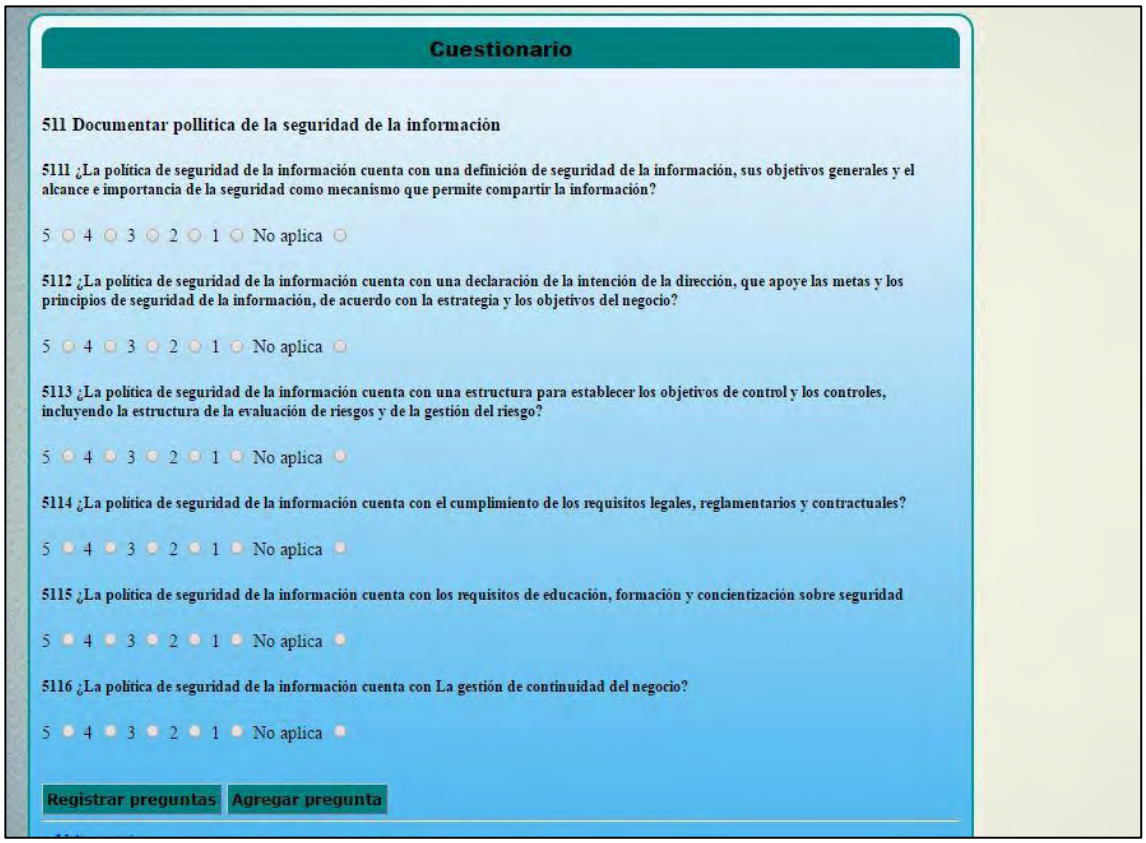


Figura 94. Ver_cuestionarios.jsp

```
<%
 ResultSet datos = Conexion.Consultar("select max(id) from controles");
 //realizo consulta para seleccionar maximo id de controles
 datos.next();
 int cont = datos.getInt(1);//guardo el resultado en la variable cont
 for (long j = 511; j <= cont; j++) {//mientras j menor  a cont
     String nom = request.getParameter("control" + j);
     //recupero el sub-objetivo de control seccionado y lo guardo en nom
     if (nom != null) {//si nom no es nulo
         String consul2 = "select *from controles where id=" + nom;
         //guardo en consul2 la consulta de los datos del control con id igual a nom
         ResultSet da1 = Conexion.Consultar(consul2);
         //llama  al metodo Consultar enviandole la cadena consul2
         da1.next();
         int ide = Integer.parseInt(da1.getString(3));
         //guardo id del resultado de la consulta
         String nom1 = da1.getString(1);//guardo el nombre del resultado de la consulta
         out.println("<div id='div" + ide + "'><br>");//creo un div(division)
         ResultSet da2 = Conexion.Consultar("select *from cuestionarios where control="+nom+" order by id asc");
         //hago una consulta de todas preguntas relacionadas  con el sub-objetivo selecionado
         while (da2.next()) {//mientras haya datos  de  la consulta
             int i=5;//variable i inicializada  en 5
             int id = da2.getInt(3);//guardo el id del resultado de la consulta(id de la pregunta)
             String nombre = da2.getString(1);//guardo el nombre del resultado de la consulta(nombre pregunta)
             out.println("<h5>" +id+"  "+nombre+"</h5>");//imprimo el id y nombre del sub-objetivo de control
             out.println("<input type='checkbox' id='radio"+id+"' name='radio"+id+"' value='"+id+"' checked style='display:none;'>" );
              //creo un checkbox invisible para guardar el id de cada pregunta
            while(i>=0){//mientras i mayor o igual que cero
                 if(i==0){//
                    out.println("No aplica <input type='radio' id='valor"+id+"' name='valor"+id+"' value='"+i+"'>");
                    //creo un radio button con valor igual a cero, llamado no aplica
                 }
                 else{
                      out.println(""+i+"  <input type='radio' id='valor"+id+"' name='valor"+id+"' value='"+i+"'>");
                      //creo un radio button con valor igual a i, de 5 a 1,
                  }
                i--;//decremento i en uno
              }
             out.println("<br>");//imprimo salto
           }
         out.println("<input type='text' id='control' name='control' value='"+nom+"' style='visibility:hidden'>");
         //creo un campo de texto invisible con valor del id del sub-objetivo selecionado
           out.println("</div>");//cierro div
            out.println("<div id='pregnuevas'>");//creo un div para adicionar nuevas preguntas

           out.println("</div>");//cierro div
            da1.close();//cierro consulta 1
           da2.close();//cierro consulta 2
     }

 }
 datos.close();//cierro consulta
%>
```

3.3.6 Implementación de la gestión de riesgos:

Cálculo de la evaluación de un control. A través de su cuestionario se suma el valor de las respuestas y se obtiene una calificación que de ser mayor o igual a setenta aprobara el control de lo contrario se reprobara. (ver figura 95-96)

Figura 95. Evaluacion.jsp

```
----creo una funcion para insertar el valor(porcentaje) a
--cada control dependiendo del valor de cada  pregunta
CREATE OR REPLACE FUNCTION insertar() RETURNS trigger AS $insertar$
BEGIN
    --actualizo el control con el valor(porcentaje) que calculo
    update controles set valor=(select round(AVG(valor)*20,0)
    FROM cuestionarios
    where valor!=0 and control=new.control GROUP BY (control))
    where id=new.control;
    return new;--retorno el valor(porcentaje)
END
$insertar$ LANGUAGE plpgsql --

--2
--creo  el trigger insertar, para que se ejecute cada vez
 --que se inserta o actualiza la tabla cuestionarios
create  trigger insertar after INSERT or UPDATE
on cuestionarios for each row execute procedure insertar();
```

Figura 96. Listado de controles y su estado

controles verificados

id	nombre	valor	estado
511	Documentar pollitica de la seguridad de la informacion	57.0	Reprobado
512	Revision de la politica de seguridad de la informacion	38.0	Reprobado
611	Compromiso de la gerencia con la seguridad de la informacion	70.0	Aprobado
612	Coordinacion de la seguridad de información	73.0	Aprobado
613	Asignación de responsabilidades de seguridad de informacion	40.0	Reprobado
614	proceso de atorización para los medios de procesamiento de información	60.0	Reprobado
615	Acuerdos de confidencialidad	76.0	Aprobado

Relación de controles reprobados. Establecer las amenazas activadas por un control que ha sido reprobado. (ver figura 97-99)

Figura 97. Validez.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>//importo la librerria sql
<%@page import="recursos.Conexion"%>//importo la clse Conexion
<%
//realizo la consulta de los controles que tengan valor menor
//a 70 o diferente de 0, y no tenga amenazas activadas y lo
//guardo en la variable dato
 ResultSet dato=Conexion.Consultar("select id from controles
                                    where valor <70 and valor!=0
                                    and amenazas_act is null
                                    order by id asc" );
 while(dato.next()){//mientras  dato tenga datos
    int id=dato.getInt(1);  //recupero el id y lo guardo
    //realizo la actualizacion del control con las amenazas
    //correspondientes a este mismo, realizando una consulta
    //interna en la tabla amecont que contiene las  amenazas
    //activadas correspondientes a cada control
    int a = Conexion.Actualizar("update controles set amenazas_act
                                =(SELECT array_to_string(array_AGG(amenazas),',')
                                As amenazas
                                FROM amecont where id="+id+" group BY id)
                                where id="+id+" ");
 }
  dato.close();  //cierro la consulta
  %>
```

A continuación, se observa un control con las amenazas que el activa

Figura 98. Tupla de tabla controles

55	617	Contacto con grupos de interes	32,33

Y las amenazas correspondientes con el campo validez en uno.

Figura 99. Amenazas activadas en tabla tipos_ame

	id integer	nombre text	validez integer
13	31	3.1 Errores de los usuarios	1
14	32	3.2 Errores del administrador	1

Ingreso de probabilidad de ocurrencia. Para las amenazas activadas se implementó una interfaz para que el usuario ingrese la probabilidad de ocurrencia de cada una de ellas. (ver figura 100)

Figura 100. Probabilidad.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>//importo la librerria sql
<%@page import="recursos.Conexion"%>//importo la clse Conexion
<%
 //consulta  las  amenenazas cuya validez sea 1 y lo guardo en la variable da
 ResultSet da=Conexion.Consultar("select id from tipos_ame where validez=1 order by id
 while(da.next()){//mientras haya datos
   int id=da.getInt(1);//recupero el valor del id
   String ide=Integer.toString(id);//convierto el valor del id a string
   //recupero el id del select
   String cprob=request.getParameter("cproba"+id);
   if(cprob!=null){//si el dato recuperado no es nulo
   //recupero la opcion seleccionada por el usuario
   String probabilidad=request.getParameter("proba"+id);
   //actualizo la tabla tipos_ame con la probabilidad seleccionada
   String act = "update tipos_ame  set probabilidad="+probabilidad+" where id="+id;
   int i = Conexion.Actualizar(act);//llamo al metodo Actualizar, enviandole la cadena
   }
 }
 da.close();  //cierro consulta
%>
```

A continuación, se muestra el ingreso de valores de probabilidad en las amenazas afectadas. (ver figura 101)

Figura 101. Interfaz para ingreso de probabilidad

Y asi queda en la tabla tipos_ame luego de la insercion:

Figura 102. Tabla tipos_ame con probabilidad insertada

	id integer	nombre text	validez integer	probabilidad integer
11	28	2.8 Condiciones inadecuadas		
12	29	2.9 Fallo de servicios de co		
13	31	3.1 Errores de los usuarios		
14	32	3.2 Errores del administrado	1	3
15	33	3.3 Errores de monitorizació	1	2
16	34	3.4 Errores de configuració	1	1
17	35	3.5 Deficiencias en la organ	1	3
18	36	3.6 Difusión de software dañ		

Cálculo de impacto. El impacto se calcula relacionando las amenazas activadas con los tipos de activos que ellas afectan. Esta relación esta determinada en Magerit. (ver figura 103-105)

Paso siguiente se obtiene el impacto basado en tres criterios:

- El número de activos afectados sobre el número total de activos
- Si los activos afectados son esenciales, es decir información o servicios, o son comunes
- El costo de los activos afectados.

Figura 103. Impacto.jsp Criterios de determinación de impacto

```
if(porafec>80 || (porafec>60 && promedioafec>3.5)
|| promedioafec>4 || poresen>(50*nactivosafec) ||
(promedioafec>3 && poresen>(40*nactivosafec)) ||
(porafec>60 && poresen>(35*nactivosafec)) ||
(porafec>40 && promedioafec>2.5 && poresen >(30*nactivosafec))){
   impacto=3;
}
else if(porafec>50 || (porafec>30 && promedioafec>2)
|| promedioafec>3 || poresen>20 || (porafec>30 && poresen>15)
|| (promedioafec>1.5 && poresen>15)
|| (porafec>20 && promedioafec>1.5 && poresen>15)){
     impacto=2;
}
else impacto=1;
```

Figura 104. Impacto.jsp Completo

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>//importo la librerria sql
<%@page import="recursos.Conexion"%>//importo la clse Conexion
<%
 int idame=0;//creo varible idame tipo entera
 int amena=0;// creo variable amena tipo entera
 //realizo la consulta de las  amenazas cuya validez sea 1 y no tengan impacto
 ResultSet da=Conexion.Consultar("select id from tipos_ame where validez=1 and impacto is null");
 while(da.next()){//mientras haya datos
  idame=da.getInt(1);//guardo el id en la variable tipo int anteriomente creada
  //creo variable tipo entero y las inicializo en cero
  //nactivos: numero de activos totales
  //nactivosafec: numero de activos afectados
  //promedioafec: tipo double promedio activos afectados
  int nactivos=0,nactivosafec=0,impacto=0,poresen=0,porafec=0;
  double promedioafec;
  promedioafec=0;
  //consulto el numero de activos existentes
  ResultSet da2=Conexion.Consultar("select count(*) from activos");
  da2.next();
  nactivos=da2.getInt(1);//guardo el numero de activos existentes
  //consulto el numero de activos afectados,porcentaje, y el promedio de los activos afectados
  ResultSet da3=Conexion.Consultar("select count(*),(count(*)*100/"+nactivos+"),(avg(valor))
                                   from ameact,activos where tiact="+idame+" and ameact.id=tipo");
  da3.next();
  nactivosafec=da3.getInt(1);//guardo el numero de activos afectados
    promedioafec=da3.getDouble(3);//guardo el promedio de activos afectados
    porafec=da3.getInt(2);//guardo el porcentaje de activos afectados
     //consulto el numero de activos afectados por 100, activos afectados cuyo tipo sea 1 o 2
    ResultSet da4=Conexion.Consultar("select (count(*)*100) from ameact,activos
                                     where (tipo=1 or tipo=2) and tipo=ameact.id and tiact="+idame+"");
    da4.next();
    poresen=da4.getInt(1);//guardo el numero de activos afectados por 100
    //realizo la deciciones correspondientes para dar el impacto de  cada  amenaza produce a los activos
    if(porafec>80 || (porafec>60 && promedioafec>3.5) || promedioafec>4 || poresen>(50*nactivosafec) || (p
       impacto=3;
    }
    else if(porafec>50 || (porafec>30 && promedioafec>2) || promedioafec>3 || poresen>20 || (porafec>30 &&
         impacto=2;
    }
    else impacto=1;
    //creo la cadena para  actualizar  la tabla tipos_ame con el impacto correspondiente de cada amenaza
    String tiposame = "update tipos_ame  set impacto="+impacto+" where id="+idame+"";
    int h = Conexion.Actualizar(tiposame);    //llamo al metodo Actualizar, enviandole la cadena anterior
    da2.close();//cierro consulta
    da3.close();//cierro consulta
    da4.close();//cierro consulta
}

da.close();//cierro consulta
 %>
```

Figura 105. Tabla tipos_ame con impacto calculado

	id integer	nombre text	validez integer	probabilidad integer	impacto integer
13	31	3.1 Errores de los usuarios			
14	32	3.2 Errores del administrado	1	3	1
15	33	3.3 Errores de monitorizació	1	2	3
16	34	3.4 Errores de configuració	1	1	3
17	35	3.5 Deficiencias en la organ	1	3	1
18	36	3.6 Difusión de software dañ			

Matriz de riesgos. Se muestra en rojo las amenazas que tengan probabilidad e impacto tres, en verde las que tengan probabilidad e impacto uno y en amarillo cualquier otra combinación. (ver figura 106-109)

Figura 106. Matriz de riesgos

nombre	Probabilidad	Impacto
3.2 Errores del administrador	3	1
3.3 Errores de monitorización	2	3
3.4 Errores de configuración	1	3
3.5 Deficiencias en la organización	3	1

Figura 107. Matriz.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>//importo la librerria sql
<%@page import="recursos.Conexion"%>//importo la clse Conexion
<%
 String color="";//variable cadena para designar el color de la celdas
 //creo una tabla con los datos nombre,probabilidad,impacto de la amenaza
 out.println("<table id='reproba' border=1 WIDTH=500  align='center'
            border='1' style='margin: 0 auto;'>");
 out.println("<tr bgcolor='#00FFFF'><td>nombre</td><td>Probabilidad</td>
            <td>Impacto</td></tr><br>");
 //realizo la consulta de nombre,probabilidad,impacto de la tabla tipos_ame
  //cuya validez sea 1
 ResultSet da=Conexion.Consultar("select nombre,probabilidad,impacto from tipos_ame
                                  where validez=1 order by id asc");
 while(da.next()){//mientras haya datos
       String nombre=da.getString(1);//guardo el nombre de la amenaza
       int probabilidad=da.getInt(2);//guardo la probabilidad de la amenaza
       int impacto=da.getInt(3);     //guardo el impacto de  la amenaza
       //si probabilidad e impacto son iguales a 3 les asigno color rojo
       if(probabilidad==3 && impacto==3) color="red";
       //si probabilidad e impacto son iguales a uno les asigno color verde
       else if(probabilidad==1 && impacto==1) color="green";
       //o si no para todas  las demas le aigno el color amarillo
       else color="yellow";
    //creo las respectivas columnas con los datos recuperados y el colo correspondiente
       out.println("<tr bgcolor='"+color+"'><td>"+nombre+"</td><td>"+probabilidad+"</td>
       <td>"+impacto+"</td></tr>");
  }
da.close();//cierro consulta
out.println("</table>");//cierro tabla
out.println("<hr>");//creo una linea horizontal
//creo una referencia a riesgopdf.jsp que me crea un  pdf
out.println("<a href='riesgopdf.jsp'>Importar a PDF</a>");
%>
```

3.3.7 Implementación norma ISO 27002

Salvaguardas. Se relaciona los objetivos de control con las salvaguardas viables para su solución en caso de ser reprobados y se muestra una lista al usuario para que pueda acceder a los url´s de las salvaguardas.

Figura 108. Tablasalvaguadas.jsp

```
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<%@page import="java.sql.*"%>//importo la librerria sql
<%@page import="recursos.Conexion"%>//importo la clse Conexion
<%
//realizo la consulta con los datos de salvaguardas afectadas con relacion a los controles
 ResultSet datos=Conexion.Consultar("select salvaguardas.id,salvaguardas.nombre,
                                    idobj,objetivos_ctrl.nombre,descripcion,
                                    link from salvaguardas,sal_obj,
                                    objetivos_ctrl where salvaguardas.id=idsal
                                    and idobj=objetivos_ctrl.id and objetivos_ctrl.id in
                                    (select obj_ctrl from controles where valor<70 and valor!=0)");
//creo una  tabla con  con los nombre de los datos consultados
 out.println("<br><table  id='tsalvaguardas' border=1 WIDTH=1310  CELLSPACING=0 CELLPADDING=0>");
 out.println("<tr bgcolor='#99FFFF'><td COLSPAN=6 align='center'>Salvaguardas</td></tr><tr>
            <td wiidth='20'>Id</td><td wiidth='400'>Nombre salvaguarda</td>
            <td wiidth='80'>Id objetivo</td><td wiidth='370'> Nombre objetivo</td>
            <td wiidth='300'> Descripción salvaguarda</td><td wiidth='140'> Link</td></tr>");
 while(datos.next()){ //mientras  haya datos  en la consulta
     int id = datos.getInt(1);//recupero el id de la salvaguarda
     String nombre=datos.getString(2);//recupero el nombre de la salvaguarda
     int idobj=datos.getInt(3);//recupero id del objetivo
     String nombreobj=datos.getString(4);//recupero el nombre del objetivo
     String desc=datos.getString(5);//recupero la descripcion de la salvaguarda
     String link=datos.getString(6);//recupero el link de la salvaguarda
       //creo las celdas correspondientes para cada dato recuperado
       out.println("<tr bgcolor='#CCCCCC'><td>"+id+"</td>"+"<td>"+nombre+"</td>"
                   +"<td>"+idobj+"</td>"+"<td>"+nombreobj+"</td>"+"<td>"+desc+"</td>"
                   +"<td align='center'><a href="+link+" align='center'>Ver salvaguarda</a><
 }
 out.println("</table>");//cierro tabla
 datos.close();//cierro consulta
 out.println("<hr>");//creo linea horizontal
 //creo una referencia al verpdf,jsp que me genera el pdf de la consulta
 out.println("<a href='verpdf.jsp'>Importar a PDF</a>");

  %>
```

Figura 109. Interfaz de lista de salvaguardas

Salvaguardas

Id	Nombre salvaguarda	Id objetivo	Nombre objetivo	Descripción salvaguarda	Link
1	Gesconsultor	51	politica de seguridad de informacion	Plataforma no gratuita que integra todos los elementos necesarios para la implantación y gestión completa del ciclo de vida de un SGSI, así como otros requisitos de cumplimiento de aspectos legales, normativos, contractuales y con terceras partes que sean de aplicación al Alcance del Sistema de Gestión. El portal web aporta información de libre disposición sobre SGSI, Esquema Nacional de Seguridad y otros marcos y políticas relevantes y cómo deben ser tratados.	Ver salvaguarda
2	Modelo Política - ICIC	51	politica de seguridad de informacion	Modelo de Política de Seguridad de la Información para la Administración pública de Argentina, basado en ISO 27002. Establece directrices para cada uno de los controles.	Ver salvaguarda
3	Directorio BIS	51	politica de seguridad de informacion	Department for Business Innovation and Skills (apoyado por el Departamento de Industria y Comercio del Reino Unido) dispone de diversos documentos relacionados con la seguridad de la información, incluídas guías de desarrollo de políticas de seguridad y diversos checklists (inglés) con el objetivo de lograr la protección y desarrollo económico de las empresas.	Ver salvaguarda
4	Series CCN	51	politica de seguridad de informacion	Los documentos CCN-STIC del Centro Criptológico Nacional español incluyen normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las TIC en la Administración española.	Ver salvaguarda
5	DIRECTION CENTRALE DE LA SÉCURITÉ DES SI	51	politica de seguridad de informacion	Guía de redacción de políticas de seguridad de la información de la " Direction Centrale de la Sécurité des Systèmes d'Information" francesa. Disponible en español.	Ver salvaguarda
6	DMOZ	51	politica de seguridad de informacion	Proyecto abierto que ha recopilado a modo de directorio todo tipo de políticas de seguridad en diversas áreas	Ver salvaguarda
7	INFOSECWRITERS	51	politica de seguridad de informacion	Documento de libre descarga (inglés) que analiza las claves para la creación con éxito de una política de seguridad para Pequeñas y Medianas Empresas.	Ver salvaguarda

3.3.8 Implementaciones de reportes. Para cada uno de los reportes diseñados se implementó también la posibilidad de exportarlos a formato pdf para que el usuario pueda elaborar su documento de auditoría. Para ello de uso la librería itextpdf-5.4.4.

El reporte se puede visualizar en el software, pero también cada reporte tiene la opción de ser documentado automáticamente, facilitando al usuario elaborar la documentación final de la auditoría. (ver figura 110-111)

Figura 110. librería itextpdf-5.4.4.

Figura 111. Código reportes

```
<%
response.setContentType("application/pdf");
//digo que  elcontenido del documento sera en formato pdf
try{// creo una excepción en caso de haber  errores
    Document doc=new Document(PageSize.LETTER);
    //creo un documento y le digo que  sera tamaño carta
    PdfWriter.getInstance(doc, response.getOutputStream());
    //creo una instancia del documento que  acabo de crear
    doc.open();//abro el documento
    //creo dos formatos de letras con  tamaño,estilo, y color de  letra
    Font f1=new Font(FontFamily.HELVETICA,18,Font.BOLDITALIC,BaseColor.BLUE);
    Font f2=new Font(FontFamily.HELVETICA,12,Font.BOLDITALIC,BaseColor.BLACK);

     PdfPTable tabla = new PdfPTable(2);//creo una tabla de dos columnas
        float[] medidas={0.7f,1.3f};//creo las medidas a las columnas
        tabla.setWidths(medidas);//le asigno las medidas a la tabla
         //tabla.setWidthPercentage(100);//
         tabla.getDefaultCell().setPadding(4);//creo espacio de relleno
         tabla.getDefaultCell().setBorderWidth(0.4f);//creo tamaño del borde
         //le digo que las celdas estaran alineadas  verticalmente arriva
         tabla.getDefaultCell().setVerticalAlignment(Element.ALIGN_TOP);
          //le digo que las celdas estaran alineadas  horizontalmente centrado
         tabla.getDefaultCell().setHorizontalAlignment(Element.ALIGN_CENTER);
         //realizo la consulta del nombre,director,colaboradores,nombre de la empresa,
```

Figura 111. Código reportes (Continuación)

```
ResultSet da=Conexion.Consultar("select  distinct  auditoria.nombre,nombre_director,colaboradores,no
da.next();//me hubico el el resultado
String nombre=da.getString(1);//guardo el nombre de la auditoria
String nomdirec=da.getString(2);//guardo el nombre del director
String nomcol=da.getString(3);//guardo el nombre de los colaboradores
String nomemp=da.getString(4);//guardo el nombre de la empresa
String nomtipo=da.getString(5);//gurado el nombre del tipo de auditoria
 //creo un nuevo parrafo y lo agrego al documento con formato f1
 doc.add(new Paragraph("REPORTE AUDITORIA: ",f1));
 doc.add(Chunk.NEWLINE);  //agrego un salto de linea al documento
 // creo un nuevo parrafo con el nombre de la auditoria y lo agrego al documento con formato f2
 doc.add(new Paragraph("NOMBRE AUDITORIA: "+nombre+"",f2));
 // creo un nuevo parrafo con el nombre del director y lo agrego al documento con formato f2
 doc.add(new Paragraph("NOMBRE DIRECTOR: "+nomdirec+"",f2));
 // creo un nuevo parrafo con el nombre de los colaboradores y lo agrego al documento con formato f2
 doc.add(new Paragraph("NOMBRE COLABORADORES: "+nomcol+"",f2));
 // creo un nuevo parrafo con el nombre de la empresa y lo agrego al documento con formato f2
 doc.add(new Paragraph("NOMBRE EMPRESA: "+nomemp+"",f2));
  // creo un nuevo parrafo con el tipo de auditoria y lo agrego al documento con formato f2
 doc.add(new Paragraph("NOMBRE TIPO: "+nomtipo+"",f2));
 da.close();//cierro la consulta
doc.add(Chunk.NEWLINE);//agrego un salto de linea aldocumento
String reporte="TABLA REPORTE AUDITORIA";
//creo un nuevo parrafo
```

Figura 111. Código reportes (Continuación)

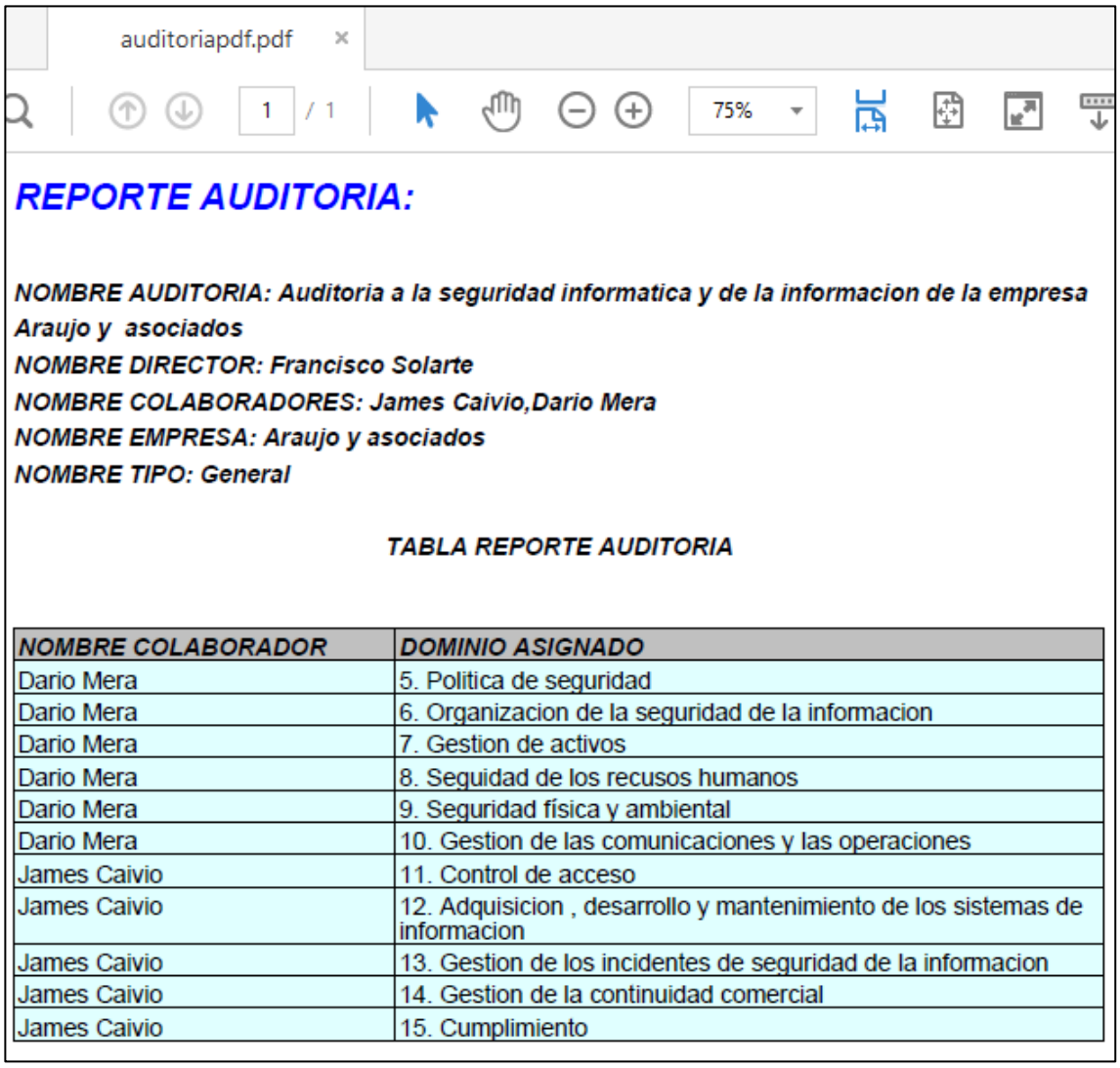
```
Paragraph parrafo = new Paragraph(reporte,f2);
//le digo que el parrafo sera  centrado
 parrafo.setAlignment(Element.ALIGN_CENTER);
 //agrego el parrofo y un salto de linea al documento
  doc.add(parrafo); doc.add(Chunk.NEWLINE);
//creo una celda
PdfPCell cellnc = new PdfPCell(new Paragraph("NOMBRE COLABORADOR",f2));
//le asigno un color de  fondo  a la  celda
cellnc.setBackgroundColor(BaseColor.LIGHT_GRAY);
//creo una celda
 PdfPCell celldo = new PdfPCell(new Paragraph("DOMINIO ASIGNADO",f2));
 //le asigno color  a la celda
celldo.setBackgroundColor(BaseColor.LIGHT_GRAY);
//agrego las  celdas credas al documento
 tabla.addCell(cellnc);tabla.addCell(celldo);
  //realizo la consulta de todos los colaboradores de la auditoria. Nombre y dominios aignados
  ResultSet d=Conexion.Consultar("select u.nombre,d.id,d.nombre from usuarios_auditoria as u,dom
  while(d.next()){//mientras haya datos
  String nombrec=d.getString(1);//recupero el nombre del colaborador
  int id=d.getInt(2);           //recupero el id del dominio asignado
  String dominio=d.getString(3);//recupero el nombre del dominio asignado
  //creo una celda con el nombre del  colaborador
   PdfPCell celln = new PdfPCell(new Paragraph(nombrec));
   celln.setColspan(1);celln.setBackgroundColor(new BaseColor(224,255,255));//le asigno un color
```

Figura 111. Código reportes (Continuación)

```
    //creo una celda con el id y el nombre del dominio asignado
    PdfPCell celld = new PdfPCell(new Paragraph(""+id+". "+dominio));
    celld.setBackgroundColor(new BaseColor(224,255,255));//le asigno un color
    //agrego las celdas creadas al documento
    tabla.addCell(celln);
    tabla.addCell(celld);
   }

    doc.add(tabla);//agrego la tabla al documento
    doc.close();//cierro el documento
    da.close();//cierro la consulta
    d.close();//cierro consulta
 }
 catch(Exception err){//muestro error si lo hay
 out.print(err.getMessage());//imprimo mensaje de error
}
%>
```

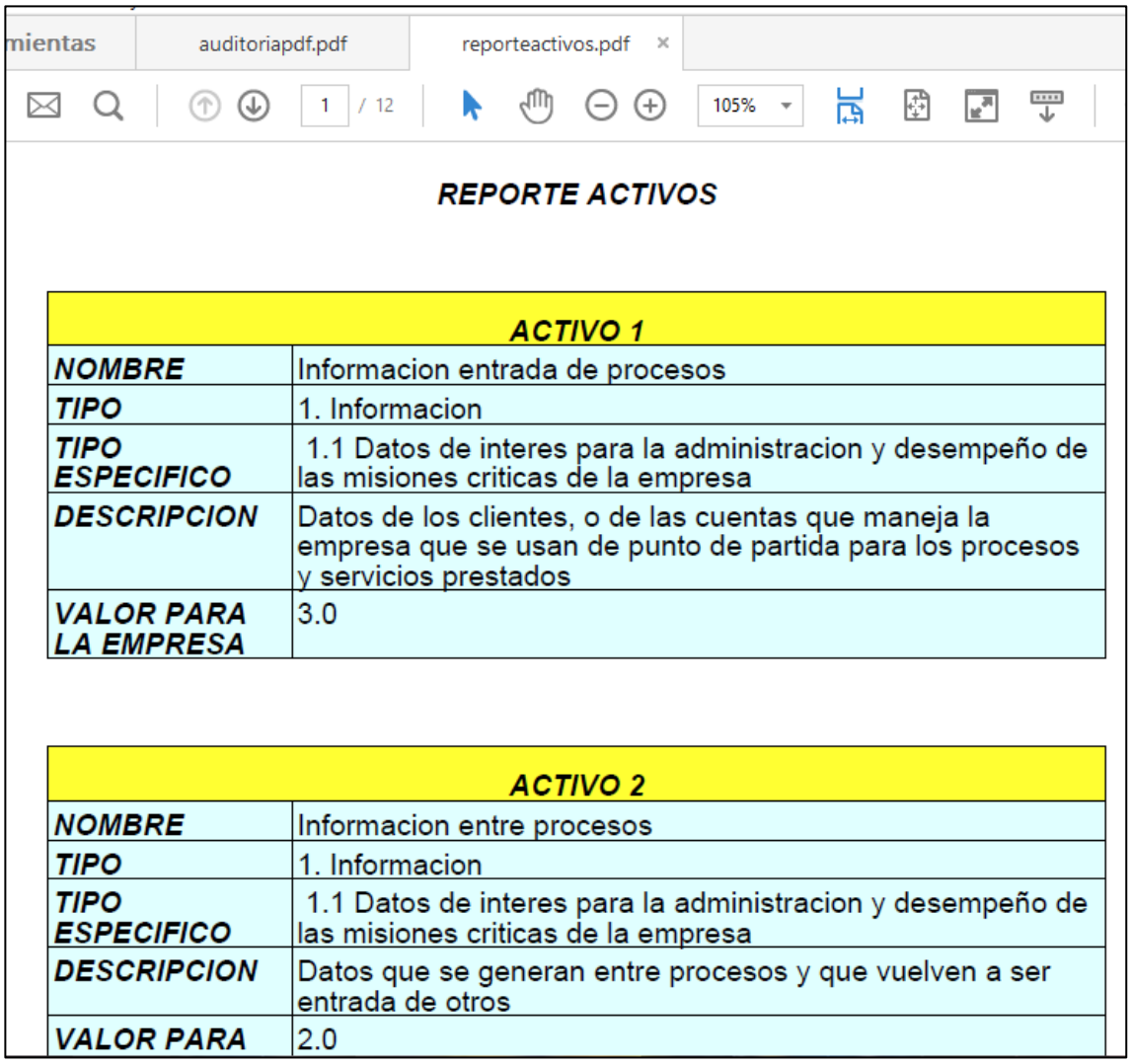
Figura 112. Reporte auditoría generado en pdf



NOMBRE COLABORADOR	DOMINIO ASIGNADO
Dario Mera	5. Politica de seguridad
Dario Mera	6. Organizacion de la seguridad de la informacion
Dario Mera	7. Gestion de activos
Dario Mera	8. Seguidad de los recusos humanos
Dario Mera	9. Seguridad física y ambiental
Dario Mera	10. Gestion de las comunicaciones y las operaciones
James Caivio	11. Control de acceso
James Caivio	12. Adquisicion , desarrollo y mantenimiento de los sistemas de informacion
James Caivio	13. Gestion de los incidentes de seguridad de la informacion
James Caivio	14. Gestion de la continuidad comercial
James Caivio	15. Cumplimiento

Este reporte es tomado del software, se genera en formato pdf, consta de dos páginas, se lo puede ver completo en Anexo 3 Reportes. (ver figura 112)

Figura 113. Reporte activos generados en pdf



REPORTE ACTIVOS

ACTIVO 1	
NOMBRE	Informacion entrada de procesos
TIPO	1. Informacion
TIPO ESPECIFICO	1.1 Datos de interes para la administracion y desempeño de las misiones criticas de la empresa
DESCRIPCION	Datos de los clientes, o de las cuentas que maneja la empresa que se usan de punto de partida para los procesos y servicios prestados
VALOR PARA LA EMPRESA	3.0

ACTIVO 2	
NOMBRE	Informacion entre procesos
TIPO	1. Informacion
TIPO ESPECIFICO	1.1 Datos de interes para la administracion y desempeño de las misiones criticas de la empresa
DESCRIPCION	Datos que se generan entre procesos y que vuelven a ser entrada de otros
VALOR PARA	2.0

Este reporte es tomado del software, se genera en formato pdf, consta de 14 páginas, se lo puede ver completo en Anexo 3, Reportes. (ver figura 113)

Figura 114. Reporte controles generado en pdf

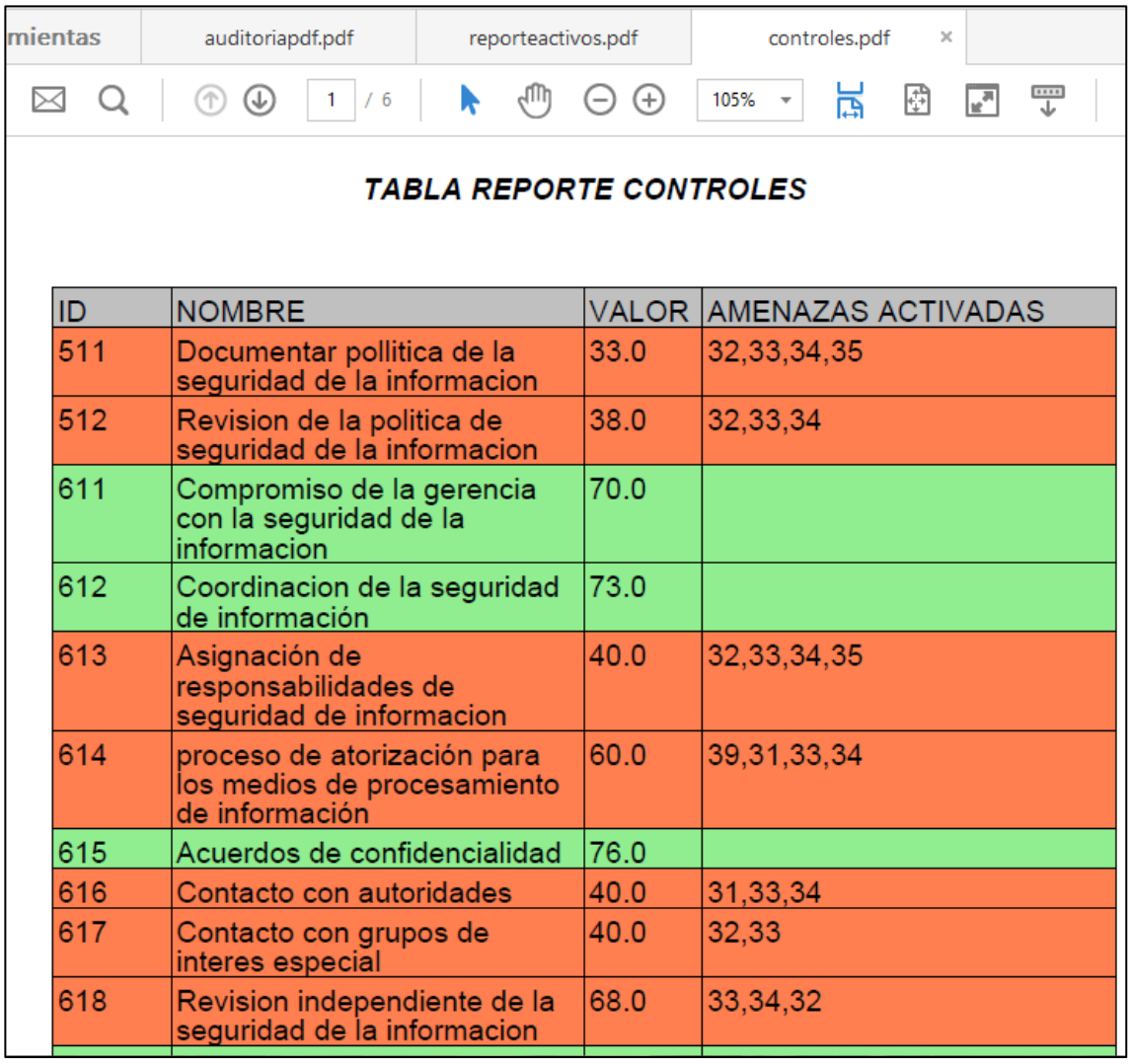
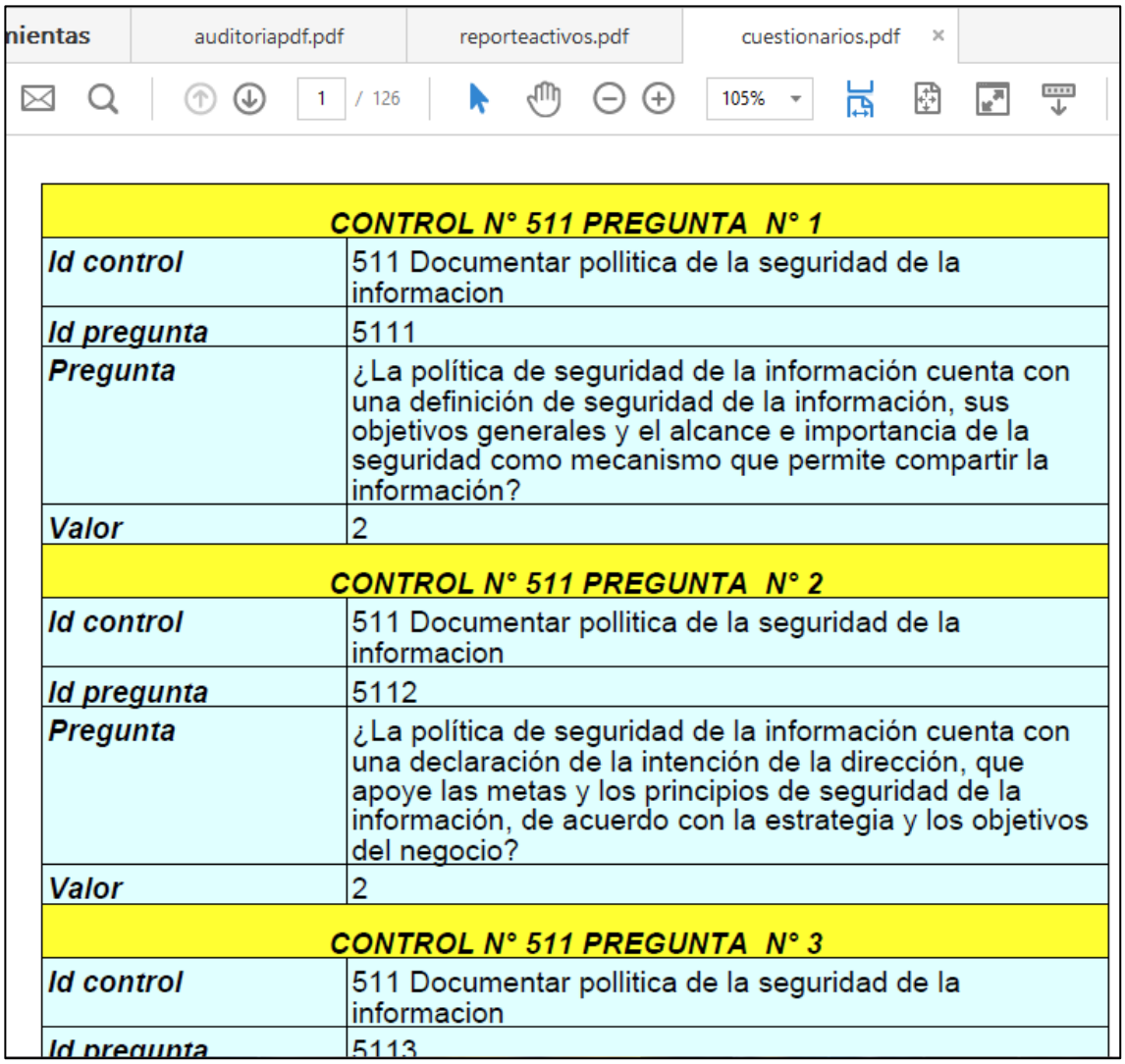


TABLA REPORTE CONTROLES

ID	NOMBRE	VALOR	AMENAZAS ACTIVADAS
511	Documentar pollitica de la seguridad de la informacion	33.0	32,33,34,35
512	Revision de la politica de seguridad de la informacion	38.0	32,33,34
611	Compromiso de la gerencia con la seguridad de la informacion	70.0	
612	Coordinacion de la seguridad de información	73.0	
613	Asignación de responsabilidades de seguridad de informacion	40.0	32,33,34,35
614	proceso de atorización para los medios de procesamiento de información	60.0	39,31,33,34
615	Acuerdos de confidencialidad	76.0	
616	Contacto con autoridades	40.0	31,33,34
617	Contacto con grupos de interes especial	40.0	32,33
618	Revision independiente de la seguridad de la informacion	68.0	33,34,32

Este reporte es tomado del software, se genera en formato pdf, consta de seis páginas, se lo puede ver completo en Anexo 3, Reportes. (ver figura 114)

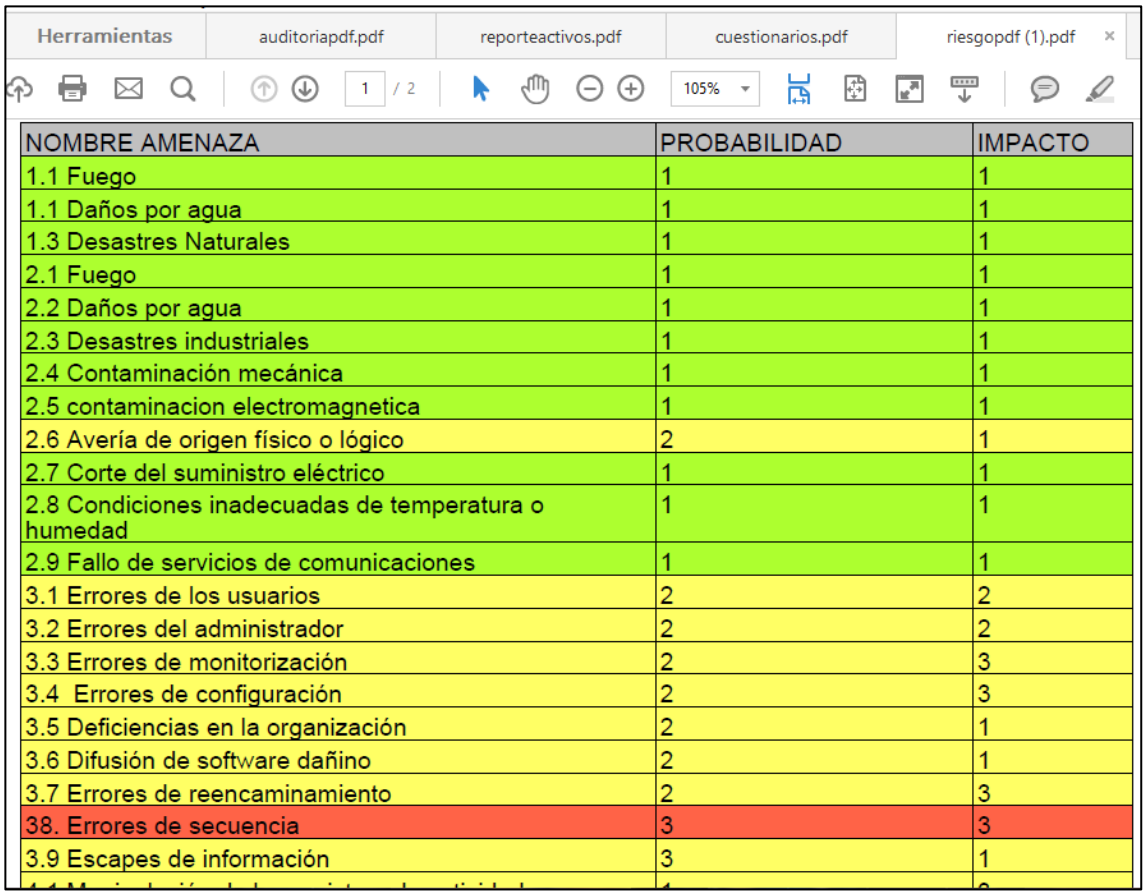
Figura 115. Reporte cuestionarios generado en pdf



CONTROL N° 511 PREGUNTA N° 1	
Id control	511 Documentar pollitica de la seguridad de la informacion
Id pregunta	5111
Pregunta	¿La política de seguridad de la información cuenta con una definición de seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información?
Valor	2
CONTROL N° 511 PREGUNTA N° 2	
Id control	511 Documentar pollitica de la seguridad de la informacion
Id pregunta	5112
Pregunta	¿La política de seguridad de la información cuenta con una declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio?
Valor	2
CONTROL N° 511 PREGUNTA N° 3	
Id control	511 Documentar pollitica de la seguridad de la informacion
Id pregunta	5113

Este reporte es tomado del software, se genera en formato pdf, consta de 126 páginas, se lo puede ver completo en Anexo 3, Reportes. (ver figura 115)

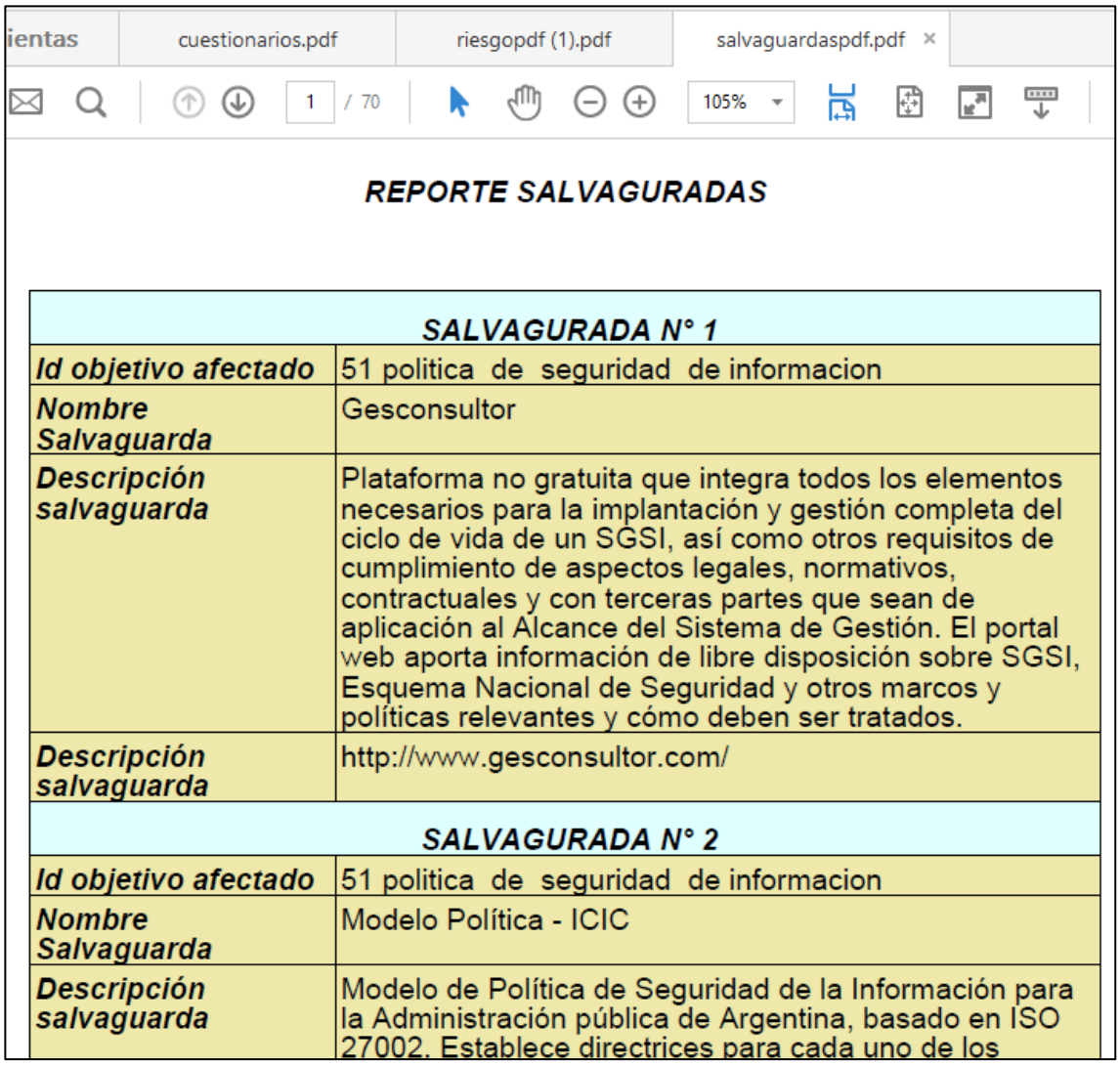
Figura 116. Reporte Matriz de riesgos generado en pdf



NOMBRE AMENAZA	PROBABILIDAD	IMPACTO
1.1 Fuego	1	1
1.1 Daños por agua	1	1
1.3 Desastres Naturales	1	1
2.1 Fuego	1	1
2.2 Daños por agua	1	1
2.3 Desastres industriales	1	1
2.4 Contaminación mecánica	1	1
2.5 contaminacion electromagnetica	1	1
2.6 Avería de origen físico o lógico	2	1
2.7 Corte del suministro eléctrico	1	1
2.8 Condiciones inadecuadas de temperatura o humedad	1	1
2.9 Fallo de servicios de comunicaciones	1	1
3.1 Errores de los usuarios	2	2
3.2 Errores del administrador	2	2
3.3 Errores de monitorización	2	3
3.4 Errores de configuración	2	3
3.5 Deficiencias en la organización	2	1
3.6 Difusión de software dañino	2	1
3.7 Errores de reencaminamiento	2	3
38. Errores de secuencia	3	3
3.9 Escapes de información	3	1

Este reporte es tomado del software, se genera en formato pdf, consta de dos páginas, se lo puede ver completo en Anexo 3, Reportes. (ver figura 116)

Figura 117. Reporte Salvaguardas generado en pdf



ientas | cuestionarios.pdf | riesgopdf (1).pdf | salvaguardaspdf.pdf ×

1 / 70 105%

REPORTE SALVAGURADAS

SALVAGURADA N° 1	
Id objetivo afectado	51 politica de seguridad de informacion
Nombre Salvaguarda	Gesconsultor
Descripción salvaguarda	Plataforma no gratuita que integra todos los elementos necesarios para la implantación y gestión completa del ciclo de vida de un SGSI, así como otros requisitos de cumplimiento de aspectos legales, normativos, contractuales y con terceras partes que sean de aplicación al Alcance del Sistema de Gestión. El portal web aporta información de libre disposición sobre SGSI, Esquema Nacional de Seguridad y otros marcos y políticas relevantes y cómo deben ser tratados.
Descripción salvaguarda	http://www.gesconsultor.com/
SALVAGURADA N° 2	
Id objetivo afectado	51 politica de seguridad de informacion
Nombre Salvaguarda	Modelo Política - ICIC
Descripción salvaguarda	Modelo de Política de Seguridad de la Información para la Administración pública de Argentina, basado en ISO 27002. Establece directrices para cada uno de los

Este reporte es tomado del software, se genera en formato pdf, consta de 70 páginas, se lo puede ver completo en Anexo 3, Reportes. (ver figura 117)

3.3.9 Especificaciones técnicas. En la implementación del aplicativo, se utilizó el lenguaje de programación java, JavaScript (Js), Java Servers Pages (jsp), con el entorno de desarrollo integrado (IDE) NetBeans, para crear el sitio web y Postgresql para crear la base de datos que utiliza el sistema.

Gestor de base de datos postgresql. En la actualidad, el software de base de datos ha experimentado un crecimiento extraordinario, debido a la gran cantidad de información que manejan la totalidad de organizaciones de hoy en día. Esta es la razón, que existan muchos gestores de base de datos, que permiten manejar la información de forma más sencilla. En este sentido encontramos a MySQL™, PostgreSQL[14]., Oracle®, Microsoft® SQL Server® entre otros.

Netbeans. Permite rápida y fácilmente desarrollar aplicaciones de escritorio Java, móviles y aplicaciones web, así como aplicaciones HTML5 con HTML, JavaScript y CSS. El IDE también proporciona un gran conjunto de herramientas para desarrolladores de PHP y C / C ++. Es gratuito y de código abierto y tiene una gran comunidad de usuarios y desarrolladores de todo el mundo. Se apoya en bibliotecas de terceros como jQuery.

Lenguaje JavaScript. Abreviado comúnmente JS es un lenguaje de programación interpretado, o para ser más claro: Es para el que la mayoría de sus implementaciones ejecuta las instrucciones directamente, sin una previa compilación del programa a instrucciones en lenguaje máquina.

Además orientado a objetos, basado en prototipos, imperativo, y dinámico.

Se utiliza principalmente en su forma del lado del cliente (client-side), implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas aunque existe una forma de JavaScript del lado del servidor (Server-side JavaScript)

Todos los navegadores modernos interpretan el código JavaScript integrado en las páginas web. Para interactuar con una página web se provee al lenguaje JavaScript de una implementación del Document Object Model (DOM).

Actualmente es ampliamente utilizado para enviar y recibir información del servidor junto con ayuda de otras tecnologías como AJAX que también hemos utilizado para el desarrollo del proyecto, Permitiendo a las páginas hacer una pequeña petición de datos al servidor y recibirla sin necesidad de cargarla página entera. El incremento de las actualizaciones “on the fly” elimina el tener que refrescar el navegador, algo bastante apreciado a la hora de operar en una aplicación web. JavaScript se interpreta en el agente de usuario al mismo tiempo que las sentencias van descargándose junto con el código HTML y JSP podemos crear aplicaciones web que se ejecuten en variados servidores web, de múltiples plataformas, ya que Java es en esencia un lenguaje multiplataforma.[15]

Lenguaje JAVA. La programación orientada a objetos te da la posibilidad de escribir una vez y utilizar muchas veces un objeto (procedimiento, método, etc). En pocas palabras, te permite simplificar tu código y te evita la necesidad de copiar y pegar muchas veces un mismo procedimiento.

Javaserver pages. JavaServer Pages (JSP) es una tecnología que ayuda a los desarrolladores de software a crear páginas web dinámicas basadas en HTML, XML, entre otros tipos de documentos. JSP es similar a PHP, pero usa el lenguaje de programación Java.

Para desplegar y correr JavaServer Pages, se requiere un servidor web compatible con contenedores servlet como Apache Tomcat o Jetty.

La principal ventaja de JSP frente a otros lenguajes es que el lenguaje Java es un lenguaje de propósito general que excede el mundo web y que es apto para crear clases que manejen lógica de negocio y acceso a datos de una manera prolija. Esto permite separar en niveles las aplicaciones web, dejando la parte encargada de generar el documento HTML en el archivo JSP.

Para terminar se usan estos lenguajes porque algunas vez un docente de gran conocimiento y carisma nos dijo mucho sobre por qué utilizarlos, de lo cual lo que más se me grabo y aún recuerdo con una enorme sonrisa es: “si alguna vez se casan háganlo orientado a objetos”. [16]

3.4 FASE DE PRUEBAS Y MANTENIMIENTO

A través de las iteraciones de las implementaciones del producto, se entregaron diferentes prototipos al director de la auditoría, en primera instancia, de estas entregas se dieron algunas mejoras especificadas a continuación.
Cabe denotar que acorde a la metodología usada, las pruebas no se hicieron en la parte final del proceso si no que al final de cada iteración.

3.4.1 Mejoras por iteraciones

Creación y posibilidad de trabajar diferentes proyectos a la vez. El producto software presentaba el inconveniente de trabajar con una conexión a la base de datos y de no permitir trabajar con una nueva mientras esta no se cerrara y terminara.

Clasificación de la auditoría por categorías. En primera instancia el usuario debía elegir los dominios y sus consecuentes subcategorías en la forma en que venían presentados en la norma ISO 27001, en siguientes iteraciones del sistema

se clasifican los dominios en categorías tales como redes, sistemas operativos, seguridad física, acceso, entre otras, con el fin de que el usuario solo deba elegir una y en ese orden de ideas le aparezcan las áreas de la norma correspondientes a su elección.

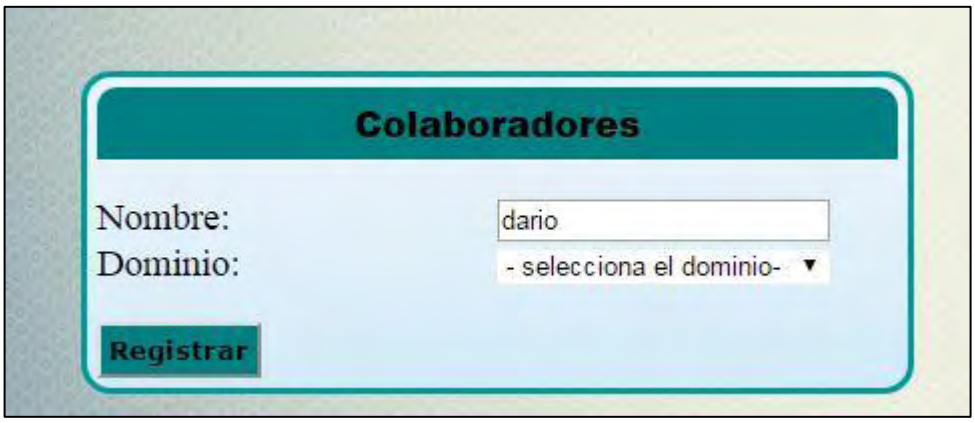
Evaluación de la auditoría por dimensiones de seguridad. Se implementó la posibilidad de elegir las áreas de auditoría a evaluar dependiendo de los objetivos de control que afecten a una de las tres dimensiones de seguridad: disponibilidad integridad y confiabilidad.

3.4.2 Pruebas. Se realizaron procesos de validación, verificación, y demostración del sistema en tres tipos diferente de pruebas, detallados a continuación:

Pruebas de validación. Se utilizaron usuarios con bajo nivel de conocimiento en áreas de uso de sistemas de computación y de auditoría con el fin de comprobar que el software este delimitado en inserción de valores correctos o posibles y de que no permita avanzar si algún paso o procedimiento se haya omitido o se haya llevado a cabo de manera errónea.

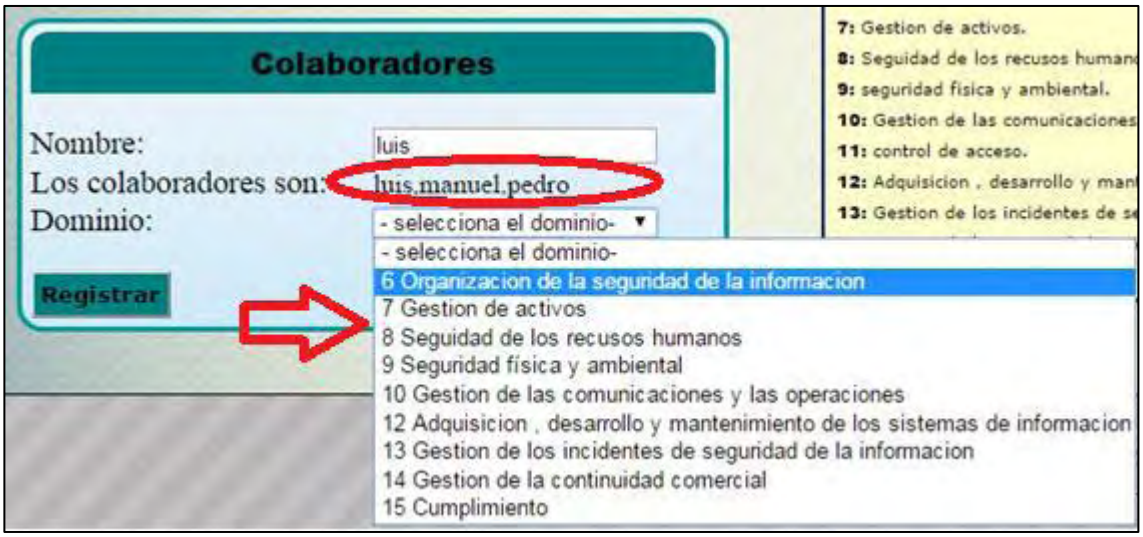
Error 1: No se distingue que se ingresen solo los usuarios validos. (ver figura 118)

Figura 118. Error 1



Mejora 1. En primera instancia se listan los usuarios posibles para ser ingresados, luego se puede proceder a ingresarlos, tienen que ser los mismos que se ingresó anteriormente en los datos de auditoría. (ver figura 119)

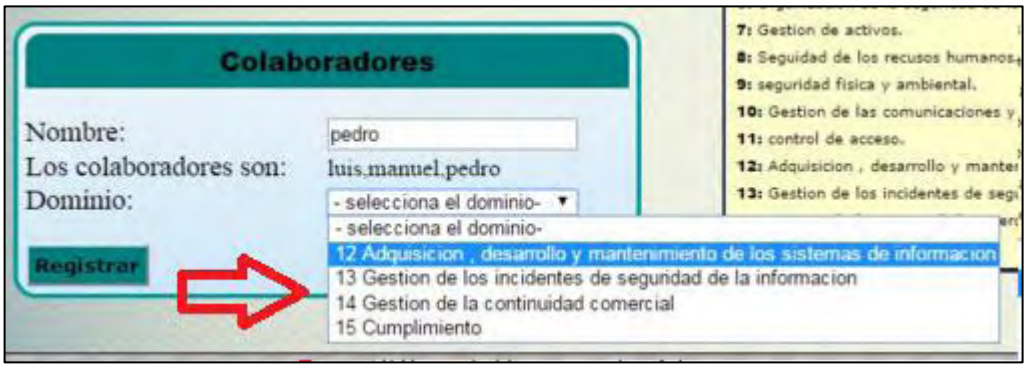
Figura 119. Mejora 1



Error 2. No se despliegan todos los dominios para asignarlos al usuario, además los usuarios presentan la sugerencia de que un dominio asignado no vuelva a salir en la lista.

Mejora 2. Como se observa en la figura, en el formulario colaboradores solo se pueden ingresar los usuarios ingresados en el formulario auditoría, además se despliega la lista de dominios para asignárselos a un usuario, solo si no se han asignado anteriormente. (ver figura 120)

Figura 120. Mejora 2



En esta figura se observa que los dominios del cinco al once ya han sido asignados y al usuario “pedro” solo se le permite elegir entre los restantes.

Además de ello, el software no permite avanzar siempre y cuando no se hallan asignado todos los dominios a un usuario.

Error 3. Después de registrar un usuario el aviso de usuario adicionado no desaparece luego intentar iniciar una nueva sesión. (ver figura 121)

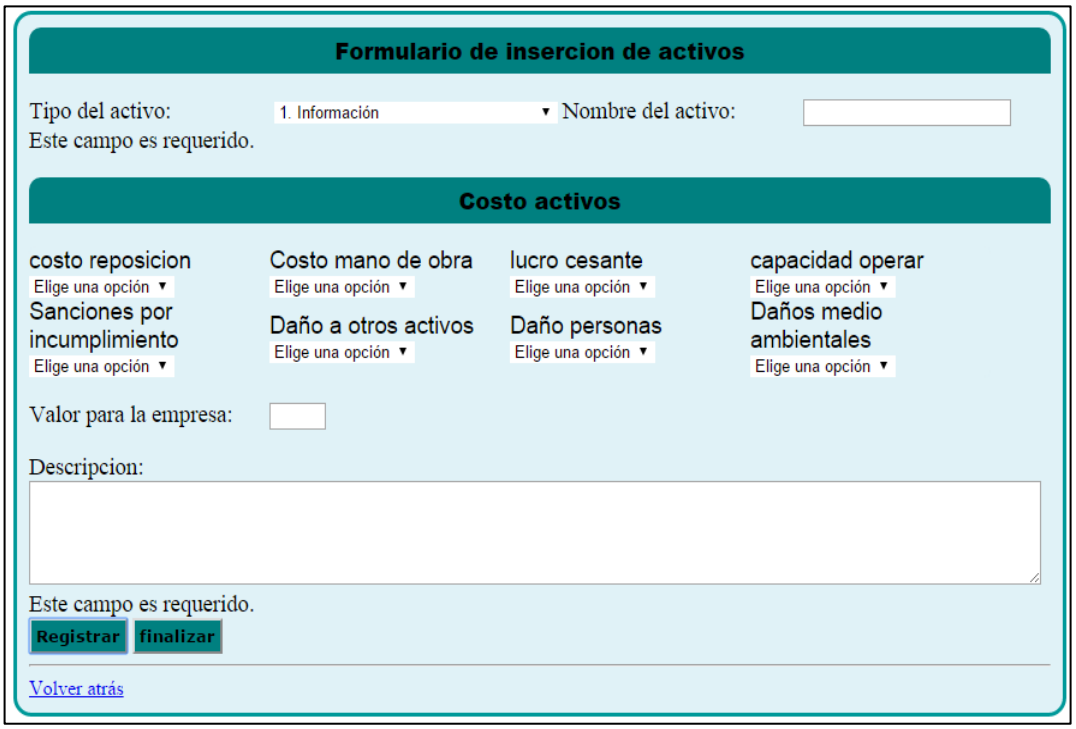
Figura 121. Error 3

Mejora 3. El aviso desaparece luego de hacer una inserción correcta y deja el formulario listo para registrar un nuevo usuario si es preciso. (ver figura 122)

Figura 122. Corrección error 3

Error 4. Al intentar registrar un activo sin diligenciar todos los campos solo aparece un aviso de campo requerido, mas no se especifica cual es. (ver figura 122)

Figura 123. Error 4



Mejora 4. Se da aviso de la falta de ingreso de uno o más campos de la sección de dimensiones de activos, y se diferencia también si el campo faltante es el tipo o subtipo de activos. (ver figura 124)

Figura 124. Mejora 4, aviso de no elección de dimensiones de activos

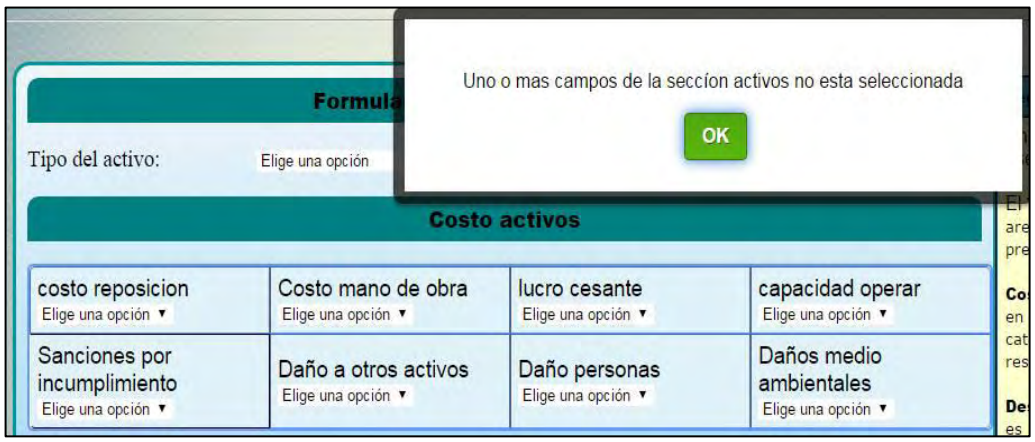
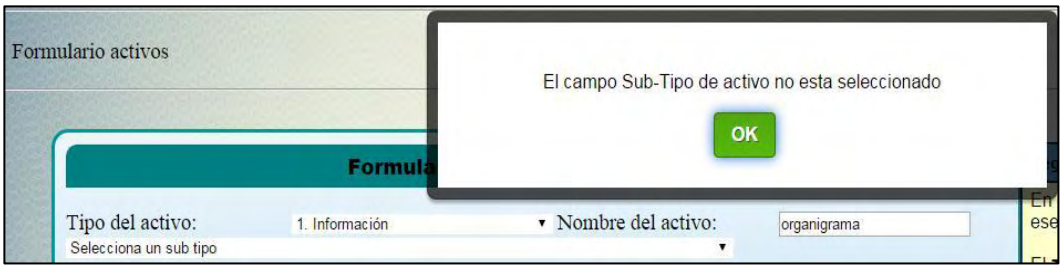
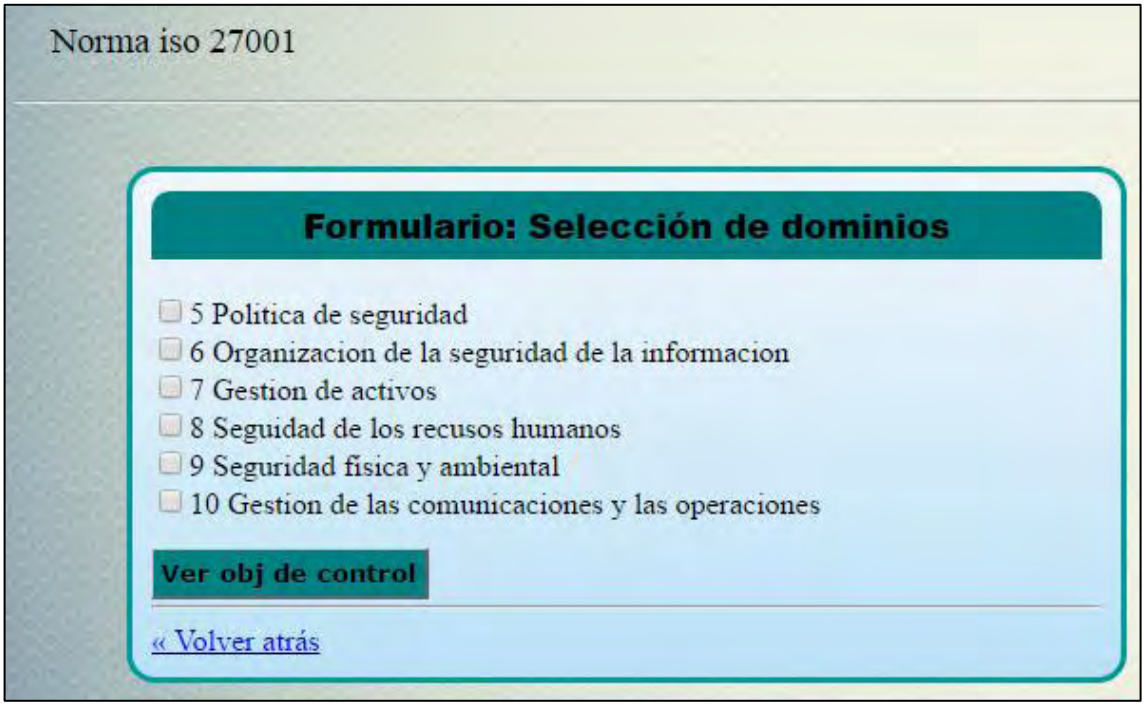


Figura 125. Mejora 4, aviso de no elección de tipo de activos



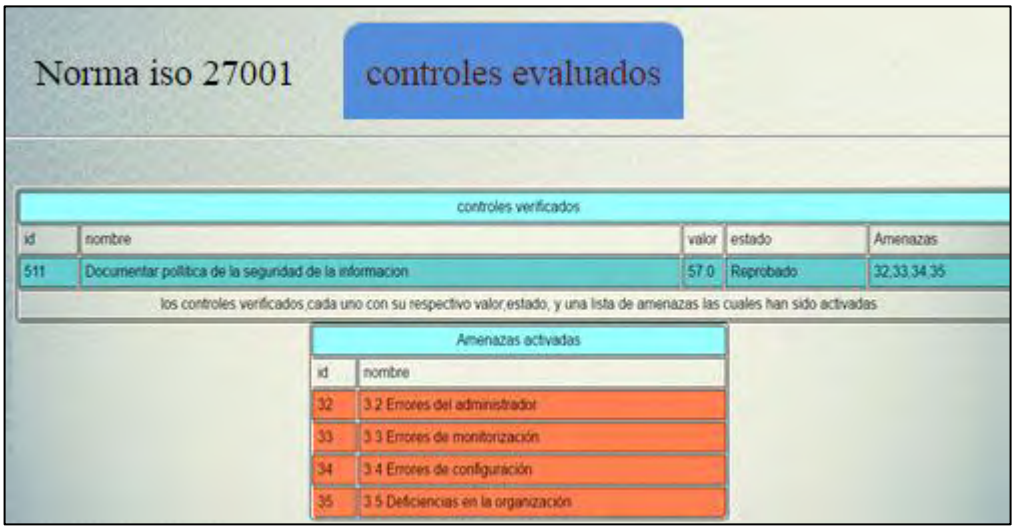
Error 5. No se cuenta con una lista de los controles y cuestionarios verificados antes de proceder a evaluar uno nuevo. Es necesario realizar el proceso de evaluación para poder mirar la lista. (ver figura 126)

Figura 126. Error 5



Mejora 5. Al lado del botón de Norma ISO 27001 aparece un botón que permite ver los controles ya evaluados para proceder con los faltantes. (ver figura 127)

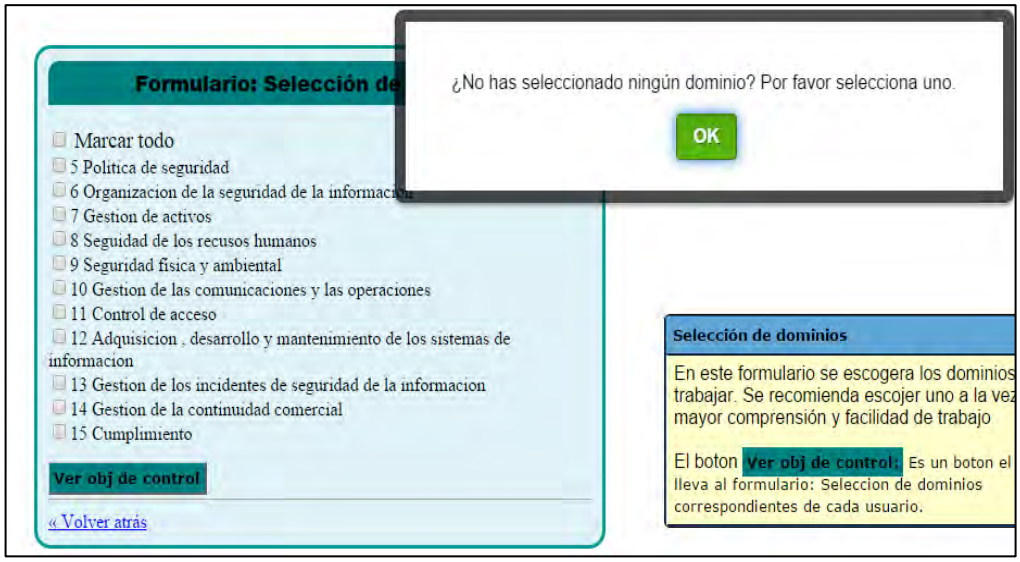
Figura 127. Mejora 5



Error 6. En el formulario de dominios al intentar acceder al siguiente nivel sin seleccionar un objetivo de control, el sistema no avanza, pero no muestra el por qué no va al siguiente nivel

Mejora 6. Aparece el aviso correspondiente. (ver figura 128)

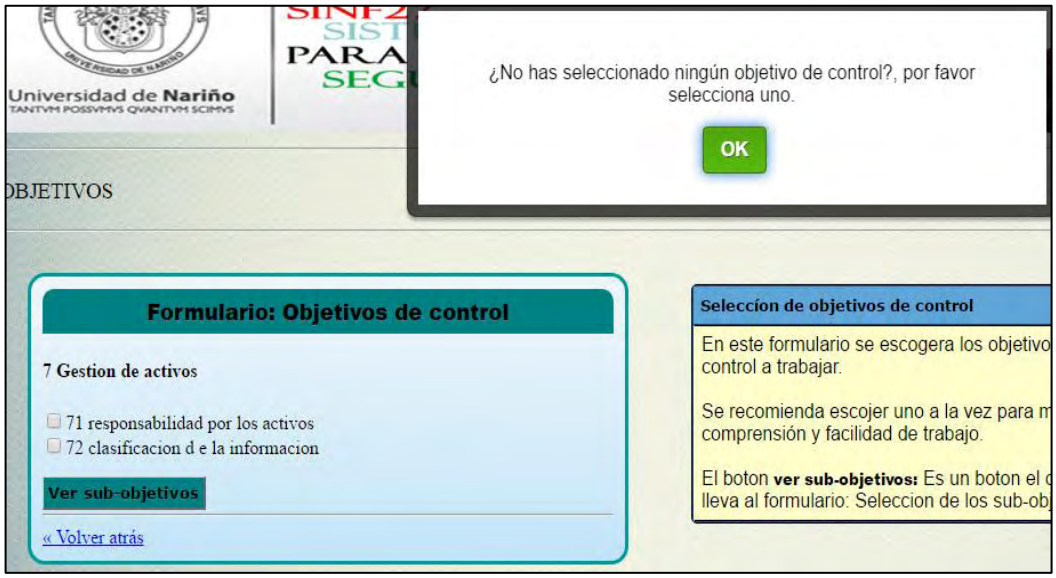
Figura 128. Mejora 6



Error 7. En el formulario de objetivos de control al intentar acceder al siguiente nivel sin seleccionar un sub objetivo de control, el sistema no avanza, pero no muestra el por qué no va al siguiente nivel. (ver figura 129)

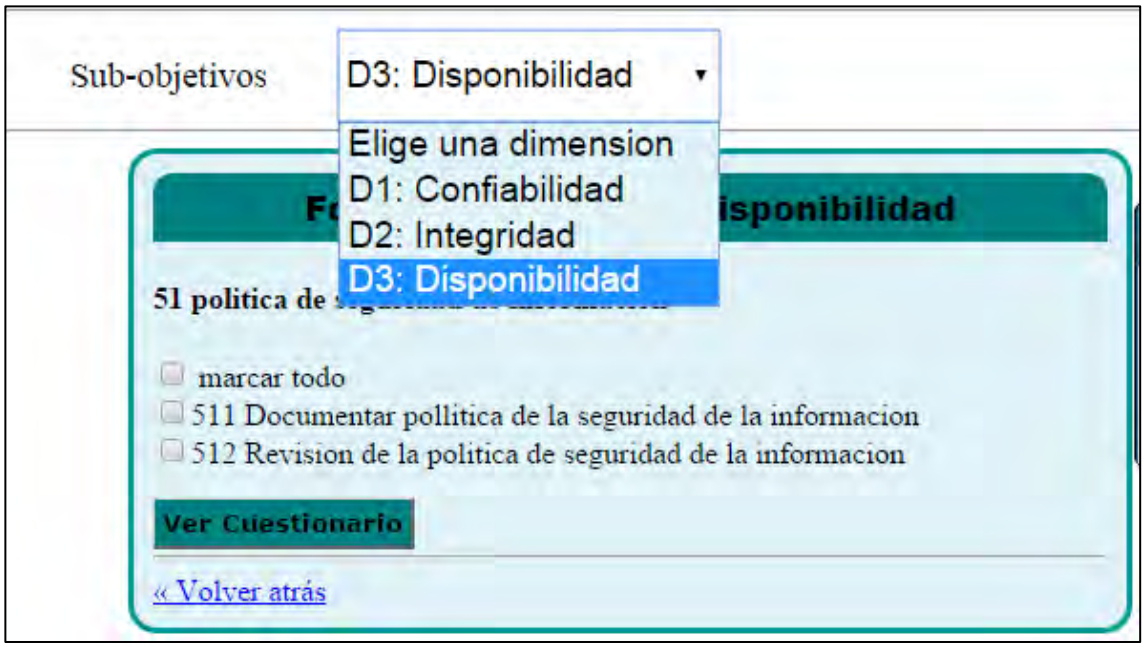
Mejora 7. Aparece el aviso correspondiente.

Figura 129. Mejora 7



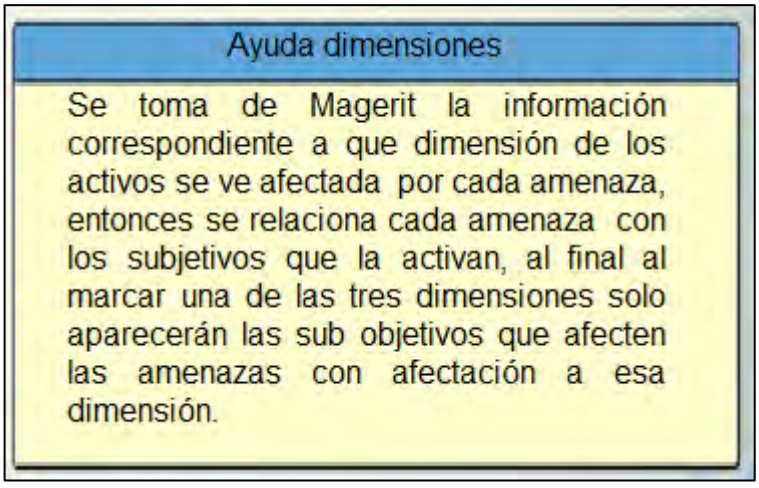
Error 8. Los usuarios manifestaron no entender el propósito de la lista que muestra las tres dimensiones de seguridad, hace falta la ayuda que explique su funcionamiento. (ver figura 130)

Figura 130. Error 8



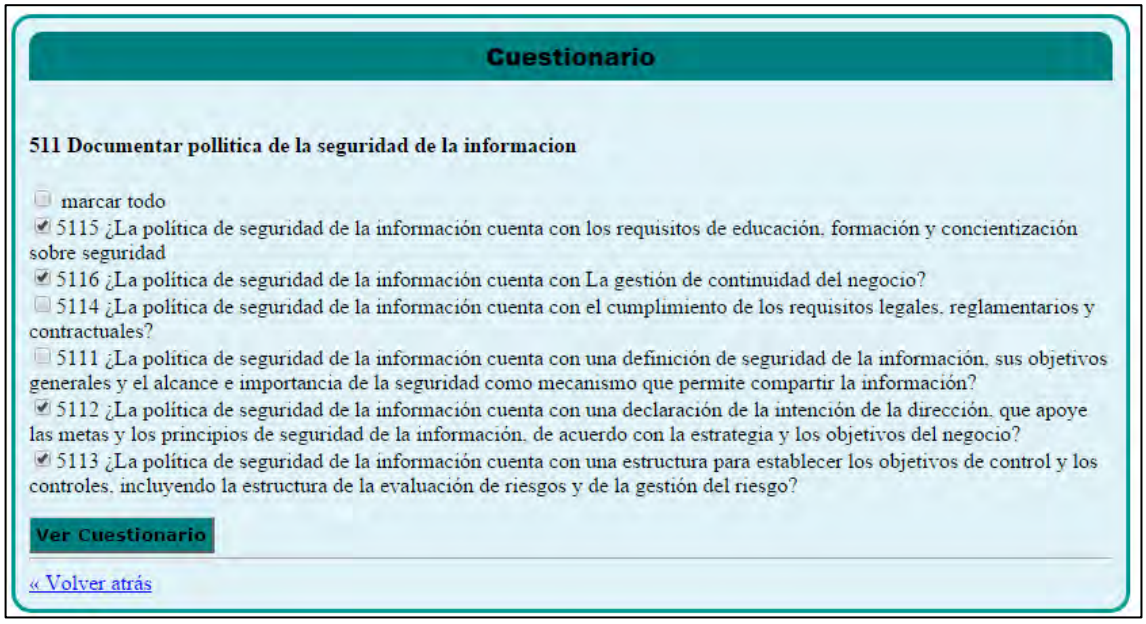
Mejora 8. Se toma de Magerit la información correspondiente a que dimensión de los activos se ve afectada por cada amenaza, entonces se relaciona cada amenaza con los subjetivos que la activan, al final al marcar una de las tres dimensiones solo aparecerán las sub objetivos que afecten las amenazas con afectación a esa dimensión. (ver figura 131)

Figura 131. Mejora 8



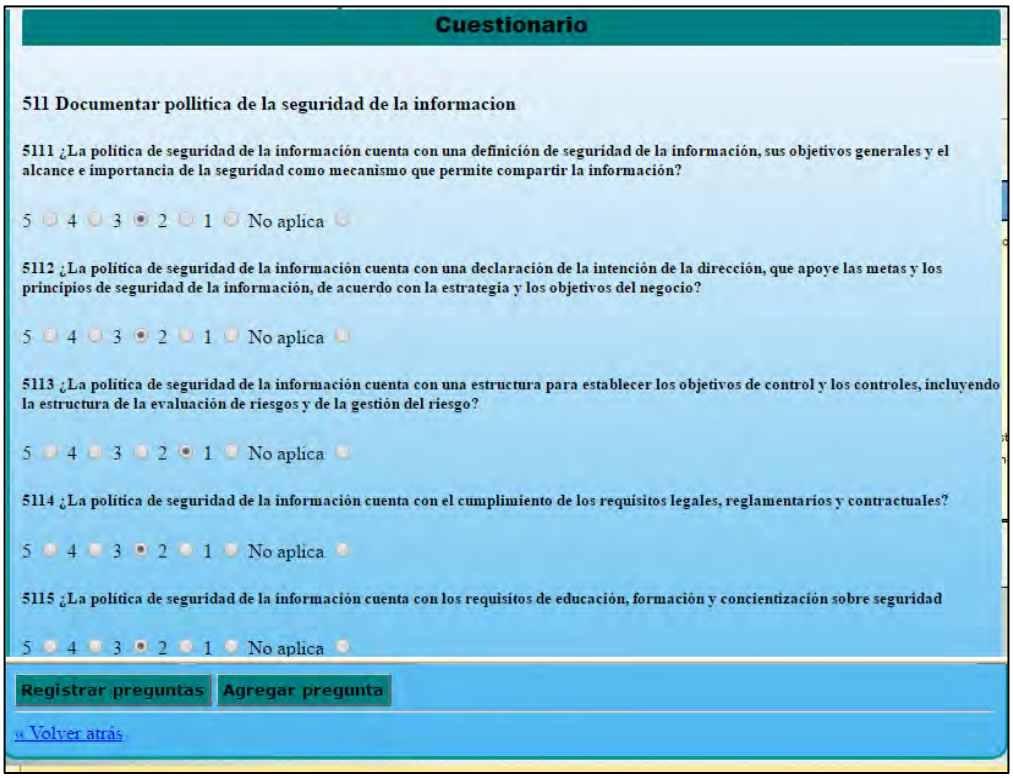
Error 9. Es necesario elegir las preguntas que harán parte del cuestionario y luego en otro paso acceder al cuestionario, a los usuarios les pareció más fácil acceder al cuestionario en un solo paso y que exista una opción de “no aplica” si la pregunta no se hace valida. (ver figura 132)

Figura 132. Error 9



Mejora 9. Se implementó el pedido de los usuarios.

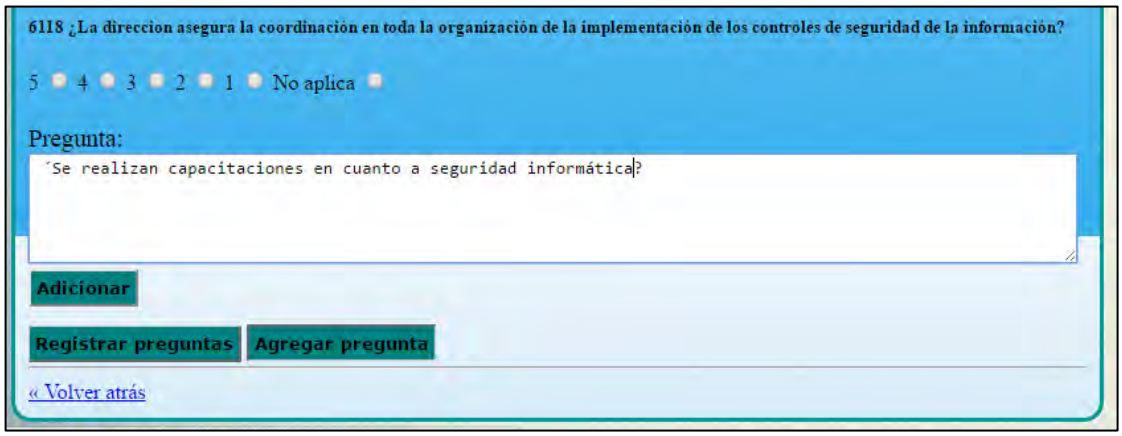
Figura 133. Mejora 9



Error 10. No existe la posibilidad de agregar más preguntas que las existentes.

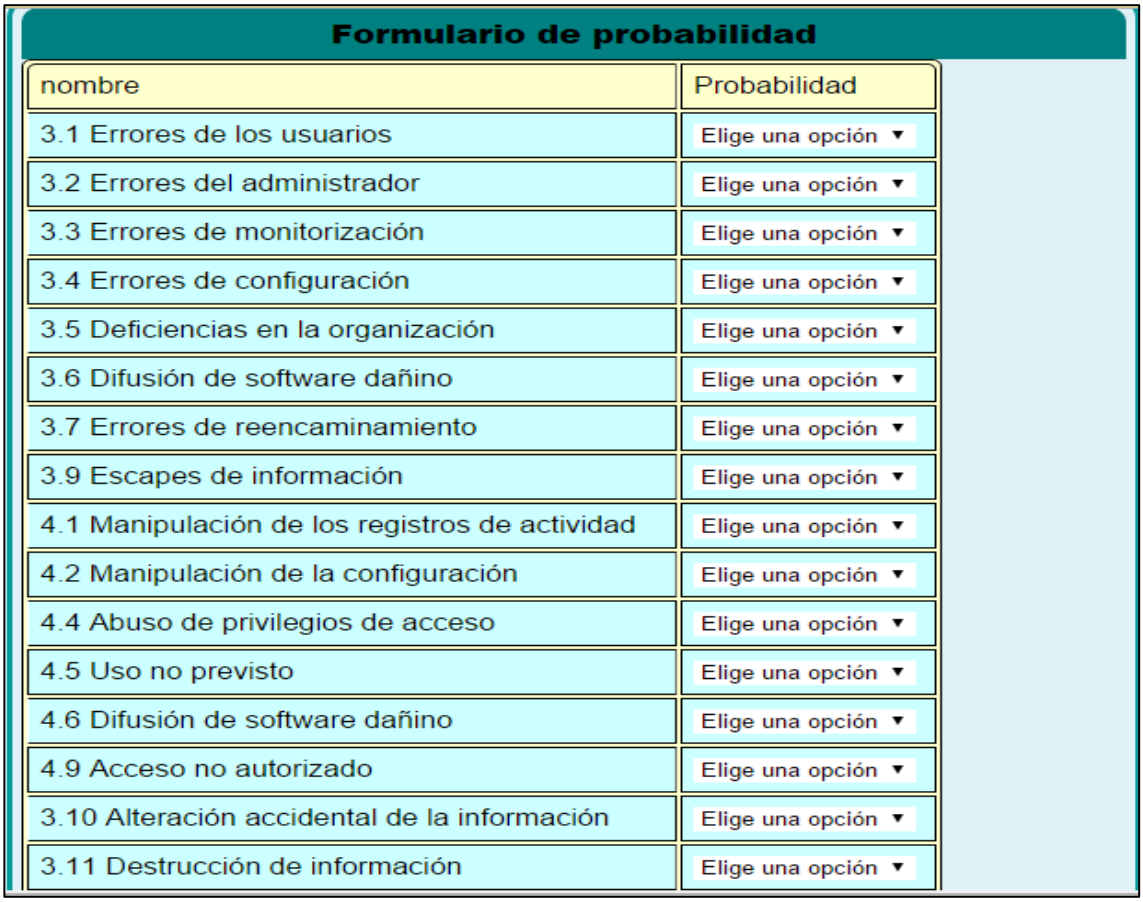
Mejora 10: Se ingresa la pregunta y se la puede responder de la misma forma que las demás. (ver figura 134)

Figura 134. Mejora 10



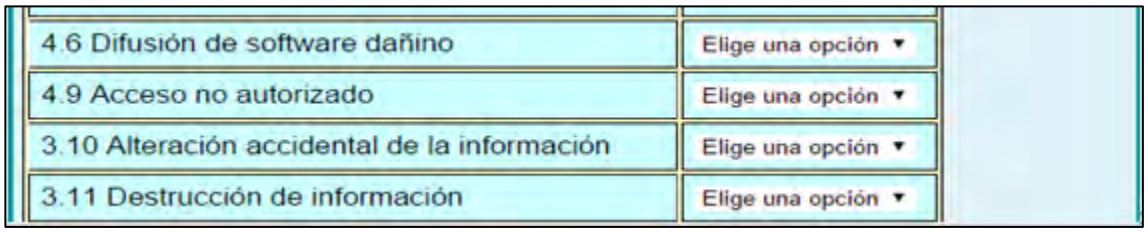
Error 11. Cada vez que se evalué un nuevo control es necesario ingresar el valor de la probabilidad para todas las amenazas, lo correcto sería que solo halla que ingresar las de las amenazas evaluadas por el último control evaluado. (ver figura 135)

Figura 135. Error 11



Mejora 11. Solo se actualizan las probabilidades que no cuentan con ingreso de probabilidad. (ver figura 136)

Figura 136. Mejora 11



Error 12. No hay un módulo organizado que presente todos los reportes que brinda el sistema. (ver figura 137)

Mejora 12. Seimplemento el modulo reportes

Figura 137. Mejora 12

Pruebas de satisfacción. Este tipo de pruebas estuvo enfocado hacia usuarios con buenos conocimientos en áreas de uso de sistemas de computación y de auditoría, a los cuales se les hizo una demostración del software con un ejercicio real y se les pidió que respondieran un formulario de satisfacción, en total se registraron 15 respuestas.

A cada individuo se lo clasificó en diferentes categorías según sus conocimientos para que de acuerdo a eso responda las preguntas.

El Formulario se realizó con la herramienta Google formas.

Los Participantes de las pruebas fueron estudiantes de ingeniería de sistemas todos de semestre 10, o egresados, para veracidad de la prueba se los nombran a continuación. (ver tabla 3)

Tabla 3. Participantes pruebas de satisfacción

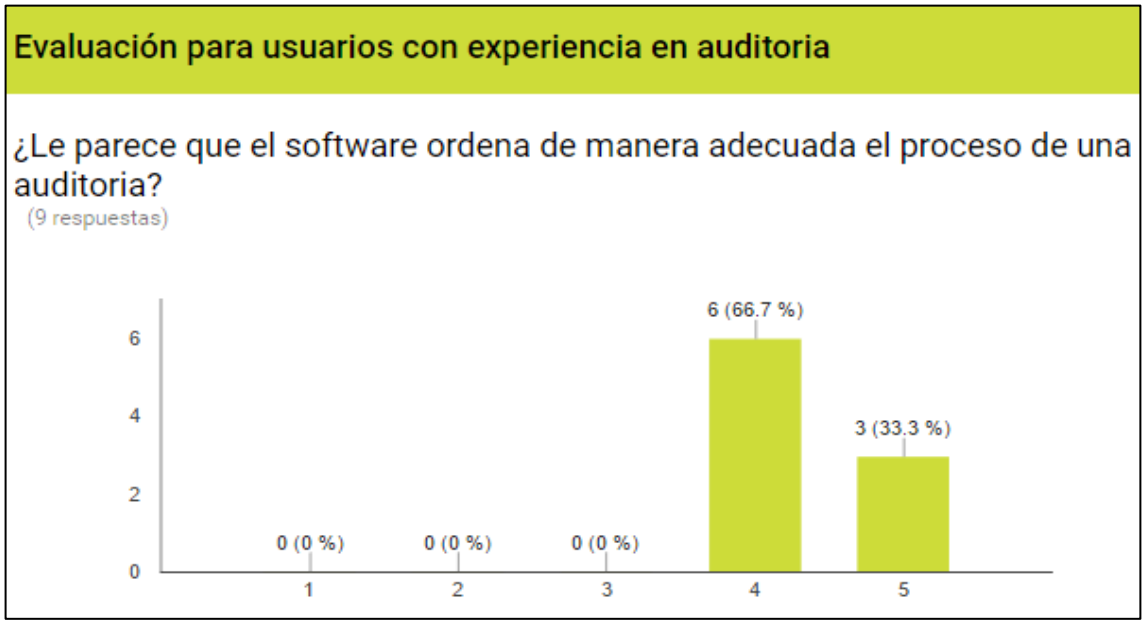
Numero	Nombre	Código Udenar
1	Carlos Muñoz	29036214
2	Luis Eduardo Narvaez	22034227
3	Mauricio Aza	2120361004
4	Cristhian Naranjo	29034287
5	Nelson Quema	28034282
6	Tatiana Castro	2101511042
7	Santiago Martínez	27034245
8	Jair Calderón	28034273
9	Jorge Luis Viveros	28034284
10	David Gómez	29034224
11	Daniel Lara	27036226
12	Francisco de la Rosa	25151232
13	David Fernando Baez	27036217
14	Santiago Cordoba	29034222
15	Wilmer Ordoñez	28039225

Figura 138. Resultado pregunta 1

A partir de esta pregunta se clasificó a los individuos en dos secciones: para poder evaluar diferentes tipos de usuarios y aplicarles diferentes preguntas según su conocimiento, se observa que hay suficientes individuos para los 2 casos y que la mayoría tiene conocimientos en procesos e auditoría.

Sección usuarios con experiencia en procesos de auditoría: para esta sección se usaron preguntas tipo rango, de uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 139)

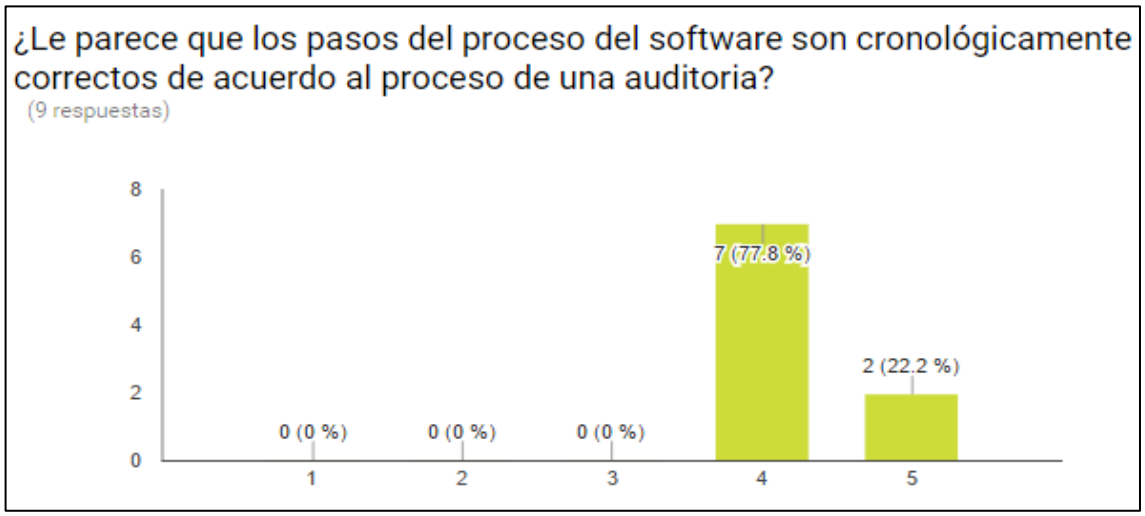
Figura 139. Resultado pregunta 2



De esta gráfica se infiere que los individuos encuestados están conformes con la forma en que el software ordena el proceso de una auditoría.

El 100% de las respuestas es igual o mayor a cuatro y el 33.3% de ellas es de satisfacción máxima. (ver figura 140)

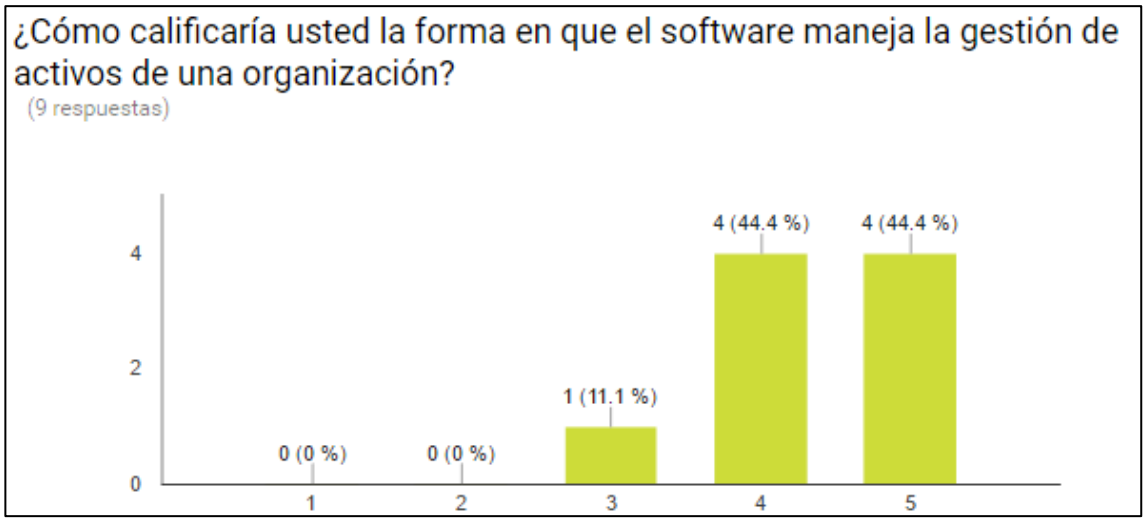
Figura 140. Resultado pregunta 3



De esta gráfica se infiere que los individuos encuestados están conformes con la forma en que se presentan cronológicamente los pasos del proceso de una auditoría.

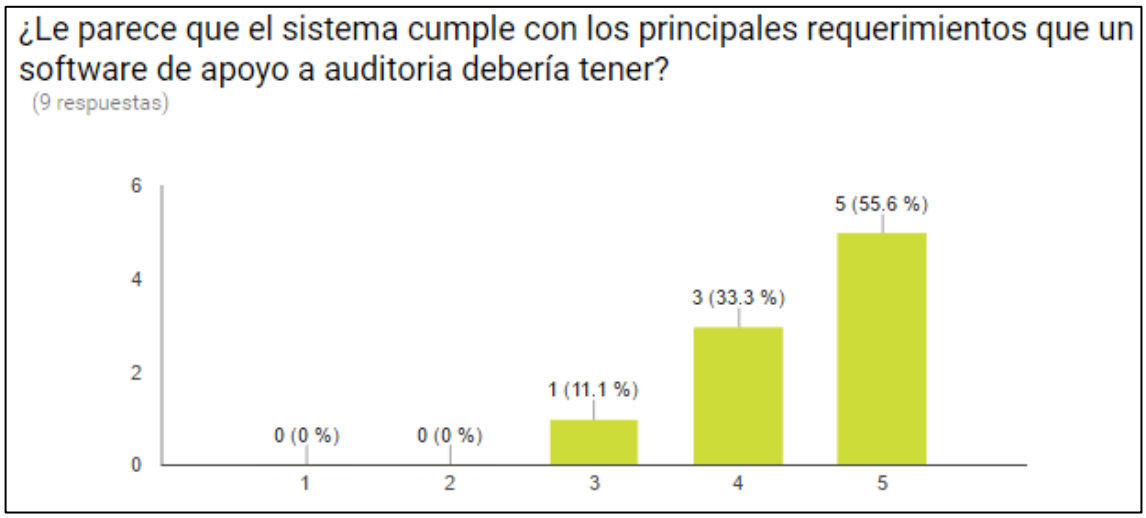
El 100% de las respuestas es igual o mayor a cuatro y el 22.2% de ellas es de satisfacción máxima. (ver figura 141)

Figura 141. Pregunta 4



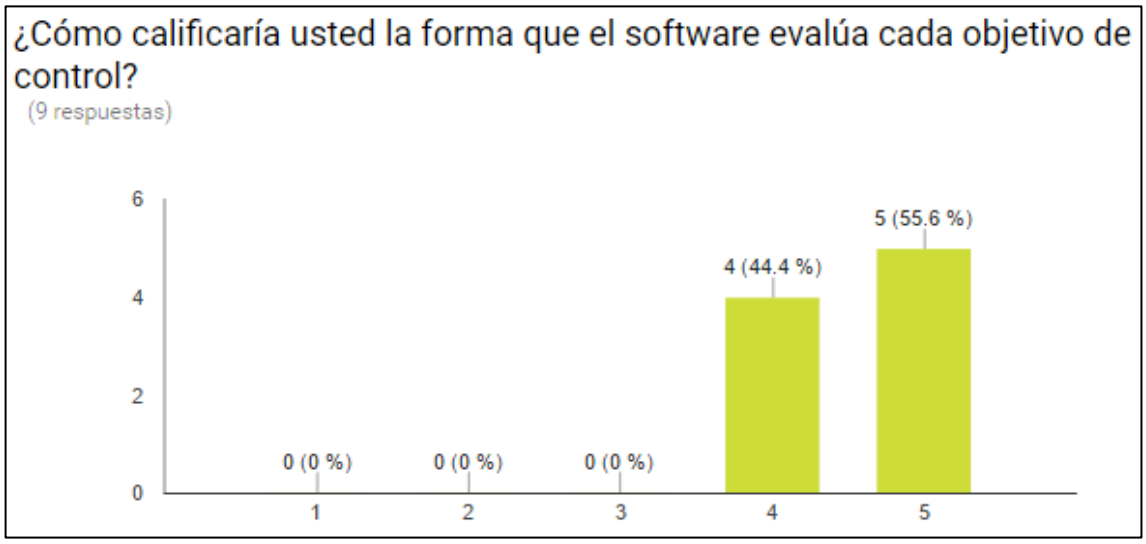
El software presenta un formulario en el cual se puede ingresar los activos informáticos de una organización y calcula el valor de cada uno de ellos mediante un algoritmo tomado de Magerit que trabaja con ocho dimensiones de valor, esta pregunta busca evaluar este proceso, de ella se infiere que la satisfacción es muy buena ya que el 88.8 % de los encuestados respondió igual o mayor a 4, solo un 11.1% respondió 3 y el 44.4% respondió que tenía una satisfacción máxima en este ítem. (ver figura 142)

Figura 142. Resultado pregunta 5



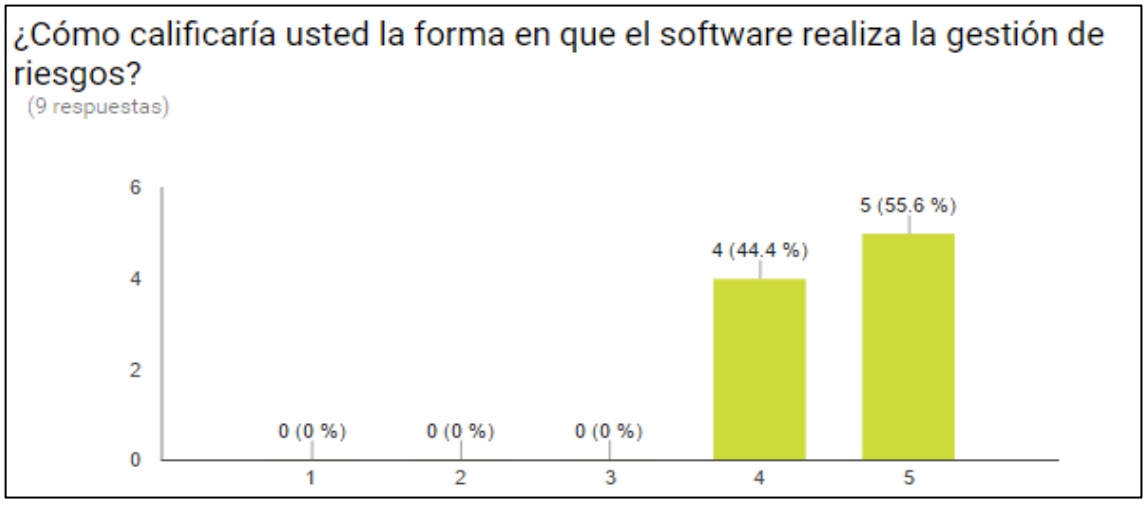
La mayoría de los individuos encuestados, un 55.5% exactamente respondió con satisfacción máxima acerca de los requerimientos que un software de auditoría debería cumplir. (ver figura 143)

Figura 143. Resultado pregunta 6



Para evaluar cada objetivo de control el software presenta unos ítems que el auditor debería evaluar, se preguntó a los usuarios como les parecía este proceso y la respuesta fue de satisfacción máxima en un 55.5% y el resto respondió en un nivel 4 de satisfacción. (ver figura 144)

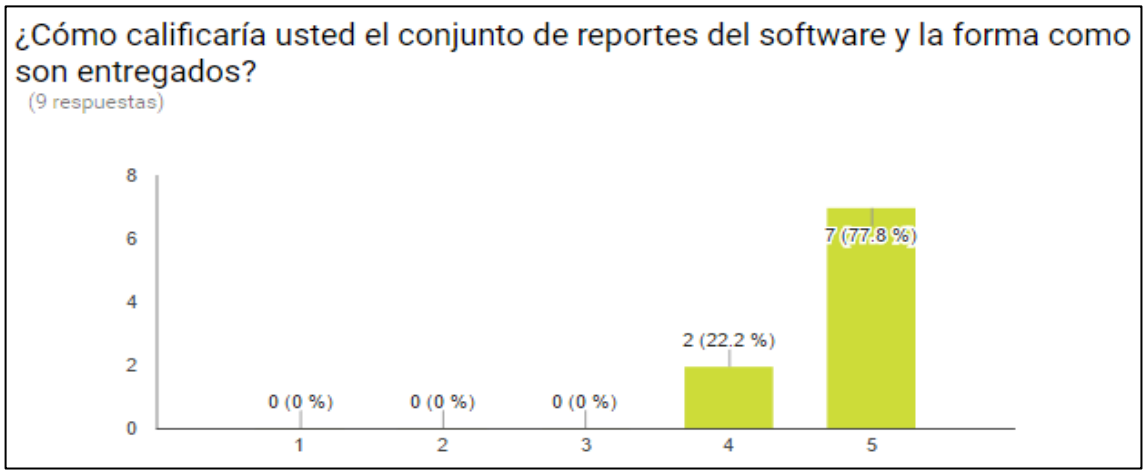
Figura 144. Resultado pregunta 7



Para realizar la gestión de riesgos el software usa los diferentes elementos de Magerit, como son activos, ventajas, algoritmos de cálculo de impacto y de valor de activos entre otros, se preguntó a los usuarios como les parecía este proceso,

el uso de estos elementos y la forma como se relacionaban y la respuesta fue de satisfacción máxima en un 55.5% y el resto respondió en un nivel 4 de satisfacción. (ver figura 145)

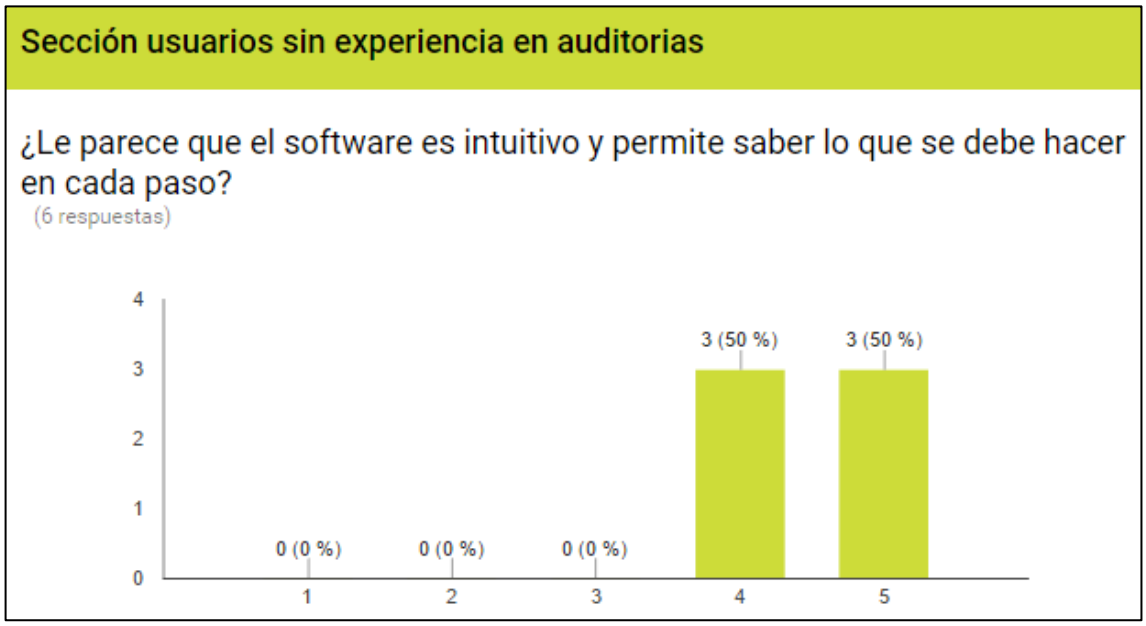
Figura 145. Resultado pregunta 8



Para entregar los reportes el software usa la información insertada y calculada que se encuentra en las diferentes tablas, y se la organizó en diferentes salidas se preguntó a los usuarios como les parecía la información suministrada y la forma como era entregada y la respuesta fue de satisfacción máxima en un 77.7% y el resto respondió en un nivel 4 de satisfacción.

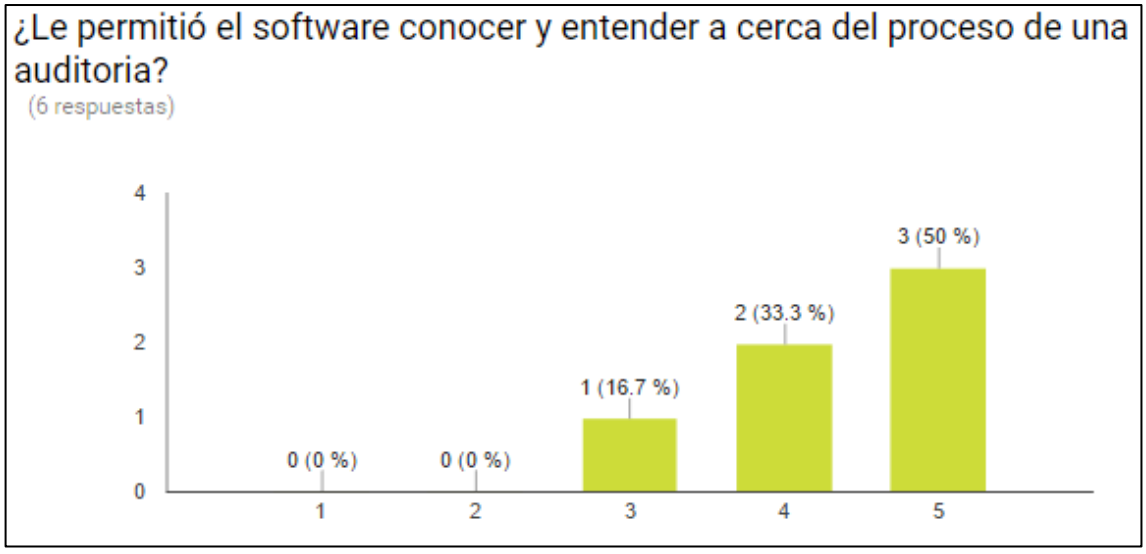
Sección usuarios sin experiencia en procesos de auditoría: para esta sección se usaron preguntas tipo rango, las cuales estaban encaminadas a conocer cuanto el software aclara este proceso para usuarios inexpertos. De uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 146)

Figura 146. Resultado pregunta 9



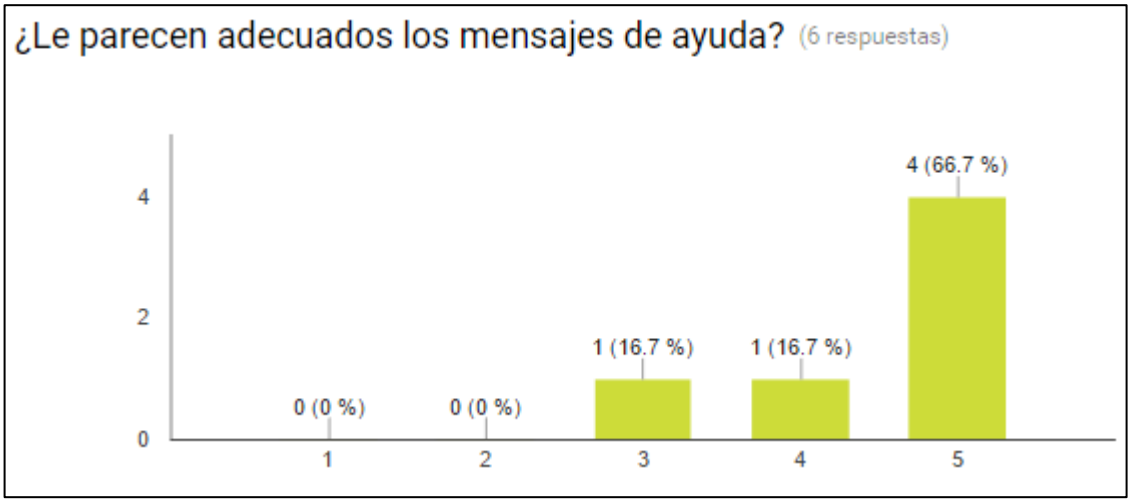
Para usuarios sin mucha experiencia en procesos de auditoría se les preguntó si el software era intuitivo y permitía saber qué hacer en cada paso y la respuesta fue de satisfacción máxima en un 50% y el resto respondió en un nivel 4 de satisfacción. (ver figura 147)

Figura 147. Resultado pregunta 10



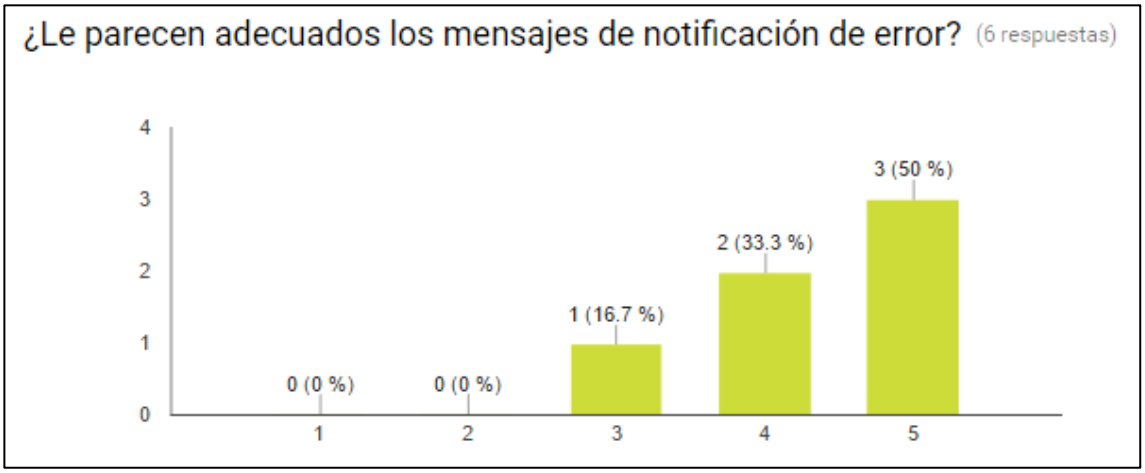
Para usuarios sin mucha experiencia en procesos de auditoría se les preguntó si el software les permitió acercarse al proceso de auditoría y la respuesta fue de satisfacción máxima en un 50%, nivel 4 en 33.4 y 3 en 16.6% de los casos. (ver figura 148)

Figura 148. Resultado pregunta 11



Para usuarios sin mucha experiencia en procesos de auditoría se les preguntó si el software les ofrecía mensajes de ayuda adecuados y la respuesta fue de satisfacción máxima en un 67%, nivel 4 en 16.6% y 3 en 16.6% de los casos. (ver figura 149)

Figura 149.Resultado pregunta 12



Para usuarios sin mucha experiencia en procesos de auditoría se les preguntó si les parecían adecuados los mensajes de notificación de error del software y la respuesta fue de satisfacción máxima en un 50%, nivel 4 en 33.4% y 3 en 16.6% de los casos. (ver figura 150)

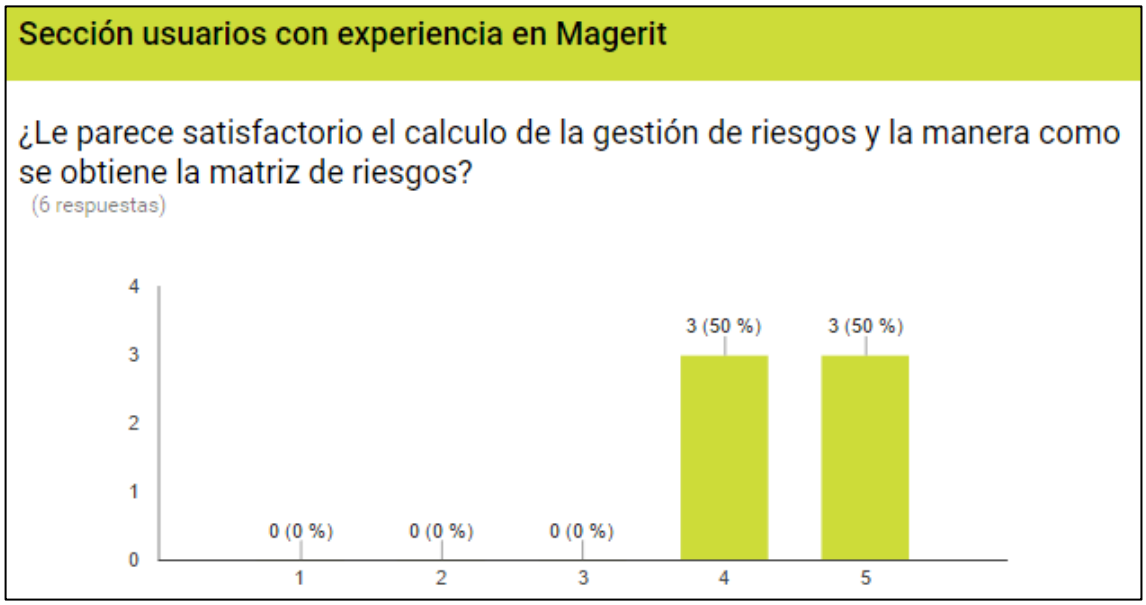
Figura 150. Resultado pregunta 13

A los 9 usuarios con experiencia en procesos de auditoría se les pregunto si tenían experiencia en Magerit, seis respondieron que sí y tres que no

A partir de esta pregunta se clasificó a los individuos en dos secciones para poder evaluar diferentes tipos de usuarios y aplicarles diferentes preguntas según su conocimiento, se observa que hay suficientes individuos para los 2 casos y que la mayoría tiene conocimientos en la norma de gestión de riesgos Magerit.

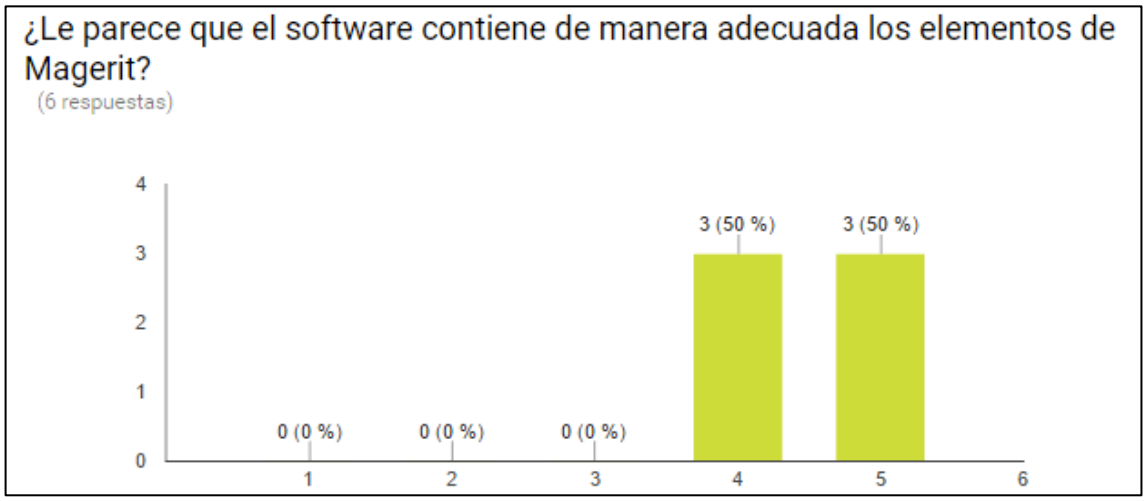
Sección usuarios con experiencia en Magerit: Para este tipo de usuarios se averiguo acerca de los elementos de Magerit, el cálculo de la gestión de riesgos y la matriz de riesgos, para esta sección se usaron preguntas tipo rango, de uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 151)

Figura 151. Resultado pregunta 14



Para usuarios con experiencia en el uso de la metodología de gestión de riesgos Magerit se les preguntó a cerca de la obtención de probabilidad e impacto y su organización en la matriz de riesgos y la respuesta fue de satisfacción máxima en un 50%, y nivel 4 en 50% de los casos. (ver figura 152)

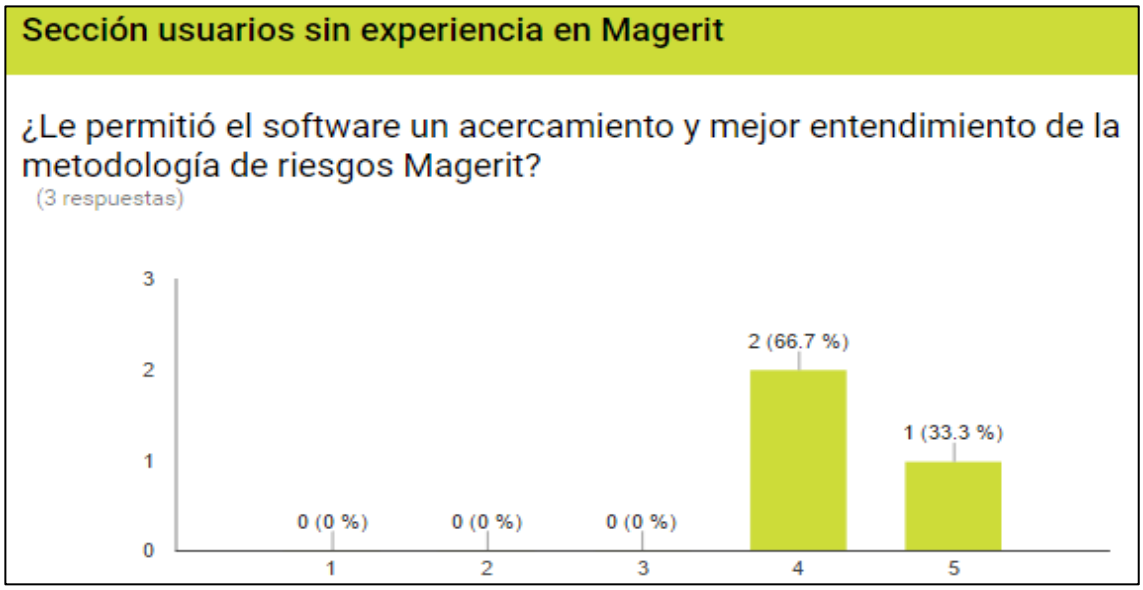
Figura 152. Resultado pregunta 15



Todos los individuos encuestados respondieron satisfactoriamente, un 50% exactamente respondió con satisfacción máxima acerca de los requerimientos que un software de auditoría debería cumplir.

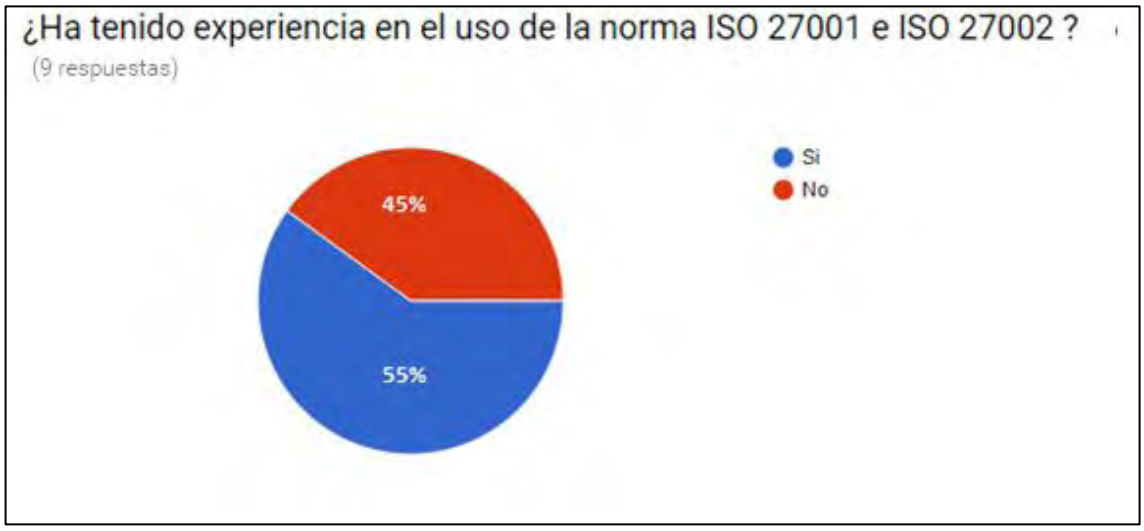
Sección usuarios sin experiencia en Magerit para esta sección se usaron preguntas tipo rango, las cuales estaban encaminadas a conocer cuanto el software aclara esta norma de gestión de riesgos para usuarios inexpertos. De uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 153)

Figura 153. Resultado pregunta 16



Para usuarios sin mucha experiencia en Magerit se les preguntó si el software les permitió acercarse a esta metodología y la respuesta fue de satisfacción máxima en un 33.3%, y nivel 4 en 66.6% de los casos. (ver figura 154)

Figura 154. Resultado pregunta 17

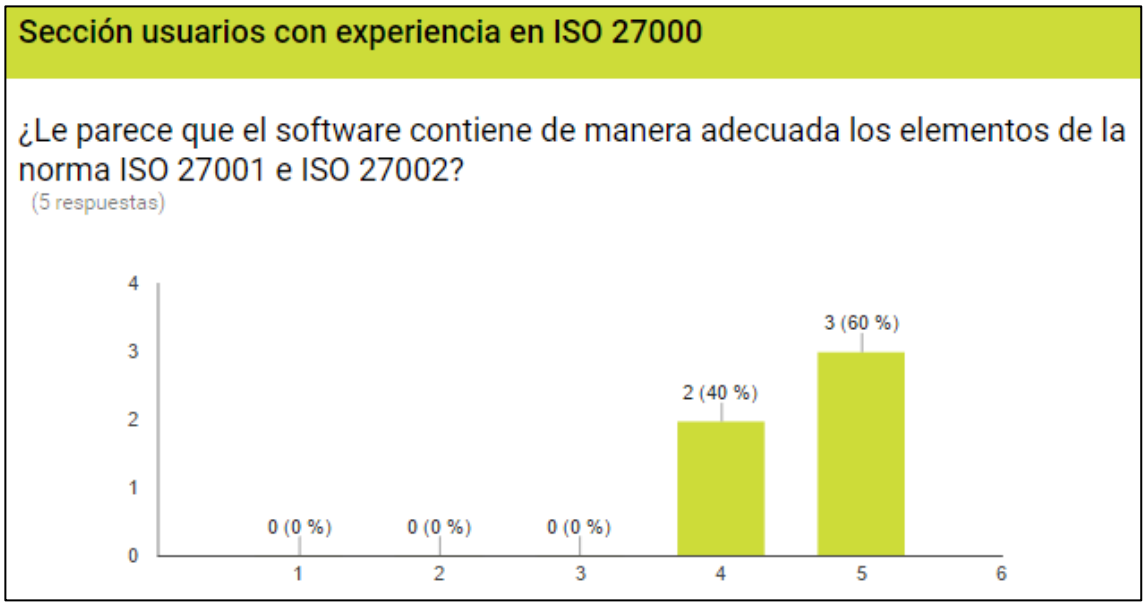


A los 9 usuarios con experiencia en Magerit se les preguntó si tenían experiencia en ISO 27001 y 27002, cinco respondieron que sí y cuatro que no.

A partir de esta pregunta se clasificó a los individuos en dos secciones para poder evaluar diferentes tipos de usuarios y aplicarles diferentes preguntas según su conocimiento, se observa que hay suficientes individuos para los 2 casos y que la mayoría tiene conocimientos en la norma ISO 27001 e ISO 27002

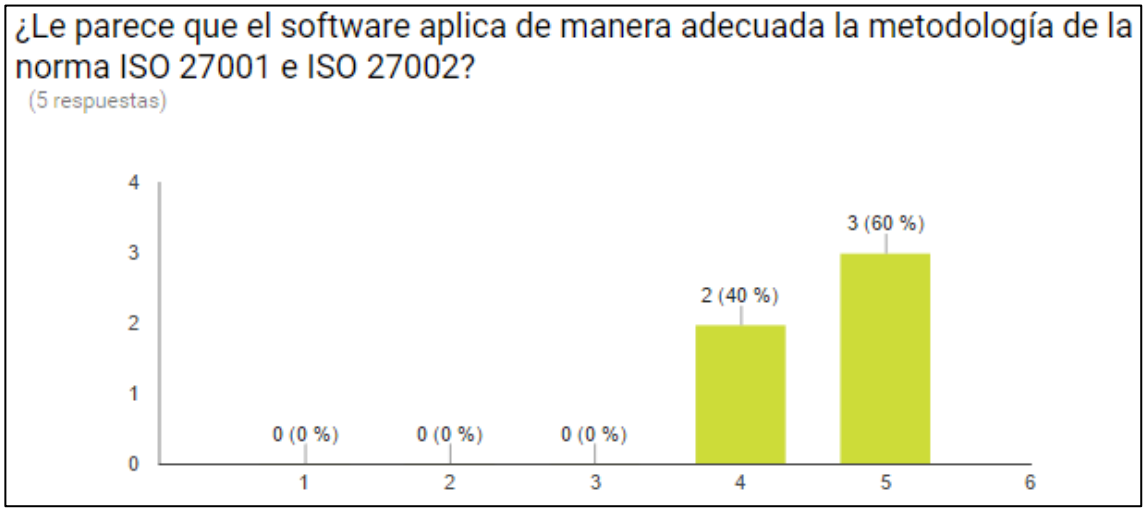
Sección usuarios con experiencia en ISO 27001Y 27002: Para este tipo de usuarios se averiguo acerca de los elementos y la aplicación de **ISO 27001 Y 27002**, para esta sección se usaron preguntas tipo rango, de uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 155)

Figura 155. Resultado pregunta 18



Se le preguntó a los usuarios acerca de como el software contiene a los elementos de las normas ISO 27000, las respuestas fueron de satisfacción máxima en un 60% y en nivel 4 en un 40%. (ver figura 156)

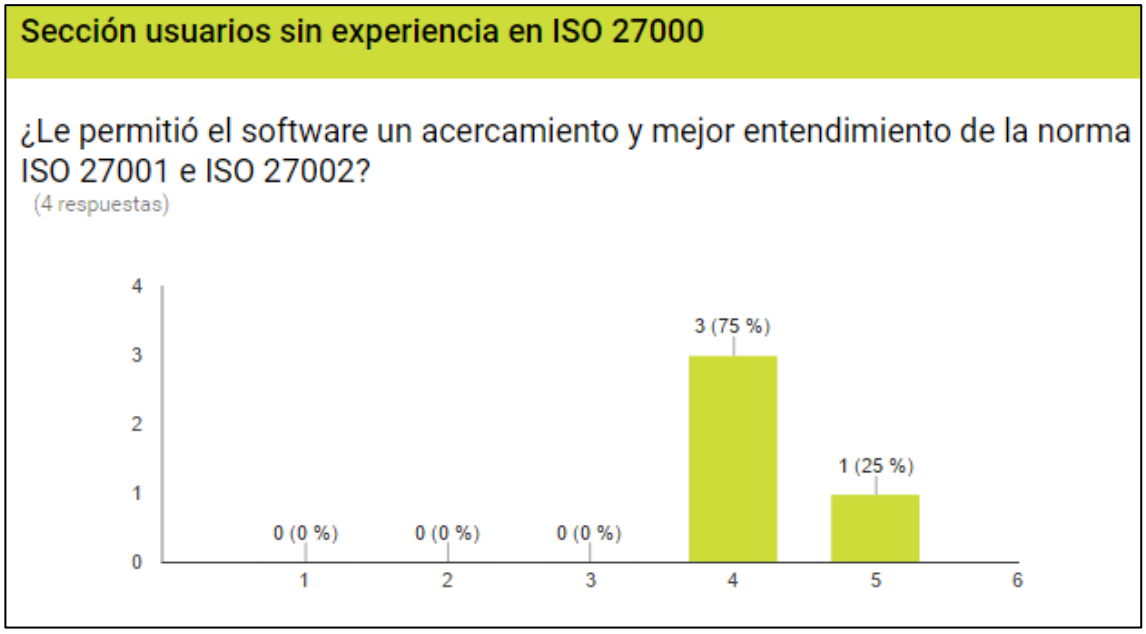
Figura 156. Resultado pregunta 19



Todos los individuos encuestados respondieron satisfactoriamente, un 60% exactamente respondió con satisfacción máxima acerca de los requerimientos que un software de auditoría debería cumplir.

Sección usuarios sin experiencia en ISO 27001Y 27002: para esta sección se usaron preguntas tipo rango, las cuales estaban encaminadas a conocer cuanto el software aclara la norma ISO 27001Y 27002 a los usuarios inexpertos. De uno a cinco, casi en todas ellas las respuestas dominantes fueron 4 y 5, demostrando la satisfacción de los usuarios. (ver figura 157)

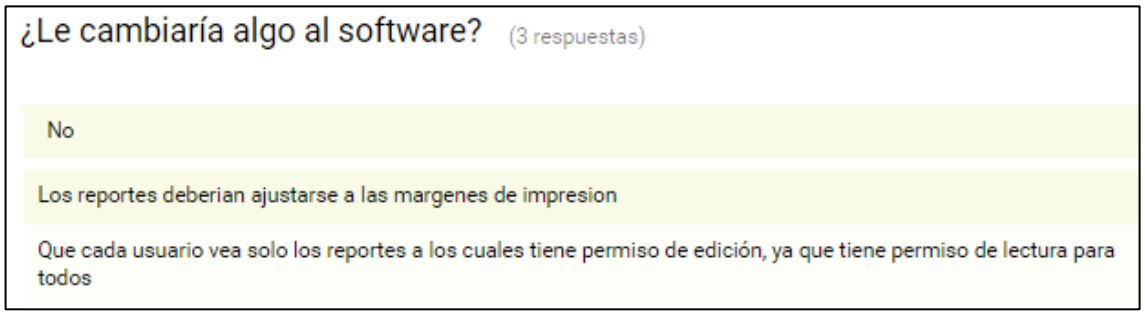
Figura 157. Resultado pregunta 20



Para usuarios sin mucha experiencia en ISO 27000 se les preguntó si el software les permitió acercarse a esta metodología y la respuesta fue de satisfacción EN NIVEL 4 en un 75%, y nivel 5 en 25% de los casos.

Interpretación de resultados de las preguntas abiertas. En todas las secciones los resultados fueron satisfactorios, no obstante los usuarios indicaron algunas posibles mejoras, en dos preguntas no obligatorias, las cuales se muestran a continuación. (ver figura 158)

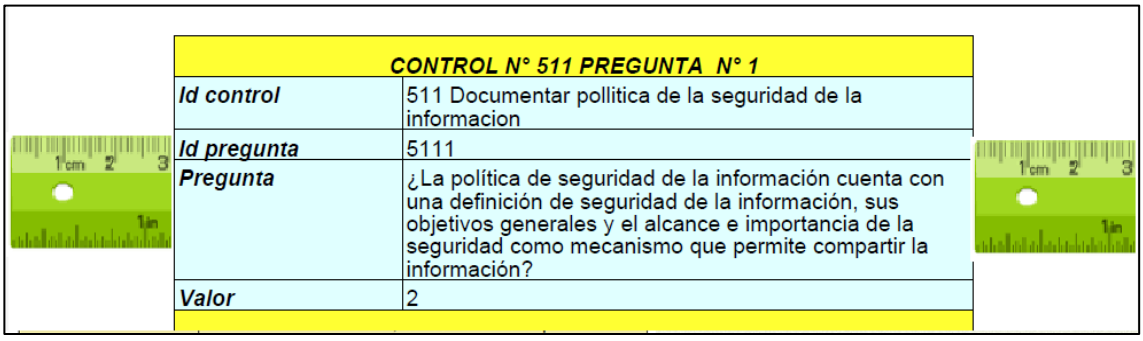
Figura 158. Resultado pregunta 21



Implementación de mejoras:

Mejora 13 Márgenes para impresión en reportes. En primera instancia las márgenes de los reportes pdf estabas muy pequeñas lo que impedía su impresión, gracias a la recomendación de un usuario se corrigió este error. (ver figura 159)

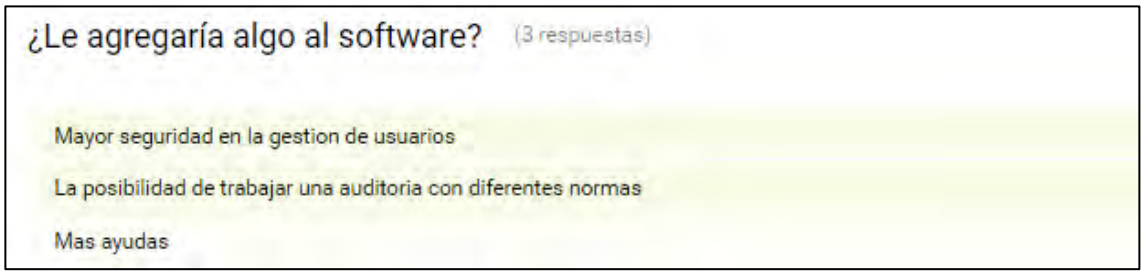
Figura 159. Mejora 13



CONTROL N° 511 PREGUNTA N° 1	
Id control	511 Documentar pollitica de la seguridad de la informacion
Id pregunta	5111
Pregunta	¿La política de seguridad de la información cuenta con una definición de seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información?
Valor	2

Mejora 14 Reportes delimitados. Los permisos de lectura para los reportes se reformaron de manera que sea acordes a las áreas de trabajo asignadas, y solo el usuario administrador tiene permiso de lectura para los reportes completos. (ver figura 160)

Figura 160. Resultado pregunta 22



Mejora 15 Gestión de usuarios. Además de la mejora anterior, para mayor seguridad se agregó la función de gestión de usuarios para el administrador en donde se puede eliminar un usuario, cambiar sus permisos y crear uno nuevo. (ver figura 161-162)

Figura 161. Mejora 15

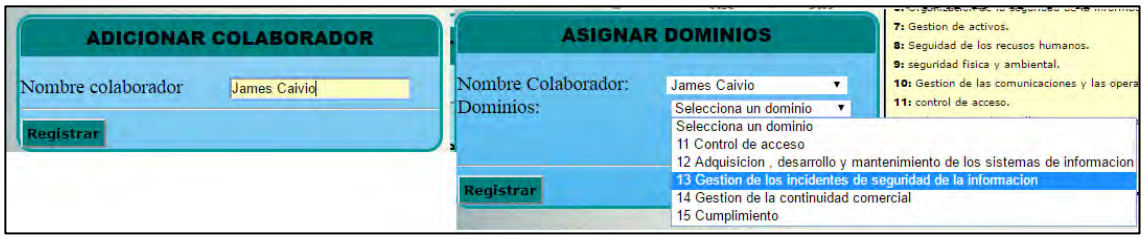


Figura 162. Mejora 15

Mejora 16 Ayudas. Se implementaron más y mejores ayudas en todo el proceso, además en cada cuestionario se muestra el estado ideal de su respectivo control para una evaluación más certera y fácil, y sr muestra una descripción de cada amenaza para el momento de insertar la probabilidad. (ver figura 163-164)

Figura 163. Mejora 16, estado ideal de un control

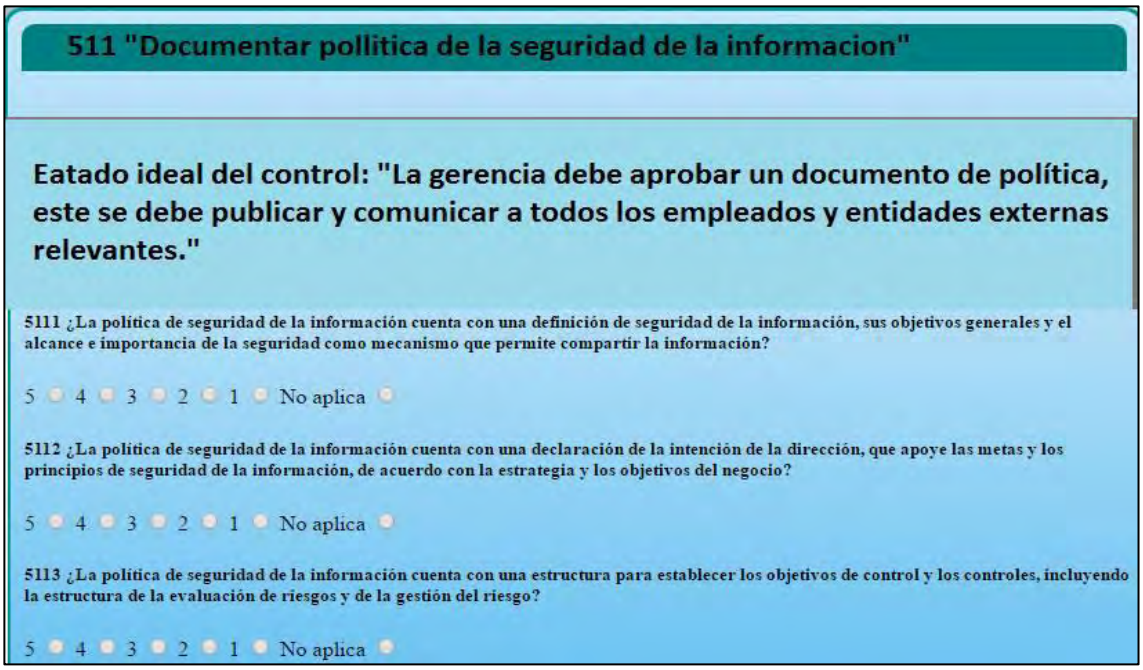
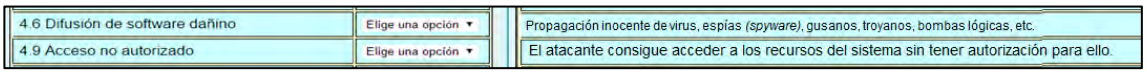


Figura 164. Mejora 16, descripción de amenazas



Prueba de demostración del proceso general de apoyo a auditoría con el software Sinf27. Se probó el software finalmente en una empresa real, de la cual se tomaron los datos para llevar a cabo todo el proceso, y se le entrego al gerente el catálogo de reportes del software para que él pueda proceder en acuerdo a esa información, y se tomaron sus impresiones y sugerencias en cuenta para la elaboración de las conclusiones del proyecto.

Introducción a la empresa: se realizó una entrevista con el gerente y propietario de la empresa el señor Guerlin Alfredo Araujo Mora, en la cual se trató principalmente el tema de los servicios y misiones críticas de la organización, la forma como se llevan a cabo los distintos procesos, y se expuso las funciones y ventajas del software Sinf 27000.

Acuerdo: se acordó una mutua colaboración en la cual los desarrolladores de software probaran el sistema en la organización y tendrán acceso a la información de activos, valor de los activos procesos, incidentes de la información y la facilidad de evaluar los procesos para verificar los dominios de la norma ISO 2700 haciendo uso del software desarrollado.

Por su parte la empresa Araujo y asociados tendrá a su disposición toda la información, reportes y recomendaciones que se generen con la prueba del uso del software, y la libertad de hacer uso de eta información como le parezca conveniente para realizar procesos de mejoramiento.

Documentos de la empresa:

- **Misión**

Dar servicio de asesoría contable en diferentes niveles, cumplir con un amplio rango del mercado, desde negocios pequeños a servicios contables de empresas, brindar asesoría tributaria, asesoría legal, declaraciones de renta, asesorías crediticias, tramitación de préstamos, y gestión de seguros, con calidad y confiabilidad.

- **Visión**

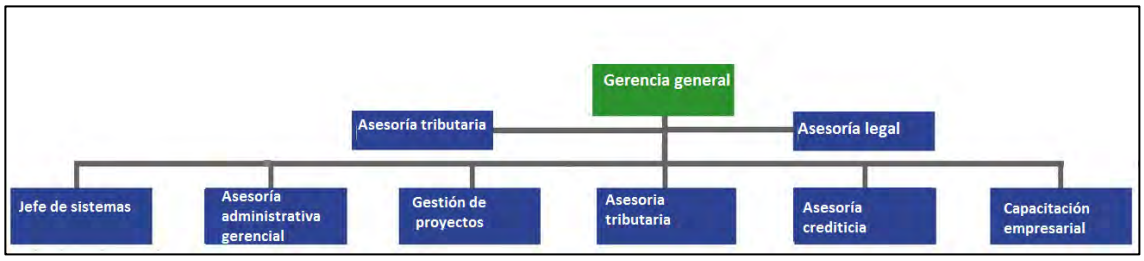
Consolidar a Araujo y asociados como una empresa indispensable en el mercado contable en la ciudad de pasto a través de una organización de la información y los servicios haciendo uso de las tecnologías de la información, con la implementación de una página Web y uso de sistemas automatizados para la gestión de información y procesos

- **RUT**

Este documento se puede ver completo en formato pdf en el anexo 4.

- **Organigrama**

Figura 165. Organigrama Araujo y asociados



Fuente: Documentos internos empresa Araujo y asociados

- **Servicios de la empresa**

Capacitación empresarial: se cuenta con relaciones de alianzas estratégicas para la prestación de asesoría y capacitación en distintas áreas, el principal cliente de este servicio es COACREMAT, quien contrata las capacitaciones para sus asociados y empleados, otro cliente habitual de este servicio es la COOPERATIVA DE VOLQUETEROS DE TUMACO.

Capacitaciones ofrecidas:

- **Cooperativismo**
- **Finanzas familiares**
- **Seguros**

Asesoría administrativa gerencial: asesoría encaminada a un completo acompañamiento de la organización contratante, abarca parte gerencial, administrativa, tributaria, legal etc. Para este servicio se cuenta con colaboradores en áreas sensibles principalmente el área legal, o laboral.

Gestión de proyectos: se cuenta con un grupo de proyectistas, quienes son los encargados de las proyecciones, los estudios de mercadeo, de contexto de afectación, etc. Y se complementa con la parte contable, legal y tributaria.

Asesoría tributaria: asesoría encaminada a consultoría fiscal, manejo de sanciones, gestión legal y proyección tributaria.

Asesoría crediticia: asesoría encaminada a promover créditos, este servicio se presenta en dos sentidos, tanto para las organizaciones que ofrecen los créditos como para las personas que quieren acceder a ellos.

- **Ciclo de vida de los procesos de la organización**

Contacto: el contacto se hace directamente con la organización ya sea a través del lugar de las instalaciones o con el personal, se manifiesta no contar con

publicidad, ni medios de promulgación de los servicios prestados.

Recepción y análisis de requerimientos de un cliente potencial:

- Clasificación del servicio y alcance requerido.
- Clasificación y organización de la documentación y requerimientos de la empresa contratante.
- Aplicar criterios de determinación del tamaño y necesidades de la empresa contratante.
- Análisis de aceptación o rechazo de un contrato
- Recepción de información de entrada de procesos.
- Asignación de tareas y procesamiento de la información
- Entrega de reportes, salidas, recomendaciones, etc.

- **Inserción de datos de la organización en el software**

Se ingresaron los datos del proyecto nuevo en el software, y se crearon, los usuarios, permiso y áreas de trabajo asignadas, lo cual genero el primer Reporte del sistema.

Luego de los acercamientos iniciales a la empresa, en conjunto con el gerente de la empresa se estableció un listado de activos, y se determinó el valor de cada uno de ellos para la organización.

La evaluación de los controles de la norma fue realizada e ingresada en el software por los desarrolladores del software

La probabilidad de ocurrencia de cada amenaza se analizó en conjunto con el gerente de la empresa.

- **Reportes para la organización**

Los reportes generados para la organización en formato pdf, son:

- Reporte de datos de auditoría
- Reporte de activos
- Reporte de controles
- Reporte de cuestionarios
- Reporte de Matriz de riesgos
- Reporte de Salvaguardas

Los reportes completos se pueden ver en el Anexo 3, reportes

4. CONCLUSIONES

Durante la realización del software se tuvo en cuenta la estructura y contenido de la norma ISO 27001 para delimitar cada evaluación hecha, teniendo en cuenta cada nivel de la misma, así: los dominios se usaron para categorizar diferentes áreas de una auditoría, y para agrupar las áreas de trabajo asignadas a los diferentes colaboradores que trabajan en un proyecto específico, luego los objetivos de control sirvieron para delimitar lo que se tenía que evaluar, y para demarcar las áreas de una organización que debían ser revisadas, también se enlazaron con las salvaguardas de la norma ISO 7002, el nivel final de la norma, los controles se usaron para especificar las evaluaciones y contener preguntas que buscaban calificar a cada uno de ellos en un cuestionario, para enlazarse con la metodología Magerit a través de las amenazas activadas por cada control. En síntesis se realizó un estudio, análisis, clasificación y uso de cada elemento de la norma para dar cuerpo al sistema.

La arquitectura del software se basó en una base de datos de 16 relaciones que agrupan cada área una auditoría, clasificadas en tres grupos, dependiendo del tipo de objetos utilizados, así: las relaciones que clasifican y usan los elementos de las normas ISO 27001 y 27001, las relaciones que clasifican y usan los elementos de la metodología de gestión de riesgos Magerit y las relaciones necesarias para clasificar los datos propios del sistema como usuarios, datos de auditoría, activos, entre otros además de tablas que relacionan y comunican diferentes partes del sistema.

Para la evaluación de las distintas evaluaciones del sistema se realizó un banco de preguntas, con alrededor de 760 ítems que la organización debería cumplir, clasificadas dentro del control correspondiente y flexibles con opción de respuesta en niveles de uno a cinco, siendo aplicables para diferentes tipos de pruebas, checklist, entrevistas, preguntas abiertas etc. Además se implementó la opción de anular una pregunta o añadir las que el usuario auditor vea necesario.

Durante la implementación del software se usó la metodología Magerit y se la implemento creando objetos que contengan los elementos de ella en el sistema, para relacionar estos elementos se implementaron procesos estipulados en Magerit, y en general se automatizo el proceso de gestión de riesgos de la metodología contando en el sistema con los algoritmos de determinación, clasificación y valoración de los activos de una organización, luego el de determinación de amenazas posibles, su impacto y probabilidad en la organización y finalmente la obtención de la matriz de riesgos.

Se puede concluir que la mejor forma de presentar reportes para n proceso de auditoría es la organización y clasificación de todos los datos obtenidos, y que para su demostración una herramienta muy eficiente y eficaz es una base datos, en este software los reportes se realizaron a través de consultas de las relaciones del software, tales como activos, datos de auditoría, controles evaluados amenazas activas, y resultados de las evaluaciones, entre otros, el sistema presenta también la facilidad de presentar estos reportes en formato pdf.

Se concluye que las pruebas del software fueron satisfactorias, la verificación de la utilidad del software se llevó a cabo en pruebas de su uso en la empresa de servicios contables Araujo y asociados en la cual se evaluaron rápida y fácilmente todos los aspectos de la norma ISO 2700 con ayuda del software, presentando todos los reportes que permitieron establecer el estado de la seguridad informática y de la información en la organización, pero antes e esta prueba general se hicieron dos pruebas, la primera de validación de funcionalidades y usabilidad con usuarios con pocos o nulos conocimientos en auditoría con el fin de evaluar si el sistema era fácil de usar y si sus funciones eran entendibles y se realizaban eficazmente, luego se realizó pruebas de demostración del software con usuarios que tenían conocimientos en el área de auditoría con el fin de implementar posibles mejoras que los usuarios sugirieran.

Se concluye que la importancia de la documentación del proceso de desarrollo de un software es primordial al momento de usarlo, ya que es a través de esta documentación que se puede realizar un uso consiente de todas la funcionalidades que el sistema ofrece, aprovechando todo su potencial usando la información documentada del mismo, también es importante la documentación, entendiendo el software como un producto, y usándola como medio de muestra exteriorización, explicación y comercialización de este producto.

5. RECOMEDACIONES

Registrar los datos de auditoría de manera ordenada y que los usuarios sean asignados a áreas de trabajo de acuerdo al conocimiento que tengan en las mismas, para eso se debe usar la funcionalidad de colaboradores que registra los usuarios y permite elegir los dominios de la norma en los cuales podrán trabajar, esto no solo para organizar el trabajo sino también para gestionar los permisos de acceso a las partes del software y manejar la seguridad del mismo.

Entender los activos al momento de insertarlos, dentro del contexto de seguridad informática y de la información, y a su valor entenderlo como lo importante que es cada activo para esa seguridad más que en cuanto a costo monetario, es este el fin dela metodología Magerit, y la tipificación de activos en ella busca categorizarlos para relacionarlos con las amenazas a la seguridad de la información y para establecer su valor dentro del algoritmo que agrupa las ocho dimensiones que podrían tener impacto en la organización a nivel general.

Tener cuidado en los objetivos de cada nivel de la norma ISO 27001, a medida que se navegue a través de ella, para realizar una evaluación consiente y bien encaminada, es importante tener en cuenta os objetivos de evaluación de un control al momento de responder sus evaluaciones y más aún si se obvia alguna pregunta tener en cuenta que parte del objetivo evaluaba y de ser posible remplazarla de acuerdo al contexto de la organización en la cual se esté trabajando.

Entender y usar las auditorías que el software presenta en cuanto a categorización de las áreas a evaluar, ya que el mismo presenta una agrupación de las posibles categorías de auditorías que se realizan dentro del marco de seguridad informática y de la información.

Usar la herramienta de evaluación por integridad, disponibilidad y disponibilidad, ya que ayuda a resolver el problema de no poder apreciar una evaluación dependiendo de las dimensiones de la organización que se quiera proteger, es muy útil determinar cuál de estas dimensiones es la más sensible en determinado momento y situación, y se ha implementado en el sistema a través de la relación que existe en Magerit de los tipos de amenazas y la dimensión a la cual cada una de ellas afecta.

Seguir la metodología Magerit, en cuanto a la parte de gestión de riesgos, en este aspecto, el problema más grande es determinar la probabilidad de ocurrencia de una amenaza estableciendo una escala combinada entre cualitativa y cuantitativa y usando as herramientas que se tengan a la mano para determinarla apoyándose

de combinación de criterios, por ejemplo, de ser posible establecer un tiempo y contar las ocurrencias en ese lapso, puesto que por motivo del mismo tiempo este criterio no siempre se puede usar se recomienda también basarse en la experiencia de las personas cercanas al contexto de ocurrencia de una amenaza. O al análisis de las variables o situaciones que inciden en la tipificación de una amenaza.

Hacer uso de los diferentes reportes que genera el sistema para la documentación de la auditoría y apoyarla con documentos propios de la empresa más que nada para el archivo de las organizaciones evaluadas.

Adjuntar las evidencias que respalden las respuestas ingresadass en el software, y complementarlas con los reportes brindados de estado de aprobación de los controles y de las respuestas ingresadas a los hallazgos

Apoyar las recomendaciones de la auditoría con los reportes generados.

BIBLIOGRAFIA

[1] LADINO A., MARTHA ISABEL, VILLA S., PAULA ANDREA, LÓPEZ E., ANA MARÍA. FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS.Scientia Et Technica [en línea] 2011, XVII (Abril-Sin mes): [Fecha de consulta: 8 de noviembre de 2015] Disponible en:< http://www.redalyc.org/articulo.oa?id=84921327061> ISSN 0122-1701

[2] Mesquida, Antoni Lluís, Mas, Antònia, Amengual, Esperança, Cabestrero, Ignacio. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software [en linea] 2010, 6 (Noviembre-Sin mes) : [Fecha de consulta: 8 de noviembre de 2015] Disponible en:< http://www.redalyc.org/articulo.oa?id=92218768002> ISSN

[3] Fernández Carlos Manuel.La norma ISO 27001. Seguridad de la información. Garantía de la confidencialidad, integridad y disponibilidad de la información. Revista mensual de la Asociación Española para la Calidad [en línea] 2012,3 (Abril-Sin mes): [Fecha de consulta: 8 de noviembre de 2015] Disponible en:< http://dialnet.unirioja.es/servlet/articulo?codigo=4867978

[4] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Tecnologías de la información: Sistemas de gestión de la seguridad de la información. Geneve: ISO, 2013. 41h. (ISO/IEC 270001/2013)

[5] MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea] 2010,6 (Junio-Sin mes): [Fecha de consulta: 15 de febrero de 2016] Disponible en:< http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VwPWyPnhDIU

[6] METODOLOGÍA DE LA INVESTIGACIÓN, MÉTODOS Y ESTRATEGIAS DE INVESTIGACIÓN: [Fecha de consulta: 17 de enero de 2016] Disponible en:< https://metinvestigacion.wordpress.com/

[7] COOPERACION EN RED EUROAMERICANA PARA EL DESARROLLO SOSTENIBLE, Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa.: [Fecha de consulta: 20 de febrero de 2016] Disponible en:< http://www.creadess.org/index.php/informate/de-interes/temas-de-interes/17300-conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa

[8] Eq-05 Inv. Cuantitativa en las Ciencias Sociales: [Fecha de consulta: 15 de

febrero de 2016] Disponible en:< http://invcuantcs.blogspot.com.co/2011/06/investigacion-cuantitativa-en-las.html

[9] Historia del pensamiento científico: [Fecha de consulta: 15 de febrero de 2016] Disponible en:< http://www.eumed.net/libros-gratis/2007a/257/7.1.htm.

[10] Definición de Método Empírico Analítico: [Fecha de consulta: 15 de febrero de 2016] Disponible en:< http://www.definicionabc.com/ciencia/metodo-empirico-analitico.php

[11] ¿Qué es norma ISO 27001?: [Fecha de consulta: 26 de febrero de 2016] Disponible en:< http://advisera.com/27001academy/es/que-es-iso-27001/

[12] ISO/IEC 27002: [Fecha de consulta: 15 de febrero de 2016] Disponible en:< https://es.wikipedia.org/wiki/ISO/IEC_27002

[13] MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: [Fecha de consulta: 26 de febrero de 2016] Disponible en:< http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VjYznLcvfIU

[14]PostgreSQL Global Development Group: [Fecha de consulta: 26 de febrero de 2016] Disponible en:< http://www.postgresql.org/download/windows/.

[15]NetBeans IDE 8.1 Download Started.: [Fecha de consulta: 26 de febrero de 2016] Disponible en:< https://netbeans.org/downloads/start.html?platform=windows&lang=es&option=all

[16]Oracle: [Fecha de consulta: 26 de febrero de 2016] Disponible en:< http://www.oracle.com/technetwork/java/javase/documentation/index.html Douglas Crockford on Functional JavaScript (2:49