UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Software de apoyo para la administración e implementación de un SGSI - SASGSI

Trabajo Fin de Máster

Presentado por: Pinzon Cortes, Deinar Alfonso

Director/a: Cuquejo Mira, Juan

Ciudad: Bogotá D.C.
Fecha: 07/05/2015

Resumen

El desarrollo de una aplicación web gratuita que permita administrar la documentación y los procesos de diseño e implementación de un SGSI surge de la necesidad de empresas y administradores de seguridad por controlar cada una de las fases de un proyecto de implementación de un SGSI. Los volúmenes de información recolectados, tratados y generados en cada uno de estos procesos son altos, por lo que la manipulación controlada de forma manual representa un gran desgaste. SASGSI es una herramienta muy útil desarrollada en PHP, MySql y siguiendo las buenas prácticas de desarrollo y es una solución a esta necesidad. En la actualidad la aplicación está siendo usada por la entidad Ministerio de Comercio, Industria y Turismo de Colombia en donde se inició el proyecto de diseño e implementación de un SGSI y ya gestiona todas las fases para el proceso de solicitud de comisiones y viáticos y se está extendiendo a otros procesos

Palabras Clave: SGSI, SASGSI, implementación.

Abstract

The development of a free web application that allows managing documents and processes of design and implementation of an ISMS arises from the need for companies and security administrators to control each of the phases of a project to implement an ISMS. Volumes of information collected, processed and generated in each of these processes are high, so the handling controlled manually represents great wear. SASGSI is a very useful tool developed in PHP, MySql and following good development practices and is a solution to this requeriment, the application currently being used by the Ministry of Commerce, Industry and Tourism of Colombia where they started the project design and implementation of an ISMS and already manages all phases for the application process fees and diems and is spreading to other processes

Keywords: SASGSI, SGSI, Implementation.

Índice

Índice de Ilustraciones y Tablas

1. Introducción

Este trabajo se desarrolla como tesis para la obtención del título de master en seguridad informática de la Universidad Internacional de la Rioja y en él se plantea el desarrollo de un software para la administración de un sistema de gestión de seguridad de la información (SGSI). Actualmente alrededor del mundo se presentan millones de incidentes informáticos que en su gran mayoría tienen como objetivo la obtención o afectación de la información. Esto es lógico dado que el avance tecnológico de la actual era digital ha convertido la información en el activo más valioso para empresas, países y personas en general y por tanto también para la ciberdelincuencia. La obtención y uso de la información es uno de los negocios más lucrativos y no es de asombrarse ya que traducido en el mundo real tener información privilegiada significa poder y esto a su vez dinero; es por eso que cada día hay más incidentes y más personas técnicamente capacitadas trabajando para lograr vulnerar los controles de seguridad. En vista de esta situación los países y empresas han trabajado conjuntamente para crear estándares, normas, herramientas, dispositivos y mecanismos que ayuden a mitigar o hacer frente a este tipo de incidentes. Una de estas normas y quizás la más sobresaliente empresarialmente hablando es la norma ISO 27001 que estructura la implementación de un sistema de gestión de seguridad de la información planteando la prevención como el arma más efectiva para hacer frente a los incidentes informáticos, abarcando los aspectos más relevantes para las organizaciones susceptibles a la afectación de la información desde el punto de vista de la confidencialidad, integridad y disponibilidad. Es por esto que las organizaciones se ven cada día más inclinadas, y en ciertos casos regulatorios, hasta obligadas a contar con la implementación o certificación de la norma porque es una forma de demostrar de que existe una preocupación por la seguridad de la información y que se hacen esfuerzos físicos, técnicos, económicos y humanos para la protección de la misma.

Sin embargo la implementación de un SGSI solamente es el primer paso de un proyecto de seguridad informática. La tecnología es un mundo cambiante que evoluciona muy rápido y requiere de mucha adaptación por parte de las personas y más aun de las empresas y es precisamente por esto que se requiere de una ardua labor de monitoreo, revisión, implementación y actualización no solo a nivel técnico, sino procedimental y documental. Todos estos cambios deben verse reflejados en el SGSI, lo que significa que la administración del mismo es una tarea dispendiosa de mucha responsabilidad y organización. En vista de esta situación se desea desarrollar un software gratuito que sirva como herramienta de administración de un SGSI que permita a los responsables de la seguridad informática y de la

información tener un repositorio centralizado, disponible y organizado de la información relevante al proyecto.

1.1. Identificación del problema

Con la evolución de las tecnologías de la información se ha encontrado la solución a muchos de los grandes obstáculos de las organizaciones como la comunicación y procesamiento de información. Ejemplo de esto son los grandes desplazamientos que habitualmente debían hacerse para transportar o acceder a la información y el gran volumen de personas que debía contratarse para manipular, clasificar y proteger la información, sin embargo hoy en día todo es más sencillo la mayoría de empresas y personas tienen acceso a tecnologías que permiten fácilmente enviar, recibir y consultar información a través de internet el cual se ha extendido masivamente en su implementación, cobertura y uso. Según el banco mundial tan solo en España 71,6 de cada 100 ciudadanos tiene acceso (Grupo Banco Mundial, 2015), esto ha llevado a que la información de las personas cada día esté más digitalizada y que los gobiernos y empresas se convirtieran en organizaciones muy eficientes en la gestión de grandes cantidades de datos mediante el uso de softwares diseñados especialmente para esto. Es por eso que prácticamente resulta inconcebible la manipulación de grandes cantidades de información de forma manual y que esta no esté disponible en el momento que se requiera ya que esto no solo significa ineficiencia y falta de adaptabilidad sino también pérdidas económicas.

Los sistemas de gestión son realmente herramientas que permiten a través de diferentes mecanismos documentar, evaluar y controlar una o varias actividades o procesos de la entidad bajo una norma específica y estos mecanismos y procesos se componen de grandes cantidades de información que debe gestionarse de forma eficiente y que debe estar disponible para todos los empleados de la empresa quienes en ultimas deben estar familiarizados y comprometidos con el sistema de gestión. Esto aplica también para el SGSI y con mucha más razón aun, ya que la base de este es la gestión de la información garantizando la confidencialidad la integridad y disponibilidad de la misma porque según el enfoque la ISO 27001 se considerada como uno de los activos más importantes de la organización. Es por eso que se hace casi indispensable para los administradores de la seguridad disponer de una herramienta que les permita interactuar fácilmente con la información relacionada a la protección de la información confidencial de la entidad y que además de esto les permita disponer de ella en el momento que lo requiera.

1.2. Justificación

En la actualidad existen más de 22.293 empresas certificadas en ISO 27001, y según el último informe de iso.org desde el 2013 este número ha crecido exponencialmente (ISO org, 2014a). Esto es muestra del gran interés de las empresas por tener mecanismos que les ayuden a gestionar la seguridad de la información sensible que poseen, sin embargo las exigencias del estándar para la implementación del mismo constan de varios documentos como por ejemplo las políticas (general y especificas), los procedimientos implementados para llevar acciones cotidianas de tal manera que cumplan con los estándares definidos por la compañía como convenientes, manuales técnicos y de usuario, informes de auditoría, informes de seguimiento hallazgos, registro de asistencia a reuniones, comités, capacitaciones como evidencia o soporte, la declaración de aplicabilidad de los controles implementados para mitigar el riesgo, informe de incidentes, tratamiento de los mismos, inventario de activos, etc. Todos estos documentos deben por especificación mantenerse como información documentada y controlada, es decir, debe almacenarse en un lugar donde esté disponible, organizada, protegida, que conserve todo su versionamiento y control de cambios. Si se piensa un poco en todos los procesos que tiene una entidad y que todos estos documentos anteriormente listados son solamente una parte de los documentos exigidos, se nota que se requiere del manejo de mucha información y que es necesario contar con una herramienta de apoyo para la gestión de los mismos que permita tener el control. Ahora bien, esto solo es una parte que conforma el mantenimiento del SGSI, el proceso de implementación también requiere de un software de apoyo ya que en esta fase se realiza la recolección y clasificación de la información, la recolección del inventario de activos y si se hacen todos estos procesos físicamente resultara dispendioso realizar un cambio, una actualización, adición o eliminación de un registro.

1.3. Motivación

Como se ha visto, al ser difícil manejar grandes cantidades de información manualmente, no contar con sistemas de gestión resulta en mayores costos para la entidad y un control insuficiente de los datos. Adicionalmente la dificultad de hacer un seguimiento porcentual del avance de las fases de implementación y diseño del SGSI conllevan a la necesidad de contar con una herramienta que permita a los administradores de la seguridad ser más eficientes en sus tareas, seguimiento a procesos y a los empleados de la organización contar con un repositorio de documentos organizado para la consulta de la diferente información, ya que ellos como parte vital de la empresa deben también estar comprometidos con el SGSI.

Actualmente las empresas están adquiriendo una mayor responsabilidad por la seguridad de la información y casi todos los países están promoviendo leyes que exijan cumplimiento de estándares que garanticen que por lo menos existen unos controles mínimos en la protección de la misma. Por ejemplo, en la actualidad el gobierno Colombiano a través de los lineamientos exigidos por el Ministerio de Tecnologías y de las comunicaciones a todas la empresas públicas y que son de obligatorio cumplimiento se solicita la evidencia de la implementación de un SGSI al menos para alguno de sus procesos misionales y el proyecto de implementación del mismo a todos los procesos de la entidad máximo a 2018 (MinTIC, 2014). Muestra de estas nuevas exigencias en todo el mundo es el aumento de empresas certificadas en la norma: según la organización ISO tan solo en España desde el año 2009 al 2013 se pasó de 23 empresas certificadas a 805 (ISO org, 2014b) y lo que puede dilucidarse por la actual situación es que este número seguirá aumentado especialmente en países de Suramérica y África en donde las regulaciones son relativamente nuevas o aun ni existen. Adicionalmente, el aumento a nivel mundial de ataques e incidentes informáticos demuestra que la ciberdelincuencia impone nuevos retos y obliga a replantear las tecnologías y su uso, al menos como se conocen hasta ahora.

Distribución de Certificaciones ISO 27001 en el mundo

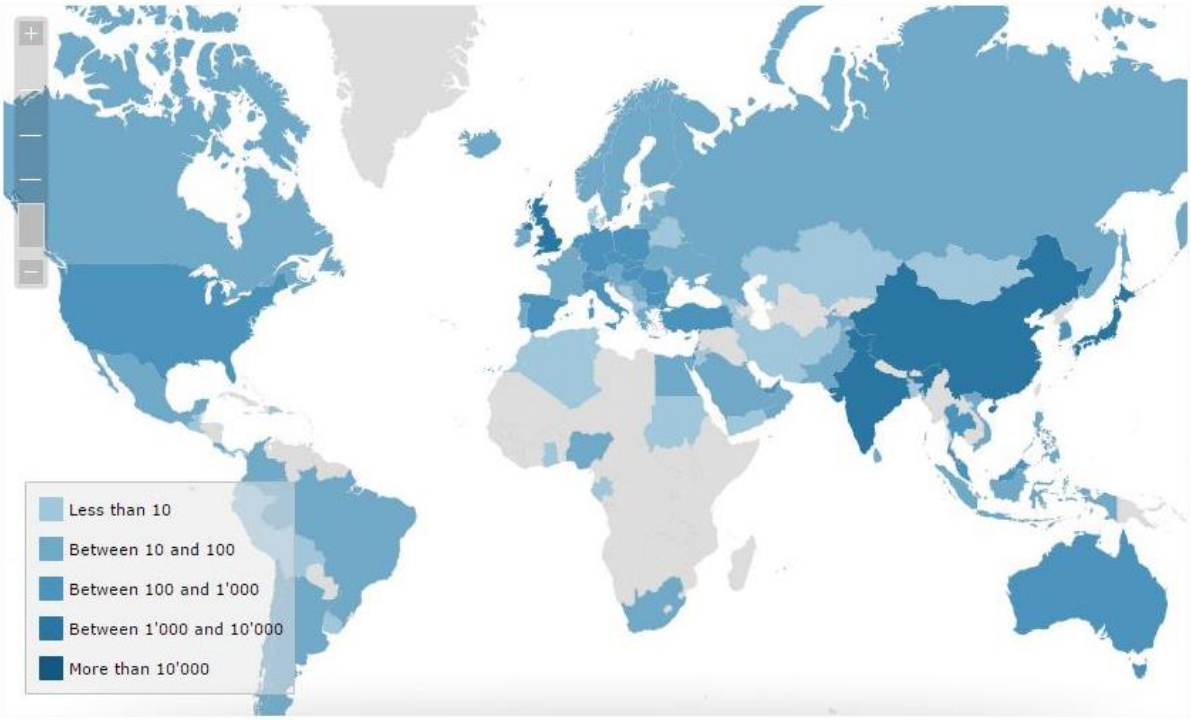


Ilustración 1 *– (ISO org, 2014 c) Distribución Certificaciones ISO en el mundo 2014.*

1.4. Planteamiento del trabajo

Evaluando las dificultades planteadas se llega a la conclusión de que la herramienta más apropiada para solucionarlas es un software que permita la gestión de la información eficazmente, que permita hacer seguimiento al proceso de implementación del SGSI en la compañía y que permita la consulta a través de una conexión a internet para consultar la información según se requiera. Para esto se plantea el desarrollo de una aplicación web desarrollada en software libre ya que uno de los valores agregados de la herramienta es que será gratuita y de libre uso. La herramienta estará compuesta de 4 módulos principales: diseño, implementación, gestión e informes, en donde el módulo de diseño ofrecerá funcionalidades como el cargue de los procesos de la entidad, cargue de dispositivos y activos, cargue de documentación, cargue de evidencias como GAP Analisys, etc. Para el módulo de implementación se agregarán funciones como la relación de recursos, activos a los procesos, cargue de dispositivos obligatorios según la norma, un módulo de plantillas para la creación de políticas y procedimientos, este módulo estará segmentado por cada uno de los dominios de la norma y sus controles relacionados. En cuanto al módulo de gestión se plantea un tablero de control grafico que muestre el avance a nivel de procesos y a nivel general indicando el grado porcentual de avance en el diseño e implementación del SGSI y finalmente el módulo de informes permitirá exportar los datos a un archivo PDF de acuerdo a un filtrado seleccionado por el usuario según la necesidad. Adicionalmente el software permitirá el manejo de perfiles que serán editables de acuerdo a la necesidad, sin embargo tendrá un usuario de perfil general que permitirá consultar información fácilmente. El diseño de la aplicación será *responsive*, es decir que se adaptará al tamaño de los dispositivos desde donde sea consultada para ofrecer una mejor funcionalidad y que resulte fácil de interactuar sin importar si se consulta desde una Tablet, Celular o PC.

1.5. Estructura del trabajo

Para llevar a cabo este proyecto se plantea un plan de trabajo organizado y estructurado que ayude a direccionar el avance y enfoque del mismo y se plantearon los siguientes capítulos:

Contexto y estado del arte:

En este capítulo se pretende investigar, consultar información relacionada al proyecto que permita identificar un marco general de la problemática aquí planteada en todo el mundo, las soluciones ofrecidas hasta el momento, las fortalezas y debilidades de la misma y como podría

esta herramienta convertirse en una solución útil y eficaz para los administradores de la seguridad.

Objetivos y metodología

Posterior a la identificación de la problemática, la posible solución y haber reconocido el entorno y las soluciones existentes entonces se planteará en este capítulo los objetivos que se pretenden alcanzar con el desarrollo de este proyecto, es decir, el a donde se quiere llegar y se describirá la metodología que planteará el cómo se va a llegar a esos objetivos.

Desarrollo de la contribución

En este capítulo se plasmarán todas las actividades desarrolladas durante el proceso de desarrollo, la identificación de requerimientos, el diseño de la aplicación, la codificación, las pruebas e implementación de la solución.

Conclusión

Aquí se documentarán todos los resultados obtenidos del desarrollo del proyecto, las dificultades que se evidenciaron, si realmente fue una solución a la problemática y como podría complementarse a futuro este proyecto, y se publicarán las fuentes de donde se recolectó la información requerida para el desarrollo del mismo.

2. Contexto y estado del arte

2.1. Antecedentes

A pesar de que se plantea el desarrollo de una aplicación como solución al problema antes descrito, debe aclararse que en la actualidad existen aplicaciones en el mercado que han sido diseñadas para este propósito; sin embargo este trabajo plantea el desarrollo de una herramienta que si bien permite la administración de un SGSI también debe decirse que se basa en un modelo totalmente diferente o innovador con respecto a las demás herramientas del mercado, ya que no es basado exclusivamente en la administración de riesgos. SASGSI incluirá funcionalidades que aportarán al seguimiento y administración del cumplimiento de la norma ISO 27001 con respecto a la implementación de la misma en determinada organización, para ello se han planteado algunas funcionalidades con diferentes innovaciones o diferencias con respecto a las actuales herramientas existentes en el mercado. El primer valor agregado es: la herramienta se publicará bajo una licencia GPL, es decir, será totalmente gratuita de libre uso y disponible para todas aquellas organizaciones que requieran de una solución para el seguimiento y administración de la seguridad de la información, otro valor agregado es que estará disponible en idioma español, esto resulta en un beneficio para los

usuarios dado que la mayoría de las herramientas han sido creadas por empresas especializadas en desarrollo de software ubicadas en países de habla inglesa y por ende las aplicaciones se encuentran en el mismo idioma. Adicionalmente el desarrollo incluirá un módulo de apoyo para la generación automática de documentos borradores de procesos, procedimientos y políticas, es decir que si el usuario selecciona un control específico de la norma, la aplicación generará un esquema o bosquejo del documento requerido para cumplimiento del mismo, este contendrá la información básica del procedimiento. Sin embargo el usuario debe ajustarlo según lo requerido por la organización y posteriormente realizar el trámite de aprobación por la dirección antes de cargarlo a la herramienta como evidencia en el módulo de implementación. Por último la aplicación incluirá un módulo grafico que corresponde al tablero de control de la implementación, este permitirá visualizar gráficamente el nivel de implementación con respecto al cumplimiento de la norma, esta evaluación se basa o realiza teniendo en cuenta puntualmente las evidencias o documentos del SGSI, es decir la norma exige una documentación que permite validar o evidenciar el cumplimiento de determinados aspectos por ejemplo: las políticas, los procedimientos, la declaración de aplicabilidad de controles, etc. SASGSI validará la existencia de los documentos y con base a esto generará graficas como informes, que permitirán visualizar el porcentaje de cumplimiento e identificar los ítems aún pendientes de ser este el caso. Con lo anteriormente descrito se espera que SASGSI no solo sea una herramienta más de la posible larga lista que se prevé existirá en el mercado teniendo en cuenta la difusión de la cultura de la seguridad de la información planteada en el capítulo anterior, sino que por el contrario sea una herramienta que aporte valor, se diferencie y destaque por su singularidad y opciones de funcionalidad. Aun así como conocimiento general se dan a conocer algunas de las soluciones existentes en el mercado y sus características más destacadas:

Ges Consultor

Ges Consultor es una solución de software muy robusta desarrollada para apoyar a empresas en la administración de diferentes aspectos relacionados con la seguridad, los servicios, protección de datos y la calidad. La aplicación enfocada especialmente a la ISO 27001 es denominada GesConsultor GRC.

Ofrece una plataforma 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. Adicionalmente proporciona capacidades diferenciadoras en su motor de cumplimiento para incorporar las nuevas versiones de las Normas y, con ello,

asegurar el mantenimiento y evolución de los proyectos basados en las mismas. La plena integración con la Capa Operativa de GesConsultor GRC ofrece una colección diferencial de automatismos que permiten conseguir niveles máximos de calidad en la implementación, mantenimiento y evolución del SGSI. Así, se minimizan las cargas internas de trabajo, sistematizando las operaciones y controles relacionados con la Seguridad TIC y enlazando directamente con los requerimientos de ISO/IEC 27001 (Monitorización, Métricas e Indicadores, Incidentes, Seguridad Gestionada, Vulnerabilidades, Formación, Gestión de Recursos, etc.). (GESDATOS Software, (s.f))

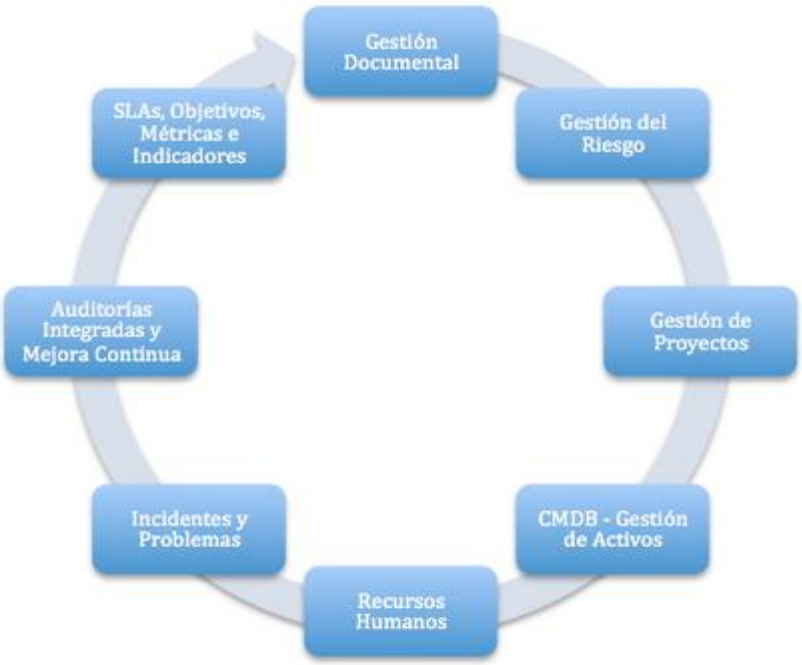


Ilustración 2 *-(GESDATOS Software, (s.f)) Módulos GesConsultor GRC*

Global Suite

Global suite es una suite de aplicaciones que se complementan o integran para ofrecer una completa solución de administración de sistemas de gestión, gestión documental, gestión de incidentes, etc. Sin embargo contiene un módulo específico para la administración de sistemas de seguridad denominada GlobalSUITE – Information Security.

Este es el software web que permite cubrir el ciclo completo de análisis, implantación, gestión y mantenimiento de la norma ISO 27001:2013. Está disponible en múltiples versiones adaptadas a las necesidades de las Multinacionales y Grandes Empresas, Administraciones

Públicas y PYMES. La versatilidad del software hace que cumpla con los requerimientos más complejos de una forma asequible e intuitiva, podrá realizar el proceso de Análisis y Gestión de Riesgos enfocado tanto a procesos como a activos, así como documentar y mantener actualizada la Declaración de Aplicabilidad alineada con los riesgos detectados y los procedimientos documentales correspondientes. (Global Suite, (s.f))

Características principales de GlobalSUITE

- Análisis diferencial (GAP Analysis)
- Definición de Servicios y Procesos
- Inventario de Activos
- Análisis y Gestión de Riesgos
- Gestión de Controles
- Configuración de las dimensiones de seguridad
- Configuración de metodologías para el cálculo de los riesgos
- Configuración de metodologías para la madurez de controles
- Declaración de aplicabilidad
- Gestión de Incidencias de Seguridad
- Publicación de Encuestas de Activos y Riesgos
- Cuadro de Mando
- Planes de Formación y Auditorías
- Gestor Documental
- Gestor de Informes
- Gestión de Proyectos
- Integración con los sistemas de la organización Interconexión con otros sistemas y software ya existentes en la organización
- Históricos y trazabilidad en el tiempo

RM Studio

Software RM Studio es una solución dinámica que combina la gestión de riesgos y la gestión de continuidad del negocio en una sola. Es una herramienta fácil de usar y simplifica la gestión del riesgo operacional e implementación de un SGSI permitiendo la implementación de estratégicas reguladas a través de un marco de aplicación de procedimientos que permiten gestionar riesgos y delinear la planificación de recuperación del negocio. RM Studio es una aplicación con las características de gran ayuda para las entidades y los administradores.

Algunas de ellas son el ahorro de tiempo y muchas opciones de personalización que se adapten a las necesidades de la organización (RM Studio, (s.f)).

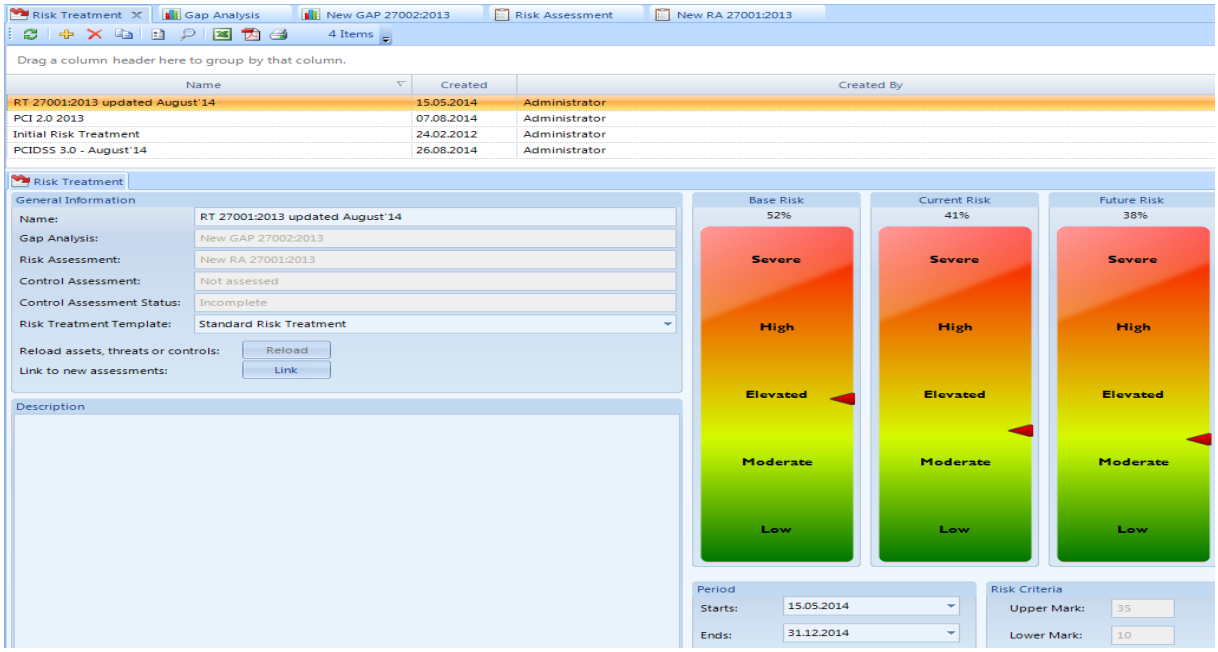


Ilustración 3 *- RM Studio. (s.f) Administración de Riesgos*

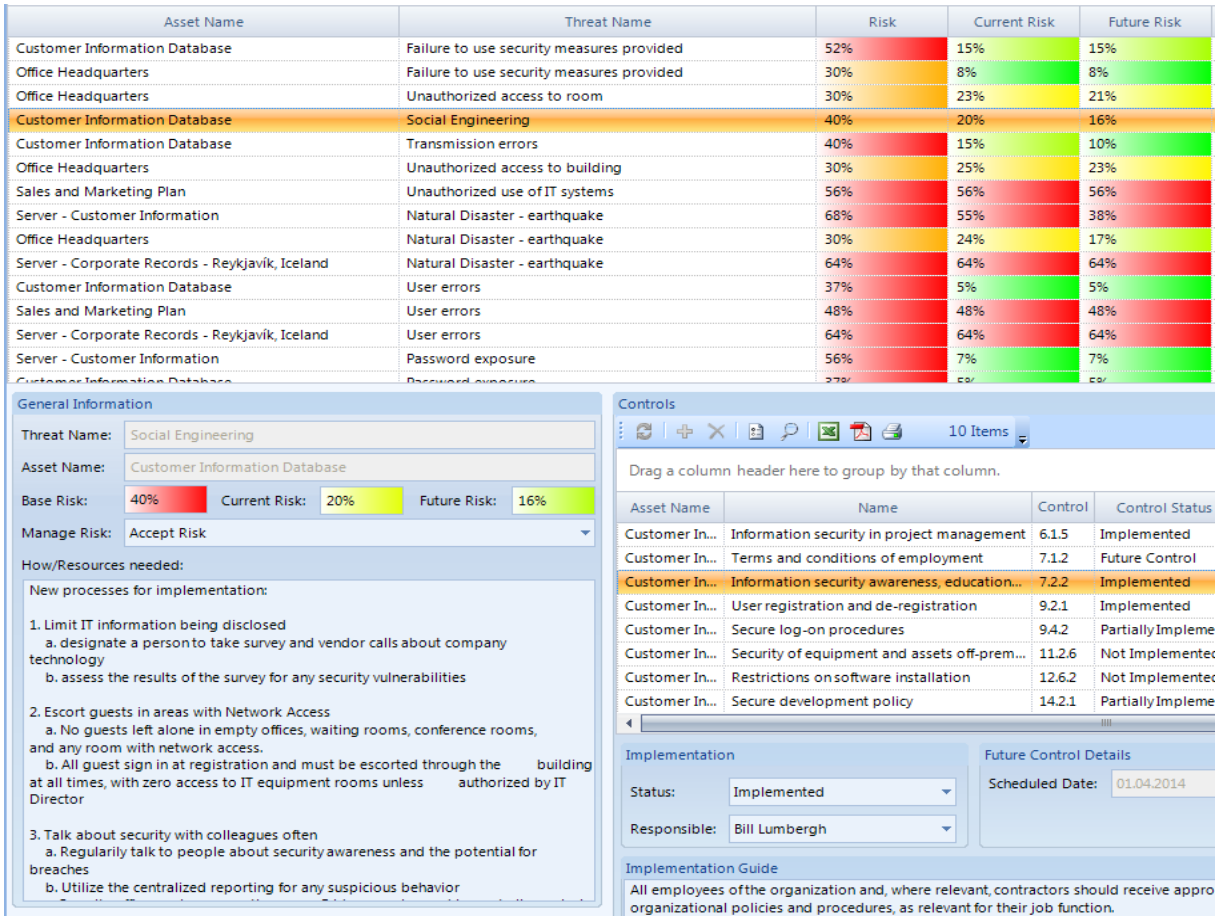


Ilustración 4 *- RM Studio. (s.f) Tratamiento de Riesgos*

EventLog Analizer – Manage Engine

Eventlog Analizer es una herramienta que ayuda a las compañías a dar cumplimiento con algunos de los controles exigidos por la norma ISO 27001, específicamente los A12.4.1, A12.4.2 y A12.4.3 que hacen referencia al almacenamiento y administración de eventos como evidencia. Adicionalmente también apoyan los controles A9.2.1, A9.2.5 y A9.4.2 que previenen accesos no autorizados a sistemas y servicios (Manage Engine, (s.f)).

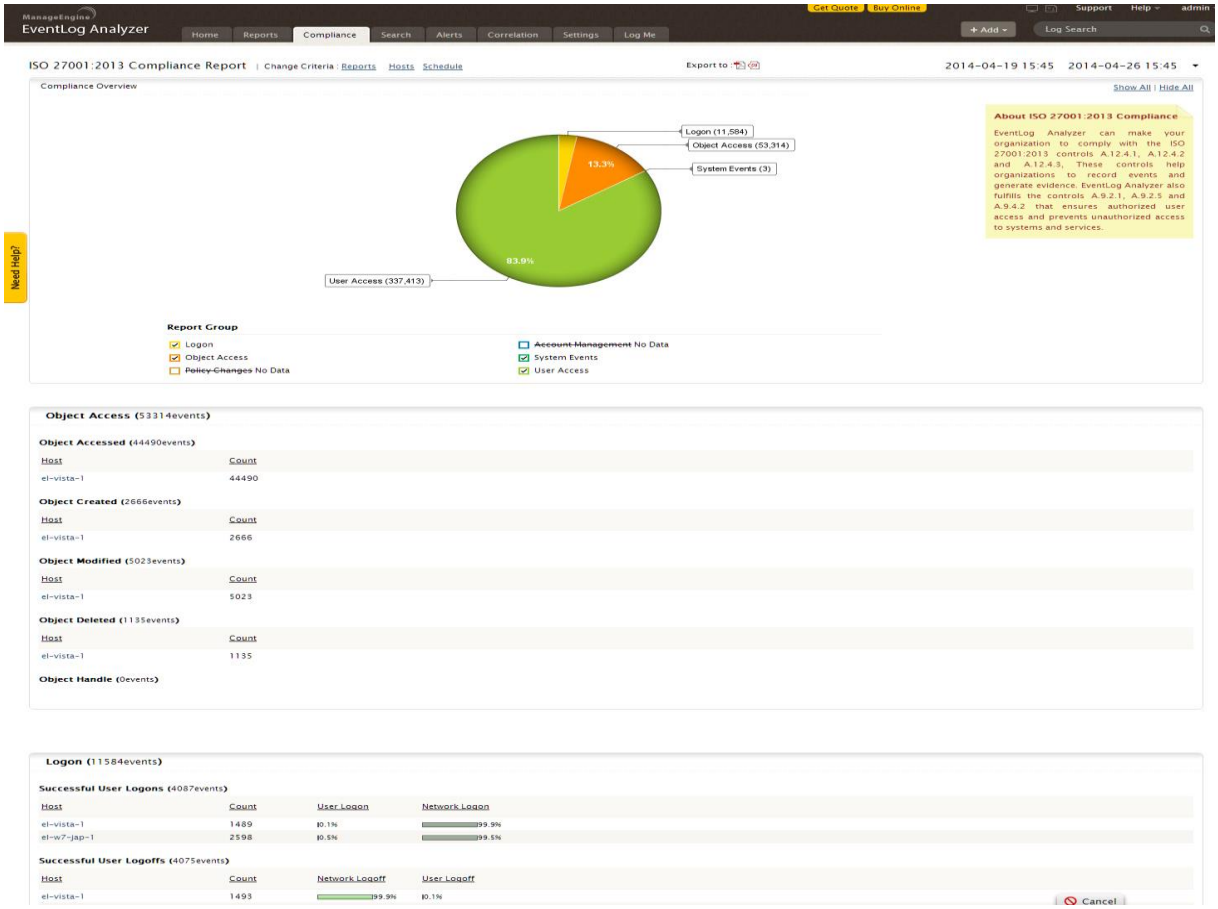


Ilustración 5 *- Manage Engine. (s.f) Análisis de Accesos*

Soft Expert

Soft Expert es una compañía que desarrolló y distribuye una solución completa llamada SoftExpert Excellence Suite que se compone de varios módulos cada uno de ellos diseñado con el propósito de apoyar determinadas actividades de la implementación del SGSI (SoftExpert, (s.f)). Estos se distribuyen de la siguiente forma:

Módulo	Requisito Normativo
SE Action Plan	• Mantener el plan de acción de seguridad de la información. • Mantener registro de eventos y acciones del SGSI. • Implementar acciones de mejora en el SGSI. • Tomar acciones correctivas y preventivas cuando sea apropiado. • Colocar en práctica las lecciones aprendidas en experiencias anteriores. • Usar acciones correctivas y preventivas para mejorar continuamente el SGSI. • Establecer un procedimiento de acciones preventivas para evitar la ocurrencia de potenciales no conformidades.
SE Audit	• Verificar si los requisitos de seguridad están siendo atendidos. • Ejecutar auditorías internas del SGSI de forma regular. • Establecer y documentar un procedimiento de auditoría interna del SGSI. • Definir la frecuencia de auditorías internas. • Programar auditorías internas en los intervalos definidos. • Dejar claro el alcance de cada auditoría del SGSI. • Especificar los criterios de auditoría de cada auditoría interna. • Definir el método de auditoría del SGSI. • Seleccionar a los auditores del SGSI. • Conducir auditorías internas regularmente, auditando controles, procesos y procedimientos del SGSI. • Utilizar los resultados de la auditoría para mejorar continuamente el SGSI.
SE BI	• Identificación, colecta y análisis de datos apropiados para demostrar la adecuación, la eficacia y la mejora continua del SGSI.
SE Competence	• Asegurar que todos los colaboradores vinculados al SGSI posean las competencias para ejecutar las actividades de su responsabilidad. • Mantener registros que evidencien la competencia de los colaboradores que ejecutan actividades que impacten en el SGSI.
SE Document	• Definir la política del SGSI de la organización • Definir documentos que registren tomas de decisión • Documentar el SGSI de la organización. • Proteger y controlar la documentación del SGSI. • Establecer un procedimiento para controlar los documentos del SGSI.

	• Establecer y mantener registros que apoyen al SGSI de la organización. • Aplicar una política de seguridad para mejorar continuamente la eficacia del SGSI.
SE Incident	• Identificar no conformidades. • Definir un procedimiento para toma de acción sobre incidentes de seguridad y no conformidades. • Utilizar el procedimiento de gestión de incidentes de la organización para identificar no conformidades.
SE Performance	• Asegurar que los cambios en el SGSI de la organización estén alcanzando los resultados esperados. • Demostrar que la alta gestión apoya y acompaña la implantación, operación, monitoreo, análisis crítico, mantenimiento y mejora continua del SGSI. • Asegurar que la alta gestión analice críticamente al SGSI a intervalos regulares. • Examinar el desempeño y eficacia del SGSI. • Analizar si el SGSI necesita cambios o mejoras. • Evaluar si la política de seguridad precisa cambios o mejoras. • Durante el análisis crítico, generar decisiones y tomas de acción para mitigar eventos que afecten el desempeño del SGSI. • Analizar y examinar: • Resultados de gestiones anteriores; • Mediciones anteriores del SGSI; • La situación de acciones de corrección tomadas anteriormente; • Oportunidades de mejora del SGSI; • Cambios que puedan afectar al SGSI
SE Problem Analysis	• Investigar y eliminar no conformidades y sus causas. • Tomar acciones de acompañamiento para asegurar que no conformidades y sus causas hayan sido eliminadas en el tiempo previsto. • Verificar si acciones correctivas sobre las causas fueron tomadas. • Reportar los resultados de las verificaciones de eficacia de las acciones. • Utilizar procedimientos para análisis e identificación de causas raíz.
SE Process	• Administrar la autorización de la alta gestión para implementación y operación del SGSI. • Administrar los recursos del SGSI de la organización. • Definir procedimientos de seguridad de la organización. • Revisar regularmente el SGSI. • Comunicar cambios del SGSI a las partes interesadas.

	• Identificar las necesidades de recursos para el SGSI • Proveer los recursos necesarios para el SGSI. • Identificar los recursos necesarios para que los procesos de seguridad de la información sustenten los requisitos de negocio. • Aplicar el proceso de mejora continua para aumentar la eficacia del SGSI.
SE Project	• Establecer programas y portafolios para educación y concienciación de la importancia de la seguridad de la información. • Planificar actividades y proyectos de auditoría interna.
SE Risk	• Definir el abordaje utilizado para el análisis de riesgo. • Identificar los riesgos de seguridad de la organización. • Analizar y evaluar los riesgos. • Identificar y evaluar las acciones y opciones de tratativa de riesgos. • Definir controles y objetivos de control para tratar riesgos. • Asegurar que la alta gestión apruebe riesgos residuales. • Preparar una declaración de aplicabilidad que liste los controles y objetivos específicos de la organización. • Desarrollar un plan de riesgos para administrar los riesgos de seguridad de la información. • Implantar un plan de tratativa de riesgos. • Implantar controles de seguridad. • Utilizar procedimientos y controles para monitorear y analizar el SGSI. • Revisar la evaluación de los riesgos regularmente.
SE Training	• Establecer programas de entrenamiento. • Evaluar la eficacia de entrenamiento de los colaboradores del SGSI. • Asegurar que los colaboradores tengan conciencia de la importancia de las actividades del SGSI.

Tabla 1 *- (SoftExpert, (s.f)) - Funcionalidades SoftExpert*

2.2. Marco Teórico

Se plantea teóricamente como se desarrollará la herramienta, que funcionalidades y por qué se van a incluir y a través de qué mecanismos se van a implementar.

La aplicación funcional y visualmente constará de 4 módulos principales relacionados a las fases de un proyecto de implementación de un SGSI, por tanto se han elegido los siguientes: diseño, implementación, gestión e informes. En cada uno de ellos se agregarán funcionalidades que están directamente relacionadas con la fase del proyecto; de esta manera se estructuran las actividades y se genera un orden visual y administrativo para el usuario de la aplicación. Por tanto, para el módulo de diseño se agregaron las siguientes funcionalidades:

Procesos y Procesos detalle

En este apartado se cargarán todos los procesos y subprocesos de la entidad y podrán clasificarse por misionales, estratégicos y de apoyo. Estos pueden obtenerse en la mayoría de los casos del sistema de gestión de calidad. Si no se cuenta con un sistema de gestión que tenga previamente identificados los procesos y procedimientos de la entidad será necesario realizar el análisis, levantamiento de información e identificarlos y documentarlos ya que estos son indispensables para el proceso de implementación del SGSI, porque nos dan el mapa de ruta a seguir puesto que teniendo el listado de los mismos y los subprocesos de cada uno se puede identificar el proceso más transversal a la organización. Esto puede saberse con facilidad si se cruzan los subprocesos que contiene con la actividad principal u objeto de la entidad. Posterior a la identificación podrá tomarse como base de ejecución del proyecto. Según las recomendaciones en grandes entidades debe seleccionarse un proceso, el más importante, y hacerse la implementación sobre este y posteriormente ir adhiriendo los demás. Esto con el ánimo de no tener un horizonte demasiado ambicioso y quizás utópico y a pesar de que estas recomendaciones son muy valiosas en empresas que están asumiendo el reto de la seguridad el sistema no tiene limitantes en la cantidad de procesos seleccionados para iniciar el proyecto, es decir si una entidad desea asumir el reto de implementar un SGSI para toda la entidad y seleccionar simultáneamente todos los procesos podrá hacerlo.

Apoyo

En este apartado de la aplicación se agregará una funcionalidad que permitirá a los administradores crear y usar plantillas previamente definidas para la creación de políticas y

procedimientos básicos apoyados en las recomendaciones o *baselines* existentes para la creación de las mismas. Esta funcionalidad se considera importante y se implementa como un valor agregado frente a otras herramientas existentes ya que la norma ISO 27001 exige como cumplimiento en algunos de sus objetivos de control y controles la creación e implementación de políticas y procedimientos. Algunos de estos son los siguientes:

A.5. Política de seguridad de la información

A.6.2.1. Política para dispositivos móviles

A.6.2.1. Política para teletrabajo

A.8.2.2. Procedimientos definidos para el etiquetado de la información

A.8.2.3. Procedimiento para el manejo de los activos

A.8.3.1. Procedimiento para gestión de medios removibles

A.8.3.2. Procedimientos para la disposición de los medios de soporte

A.9.1.1. Política de control de acceso

A.9.2.4. Procedimiento de gestión de información secreta de autenticación

A.10.1.1. Políticas sobre el uso de controles criptográficos

A.10.1.2. Política de gestión de claves criptográficas

A.11.2.9.Politica de escritorio limpio

A12.1.1. Procedimiento de operación documentada

A.12.3.1. Política de copias de respaldo de la información

A.12.5.1. Procedimiento de instalación de software en sistemas operativos

A.13.2.1. Políticas y procedimientos para la transferencia de información

A.16.1.7. Establecer procedimientos para la recolección, adquisición y preservación de evidencia

A.18.1.2. Procedimientos para garantizar cumplimiento a derechos de propiedad intelectual

Como podemos evidenciar son varios ítems en los que debe crearse este tipo de documentación y en la mayoría de los casos son estructuralmente muy parecidos; solo se diferencian en algunos aspectos en los que reflejan actividades propias de la entidad. Aun así

si se considera que si el administrador o líder de seguridad cuenta con una plantilla que guie el proceso de creación de estos documentos resultaría más práctico y rápido de implementar o tener al menos un bosquejo para llevar a discusión al comité de gobierno de seguridad.

En cuanto al módulo de implementación se eligieron funcionalidades que están involucradas en esta fase del proyecto es decir actividades propias del cumplimiento de la norma y en cada una de ellas el software permitirá el cargue de información que evidencia el cumplimiento para su seguimiento y mantenimiento, estas funcionalidades son:

Activos

En el menú del módulo de implementación aparece una opción que se denominará activos. Este apartado permitirá el cargue, actualización y borrado de activos de información que de acuerdo al objetivo de control A.8 de la norma denominado gestión de activos deben identificarse y administrarse incluso hasta cuando se dan de baja del inventario en el caso de los equipos físicos y servers. La aplicación en este apartado contendrá varios submenús (aplicaciones, bases de datos, servidores, equipos, licencias, empleados) y esto únicamente porque la norma establece que un activo de información es todo aquello que puede contener información relevante para la organización y por ende debe controlarla y protegerla. La aplicación permitirá realizar ingresos manuales de la información en caso de ser necesario, sin embargo se dispondrá de la posibilidad de realizar cargues masivos desde archivos en formatos *XLS, XLSS* o *CSV*, está función facilitará en gran medida la labor del administrador, ya que dependiendo del tamaño de la compañía el listado de activos podría resultar en un número muy alto de registros como para realizarlo individualmente.

Riesgo y Controles

En este apartado están las funcionalidades de asignación de riesgos a cada uno de los activos de acuerdo al tipo de evaluación previamente definido por el gobierno. También está la funcionalidad de asignación de controles para contrarrestar los riesgos identificados y con base a esto se obtendrá automáticamente la matriz de riesgos y la declaración de aplicabilidad, que son documentos exigidos como cumplimiento en la norma. La aplicación tendrá precargados controles y riesgos de normas, metodologías internacionales como la ISO 31000, MAGERIT e ISO 27005, esto con el fin de facilitar al administrador el proceso de asignación a cada uno de los activos; sin embargo el usuario podrá agregar manualmente un control o riesgo personalizado si así lo considera.

Documentación

En esta opción del módulo aparecerá el listado de documentos exigidos por la norma para dar cumplimiento a cada uno de los controles y objetivos de control, es decir contendrá los archivos donde se documentaron los procesos, políticas, procedimientos y también la declaración de aplicabilidad, el listado de controles implementados, el plan de tratamiento y la matriz de riesgo, algunos de estos identificados automáticamente en la funcionalidad de riesgo y control descrita anteriormente. La aplicación tendrá una funcionalidad de *checklist* en este apartado que permitirá visualmente al administrador identificar un posible faltante en el cumplimiento.

El tercer módulo de la aplicación corresponde a la gestión y permitirá ver el seguimiento realizado al SGSI y cada uno de sus apartados y precisamente por esto es que se seleccionaron las siguientes funcionalidades:

Gobierno

En este apartado se listarán los miembros del comité de seguridad los cuales componen el gobierno encargado de marcar el horizonte de la compañía con respecto a la seguridad informática, y que son responsables de crear y aprobar las políticas, procedimientos, procesos y reglas seleccionadas para dar cumplimiento a la norma y para mejorar la seguridad de la información en la entidad.

Reuniones

En este apartado podrán documentarse las reuniones realizadas por el comité, los documentos tratados o trabajados para consulta de los interesados y autorizados. Adicionalmente podrá cargarse como evidencia el listado de asistencia de la misma y el acta de la reunión.

Auditorias

La funcionalidad de auditorías contendrá dos sub-funciones o submenús, uno denominado programación y otro denominado resultados y como su nombre lo indica en cada uno de ellos podrá cargarse información relevante. En el caso de la programación las fechas de las auditorías realizadas y las venideras, en el ítem de resultados se cargará el informe de auditoría con las opciones de mejoras, los hallazgos e inconformidades, esto con el fin de

tener a la mano información relevante que ayude al comité a decidir cómo y qué solucionar de acuerdo a la prioridad.

Por ultimo está el módulo de informes que permitirá ver gráficamente el estado de la implementación y algunos aspectos relevantes que permitirán fácilmente a una persona ajena ver el estado de madurez del SGSI de la compañía, y se considera relevante porque es quizás una forma más efectiva de cuantificar. Aunque se tenga la información en cada uno de los anteriores módulos seria dispendioso dar siquiera un porcentaje supuesto del cumplimiento; sin embargo si tenemos una herramienta grafica que automáticamente entregue un resultado en tiempo real se incrementará la eficiencia, y para ello se implementaran los siguientes tableros:

- **Diseño**

La funcionalidad de informes gráficos para el ítem diseño mostrará gráficamente el listado de procesos y sub procesos de la compañía indicando un porcentaje en cada uno de ellos. Esto no solo permitirá la opción de tener un listado de los mismos en una vista gráfica sino que también permitirá identificar cual es el que tiene más subprocesos y a sus actividades. Con esto se puede evaluar visualmente cuáles son los más relevantes para la compañía.

- **Implementación**

En el submenú implementación se encuentra quizás el valor más grande en esta funcionalidad y es que de acuerdo al *checklist* de documentos la aplicación permitirá reconocer el estado real de cumplimiento del SGSI en la compañía e identificará las actividades pendientes para lograr el 100% de la implementación y los controles de la norma afectados por la misma.

2.3. Marco Conceptual

En este apartado se documenta el significado de cada uno de los términos que se utilizan durante el proyecto para contextualizar y enfocar en la misma línea.

SGSI

La sigla SGSI corresponde a Sistema de Gestión de la Seguridad de la Información, el cual es un compendio de políticas y procedimientos que establecen mecanismos de control y buenas prácticas para la protección de la información desde el punto de vista de la

confidencialidad, integridad y disponibilidad. En la mayoría de los casos cuando se hace referencia al sistema de gestión de seguridad de la información se relaciona con la norma ISO 27001, la cual es una guía para la implementación del mismo.

Seguridad informática

La seguridad informática en términos generales hace referencia a todos aquellos dispositivos físicos implementados desde la parte de TI y adoptados por la entidad para la protección de la información tales como firewall, IDS´s, sniffers, antivirus, control de acceso físico, etc.

Seguridad de la información

La seguridad de la información hace referencia a todos aquellos mecanismos documentales implementados por la entidad para la protección de la información, es decir las políticas, procesos y procedimientos implementados para garantizar la confidencialidad, integridad y disponibilidad de la información.

Integridad

Integridad es el grado de exactitud que un elemento determinado puede tener con respecto a su estado original. En este caso, al hablar de integridad se entiende como una característica de la información, por lo tanto hace referencia a la exactitud de un dato con respecto al dato original, es decir, que un dato es integro cuando no ha sido alterado o manipulado por ninguno de los procesos por los que haya tenido que pasar.

Confidencialidad

La confidencialidad es la propiedad que hace referencia a que la información solo sea accedida por quienes tienen la autorización para hacerlo, es decir, que debe seleccionarse quien puede visualizarla, usarla, etc. y disponerse de mecanismos que garanticen que no es accedida por terceros ajenos que carecen de autorización.

Disponibilidad

Hace referencia a que la información sea accesible en el momento en que es requerida, que pueda consultarse y usarse de acuerdo a la necesidad en el momento que se requiera. Para esto es necesario disponer de mecanismos que garanticen que la información no es solo disponible sino que además es legible, interpretable y organizada.

Hardware

Son todas aquellas partes físicas de un sistema de cómputo, computadora o sistema informático, todo aquello que los compone físicamente

Software

Son todas las partes no físicas de un sistema, es decir la parte lógica que le permite interactuar con los dispositivos físicos, habitualmente creados en lenguajes de programación que permiten crear una estructura lógica para que realice acciones o procesos según un objetivo o necesidad. Entre estos pueden contarse las aplicaciones, sistemas operativos, los paquetes ofimáticos, etc.

Sistema operativo

Es el sistema o software principal que gestiona los recursos de hardware y servicios para que otras aplicaciones puedan ejecutarse con los privilegios adecuados y de forma correcta para ofrecer al usuario la posibilidad de interactuar de forma estable con la computadora, dispositivo o sistema.

Lenguaje de programación

Un lenguaje de programación es un conjunto de sentencias y palabras reservadas que al ser organizadas lógicamente y con algunos parámetros de origen pueden realizar procesos automáticos. Los códigos de un lenguaje de programación tras compilarse, también son conocidos como código de maquina ya que básicamente son sentencias capaces de ser interpretadas por las maquinas porque se traducen en 0 y 1.

PHP

PHP (Hypertext Pre-processor) “es un lenguaje de programación diseñado para la programación web que puede integrarse en directamente en un documento HTML. Es uno de los lenguajes de programación más conocidos y usados ya que además de ser *open source* es uno de los más flexibles, potentes y de alto rendimiento” (Wikipedia, (s.f. a)).

MYSQL

Mysql es un sistema de gestión de bases de datos relacional multihilo y multiusuario que permite la gestión y almacenamiento de información de forma relacional. Mysql actualmente pertenece a Oracle Corporation que han implementado un licenciamiento dual para la solución, es decir, que a pesar de que continúa siendo libre y compatible con aplicaciones de licencia GNU GPL las empresas que deseen incorporarlo en productos privativos deberán pagar un licenciamiento. Mysql fue desarrollado en su mayor parte en ANSI C (Wikipedia, (s.f. b)).

Base de datos

“Se le llama base de datos a los bancos de información que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto. Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. Existen programas denominados sistemas gestores de bases de datos, abreviado DBMS, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada” (Wikipedia, (s.f. c)).

Aplicación

Es un software, un programa informático que fue diseñado como una herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos y a pesar de que se encuentra dentro del grupo del software, este no hace parte de los sistemas operativos si no que son por así decirlo utilitarios que permiten proporcionar una solución para algún tipo de necesidad de automatización de tareas complicadas (Wikipedia, (s.f. d)).

Accesibilidad

La accesibilidad en el contexto web hace referencia a los mecanismos usados desde el enfoque del diseño para que un sitio web permita a las personas percibir, entender, navegar e interactuar con el mismo. Habitualmente se enfoca en personas con discapacidad o de edad avanzada quienes pueden tener baja visión y poca motricidad (Universidad de Granada, (s.f.).).

2.4. Hipótesis

El uso de la aplicación SASGSI permitirá a los administradores de seguridad de la información tener una herramienta de apoyo en la implementación del SGSI. En la actualidad el gobierno Colombiano a través del decreto 2573 de 2014 obliga a todas las entidades públicas a implementar sistemas de gestión de seguridad de la información en un periodo máximo de 3 años, es decir, a 2018 (MinTIC, 2014). Colombia actualmente tiene unas 9.041 entidades públicas, o sea, que el espectro de empresas certificadas en la norma ISO 27001 crecerá considerablemente y aunque el decreto no exige la certificación sí exige el diseño e implementación, fases en las que la aplicación contiene funciones relevantes y de gran apoyo. Considerando además que esta será una herramienta gratuita y muy intuitiva podremos intuir que esta solución se convertirá en una opción muy probable para aquellas personas que requieran de una solución como SASGSI, y se espera que al poner el código a disposición de los usuarios cada vez le sean incluidas muchas más funcionalidades que hagan la solución más robusta, más completa. Precisamente esa es una de las razones por las que la aplicación se codificará en PHP un lenguaje de programación web muy común.

2.5. Ventajas SASGSI

En los anteriores capítulos se ha expuesto el contexto de la seguridad de la información a nivel empresarial, permitiendo evidenciar las tendencias y posiciones de las mismas frente a esta temática, los problemas y retos que actualmente afrontan o deberán afrontar. Posterior a esto se ha planteado una necesidad, se ha realizado un acercamiento a algunas de las posibles soluciones existentes, y a pesar de ser aplicaciones muy robustas puede notarse que ninguna satisface al 100% la necesidad. Es por ello que se ha planteado una solución mediante el desarrollo de SASGSI, una aplicación con unas funcionalidades y características muy particulares tal como se describieron en el numeral 2.2 Marco Teórico, enfocadas en el seguimiento al cumplimiento de la norma ISO 27001 y en aportar información relevante a los administradores del SGSI referente a la implementación. Son precisamente estos dos

aspectos los que permiten que SASGSI sea una solución diferente e innovadora y que en la actualidad no pueda suplirse con una misma aplicación. Para visualizar mejor estos aspectos se ha seleccionado un listado de funcionalidades comunes en los software de administración o de apoyo de los SGSI, junto con algunas de las planteadas en los requisitos funcionales y las requeridas en la solución según el planteamiento del problema y se ha procedido a evaluar SASGSI frente a las herramientas existentes más reconocidas en el mercado y el resultado es el siguiente:

RELACION SASGSI OTRAS HERRAMIENTAS

	Ges Consultor	Global Suite	RM Studio	SASGSI
Administración de Activos	✓	✓	✓	✓
Administración de Riesgos	✓	✓	✓	✓
Gestión de Incidentes	✓	✓	✘	✓
Gestión Controles	✓	✓	✓	✓
Planes de Formación y Auditoria	✓	✓	✓	✓
Repositorio de Documentos	✓	✓	✘	✓
Manejo de Perfiles	✓	✓	✓	✓
Cargues masivos	✘	✘	✘	✓
Informes Gráficos	✓	✓	✓	✓
Apoyo creación documentos	✓	✘	✘	✓
Administración de Procesos	✘	✓	✘	✓
Gráficos de Nivel de Implementación	✘	✘	✘	✓
Gratuito	✘	✘	✘	✓
Idioma Español	✓	✓	✘	✓
Exportar Archivos	✘	✘	✘	✓

Tabla 2 *- Relación SASGSI I*

RELACION SASGSI OTRAS HERRAMIENTAS

	EventLog	SoftExpert	SASGSI
Administración de Activos	✓	✓	✓
Administración de Riesgos	✓	✓	✓
Gestión de Incidentes	✘	✓	✓
Gestión Controles	✓	✘	✓
Planes de Formación y Auditoria	✘	✓	✓
Repositorio de Documentos	✘	✓	✓
Manejo de Perfiles	✓	✓	✓
Cargues masivos	✘	✘	✓
Informes Gráficos	✓	✓	✓
Apoyo creación documentos	✘	✓	✓
Administración de Procesos	✘	✓	✓
Gráficos de Nivel de Implementación	✘	✘	✓
Gratuito	✘	✘	✓
Idioma Español	✘	✓	✓
Exportar Archivos	✘	✘	✓

Tabla 3 *- Relación SASGSI II*

Como puede notarse SASGSI es una aplicación que integrará funcionalidades muy particulares y a pesar de ser una aplicación muy básica teniendo en cuenta el amplio número de posibles funciones que podrían integrarse con respecto a la seguridad informática y de la información, esta ofrece no solo los aspectos básicos de una solución de este tipo, sino que además va un poco más allá integrando valor funcional a los usuarios. Este valor precisamente surge a raíz de los vacíos de las demás aplicaciones en referencia a la administración de un SGSI, ya que el concepto general tradicional de las aplicaciones descritas se focaliza casi de

forma exclusiva a la administración de riesgos, la identificación, valoración y documentación para la mitigación de los mismos. Sin embargo el enfoque de SASGSI es completamente diferente e innovador desde la siguiente perspectiva: a pesar de que tendrá en cuenta la administración de los riesgos por que la norma ISO 27001 así lo considera (ISO Org, s.f). Esta no es su única funcionalidad o enfoque, ya que ofrece otras herramientas claves en la implementación y gestión. Algunas de ellas son el módulo de apoyo en la creación de documentos, este permitirá que los administradores sin mucho esfuerzo y amplio conocimiento técnico puedan generar borradores de documentos claves para el cumplimiento y por ende requeridos en la implementación. Adicionalmente la funcionalidad de repositorio de documentos que permitirá fácilmente identificar la documentación básica obligatoria de la norma, lo cual de forma intrínseca provee un mapa de ruta en la implementación dado que podrán precisarse las actividades a desarrollar para obtener la documentación y como esta funcionalidad es usada para generar el grafico de nivel o porcentaje de implementación puede decirse que está finalmente también se convierte en un mecanismo de gestión y seguimiento.

SASGSI es una herramienta que tal como se describe en el planteamiento del problema tiene como uno de sus objetivos gestionar la implementación del SGSI, esto la hace diferente a las existentes. Además está planteada de tal forma que cualquier individuo con un conocimiento mínimo de seguridad de la información pueda entender y realizar la implementación de seguridad de la información bajo los requisitos de la norma ISO 27001.

3. Objetivos y metodología

3.1. Objetivos Generales

- Diseñar, Codificar e implementar un software para la gestión y administración de un SGSI.

3.2. Objetivos Específicos

- Identificar los requerimientos de los administradores de seguridad referentes a la administración del SGSI.
- Codificar los requerimientos detectados.
- Diseñar una aplicación funcional, adaptable, escalable y usable.
- Implementar la solución y realizar pruebas de funcionalidad.

3.3. Metodología

La metodología planteada para el desarrollo de este proyecto es la siguiente:

- **Fase de Pre análisis**
  - Recolección de fuentes y documentos referentes al tema
  - Identificación del problema

- **Fase Análisis**
  - Análisis de una posible solución
  - Investigación de antecedentes del problema y la solución
  - Identificación de requerimientos
  - Determinar viabilidad técnica, operacional y económica

- **Fase de estructuración y diseño**
  - Planteamiento del problema
  - Planteamiento de la solución
  - Identificación de los objetivos
  - Determinar el alcance

- **Fase desarrollo**
  - Identificación de requerimientos funcionales y no funcionales
  - Definición del diseño
  - Identificación de las herramientas en las que se va a desarrollar la aplicación
  - Codificación y pruebas de cada uno de los módulos

- **Fase de pruebas, análisis de resultados y pruebas**
  - Ejecutar pruebas de funcionalidad a cada uno de los módulos
  - Realizar ajustes a las fallas funcionales detectadas
  - Ejecutar pruebas de seguridad y codificación a cada uno de los módulos
  - Realizar ajustes a las detecciones
  - Generación de informes de los errores funcionales y de seguridad detectados.
  - Crear la documentación: manuales de usuario y técnicos de la herramienta.

- **Conclusiones**
  - Documentar las conclusiones de la realización del proyecto
  - Documentar las fuentes usadas
  - Plantear posibles líneas de investigación para complementar el trabajo realizado

4. Desarrollo de la contribución

4.1. Identificación de requisitos

En esta sección se documentarán todos los mecanismos y resultados del proceso de análisis y recolección de información realizada a personas que están interesadas en este campo o que son administradores de seguridad para identificar las necesidades que la herramienta debe satisfacer para cumplir con el objetivo para el que se ha planteado incluyendo las funcionalidades que ellos consideren.

Para el desarrollo de la aplicación, en primera instancia, procedió a realizarse una identificación de requisitos funcionales y técnicos que satisficieran las necesidades reales de los posibles usuarios de sistemas de gestión de seguridad de la información, para ello se solicitó a administradores de seguridad, administradores de aplicaciones y personal de infraestructura tecnológica de diferentes empresas responder a un cuestionario diseñado para identificar los requisitos a incluir para solucionar la problemática planteada.

Después de evaluadas las respuestas y el contenido de cada una de los cuestionarios se identificaron los siguientes requisitos funcionales y técnicos de la aplicación:

4.1.1. REQUISITOS FUNCIONALES

- La aplicación debe tener un sistema de protección o mecanismo de autenticación que restrinja el acceso a personas no autorizadas.
- La aplicación debe tener manejo de perfiles o roles que ayuden a que algunas de las funcionalidades solo sean usadas por personas autorizadas.
- La aplicación deberá permitir cargues masivos de información, especialmente en el inventario de activos, el listado de controles, procesos y procedimientos de la entidad y listado de riesgos.
- La aplicación deberá permitir asignar riesgos y controles al listado de activos.
- La aplicación debe contener un repositorio de documentos. En él se debe permitir la subida de documentos escaneados correspondientes a las políticas, procesos y procedimientos firmadas y aprobadas por la alta dirección y el gobierno de seguridad.
- La aplicación debe permitir exportar datos a Excel para ser analizados más fácilmente.
- La aplicación debe permitir cambiar el *password* únicamente para los roles de administrador.

- Debe existir la opción de ingresar como visitante para acceder a la información pública y de consulta general al sistema.
- Desde la aplicación podrán enviarse impresiones.
- La aplicación debe tener una política para la gestión de contraseñas

4.1.2. REQUISITOS TÉCNICOS

- La aplicación debe poder ser accesible vía web.
- La aplicación debe poder consultarse desde cualquier dispositivo (Tablet, Celular, Computador Personal, Computador Portátil).
- Debe poder visualizarse desde cualquiera de los navegadores web más comunes (Firefox, Internet Explorer, Google Chrome).
- La aplicación de tener un segmento de ayuda en donde se tenga información del uso del aplicativo.
- La aplicación debe ser multiplataforma, es decir debe poder instalarse tanto en sistemas Linux como Windows.
- La aplicación debe ser compatible con las últimas versiones de PHP, Apache y Mysql.
- Las claves de los usuarios de la aplicación deben almacenarse cifrados en la base de datos.

4.2. Descripción de la herramienta

Para el desarrollo de SASGSI, se aplicaron conceptos de la metodología de desarrollo de software orientada a objetos que se denomina OMT (Object Modeling Thechnique) que junto con UML (Unificated Model Lenguage) son las más usadas en la actualidad porque ofrecen elementos que grafican las interacciones, estados y objetos de la aplicación, aspectos claves en el desarrollo actual. Los conceptos adoptados en este proyecto pertenecen específicamente a las fases de análisis y diseño de las mismas. El uso de una metodología como guía permite tener un control sobre las actividades realizadas durante el ciclo de vida del sistema con el fin de garantizar que estas se realizan bajo buenas prácticas y para garantizar que la aplicación cumplirá con los objetivos para los que fue desarrollada, es por ello que luego de haber identificado los requisitos funcionales y técnicos se procederá a realizar la identificación y diagramación de los casos de uso de la aplicación. Estos identificarán los posibles usos y desusos de la aplicación mediante la diagramación de una

secuencia de interacciones llevada a cabo por cada uno de los usuarios o los servicios que interactúen con la misma. Los casos de uso son de suma importancia, ya que permiten aclarar el funcionamiento brindando una visión global y relacional de la aplicación, esto a su vez permite identificar puntos débiles y es precisamente por esa importancia que se desarrollarán.

Los casos de uso de la aplicación SASGSI son:

4.2.1. CASOS DE USO

Caso de Uso:	Acceder a la aplicación autenticación
Actores:	Administradores
Tipo:	Primario
Descripción:	Autentica un usuario y otorga acceso
Flujo Normal	El usuario ingresara a la URL a través del navegador y digita el usuario y contraseña otorgado previamente y adicionalmente deberá ingresar un código captcha, el sistema valida contra la base de datos y otorga o deniega el acceso
Precondiciones	Ninguna

Caso de Uso:	Cambiar contraseña
Actores:	Administradores
Tipo:	Primario
Descripción:	Actualiza la contraseña de un usuario
Flujo Normal	Click sobre el menú perfil y seleccionar área admin seleccionar el menú añadir o editar usuarios, editar el usuario y actualizar campo contraseña.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Ingresar el listado de activos
Actores:	Administradores
Tipo:	Primario
Descripción:	Permite agregar activos
Flujo Normal	El administrador hace click en el módulo diseño y posteriormente en el menú activos. Selecciona el botón “más” del menú que desplegará la opción “importar”. Al seleccionarla, carga un menú que permite agregar registros masivamente a través de un archivo Excel.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Ingresar el listado de riesgos
Actores:	Administradores
Tipo:	Primario
Descripción:	Permite agregar riesgos

Flujo Normal	El administrador da click en el módulo “implementación” y selecciona la opción “riesgos”. Se mostrará un menú de botones y selecciona “añadir nuevo”.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Ingresar el listado de controles
Actores:	Administradores
Tipo:	Primario
Descripción:	Permite agregar controles
Flujo Normal	El administrador al dar click en el módulo implementación y seleccionar la opción controles Hará que se muestre un menú y da click en el botón “añadir nuevo”.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Ingresar el listado de procedimientos
Actores:	Administradores
Tipo:	Primario
Descripción:	Ingresar procedimientos de la entidad
Flujo Normal	El administrador al dar click en el módulo diseño y seleccionar la opción procesos hará que se desplegué la opción cargue masivo.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Eliminar o Editar Procesos
Actores:	Administradores
Tipo:	Primario
Descripción:	Borra o actualiza un proceso
Flujo Normal	El administrador al dar click en el módulo diseño y seleccionar procesos, selecciona cada uno de los procesos en la casilla, da click en el botón denominado con los seleccionados y selecciona la opción editar o eliminar.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Imprimir Procesos
Actores:	Administradores
Tipo:	Primario
Descripción:	Imprime los procesos seleccionados
Flujo Normal	El administrador al dar click en el módulo diseño y seleccionar procesos, selecciona cada uno de los procesos en la casilla, da click en el botón denominado con los seleccionados y selecciona la opción imprimir
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Eliminar o Editar Riesgos
Actores:	Administradores
Tipo:	Primario
Descripción:	Borra o actualiza un riesgos
Flujo Normal	El administrador al dar click en el módulo implementación y seleccionar procesos, selecciona cada uno de los riesgos en la casilla, da click en el botón más y selecciona la opción editar o eliminar.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Imprimir Riesgos
Actores:	Administradores
Tipo:	Primario
Descripción:	Imprime los riesgos seleccionados
Flujo Normal	El administrador al dar click en el módulo implementación - riesgos, selecciona cada uno de los riesgos marcando la casilla, luego da click en el botón denominado con los seleccionados y selecciona la opción imprimir
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Eliminar o Editar Controles
Actores:	Administradores
Tipo:	Primario
Descripción:	Borra o actualiza un control
Flujo Normal	El administrador al dar click en el módulo implementación y seleccionar controles, selecciona cada uno de los controles en la casilla, da click en el botón más y selecciona la opción editar o eliminar.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Imprimir Controles
Actores:	Administradores
Tipo:	Primario
Descripción:	Imprime los controles seleccionados
Flujo Normal	El administrador al dar click en el módulo implementación - controles, selecciona cada uno de los controles marcando la casilla, luego da click en el botón denominado con los seleccionados y selecciona la opción imprimir
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Asignar riesgos a activos
Actores:	Administradores
Tipo:	Primario
Descripción:	Asigna riesgo a un activo según la evaluación previa realizada por los involucrados

Flujo Normal	Dar click sobre el modulo implementación, seleccionar el activo a tratar, dar click en añadir nuevo, se selecciona el activo cargado previamente, y se agrega el valor a la casilla riesgos.
Precondiciones	EL usuario debe estar autenticado, deben estar precargados activos, riesgos.

Caso de Uso:	Asignar controles a activos
Actores:	Administradores
Tipo:	Primario
Descripción:	Asignar un control que disminuya o contrarreste el riesgo de un activo
Flujo Normal	Dar click sobre el modulo implementación – controles, luego click en añadir nuevo, se seleccionan los campos ya precargados y se asigna el control.
Precondiciones	El usuario debe estar autenticado y deben existir activos y controles precargados en el sistema.

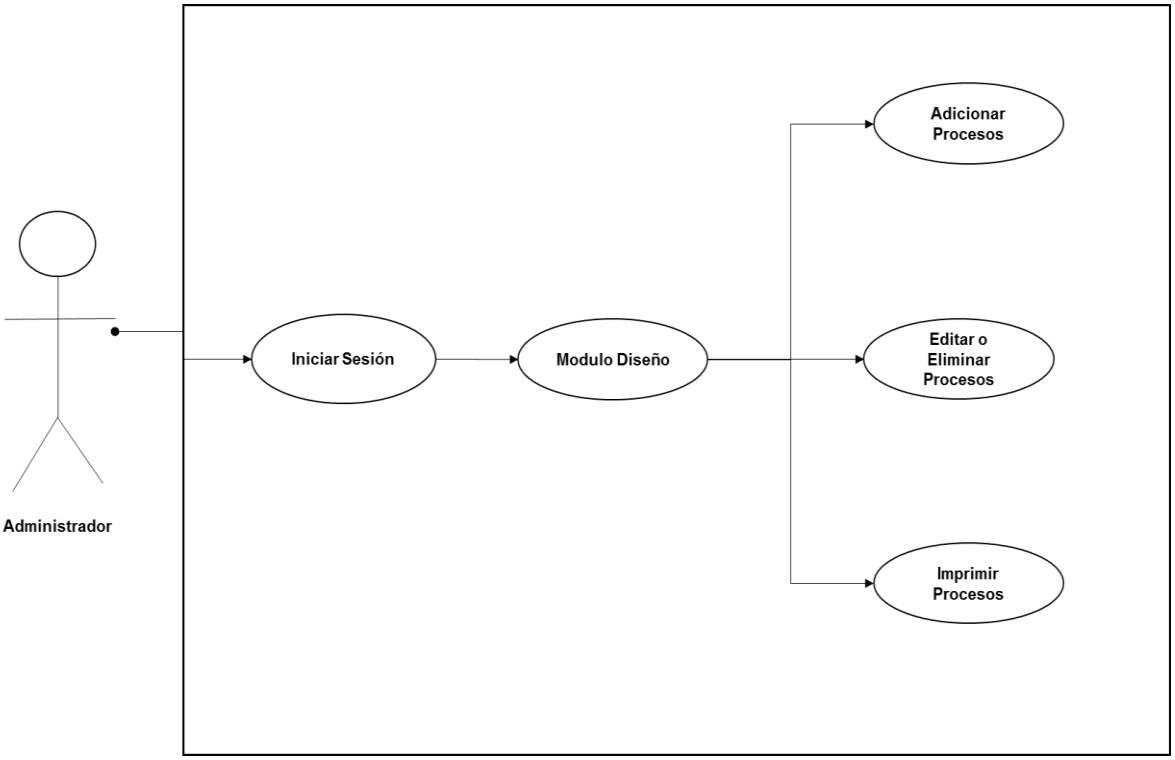
Caso de Uso:	Cargue de documentación
Actores:	Administradores
Tipo:	Primario
Descripción:	Cargar documentación correspondiente a los objetivos de control o controles exigidos
Flujo Normal	Dar click sobre el modulo implementación y en el submenú documentación aparecerá un listado de controles que en la parte final tienen una casilla y un botón examinar. Al dar click en este se puede ir a seleccionar un archivo, luego de seleccionado aparece la opción cargar.
Precondiciones	El usuario debe estar autenticado

Caso de Uso:	Visualizar informes gráficos
Actores:	Administradores – Invitados
Tipo:	Primario
Descripción:	Visualizar
Flujo Normal	Al ingresar a la aplicación se selecciona el modulo informes y en los submenús diseño e implementación podrá seleccionar alguna de los dos y automáticamente se cargarán las gráficas.
Precondiciones	Ninguna

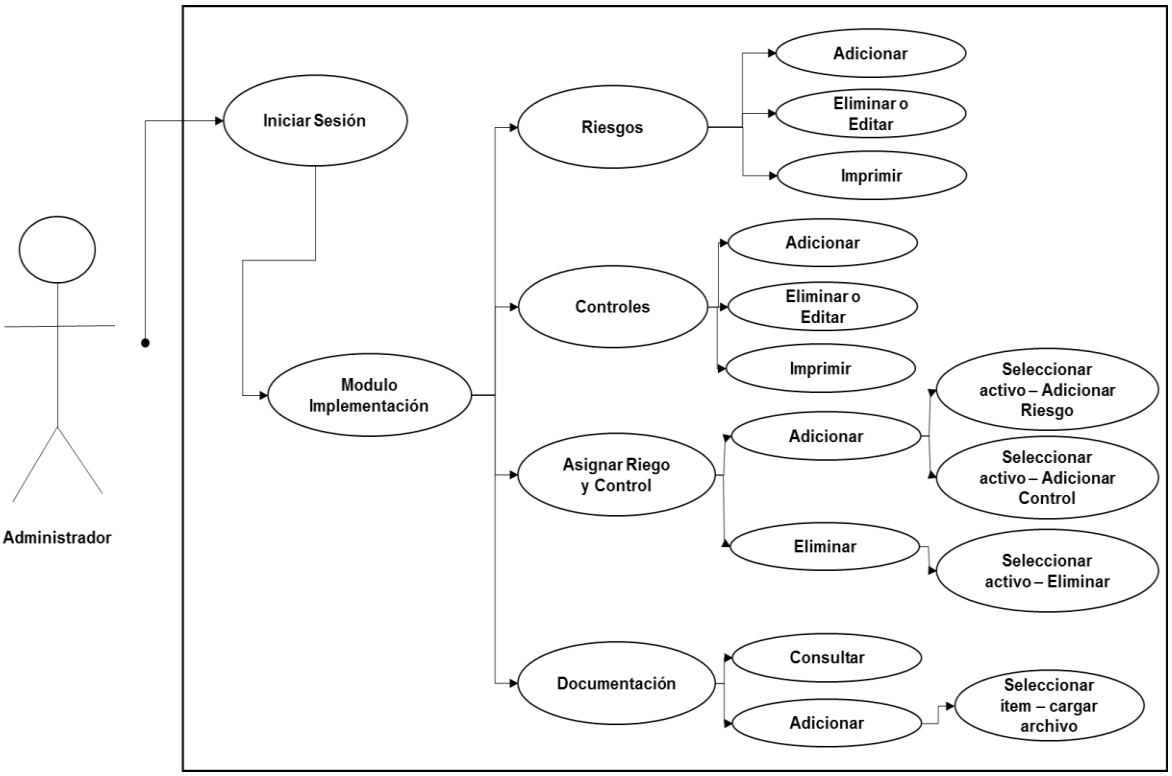
Caso de Uso:	Acceder a la aplicación como invitado
Actores:	Empleados en general no administradores
Tipo:	Primario
Descripción:	Accede a la información pública de la aplicación
Flujo Normal	El usuario ingresará a la URL a través del navegador y selecciona la opción ingresar como invitado.
Precondiciones	Ninguna

4.2.2. DIAGRAMAS CASOS DE USO

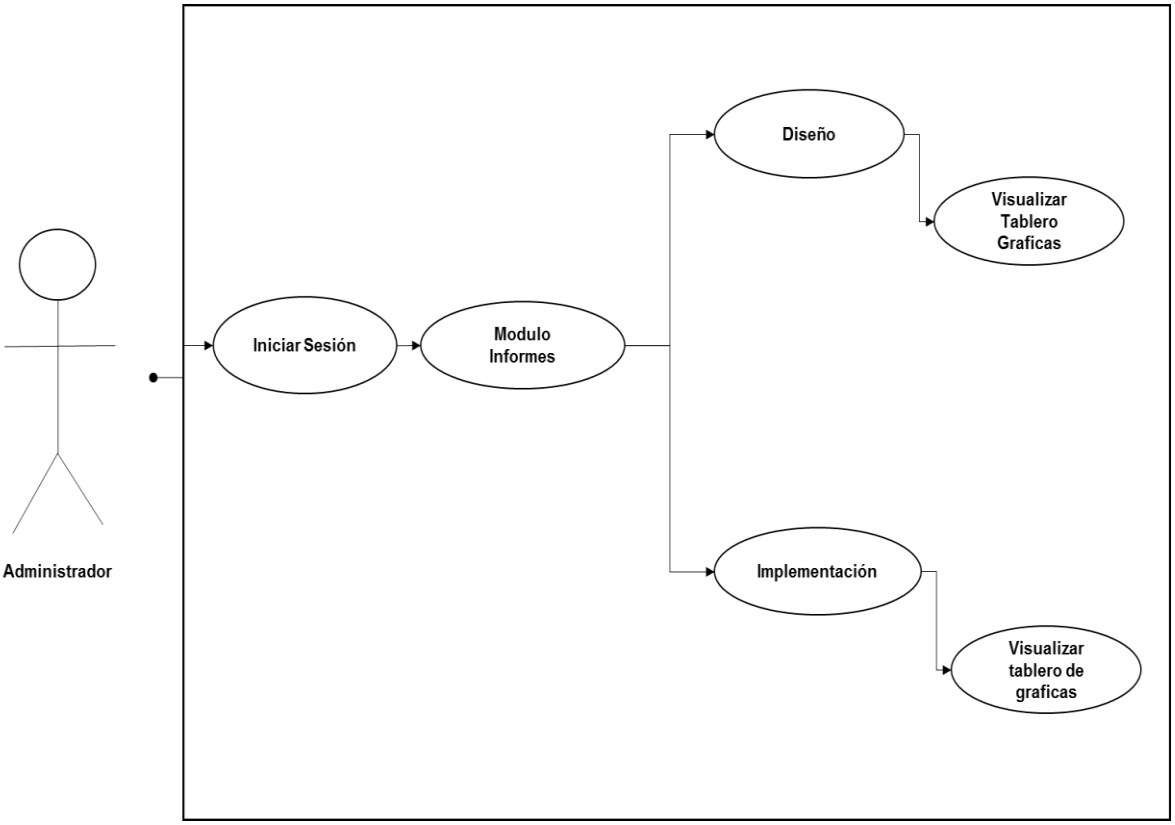
Caso de uso Administrador Modulo Diseño



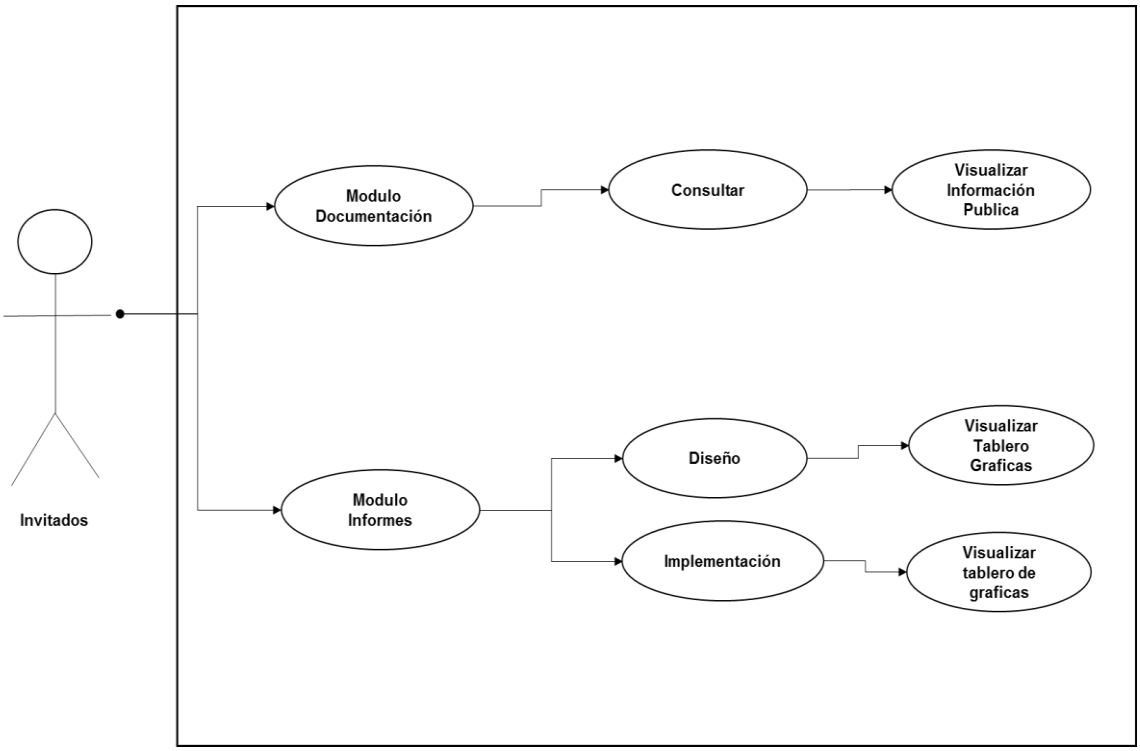
Caso de uso Administrador Modulo Implementación



Caso de uso Administrador Modulo Informes



Caso de uso usuario invitado



4.2.3. PROTOTIPO VISTAS DE LA APLICACIÓN

Autenticación

La ventana principal o de autenticación de la aplicación solicita un usuario y contraseña válidos para registrarse en el sistema. Adicionalmente exige el ingreso de un código captcha.

Ilustración 6 - *Autenticación SASGSI*

Módulo de Diseño

Luego de autenticarnos aparecerán todas las opciones de la aplicación en un menú al costado izquierdo, entre ellas la primera que es el diseño. Allí se podrán listar los procesos y si el usuario se ubica sobre un proceso específico por unos segundos el sistema automáticamente cargará una nueva ventana con los subprocesos.

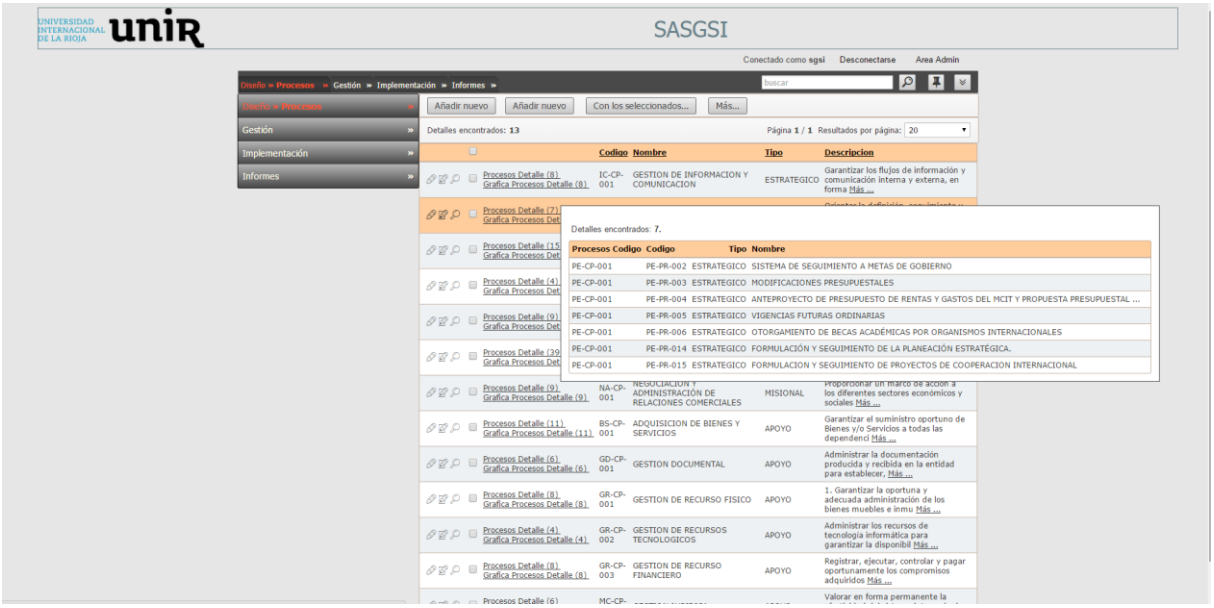


Ilustración 7 *- Listado procesos SASGSI*

Módulo Implementación

En este módulo se podrá acceder a los listados de activos, controles y riesgos. En el caso de los activos se podrán listar en conjunto o discriminados por Aplicaciones, equipos, servidores, funcionarios, etc.

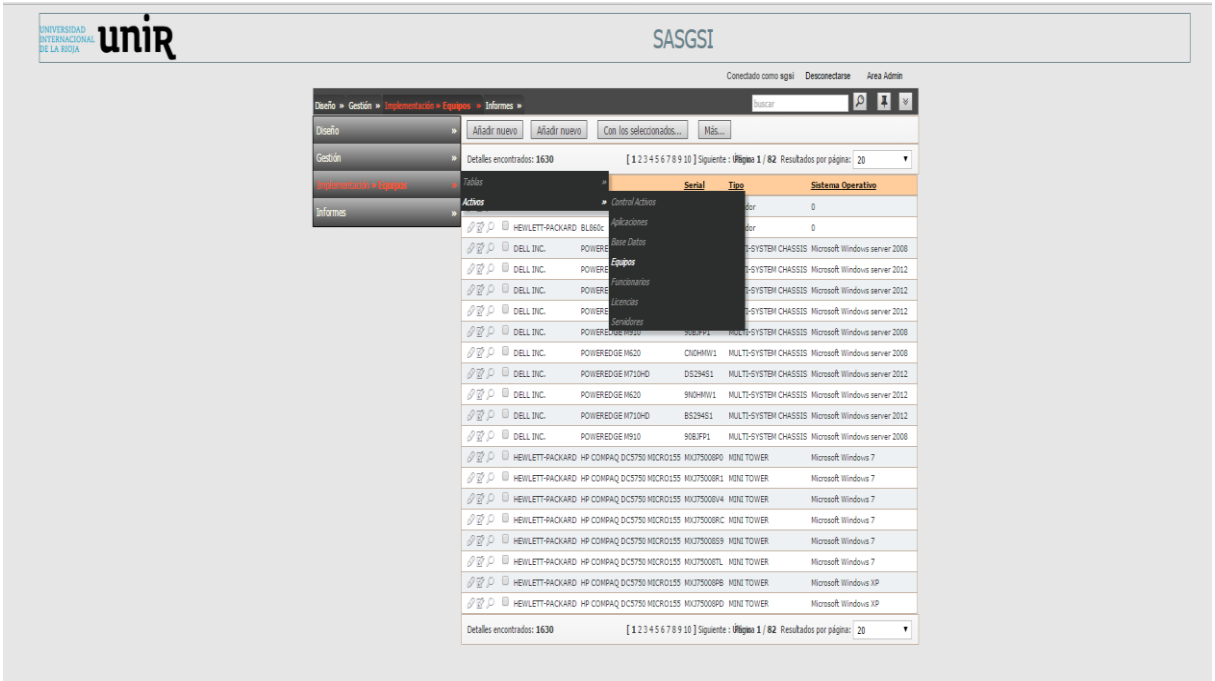


Ilustración 8 *- Listado de equipos SASGSI*

También puede visualizarse la matriz de riesgo donde será posible hacerse una idea de los dispositivos que son más vulnerables y por ende tienen un nivel de riesgo más alto. En esta matriz pueden evidenciarse los riesgos totales calculados con base al nivel de impacto y ocurrencia. Este proceso lo realiza el sistema automáticamente, adicionalmente la matriz automáticamente nos indicará si es necesario tratar el riesgo detectado.

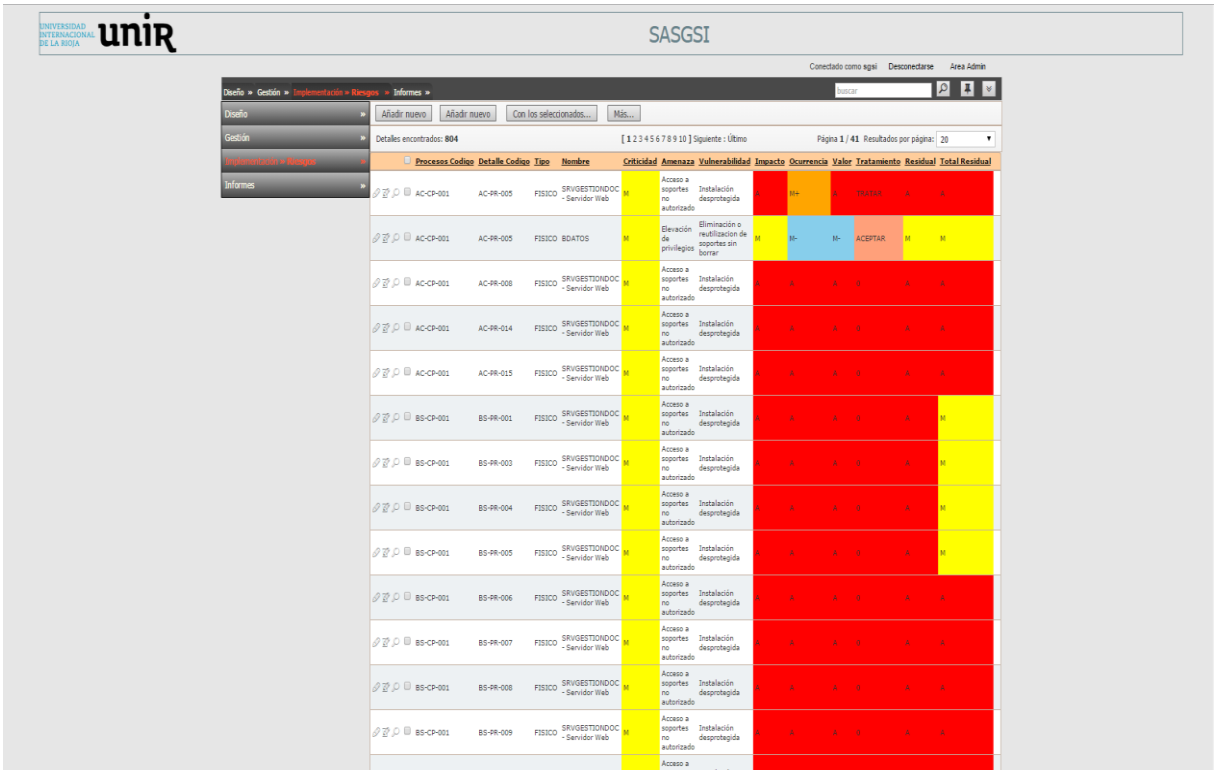


Ilustración 9 *- Matriz de riesgo I SASGSI*

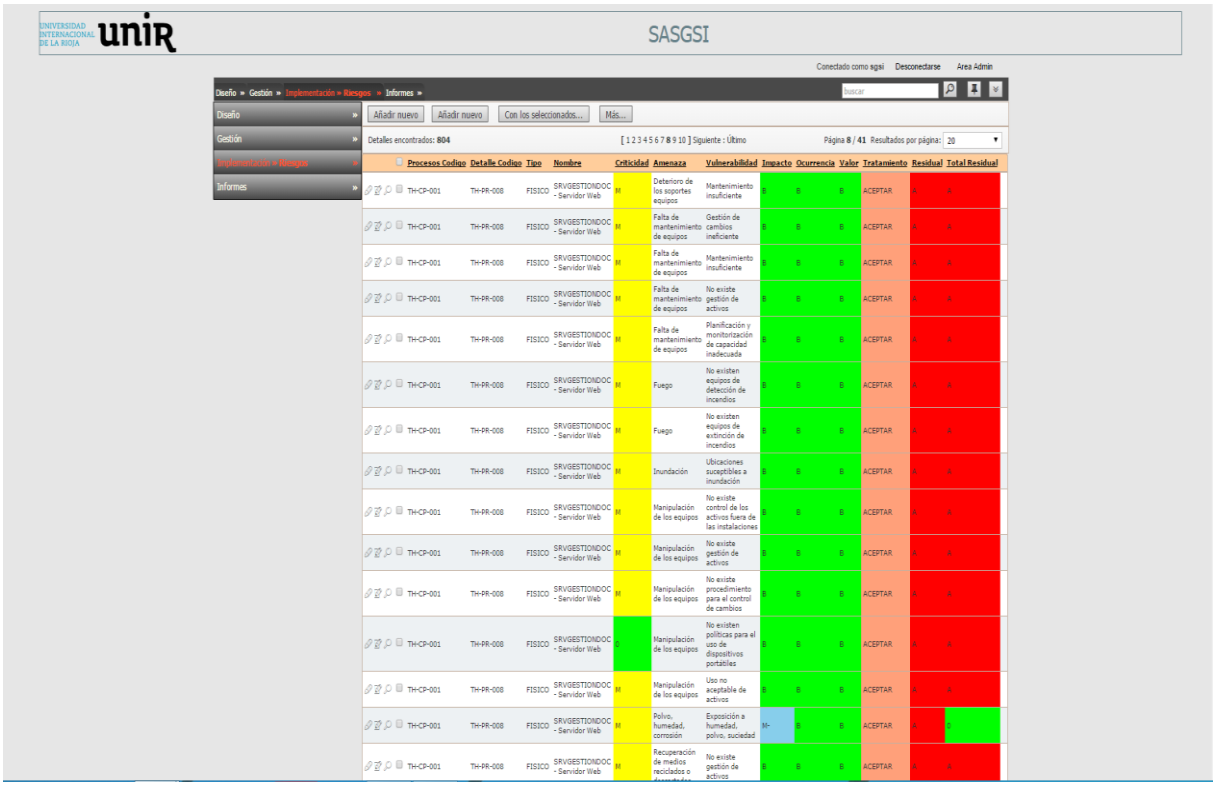


Ilustración 10 *- Matriz de riesgo II SASGSI*

Módulo de Gestión

El módulo de gestión, permitirá al usuario acceder a todas las opciones de gobierno como las reuniones llevadas a cabo, los documentos tratados en las reuniones, las auditorías realizadas y la programación de las reuniones venideras.

Ilustración 11 *- Modulo Reuniones I SASGSI*

Ilustración 12 - *Modulo Reuniones II SASGSI*

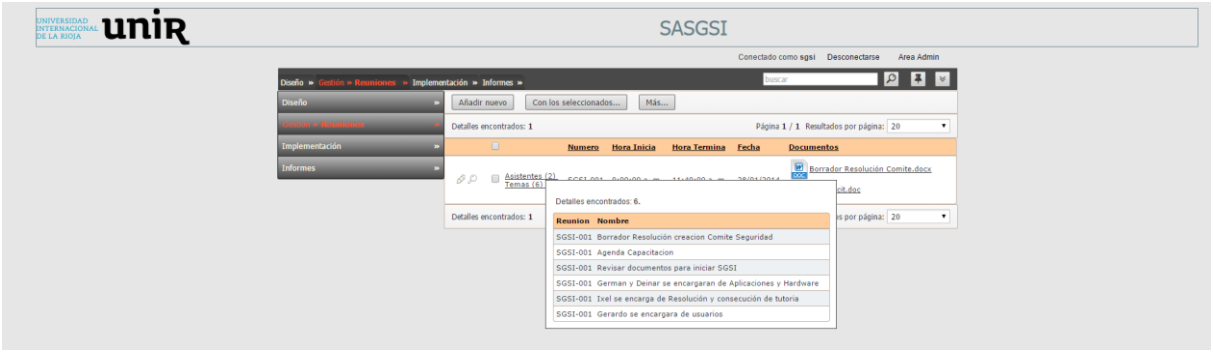


Ilustración 13 *- Modulo reuniones III SASGSI*

Módulo de Informes

En el módulo de informes podrán visualizarse las gráficas con porcentajes por diseño e implementación que indicarán el grado de madurez del SGSI y sus falencias.

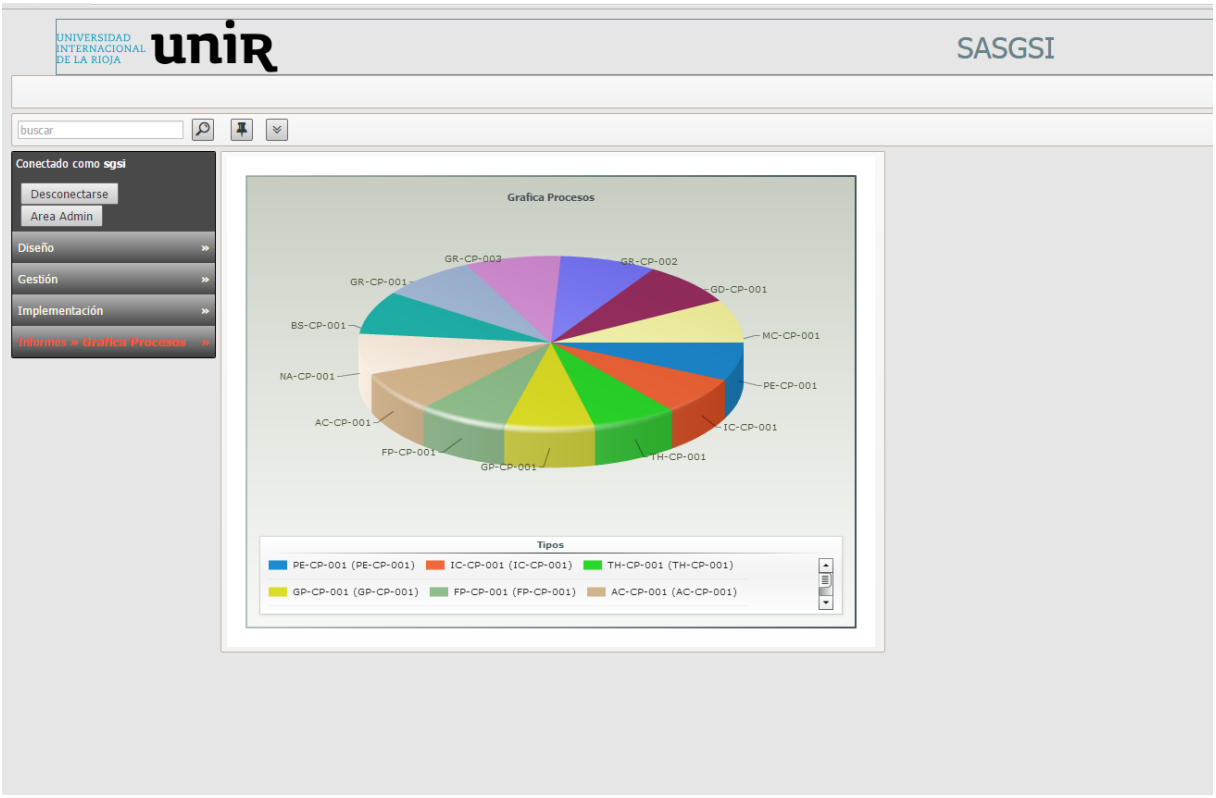


Ilustración 14 *- Modulo de Informes I SASGSI*

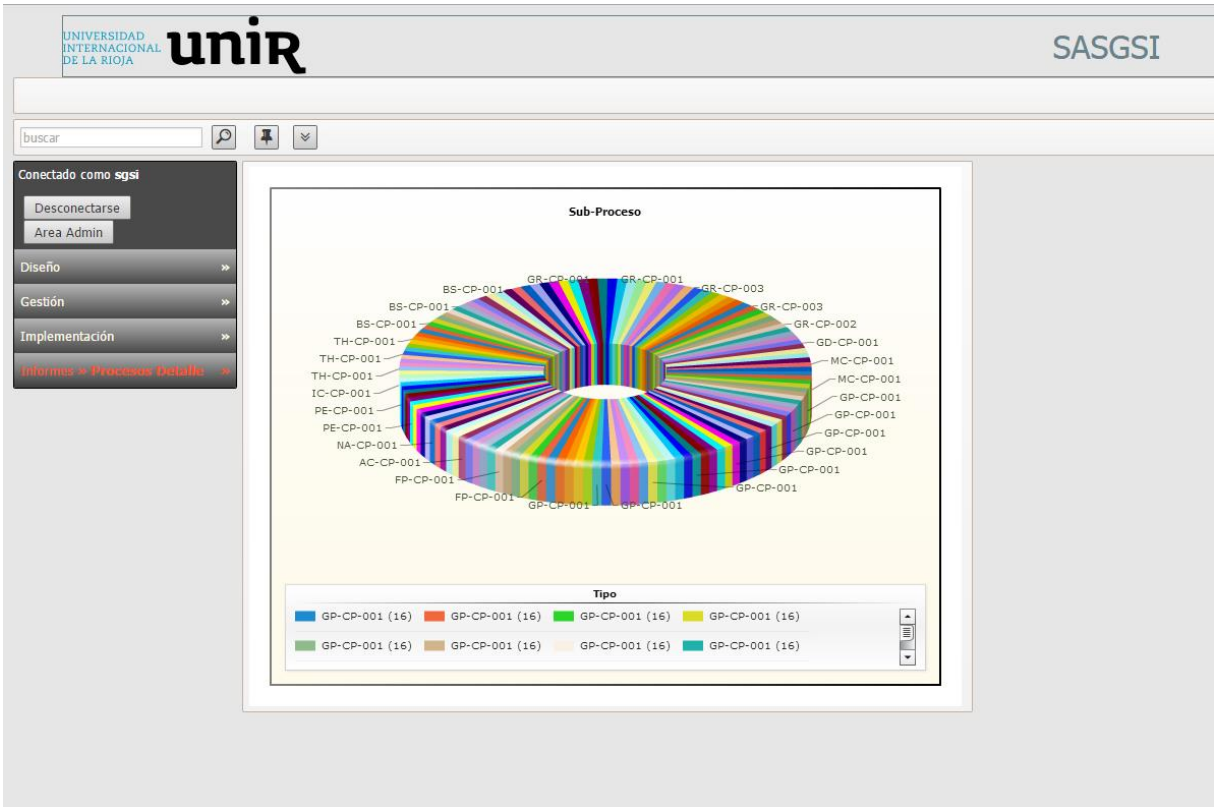


Ilustración 15 *- Modulo Informes II SASGSI*

4.2.4. MODELADO DE DATOS LÓGICO

Tabla aplicaciones

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_aplicaciones	int	11	PK
aplicaciones_codigo	int	11	
aplicaciones_nombre	varchar	100	
aplicaciones_version	varchar	15	
aplicaciones_empresa	int	11	
aplicaciones_contrato_soporte	int	11	
aplicaciones_propietario	int	11	
aplicaciones_area_uso	int	11	
aplicaciones_custodio	int	11	
aplicaciones_tamano_aplicacion	decimal	15	
aplicaciones_sistema_operativo	int	11	

Tabla asistentes

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_asistentes	int	11	PK
asistentes_reunion	varchar	20	
asistentes_nombre	int	11	

Tabla base_datos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_base_datos	int	11	PK
base_datos_nombre	varchar	100	

base_datos_marca	int	11	
base_datos_version	varchar	15	
base_datos_contrato_soporte	int	11	
base_datos_propietario	int	11	
base_datos_area_uso	int	11	
base_datos_custodio	int	11	
base_datos_tamano_aplicacion	decimal	15	
base_datos_sistema_operativo	int	11	

Tabla cargos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_cargo	int	11	PK
cargo_codigo	char	6	
cargo_nombre	char	60	

Tabla controles

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_controles	int	11	PK
controles_nombre	varchar	600	

Tabla dependencias

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_dependencia	int	11	PK
dependencia_codigo	int	11	
dependencia_nombre	char	60	

Tabla documentación

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_documentacion	int	11	PK
documentacion_codigo	int	11	
documentacion_nombre	varchar	200	
documentacion_documento	tinytext	0	

Tabla empresas

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_empresas	int	11	PK
empresas_codigo	int	11	
empresas_nombre	varchar	200	

Tabla Equipos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_equipos	int	11	PK
equipos_marca	int	11	
equipos_modelo	varchar	200	
equipos_serial	varchar	100	
equipos_tipo	int	11	
equipos_sistema_operativo	int	11	

Tabla estado

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_estado	int	11	PK

estado_codigo	int	11	
estado_nombre	varchar	100	

Tabla Funcionarios

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_funcionarios	int	4	PK
funcionarios_cedula	varchar	15	
funcionarios_nombre	varchar	100	
funcionarios_dependencia	int	11	
funcionarios_cargo	int	11	
funcionarios_email	varchar	50	

Tabla Impacto

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_impacto	int	11	PK
impacto_codigo	int	5	
impacto_nombre	varchar	30	
impacto_descripcion	varchar	300	
impacto_clase	varchar	5	
impacto_clase_nombre	varchar	20	
impacto_clase_descripcion	varchar	40	
impacto_dependencia	varchar	20	
impacto_dependencia_descripcion	varchar	300	
impacto_sumatoria_descripcion	varchar	600	
impacto_sumatoria_rto	varchar	100	
impacto_sumatoria_severidad	varchar	100	

impacto_sumatoria_rpo	varchar	100	

Tabla iso_2005

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_iso5	int	11	PK
iso5_dominio_codigo	int	11	
iso5_dominio	varchar	100	
iso5_objetivo_codigo	int	11	
iso5_objetivo	varchar	200	
iso5_control_codigo	int	11	
iso5_control	varchar	300	

Tabla iso_2013

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_iso13	int	11	PK
iso13_dominio_codigo	int	11	
iso13_dominio	varchar	100	
iso13_objetivo_codigo	int	11	
iso13_objetivo	varchar	200	
iso13_control_codigo	int	11	
iso13_control	varchar	400	

Tabla iso_medida

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_escala	int	11	PK
escala_y	varchar	5	

escala_b	varchar	5	
escala_mb	varchar	5	
escala_m	varchar	5	
escala_ma	varchar	5	
escala_a	varchar	5	
escala_procentaje	decimal	15	

Tabla Licencias

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_licencias	int	11	PK
licencias_fabricante	int	11	
licencias_producto	varchar	200	
licencias_version	varchar	20	
licencias_cantidad	int	11	
licencias_cd	varchar	10	
licencias_open_license	varchar	200	
licencias_contrato	varchar	30	
licencias_contratista	int	11	
licencias_observaciones	varchar	400	

Tabla matriz_amenazas

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_amenazas	int	11	PK
matriz_amenazas_nombre	varchar	200	

Tabla matriz_auditoria

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_auditoria	int	11	PK
matriz_auditoria_procesos_codigo	varchar	20	
matriz_auditoria_detalle_codigo	varchar	20	
matriz_auditoria_fecha	date	0	
matriz_auditoria_no_conformidad	int	11	
matriz_auditoria_descripcion_conformidad	varchar	600	
matriz_auditoria_accion_correctiva	int	11	
matriz_auditoria_descripcion_correctiva	varchar	600	
matriz_auditoria_preventiva	int	11	
matriz_auditoria_descripcion_preventiva	varchar	600	
matriz_auditoria_estado	int	11	
matriz_auditoria_funcionario	varchar	15	
matriz_auditoria_tratamiento	varchar	600	
matriz_auditoria_cumplimiento	decimal	15	

Tabla matriz_capacitación

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_capacitacion	int	11	PK
capacitacion_procesos_codigo	varchar	20	
capacitacion_detalle_codigo	varchar	20	
capacitacion_tipo	int	11	
capacitacion_fecha	date	0	

capacitacion_meta_mes	int	11	
capacitacion_ejecutadas_mes	int	11	
capacitacion_cumplimiento	decimal	10	
capacitacion_documento	tinytext	0	
capacitacion_contenido	tinytext	0	

Tabla matriz_controles

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_controles	int	11	PK
controles_procesos_codigo	varchar	20	
controles_detalle_codigo	varchar	20	
controles_tipo	int	11	
controles_clase	int	11	
controles_codigo_dominio	int	11	
controles_dominio	varchar	100	
controles_codigo_objetivo	int	11	
controles_objetivo	varchar	200	
controles_codigo_control	int	11	
controles_control	varchar	400	
controles_dependencia	int	11	
controles_funcionario	varchar	15	

Tabla matriz_dda

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_dda	int	11	PK
matriz_dda_procesos_codigo	varchar	20	

matriz_dda_detalle_codigo	varchar	20	
matriz_dda_fecha	date	0	
matriz_dda_control_codigo	int	11	
matriz_dda_control	varchar	400	
matriz_dda_aplicable	int	11	
matriz_dda_motivo	varchar	500	
matriz_dda_objetivo	int	11	
matriz_dda_estado	int	11	
matriz_dda_fisico	int	11	
matriz_dda_fisico_detalle	int	11	
matriz_dda_aplicacion	int	11	
matriz_dda_aplicacion_detalle	int	11	

Tabla matriz_incidentes

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_incidentes	int	11	PK
matriz_incidentes_proceso_codigo	varchar	20	
matriz_incidentes_detalle_codigo	varchar	20	
matriz_incidentes_fecha	date	0	
matriz_incidentes_tipo	int	11	
matriz_incidentes_clase	int	11	
matriz_incidentes_prioridad	int	11	
matriz_incidentes_entregable	int	11	
matriz_incidentes_incidente	varchar	600	
matriz_incidentes_accion	int	11	
matriz_incidentes_resultado	varchar	600	

matriz_incidentes_observaciones	varchar	600	

Tabla de matriz_riesgos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_riesgos	int	11	PK
matriz_riesgos_procesos_codigo	varchar	20	
matriz_riesgos_detalle_codigo	varchar	20	
matriz_riesgos_tipo	int	11	
matriz_riesgos_nombre	varchar	200	
matriz_riesgos_criticidad	int	5	
matriz_riesgos_amenaza	int	11	
matriz_riesgos_vulnerabilidad	int	11	
matriz_riesgos_impacto	int	5	
matriz_riesgos_ocurrencia	int	5	
matriz_riesgos_valor	int	5	
matriz_riesgos_tratamiento	int	11	
matriz_riesgos_residual	int	5	
matriz_riesgos_total_residual	int	5	

Tabla matriz_vulnerabilidades

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_matriz_vulnerabilidades	int	11	PK
matriz_vulnerabilidades_nombre	varchar	200	

Tabla nivel_impacto

Nombre Campo	Tipo de Dato	Tamaño	Llaves

ide_nivel_impacto	int	11	PK
nivel_impacto_descripcion	varchar	600	

Tabla Procesos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos	int	11	PK
procesos_codigo	varchar	20	
procesos_nombre	varchar	100	
procesos_tipo	int	11	
procesos_descripcion	varchar	700	

Tabla procesos_aplicaciones

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos_aplicaciones	int	11	PK
procesos_aplicacioens_procesos_codigo	varchar	20	
procesos_aplicaciones_detalle_codigo	varchar	20	
procesos_aplicaciones_codigo	int	11	
procesos_aplicaciones_version	varchar	15	
procesos_aplicaciones_empresa	int	11	
procesos_aplicaciones_contrato_soporte	int	11	
procesos_aplicaciones_propietario	int	11	
procesos_aplicaciones_area_uso	int	11	
procesos_aplicaciones_custodio	int	11	
procesos_aplicaciones_tamano_aplicacion	decimal	15	
procesos_aplicaciones_sistema_operativo	int	11	

Tabla procesos_continuidad

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_proceso_continuidad	int	11	PK
continuidad_procesos_codigo	varchar	20	
continuidad_detalle_codigo	varchar	20	
continuidad_rto_procedimiento	int	5	
continuidad_recuperacion_procedimiento	varchar	100	
continuidad_rto_aplicacion	int	5	
continuidad_recuperacion_aplicacion	varchar	100	
continuidad_rto_total	int	11	
continuidad_rpo_aplicacion	int	5	
continuidad_prioridad_recuperacion	varchar	100	
continuidad_estrategia_recuperacion	varchar	600	
continuidad_estrategia_procedimiento	varchar	600	
continuidad_rto_prioridad	varchar	30	

Tabla procesos_detalle

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos_detalle	int	11	PK
procesos_detalle_procesos_codigo	varchar	20	
procesos_detalle_codigo	varchar	20	
procesos_detalle_tipo	int	11	
procesos_detalle_nombre	varchar	700	

Tabla procesos_entregables

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos_entregables	int	11	PK
procesos_entregables_procesos_codigo	varchar	20	
procesos_entregables_detalle_codigo	varchar	20	
procesos_entregables_clase	int	11	
procesos_entregables_documento	tinytext	0	

Tabla procesos_hardware

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_hardware	int	11	PK
hardware_procesos_codigo	varchar	20	
hardware_detalle_codigo	varchar	20	
hardware_nombre	int	11	
hardware_sistema_operativo	int	11	
hardware_clase	int	11	
hardware_observaciones	varchar	300	

Tabla procesos impactados

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos_impactados	int	11	PK
procesos_impactados_procesos_codigo	varchar	20	
procesos_impactados_detalle_codigo	varchar	20	
procesos_impactados_proceso	varchar	20	
procesos_impactados_nombre	varchar	700	

procesos_impactados_escala	int	5	
procesos_impactdos_escala_descripcion	varchar	600	

Tabla procesos impacto

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_proceso_impacto	int	11	PK
impacto_procesos_codigo	varchar	20	
impacto_detalle_codigo	varchar	20	
impacto_semana	int	5	
impacto_mes	int	5	
impacto_dia	date	0	
impacto_interrupcion__financiero	int	11	
impacto_interrupcion_comercial	int	11	
impacto_interrupcion_operativo	int	11	
impacto_interrupcion_imagen	int	11	
impacto_interrupcion_legal	int	11	
impacto_interrupcion_proveedor	int	11	
impacto_negocio_operacional	int	5	
impacto_negocio_economico	int	5	

Tabla procesos_negocio

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_proceso_negocios	int	11	PK
procesos_negocios_procesos_codigo	varchar	20	
procesos_negocios_detalle_codigo	varchar	20	
proceso_negocios_procedimiento	int	11	

proceso_negocios_funcion_critica	int	11	
proceso_negocios_impacto	int	11	
proceso_negocios_impacto_escala	varchar	5	
proceso_negocios_escenario	varchar	300	

Tabla procesos_proveedores

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_procesos_proveedores	int	11	PK
procesos_proveedores_procesos_codigo	varchar	20	
procesos_proveedores_detalle_codigo	varchar	20	
procesos_proveedores_empresa	int	11	

Tabla procesos_recursos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_recursos	int	11	PK
recursos_procesos_codigo	varchar	20	
recursos_detalle_codigo	varchar	20	
recursos_dependencia	int	5	
recursos_dependencia_medida	varchar	5	
recursos_dependencia_descripcion	varchar	300	
recursos_nombre_funcionario	int	11	
recursos_cargo_funcionario	int	11	
recursos_funcionario_permisos	int	11	
recursos_funcionario_tipo	int	11	
recursos_nombre_suplente	int	11	
recursos_cargo_suplente	int	11	

recursos_suplente_permisos	int	11	
recursos_suplente_tipo	int	11	
recursos_aprobado_direccion	int	11	
recursos_fecha_aprobacion	date	0	
recursos_tipo_evaluacion	int	11	
recursos_verificacion_evaluacion	int	11	
recursos_fecha_evaluacion	date	0	

Tabla procesos_registros_vitales

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_registros_vitales	int	11	PK
registros_vitales_proceso_codigo	varchar	20	
registros_vitales_detalle_codigo	varchar	20	
registros_vitales_base_datos	int	11	
procesos_registros_vitales_nombre_base_datos	int	11	
procesos_registros_vitales_nombre_tabla	varchar	600	
procesos_registros_vitales_ruta_registros	varchar	400	

Tabla reuniones

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_reuniones	int	11	PK
reuniones_numero	varchar	20	
reuniones_hora_inicia	time	0	
reuniones_hora_termina	time	0	
reuniones_fecha	date	0	
reuniones_documentos	varchar	500	

Tabla riesgos

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_riesgos	int	11	PK
riesgos_codigo	varchar	6	
riesgos_nombre	varchar	30	
riesgos_descripcion	varchar	300	

Tabla servidores

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide-servidores	int	11	PK
servidores_nombre	varchar	150	
servidores_sistema_operativo	int	11	
servidores_ip_publica	varchar	30	
servidores_ip_interna	varchar	30	
servidores_clase	int	11	
servidores_observaciones	varchar	500	

Tabla sgsi_audit

Nombre Campo	Tipo de Dato	Tamaño	Llaves
Id	int	11	PK
Datetime	datetime	0	
Ip	varchar	40	
User	varchar	300	
Table	varchar	300	
Action	varchar	250	

Description	mediumtext	0	

Tabla sgsi_uggroups

Nombre Campo	Tipo de Dato	Tamaño	Llaves
GroupID	int	11	PK
Label	varchar	50	

Tabla sgsi_ugmembers

Nombre Campo	Tipo de Dato	Tamaño	Llaves
UserName	varchar	50	PK
GroupID	int	11	FK

Tabla sgsi_ugrights

Nombre Campo	Tipo de Dato	Tamaño	Llaves
TableName	varchar	50	PK
GroupID	int	11	FK
AccessMask	varchar	10	

Tabla temas

Nombre Campo	Tipo de Dato	Tamaño	Llaves
ide_temas	int	11	PK
temas_reunion	varchar	20	
temas_nombre	varchar	200	

Tabla usuarios

Nombre Campo	Tipo de Dato	Tamaño	Llaves

id_usuario	int	4	PK
nombre_usuario	varchar	50	
usuario_clave	varchar	50	
usuario_mail	varchar	50	
usuario_nombre	varchar	50	
usuario_apellido	varchar	50	
usuario_codigo	int	20	

4.2.5. MODELO FÍSICO

En este modelo se plantea el esquema grafico de las tablas anteriormente descritas a modo de diseño en este podremos identificar visualmente las características de cada uno de los campos. Durante la construcción del diseño físico el cual es necesariamente posterior al modelado lógico se transforman las entidades en tablas, las instancias en filas y los atributos en columnas.

El diseño físico de los datos permite que la identificación de campos claves como por ejemplo las llaves primarias, foráneas o campos con características especiales como por ejemplo los que por su funcionalidad dentro de la aplicación serán autoincreméntales, únicos, nulos, etc. Este orden o claridad en las características de los datos contribuye a que la base de datos optimice su rendimiento y sea más integra evitando la repetición innecesaria de datos.

Dado que el diseño físico se relaciona mucho con el motor de base de datos se seleccionó MySQL Workbrench para la construcción del modelo. MySQL Workbrech es una herramienta grafica para la administración de bases de datos especializada en el motor MySQL, esta es distribuida por el mismo proveedor del motor por ende ofrece muchas funcionalidades de integración, por ejemplo: la construcción de modelos lógicos y físicos capaces de sincronizarse con una base de datos, valiéndose de la capacidad de generar automáticamente scripts en lenguaje SQL a través de un asistente que ejecuta las peticiones realizadas por el usuario desde el tablero de control.

El Modelo o diseño físico de la aplicación SASGSI es el siguiente:

4.2.5.1. Diseño Físico

Diagrama entidad relación (ER) aplicación SASGSI para el modelamiento de datos que representa las interrelaciones y propiedades.

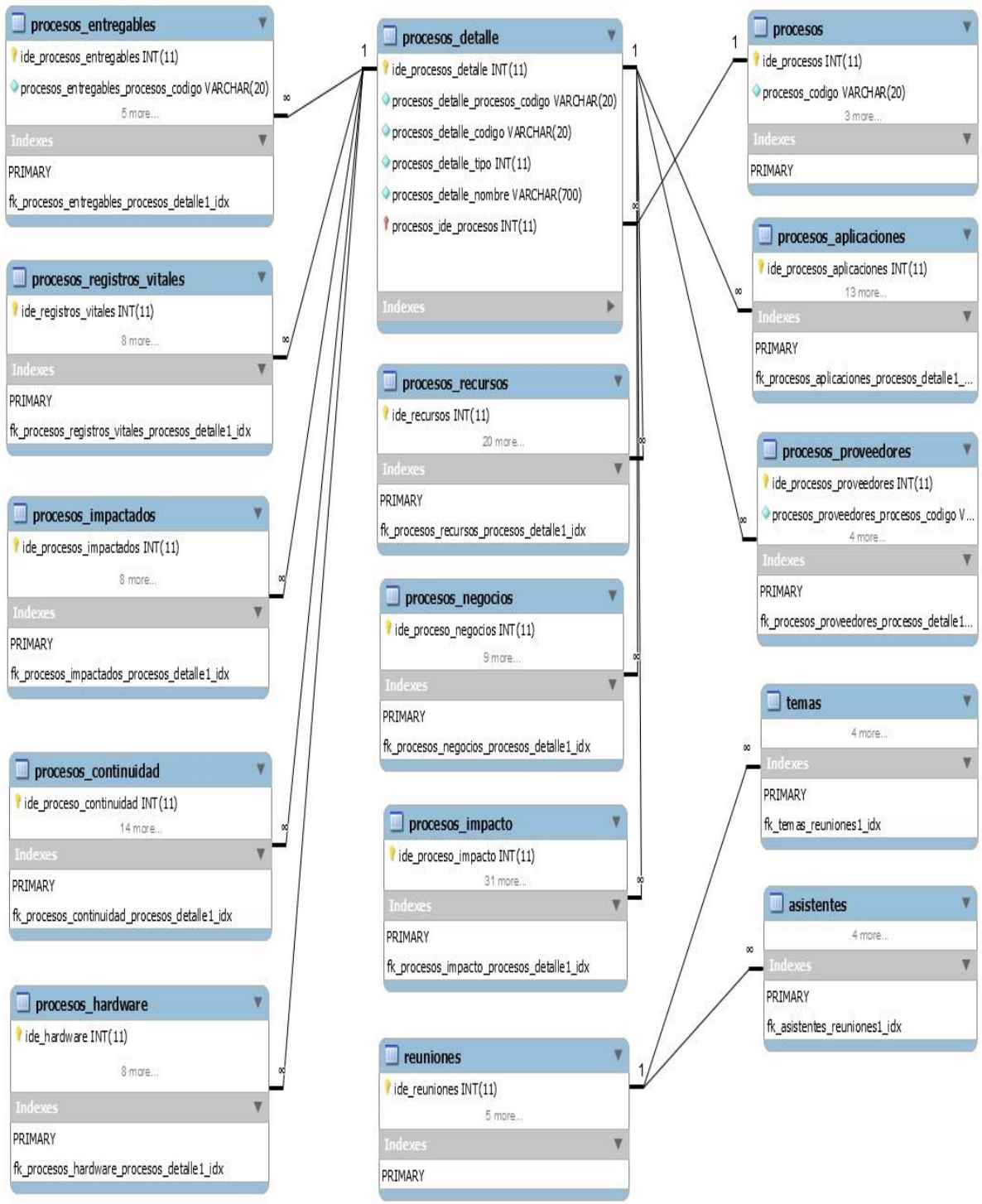


Ilustración 16 - *Modelo ER I SASGSI*

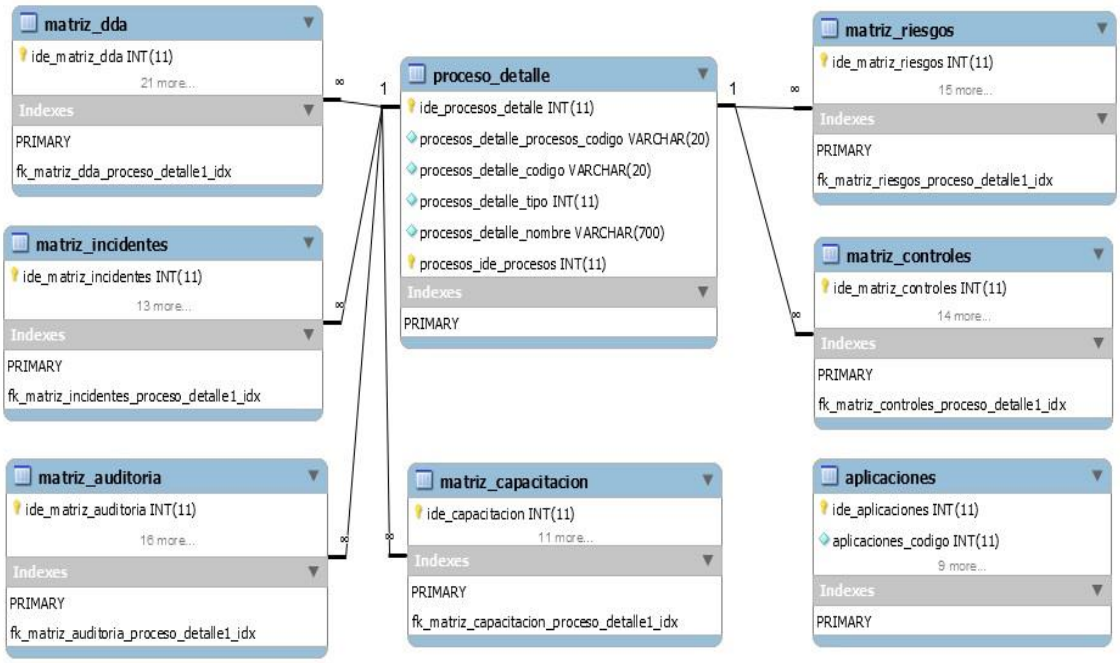


Ilustración 17 *- Modelo ER II SASGSI*

4.3. Evaluación

En esta fase se documentarán los procesos de implementación y pruebas realizados a la herramienta. Se documentarán los tipos de pruebas realizados, los resultados y solución a los hallazgos.

4.3.1. FUNCIONALIDAD

Las pruebas de funcionalidad permiten identificar errores en el procesamiento de datos, por lo que resultan de gran importancia en cualquier proyecto de desarrollo, en este caso SASGSI no contiene mucho procesamiento de información ya que la función principal es la de almacenar y organizar información, sin embargo existen puntos estratégicos dentro de la

aplicación en los que deben validarse los ingresos y resultados. Para esto se documentaron cada una de las pruebas realizadas de la siguiente manera:

Nro.	Prueba	Resultados		Acciones	Responsable
		Test	Esperado		
1	Autenticación de Usuarios	Usuario OK Password NO	SI – Se obtuvo un error de autenticación	Se cambió el mensaje de error para no indicar la causa.	Deinar Pinzon
2	Autenticación de Usuarios	Usuario NO Password OK	SI – Se obtuvo un error de autenticación	Ninguna	Deinar Pinzon
3	Autenticación de Usuarios	Usuario OK Password OK Captcha NO	SI – Se obtuvo un error de autenticación	Ninguna	Deinar Pinzon
4	Autenticación de Usuarios	Usuario OK Password OK Captcha OK	SI – se permitió la autenticación	Ninguna	Deinar Pinzon
5	Carga de archivos	Extensión valida NO	SI – se obtuvo un error de extensión.	Ninguna	Deinar Pinzon
6	Carga de archivos	Extensión Valida SI Tamaño NO	SI – se obtuvo error por el tamaño de archivo	Ninguna	Deinar Pinzon
7	Carga de archivos	Extensión SI Tamaño SI	SI – archivo cargado.	Ninguna	Deinar Pinzon
8	Carga de archivos	Consulta del archivo	SI – el archivo se subió al servidor	Ninguna	Deinar Pinzon
9	Carga masiva de Controles, Activos y Riesgos	Extensión NO	NO – los datos no se cargaron pero la aplicación no informo del error	Crear mensaje de error informativo para el usuario y se agregó a la aplicación para seguimiento	Deinar Pinzon
10	Carga masiva de Controles, Activos y Riesgos	Extensión SI Estructura NO	SI – Aunque la validación se hace por que la aplicación exige la especificación de la estructura	Se implementó un mensaje de error se documentó y añadió para cuando se presente este tipo de casos	Deinar Pinzon
11	Carga masiva de Controles, Activos y Riesgos	Extensión SI Estructura SI	SI – la información fue añadida	Ninguna	Deinar Pinzon

12	Asignación de Controles y Riesgos a activos	Información Valida SI	SI – los dato s fueron asignados	Ninguna	Deinar Pinzon
13	Asignación de Controles y Riesgos a activos	Información Valida NO	NO – se agregó información de un activo no relacionado a un proceso	El único dato que permite ingreso manual en esta opción era el de ID proceso, por lo tanto podía agregarse id o procesos incorrectos, se relacionó el campo proceso con la tabla procesos y se ingresará por lista desplegable para evitar errores de digitación	Deinar Pinzon
14	Asignación de Controles y Riesgos a activos	Información Valida SI	SI – la información se agregó correctamente	Ninguna	Deinar Pinzon
15	Exportar datos	N/A	SI – la información se exporto	Ninguna	Deinar Pinzon
16	Editar Perfil	Nombre NO Apellido Mail	SI – el software solo permite el ingreso de letras en estos campos	Ninguna	Deinar Pinzon
16	Editar Perfil	Nombre SI Apellido NO Mail	SI – el software solo permite el ingreso de letras en estos campos	Ninguna	Deinar Pinzon
17	Editar Perfil	Nombre SI Apellido SI Mail NO	SI – el software exige datos característicos de una dirección de correo	Ninguna	Deinar Pinzon
18	Editar Perfil	Nombre SI Apellido SI Mail SI	Si – los datos se agregaron	Ninguna	Deinar Pinzon
19	Cambio de Contraseña	Contraseña débil SI	SI – la aplicación exige el uso de caracteres, números y letras.	Ninguna	Deinar Pinzon

20	Cambio de contraseña	Contraseña débil NO	SI – la aplicación permitió el cambio y actualizo el campo correctamente	Ninguna	Deinar Pinzon

Tabla 4 *- Resultados pruebas de funcionalidad SASGSI*

4.3.2. DESEMPEÑO

Las pruebas de desempeño permitirán evaluar que tan eficiente es la aplicación para realizar procesos de consulta e inserción de información con respecto al tiempo. El desempeño de una aplicación es determinante ya que es una característica fundamental que influye en la aceptación y funcionalidad de la misma. Se digitalizan soluciones para tener acceso más rápido a la información y optimizar tiempos de respuesta; esto influye directamente con la función de la empresa y su economía.

Para SASGSI las pruebas se realizaron midiendo el tiempo de respuesta de la base de datos al momento de realizar inserciones de datos tanto unitarios como masivos, consultar varios ítems y realizar búsquedas específicas por diferentes ítems. Una parte de la obtención de tiempos de respuesta se realizó con la información que genera directamente el motor de base de datos al responder una consulta, el cual es entregado en el resultado de la misma. Sin embargo, se hizo uso de diferentes herramientas para validar que los tiempos se correspondieran con el uso real de la aplicación. En primera instancia se usó MySQL Workbrench como aplicación de ayuda para obtener los datos al ejecutar la consulta directamente en la base de datos. Ahora bien, teniendo en cuenta que el uso por parte de un usuario real no se hace directamente sobre la base de datos, sino que de por medio está el navegador como intermediario para la presentación de datos se usaron dos herramientas denominadas Iron WASP y Owasp Zap. Aunque estas herramientas se usan para la identificación de vulnerabilidades, también ofrecen información relevante con respecto al desempeño de las aplicaciones ya que documentan el tiempo de respuesta de cada consulta que automáticamente realizan sobre el sitio, es por ello que se han tomado como datos de referencia para la evaluación de desempeño de SASGSI. Tras obtener la información con los mecanismos anteriormente descritos los resultados fueron plasmados en la siguiente tabla:

Nro.	Consulta	Número de registros	Respuesta esperada	Tiempo
1	Consulta de un registro del ítem de activos equipo serial JGZ991GD700139	1	SI	0.023ms
2	Consulta de equipos	1630	SI	0.016ms
3	Ingreso de un riesgo	1	SI	0.22ms
4	Ingreso de un masivo a través de un archivo para cargarse en la tabla funcionarios	453	SI	5.03 Seg
5	Búsqueda de un servidor de nombre srvbdsql	1	SI	0.027ms
6	Búsqueda de todas los activos aplicaciones	45	SI	0.051ms

Tabla 5 *- Tiempos de respuesta SASGSI*

4.3.3. SEGURIDAD Y CONTROL DE ACCESO

La seguridad de una aplicación nueva o en desarrollo es una de los componentes más importantes, especialmente hoy en día que los ataques cibernéticos son tan populares. Además, porque las aplicaciones con vulnerabilidades de seguridad a nivel de codificación resultan muy costosas de parchar o corregir y en ocasiones resulta más económico hacerlas nuevamente. Es por ello que durante todo el proceso de desarrollo de la aplicación se ha tenido estricto cuidado con la codificación y la seguridad de la aplicación y para validar estos aspectos se ha ejecutado la herramienta gratuita de detección de vulnerabilidades **w3af** el resultado completo del procedimiento se adjunta en el anexo 2. Sin embargo luego de una revisión exhaustiva de los hallazgos y una selección y exclusión de falsos positivos se encontraron los siguientes errores y se realizaron las acciones correspondientes relacionadas en la siguiente tabla:

Nro.	Descripción vulnerabilidad	Tipo	Acciones
1	Divulgación de código en el archivo login.php la consulta muestra información de la versión, path y el host	Code Disclousure	Se incluye un archivo de configuración que cargue y deshabilite opciones que permiten la divulgación de la información en apache.
2	Divulgación de rutas al realizar un get responde con un parámetro Refer que indica la ruta o path de ubicación del sitio	pathDisclousure	Se cambia la opción Indexes del directorio del servidor web, y como medida adicional se incluye con un mensaje controlado.
3	La ruta sgsi/login.php permite autocompletar y es el archivo de autenticación de la aplicación	formAutocomplete	Se deshabilitó el autocomplete a través de código HTML para el formulario que contiene las

			casillas de usuario y contraseña en el archivo login.php, esto evita que se traiga datos pre almacenados por el navegador.
4	La información de la cookie enviada dese el path sgsi/login.php muestra información del path y el host	Cookies	Proteger la cookie de sesión, para evitar el secuestro de la misma, evitar el uso de autenticaciones múltiples con la misma cookie de sesión
5	Al tratar de autenticar en la página login.php la cookie enviada lleva información de la autenticación en texto claro.	Cookies	Se cifra el contenido de usuario y contraseña con sha1

Tabla 6 *- Pruebas de Seguridad SASGSI*

4.3.4. GUI

La interfaz gráfica de la aplicación se seleccionó teniendo en cuenta varios aspectos como el tipo de letra, tamaño, colores, ubicación de los botones, menús, etc. Estos se trabajaron bajo el estándar W3C, específicamente la iniciativa WAI (Web Accessibility Initiative), la cual tiene como marco la guía denominada WCAG (Web Content Accessibility Guidelines) 2.0 de la cual se tomaron algunas sugerencias para ofrecer a la aplicación un componente de accesibilidad web. De esta manera no solo se ofrece una solución funcional y eficiente sino también llamativa y agradable visualmente. La explicación técnica de cada una de estas características y la justificación de su selección se describe a continuación.

Colores

Dado que la aplicación contiene muchos registros y la carga de información es alta se seleccionaron colores oscuros para los menús y la letra, pero un fondo claro que facilite la visualización del contenido evitando la carga visual provocada por el brillo de los colores claros. En cuanto a la letra en los menús se seleccionó de color blanco para que resalte sobre el color oscuro de los mismos. En el resto de la aplicación se usan diferentes tonalidades de la escala de grises y un fondo naranja suave para destacar la información seleccionada.

Fuente

La fuente elegida para esta aplicación es Arial y se selecciona este tipo porque además de ser una de las más populares en el ámbito de la informática y en especial en los sistemas operativos Windows también porque es una letra legible que tiene entre cada una de las letras

un espaciado exacto y un peso lo suficientemente alto como para ser leída en una pantalla sin mucho esfuerzo, propósito original para el que fue creada. Adicionalmente porque cumple con las especificaciones en cuanto a legibilidad y espaciado sugeridas por el W3C en la guía WCAG 2.0 en su item 1.4.8 Presentación Visual (W3C, 16 Sept 2014 a).

Tamaño

Como se indicó en la descripción del color, la cantidad de información presentada por la aplicación es alta por lo que se evita al máximo la saturación, pero cuidando que la misma se vea completa guardando la estética, legibilidad y claridad. Por lo tanto después de usar varias opciones se seleccionó un tamaño 12 pixeles que se adapta a la resolución y tamaño de las secciones en las que se cargan los registros. Adicionalmente porque este tamaño se ajusta a los requerimientos de la norma en el ítem mencionado en el ítem fuente.

Menús

Siguiendo con las recomendaciones del estándar W3C a través de la guía WCAG los ítems 2.4.5, 2.4.8 y 2.4.2 agrupados bajo el titulo Navegación y Localización en los que se indica que los enlaces, opciones de funcionalidad o servicios de un sitio web deben agruparse de acuerdo a su naturaleza, importancia o criterio de relación de acuerdo a la temática del mismo. Adicionalmente la guía sugiere que esta agrupación se realice de tal manera que el texto principal o título del grupo no solo esté relacionado sino que además se destaque o diferencie, es por ello que en las aplicaciones web habitualmente existen menús agrupados es decir que se componen de submenús (W3C, 16 Sept 2014 b). SASGSI posee un menú que agrupa todas las funcionalidades de la aplicación, para la construcción de este se han usado cuatro secciones o grupos principales los cuales hacen referencia a cada uno de los módulos de la aplicación, como submenú de estos se han puesto todas las funcionalidades asociadas al módulo principal; esto permitirá al usuario mayor usabilidad y accesibilidad. Adicionalmente dado que la aplicación se ha desarrollado para un país de occidente donde la lectura se realiza de izquierda a derecha se ha decidido ubicar el menú al costado izquierdo del navegador para ofrecer una mejor ubicación visual al usuario.

Botones

Los botones han sido ubicados en la parte superior de la aplicación para que siempre estén disponibles para ser usados independientemente del registro que se esté revisando. Adicionalmente se les ha agregado la funcionalidad para que se autoajusten a tamaño del texto que describe su funcionalidad y se ha aplicado un color gris claro para seguir la línea de colores de la plantilla y para destacarlo y hacerlo visible.

4.3.5. USABILIDAD

Las pruebas de usabilidad son importantes en el desarrollo de software ya que permiten garantizar que el software es de fácil uso, e intuitivo, lo que conlleva directamente a la rápida aceptación del mismo. Además en la mayoría de los casos también optimiza la productividad de los administradores u operarios ya que les permite realizar tareas de forma eficiente mucho más fácil, evitando la inclusión de pasos repetitivos o de la ejecución de muchos clicks para llevar a cabo un proceso.

La aplicación SASGSI está diseñada siguiendo parámetros de uso básicos como por ejemplo el uso de menús para acceder a las funciones claves de la aplicación, uso de palabras estándar para describir las funcionalidades, etc. La validación de esta estrategia se puso a consideración de usuarios externos al proceso de codificación y diseño de la misma mediante una evaluación realizada y documentada (Anexo 3) por parte de los funcionarios del Ministerio quienes interactuaron con la herramienta sin ningún tipo de ayuda más que la experticia del uso de aplicaciones del diario empresarial como soluciones ofimáticas o populares herramientas web y se obtuvo aceptación del producto en diferentes aspectos relacionados con la usabilidad según la encuesta posteriormente realizada así:

Test	Aspecto a Evaluar	Ponderación
1	Autenticación de usuario – Ingreso a la aplicación	100 %
2	Búsqueda de información	70 %
3	Ingreso de un archivo	90 %
4	Consulta de un proceso	90 %
5	Consulta de un control	90 %
6	Asignación de riesgo a un activo	70 %
7	Exportación de archivos	100 %
8	Consulta de un activo	90 %
9	Consulta de reuniones	100 %
10	Cambios en la información de la cuenta de usuario	80 %
11	Visualización de informes gráficos	100 %

Tabla 7 *- Resultados Usabilidad SASGSI*

4.3.6. PRUEBAS DE INSTALACIÓN

La instalación de la aplicación SASGSI es muy sencilla por ser una aplicación web; basta con copiar el sitio en la carpeta asignada para este proceso en el servidor web y crear la base de datos en el servidor mysql. Seguido a esto se establece la comunicación entre la aplicación y la base de datos. Este es, quizás, el paso más complejo: hay que ingresar al archivo MySQLConnection.php que se ubica en el directorio Connections y realizar los respectivos cambios en los valores de las siguientes variables:

```
$data["connId"] = "IP o Host del servidor Base de Datos";

$data["connName"] = "Nombre de la Base de Datos";

$data["ODBCUID"] = "Usuario con permisos sobre la Base de Datos";

$data["ODBCPWD"] = "Password del Usuario";
```

Con estas configuraciones el sitio funciona correctamente, sin embargo para facilitar esta fase especialmente a personas que no tienen conocimiento técnico de Informatica se creó un archivo descomprimible automático que solicita una ruta para alojar el directorio con el sitio. También se construyó un archivo con extensión .sql que se ejecuta en el servidor mysql y automáticamente crea la base de datos con la estructura y datos requeridos y finalmente se creó un pequeño archivo ejecutable que permite modificar los datos del archivo de cadena de conexión de forma automática.

Haciendo uso de estas herramientas e instalaciones manuales en el caso de los servidores Linux, se realizaron pruebas de instalación en 4 ambientes distintos. En primer lugar se usó un servidor Windows 2008 con la base de datos localmente, en el segundo un servidor Windows con la base de datos remota, en el tercero un servidor Linux con la base de datos local, y por ultimo un Linux con la base de datos remota validando así el proceso de instalación de la aplicación. Los resultados obtenidos para estas pruebas fueron los siguientes:

Ambiente	**Versiones**	**Resultado**
Servidor Windows con base de datos local	Windows Server 2008 IIS 7.5 Mysql 5.5	La instalación se ejecutó haciendo uso de las herramientas de instalación creadas y el sitio se publicó sin ningún error.
Servidor Windows con conexión a base de datos remota (servidor Linux Debian con Mysql)	**Servidor Aplicación** Windows Server 2008 IIS 7.5 **Servidor Base de Datos** Linux Debian Jessy Mysql 5.6	La instalación se realizó haciendo uso de las herramientas de instalación y el sitio se publicó, sin embargo en la configuración del servidor Linux fue necesario habilitar la aceptación de conexiones remotas para el servicio de mysql.

Servidor Linux con conexión a la base de datos local	Linux Debian Jessy Apache 2.4 Mysql 5.6	Aunque en este ambiente el ejecutable de descompresión no funciona, si lo hace el archivo sql que crea la base de datos y la estructura, por lo tanto el sitio se copió manualmente en el directorio web y se editó el archivo de conexión a la base de datos. La instalación fue satisfactoria, el sitio se publicó.
Servidor Linux con conexión a la base de datos remota	**Servidor Aplicación** Linux Debian Jessy Apache 2.4 **Servidor Base de Datos** Windows Server 2008 Mysql 5.5	La instalación se realizó al igual que en el caso anterior usando el archivo .sql pero descomprimiendo manualmente el sitio en el directorio web. La instalación fue satisfactoria, el sitio se publico

Tabla 8 *- Pruebas Instalación SASGSI*

4.3.7. IMPLEMENTACIÓN

La fase de implementación de un desarrollo es quizás una de las más exigentes, ya que es realmente en la que se hace un uso real de la aplicación teniendo que soportar la carga de usuarios y datos exigida o requerida para el funcionamiento. Es en este paso en el que realmente se ponen a prueba todas las codificaciones y funcionalidades implementadas y obviamente en la que surgen las inconsistencias o errores, es por ello que se han diseñado varias metodologías para realizar las implementaciones dependiendo del ambiente, algunas de ellas son: implementaciones en paralelo, cambio directo, espera en caliente, pruebas piloto.

La aplicación SASGSI fue autorizada para ser implementada en el Ministerio de Comercio, Industria y Turismo (MinCit) entidad de gobierno Colombiana quien la usa como un piloto para la administración del SGSI que en están en proyecto de implementar, sin embargo con acompañamiento de una consultoría contratada en 2014 por una entidad de gobierno llamada el Ministerio de las Tecnologías de información se realizaron las fases de diseño e implementación en uno de los procesos de la entidad denominado el sistema de viáticos y comisiones (SISCO). Toda la documentación obtenida en este proceso y los formatos creados y que estaban en poder de la oficina de sistemas del MinCit fue almacenada en el sistema SASGSI como plan de pruebas, donde pudo evidenciarse que la aplicación funciona de acuerdo a las necesidades ofreciendo una solución a la administración y centralización. En la

actualidad la herramienta ha adquirido un mayor valor funcional ya que está sirviendo para obtener información insumo de otro proyecto que implementará arquitectura empresarial en las entidades públicas bajo los parámetros del decreto 2573 de la legislación Colombiana.

Actualmente SASGSI está instalada en la infraestructura del Ministerio bajo un esquema de dos capas: aplicación y base de datos, las dos funcionando sobre plataformas Linux con las siguientes características:

Componente	Versión
Sistema Operativo:	Linux Red Hat 7.0
Mysql:	Mysql 5.5
Servidor Web:	Apache 2.4
PHP:	Php 5.4

Tabla 9 *- Características instalación actual - SASGSI*

5. Conclusiones y trabajo futuro

5.1. Futuras líneas de Investigación

El desarrollo de la aplicación SASGSI trajo consigo además, de una solución a una necesidad, un alto conocimiento del medio de la seguridad de la información en las empresas y las necesidades que hay en cada una de ellas. Hablando específicamente de Colombia lugar en donde se desarrolló esta tesis, actualmente hay una necesidad latente en el campo de la seguridad informática. Algunos de los elementos necesarios son la implementación de sistemas de gestión de seguridad de la información, la contratación de servicios de acompañamiento y consultoría que apoye los procesos de diseño e implementación de los mismos, la adquisición de herramientas que ayuden en la administración de los SGSI, herramientas que hagan pruebas de seguridad, herramientas de Informática forense, correlación de eventos monitoreo, etc. Y todo esto ha venido fortaleciéndose ya que por regulación nacional todas las entidades públicas deben cumplir con la normativa que exige la implementación de sistemas de gestión, procesos y procedimientos de seguridad definidos.

Con base en lo anterior se considera que la futura línea de investigación es darle continuidad al proyecto implementando más funcionalidades a la aplicación, robusteciéndola y permitiendo que ofrezca muchos más servicios a las entidades u organizaciones que la implementen. Una de estas es la implementación de módulos de administración para los ítems de la arquitectura empresarial normada bajo el decreto 2573 de 2014 del Ministerio de las Tecnologías de la Información del Gobierno Colombiano en el que se exige a todas las entidades públicas iniciar un proceso de diseño e implementación gradual y calificable anualmente desde 2015 a 2020 y que exige cumplimiento en 3 componentes adicionales a la seguridad y privacidad de la información que son:

- Tecnologías de la Información y Comunicación para servicios
- Tecnologías de la Información y Comunicación para el gobierno abierto
- Tecnologías de la Información y Comunicación para la gestión

Y para cada uno de estos se han establecido unos parámetros de cumplimiento y se regulan bajo el documento mapa de ruta que puede consultarse en las páginas del Ministerio de Información y Telecomunicaciones.

5.2. Conclusiones

El desarrollo del actual trabajo de fin de master ha sido de aporte no solo por la obtención de la herramienta sino por el conocimiento adquirido en el proceso acerca del entorno de la seguridad de la información en el día a día de las empresas y su importancia. Habitualmente en las áreas de conocimiento el mundo de la teoría y la realidad resultan un poco dispersos, en la seguridad de la información no es una excepción y más por temas económicos que por divergencias en los estándares o normas. Y es que aún resulta complicado que personas no técnicas ajenas al mundo de la información digital entiendan la importancia de implementar mecanismos de protección sobre la información y más aún que estos le van a costar una inversión que supuestamente no se traduce en ningún beneficio económico para la compañía. Sin embargo mediante el desarrollo de aplicaciones e investigaciones que sigan demostrando la importancia y grandes beneficios de la seguridad informática, este panorama empezará a cambiar y más aun con el fuerte cambio digital que se está presentando a nivel mundial.

La aplicación SASGSI se ha desarrollado como un proyecto de software gratuito que puede ser usado libremente con funcionalidades incorporadas para convertirse en una herramienta fundamental en la gestión de activos, riesgos y controles, y es lo que se ha visto en la experiencia de implementación piloto realizada en el MinCit en donde aún se tiene trabajando como herramienta de gestión y sobre el cual se están realizando proyectos de implementación de seguridad sobre los demás procesos de la entidad y en donde el funcionamiento del mismo ha sido satisfactorio.

5.3. Referencias

- Grupo Banco Mundial. (2015). Usuarios de Internet (por cada 100 personas). Junio, de Banco Mundial Sitio web: http://datos.bancomundial.org/indicador/IT.NET.USER.P2
- ISO org. (2014a). ISO Survey 2013. Junio 2015, de ISO Sitio web: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013
- MinTIC (Ministerio de las Tecnologías de la Información y de la Información y de las Comunicaciones). (2014). Decreto 2573. Junio de 2015, de Presidencia de la República de Colombia Sitio web: http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf
- ISO org. (2014b). Evolution of ISO/IEC 27001 certificates in Spain. Junio 2015, de ISO Sitio web: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=ES#countrypick
- ISO org. (2014c). World distribution of ISO/IEC 27001 certificates in 2013. Septiembre 2014, de ISO org Sitio web: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=AF#standardpick
- GESDATOS Software, S.L. (s.f). ISO 27001 – Sistema de Gestión de la Seguridad de la Información. Junio 2015, de GESDATOS Software, S.L. Sitio web: http://www.gesconsultor.com/iso-27001.html
- Global Suite. (s.f). Hoja de Vida del Producto. Junio 2015, de Global Suite - Solución Integral de Sistemas de Gestion Sitio web: http://www.globalsuite.es/images/Productos/HojasProducto/GlobalSUITE-InformationSecurity.pdf
- RM Studio. (s.f). Why RM Studio?. Junio 2015, de RM Studio Sitio web: http://www.riskmanagementstudio.com/features
- Manage Engine. (s.f). Event Log Analizer. Junio 2015, de Manage Engine Sitio web: https://www.manageengine.com/products/eventlog/
- SoftExpert. (s.f). SoftExpert Excellence Suite. Junio 2015, de SoftExpert Sitio web: http://www.softexpert.es/se-suite.php
- Wikipedia. (s.f a). PHP. Julio 2015, de Wikipedia org Sitio web: https://es.wikipedia.org/wiki/PHP
- Wikipedia. (s.f b). MySQL. Julio 2015, de Wikipedia org Sitio web: https://es.wikipedia.org/wiki/MySQL
- Wikipedia. (s.f c). Base de Datos. Julio 2015, de Wikipedia org Sitio web: https://es.wikipedia.org/wiki/Base_de_datos
- Wikipedia. (s.f. d). Aplicación Informatica. Julio 2015, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica
- Universidad de Granada. (s.f.). Accesibilidad sitio web. Julio 2015, de Biblioteca - Universidad de Granada Sitio web: http://biblioteca.ugr.es/static/Validador
- W3C. (16 Sept 2014 a). Visual Presentation. Agosto 2015, de W3C Org Sitio web: http://www.w3.org/WAI/WCAG20/quickref/#visual-audio-contrast-visual-presentation
- W3C. (16 Sept 2014 b). Headings and Labels. Agosto 2015, de W3C Org Sitio web: http://www.w3.org/WAI/WCAG20/quickref/#navigation-mechanisms-mult-loc

- MinTIC. (14 de julio 2011). Conpes 3701. Junio 2015, de Ministerio de Tecnologías de la Información y las Comunicaciones Sitio web: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

- ISO Org. (s.f.). ISO/IEC 27005:2011(en). Septiembre 2015, de ISO Org Sitio web: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

- Cataldi, Z. (2000). Metodología de Diseño, desarrollo y evaluación de software educativo. Tesis de Maestría no publicada, Universidad de la Plata, Argentina.

- Diez E. (2003). Generador del Mapa de actividades de un proyecto de desarrollo de software. Tesis de Maestría no publicada, Universidad Politécnica de Madrid, Buenos Aires, Argentina.

- David Sklar, Adam Trachtenberg. (Noviembre 2002). PHP Cookbook. EEUU: O'Reilly.

- IEEE. (1983). ANSI/IEEE STD: 829-1983 software test documentation. Agosto 2015, de IEE Org Sitio web: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=263938&newsearch=true&queryText=829

- OWASP. (s.f). TOP 10 OWASP. Agosto 2015, de OWASP Org Sitio web: https://www.owasp.org/index.php/Main_Page

5.4. Anexos

5.4.1. Anexo 1 – Cuestionario Determinación de Requerimientos

Teniendo en cuenta la gran difusión en la implementación de la norma ISO 27001 en Colombia y considerando la latente necesidad de administrar eficazmente la información de un Sistema de Gestion de Seguridad de la Información.

Por favor responda lo siguiente:

SASGSI
¿Considera que tener un software para la administración de un SGSI aporta valor? RTA: Si, siempre y cuando la aplicación tenga un alto nivel de usabilidad de lo contrario puede convertirse en un problema peor para la organización.
¿Qué tipos de archivos son comúnmente usados para gestionar la información de un SGSI? RTA: Hojas de Cálculo • Procesadores de texto • Archivos en formato PDF
¿Ha tenido algún acercamiento con un software de administración de un SGSI? ¿Cuál? RTA: No, sin embargo he usado el aplicativo ISOLUCION para la administración del sistema de calidad.
¿Qué funciones considera usted obligatorias en un software de administración para un SGSI? RTA: La aplicación debe apegarse a las exigencias de la norma para así poder ser un mecanismo de gestión eficaz • Debe proveer seguridad o control de acceso a la información que almacena • Gestionar Activos • Gestionar riesgos • Gestionar Incidentes • Hacer seguimiento a las no conformidades de la auditoria interna y externa. • Gestionar documentación relacionada al sistema • Llevar control de la vinculación y desvinculación de empleados
¿Qué funciones adicionales le gustaría tener en un software de administración de un SGSI? RTA: • Consultable desde dispositivos móviles • Cargue masivo de información

¿Usaría o recomendaría el uso de un software GRATUITO para la administración de un SGSI? RTA: Si, siempre y cuando me asegure la confidencialidad de la información.

Carmen Elena Aguilar Daza

Coordinadora Grupo Calidad

Ministerio de Comercio, Industria y Turismo

CUETIONARIO DETERMINACION DE REQUISITOS

Teniendo en cuenta la gran difusión en la implementación de la norma ISO 27001 en Colombia y considerando la latente necesidad de administrar eficazmente la información de un Sistema de Gestion de Seguridad de la Información.

Por favor responda lo siguiente:

SASGSI
¿Considera que tener un software para la administración de un SGSI aporta valor? RTA: Si, porque sistematiza la información
¿Qué tipos de archivos son comúnmente usados para gestionar la información de un SGSI? RTA: todos los componentes del Office
¿Ha tenido algún acercamiento con un software de administración de un SGSI? ¿Cuál? RTA: NO.
¿Qué funciones considera usted obligatorias en un software de administración para un SGSI? RTA: • Debe permitir accederse remotamente • Ser seguro • Permitir el manejo de roles que limiten el acceso a cierta información • Permitir controlar documentos • Debe permitir la inclusión y comparación de buenas prácticas de aseguramiento de los equipos • Debe permitir registrar las debilidades de seguridad de los equipos • Monitorear el nivel de disponibilidad • Registrar incidentes de seguridad

¿Qué funciones adicionales le gustaría tener en un software de administración de un SGSI? RTA: • Conocer el nivel porcentual de cumplimiento.
¿Usaría o recomendaría el uso de un software GRATUITO para la administración de un SGSI? RTA: No.

Hernán Darío Guevara

Ingeniero de Sistemas

Efecty

CUETIONARIO DETERMINACION DE REQUISITOS

Teniendo en cuenta la gran difusión en la implementación de la norma ISO 27001 en Colombia y considerando la latente necesidad de administrar eficazmente la información de un Sistema de Gestion de Seguridad de la Información.

Por favor responda lo siguiente:

SASGSI
¿Considera que tener un software para la administración de un SGSI aporta valor? RTA: Si.
¿Qué tipos de archivos son comúnmente usados para gestionar la información de un SGSI? RTA: Word, Excel, Access, Mysql.
¿Ha tenido algún acercamiento con un software de administración de un SGSI? ¿Cuál? RTA: NO.
¿Qué funciones considera usted obligatorias en un software de administración para un SGSI? RTA: • Permitir la gestión de documentos, que equivalen a políticas, procedimientos y procesos definidos por la entidad para dar cumplimiento a la norma y que en algunos casos son obligatorios

• Administrar (Ingresar, Editar, Eliminar) elementos del inventario de activos teniendo en cuenta que estos pueden ser personas, equipamiento, información, etc. • Calcular la evaluación de riesgos. • El software debe permitirme enviar alertas o documentos • El software debe permitir (Ingresar, Editar, Eliminar) los documentos que se publican • El software debe ser web • El software debe permitir hacer seguimiento de las no conformidades o hallazgos detectados en auditorias o revisiones previas • Debe proteger el acceso a la información con el uso de password • Debe tener un módulo de administración de usuarios o perfiles • El software debería permitirme consultar la hoja de vida de los equipo • Debe permitir el ingreso y modificación de los criterios definidos para la evaluación
¿Qué funciones adicionales le gustaría tener en un software de administración de un SGSI? RTA: • El software debería permitirme la generación de reportes en línea.
¿Usaría o recomendaría el uso de un software GRATUITO para la administración de un SGSI? RTA: Si, lo recomendaría y usaría

Juan Daniel Valero Duran

Ingeniero de Sistemas – Auditor Interno ISO 27001

Ministerio de Comercio, Industria y Turismo

CUETIONARIO DETERMINACION DE REQUISITOS

Teniendo en cuenta la gran difusión en la implementación de la norma ISO 27001 en Colombia y considerando la latente necesidad de administrar eficazmente la información de un Sistema de Gestión de Seguridad de la Información.

Por favor responda lo siguiente:

SASGSI
¿Considera que tener un software para la administración de un SGSI aporta valor? RTA: Si,
¿Qué tipos de archivos son comúnmente usados para gestionar la información de un SGSI?

RTA: Word, Excel.
¿Ha tenido algún acercamiento con un software de administración de un SGSI? ¿Cuál? RTA: Si, VERINICE
¿Qué funciones considera usted obligatorias en un software de administración para un SGSI? RTA: • Importación, Exportación de archivos • Evaluación de riesgos • Permitir accederse remotamente tener la disponibilidad de la información • Tener control de acceso por perfiles • Notificaciones vía email • Ser multiusuario • Multiplataforma • Tener un Administrador de documentos centralizado • Tener acceso seguro
¿Qué funciones adicionales le gustaría tener en un software de administración de un SGSI? RTA: • Permita la generación de informes • Enviar formatos por correo • Haga seguimiento de las consultas de los empleados.
¿Usaría o recomendaría el uso de un software GRATUITO para la administración de un SGSI? RTA: Si.

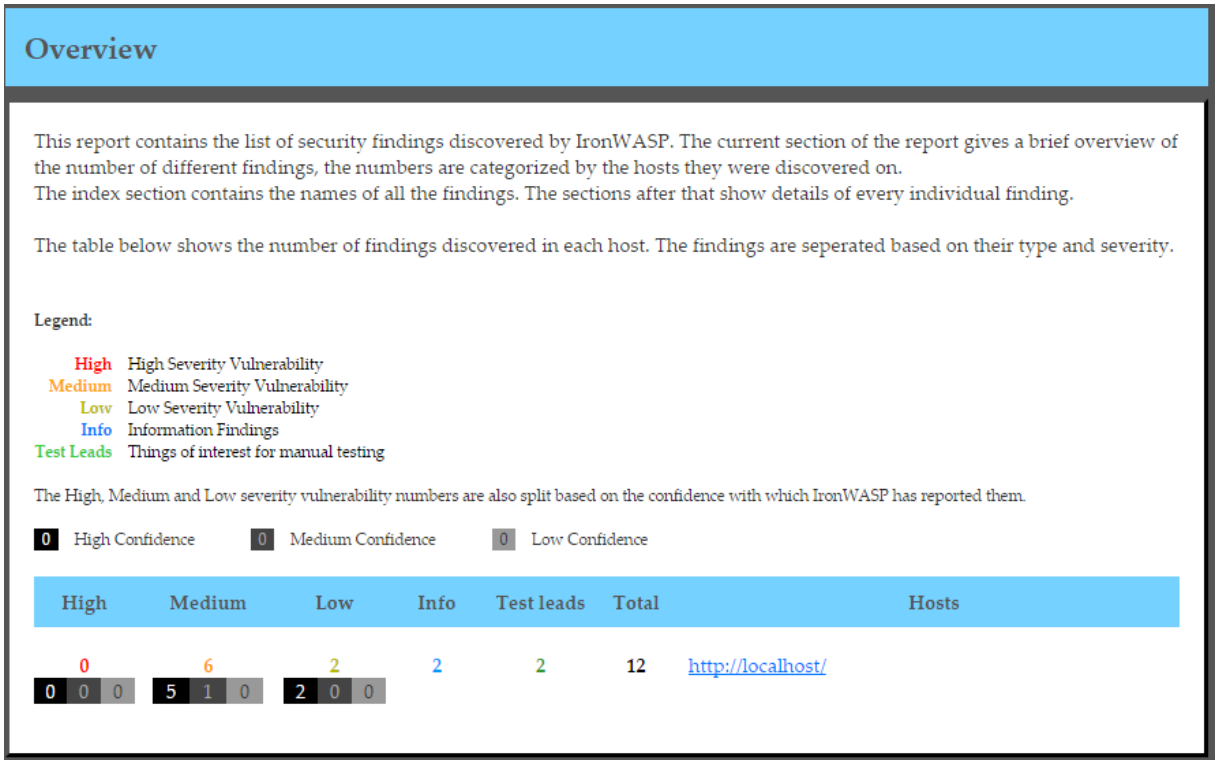
German Augusto Perez

Asesor TI Seguridad

Ministerio de Comercio Industria y Turismo

5.4.2. Anexo 2 – Pruebas de seguridad

Sumario de informe total de detecciones reportado por la herramienta IronWASP.



Overview

This report contains the list of security findings discovered by IronWASP. The current section of the report gives a brief overview of the number of different findings, the numbers are categorized by the hosts they were discovered on.
The index section contains the names of all the findings. The sections after that show details of every individual finding.

The table below shows the number of findings discovered in each host. The findings are seperated based on their type and severity.

Legend:

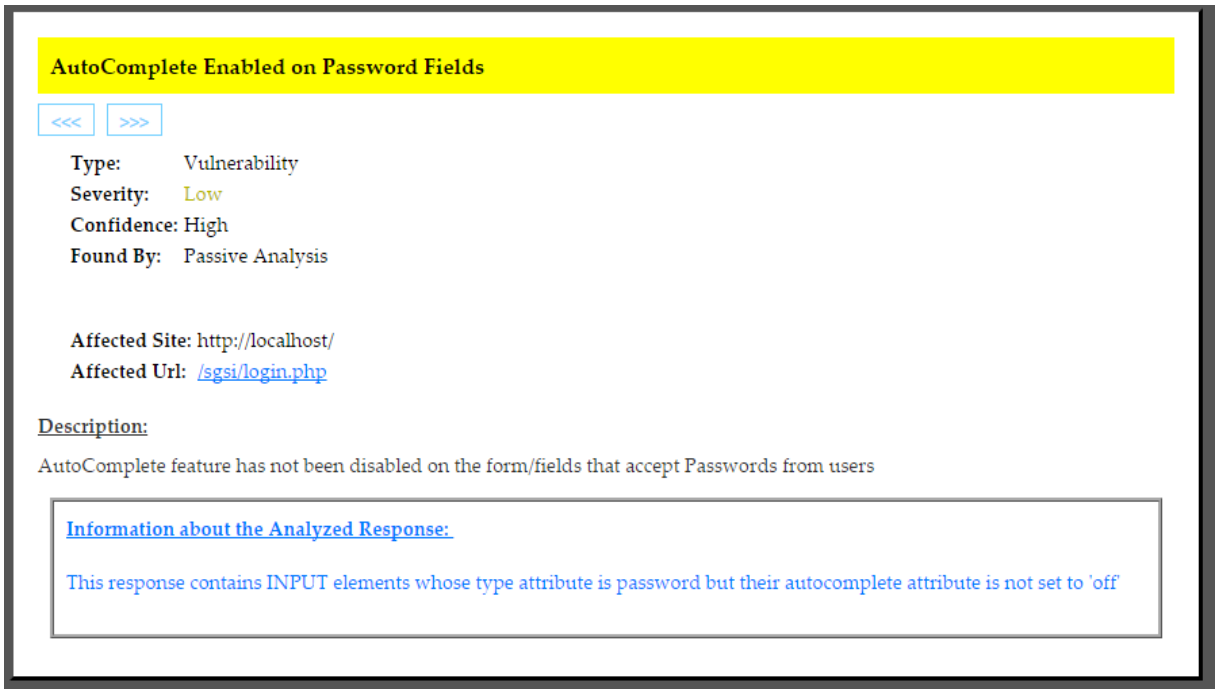
High	High Severity Vulnerability
Medium	Medium Severity Vulnerability
Low	Low Severity Vulnerability
Info	Information Findings
Test Leads	Things of interest for manual testing

The High, Medium and Low severity vulnerability numbers are also split based on the confidence with which IronWASP has reported them.

0 High Confidence 0 Medium Confidence 0 Low Confidence

High	Medium	Low	Info	Test leads	Total	Hosts
0 0 0 0	6 5 1 0	2 2 0 0	2	2	12	http://localhost/

Detección de opción de autocompletar



AutoComplete Enabled on Password Fields

<<< >>>

Type: Vulnerability
Severity: Low
Confidence: High
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/login.php

Description:

AutoComplete feature has not been disabled on the form/fields that accept Passwords from users

Information about the Analyzed Response:

This response contains INPUT elements whose type attribute is password but their autocomplete attribute is not set to 'off'

Detecciones sobre el archivo Index de la aplicación

Index

The titles of all the findings are listed below categorized by the host they were discovered on. All items in the list below are links to relevant sections in the report.

http://localhost/

- Cookie s1434645778 missing the HttpOnly flag
  1. /sgsi/menu.php
- Sensitive Form loaded and submitted Insecurely
  1. /sgsi/login.php
  2. /sgsi/login.php
- Cookie username missing the HttpOnly flag
  1. /sgsi/login.php
- Cookie password missing the HttpOnly flag
  1. /sgsi/login.php
- Charset Not Set By Server
  1. /sgsi/
- Server leaks version number
  1. /sgsi/menu.php
- AutoComplete Enabled on Password Fields
  1. /sgsi/login.php
- Runs on Apache/2.4.9 (Win64) PHP/5.5.12
  1. /sgsi/menu.php
- Technologies identified on Server
  1. /sgsi/menu.php
- Cookie username may contain sensitive information
  1. /sgsi/login.php
- Cookie password may contain sensitive information
  1. /sgsi/login.php

Cookies

Cookie s1434645778 missing the HttpOnly flag

>>>

Type: Vulnerability
Severity: Medium
Confidence: High
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/menu.php

Description:

The HttpOnly flag was missing on the cookie: s1434645778. This may allow an attacker to get the cookie information using XSS attacks.

Analyzed Response:

The value of the cookie is not protected by HttpOnly flag and hence becomes accessible from JavaScript

```
HTTP/1.1 302 Found
Date: Tue, 08 Sep 2015 05:16:57 GMT
[---- Snipped parts of HTTP headers section for brevity ----]
Set-Cookie: s1434645778=duan8frtsbrdqp3db4kj6f2pb6; path=/
[---- Snipped parts of HTTP headers section for brevity ----]
Content-Type: text/html; charset=utf-8
```

Cookie username missing the HttpOnly flag

<<< >>>

Type: Vulnerability
Severity: Medium
Confidence: High
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/login.php

Description:

The HttpOnly flag was missing on the cookie: username. This may allow an attacker to get the cookie information using XSS attacks.

Analyzed Response:

The value of the cookie is not protected by HttpOnly flag and hence becomes accessible from JavaScript

```
HTTP/1.1 200 OK
Date: Tue, 08 Sep 2015 05:19:26 GMT
[---- Snipped parts of HTTP headers section for brevity ----]
Set-Cookie: username=xxxxx; expires=Wed, 07-Sep-2016 05:19:26 GMT; Max-Age=31536000
[---- Snipped parts of HTTP headers section for brevity ----]
Content-Type: text/html; charset=utf-8
```

Cookie username may contain sensitive information

<<< >>>

Type: Test Lead
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/login.php

Description:

The cookie: username might contain sensitive information which could be easily accessed or modified to exploit the web application.

Analyzed Response:

The cookie name or value indicates that it could hold important information

```
HTTP/1.1 200 OK
Date: Tue, 08 Sep 2015 05:19:26 GMT
[---- Snipped parts of HTTP headers section for brevity ----]
Set-Cookie: username=xxxxx; expires=Wed, 07-Sep-2016 05:19:26 GMT; Max-Age=31536000
[---- Snipped parts of HTTP headers section for brevity ----]
Content-Type: text/html; charset=utf-8
```

Cookie password may contain sensitive information

<<< >>>

Type: Test Lead
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/login.php

Description:

The cookie: password might contain sensitive information which could be easily accessed or modified to exploit the web application.

Analyzed Response:

The cookie name or value indicates that it could hold important information

```
HTTP/1.1 200 OK
Date: Tue, 08 Sep 2015 05:19:26 GMT
[---- Snipped parts of HTTP headers section for brevity ----]
Set-Cookie: password=xxxxx; expires=Wed, 07-Sep-2016 05:19:26 GMT; Max-Age=31536000
[---- Snipped parts of HTTP headers section for brevity ----]
Content-Type: text/html; charset=utf-8
```

Cross Site Scripting

Charset Not Set By Server

<<< >>>

Type: Vulnerability
Severity: Medium
Confidence: Medium
Found By: Active Scanning

Affected Site: http://localhost/
Affected Url: /sgsi/
Affected Parameter:
Parameter Location: URL

Description:

The Charset of the response content is not explicitly set by the server. Lack of charset can cause the browser to guess the encoding type and this could lead to Cross-site Scripting by encoding the payload in encoding types like UTF-7.

The relevant parts of the requests/responses pairs associated with the check that discovered this issue are available below.

Information about the Response from the Server:

This response does not have an explicit declaration for what character encoding is used in it.

Falta de certificado SSL

Sensitive Form loaded and submitted Insecurely

<<< >>>

Type: Vulnerability
Severity: Medium
Confidence: High
Found By: Passive Analysis

Affected Site: http://localhost/
Affected Url: /sgsi/login.php

Description:

Form with sensitive contents, which includes password fields, is loaded and submitted over HTTP

Analyzed Request:

This Request was made over HTTP

POST http://localhost/sgsi/login.php HTTP/1.1
Host: localhost
[---- Snipped parts of HTTP headers section for brevity ----]
Cookie: s1434645778=mtiqn84n0a0qt0rob1715443p6

Interesting part of Analyzed Response:

The HTML form containing password fields is displayed below. The unnecessary elements from this form have been stripped away for clarity.

IronWASP is not able to automatically highlight the interesting section of the Response, you would have to identify it manually.
IronWASP's Passive Analyzer reported the following text as being of interest in this case:

----- START OF INTERESTING TEXT -----
<form method="post" action="login.php" id="form1" name="form1"><input type="hidden" name="btnSubmit" value="Login"><input name="username" type="text" value="xxxxx"><input name="password" type="password" value="xxxxx"><input type="checkbox" name="remember_password" value="1" checked=""><input type="text" value="" name="value_captcha_1" style="" id="value_captcha_1"></form>
----- END OF INTERESTING TEXT -----

Detecciones en el index de la aplicación

Index

The titles of all the findings are listed below categorized by the host they were discovered on. All items in the list below are links to relevant sections in the report.

http://localhost/

- Cookie s1434645778 missing the HttpOnly flag
  1. /sgsi/menu.php
- Sensitive Form loaded and submitted Insecurely
  1. /sgsi/login.php
  2. /sgsi/login.php
- Cookie username missing the HttpOnly flag
  1. /sgsi/login.php
- Cookie password missing the HttpOnly flag
  1. /sgsi/login.php
- Charset Not Set By Server
  1. /sgsi/
- Server leaks version number
  1. /sgsi/menu.php
- AutoComplete Enabled on Password Fields
  1. /sgsi/login.php
- Runs on Apache/2.4.9 (Win64) PHP/5.5.12
  1. /sgsi/menu.php
- Technologies identified on Server
  1. /sgsi/menu.php
- Cookie username may contain sensitive information
  1. /sgsi/login.php
- Cookie password may contain sensitive information
  1. /sgsi/login.php

5.4.3. Anexo 3 – Entrevistas pruebas de usabilidad

SASGSI					
PREGUNTA	5	4	3	2	1
¿El proceso de autenticación es sencillo?	X				
¿La accesibilidad de las diferentes pantallas funciona de forma fácil y correcta?			X		
¿La información es verídica al momento de realizar las respectivas búsquedas?	X				
¿El proceso de carga de archivos es sencillo?		X			
¿La creación, modificación y eliminación de cuentas o usuarios es intuitiva?			X		
¿La respuesta del Software es suficiente, acertada?	X				
¿La consulta de procesos es sencilla y confiable?	X				
¿La consulta de controles es sencilla y confiable?	X				
¿La consulta de activos es sencilla y confiable?	X				
¿La consulta de reuniones es sencilla?	X				
¿Se identifica fácilmente el proceso para la asignación de riesgos a los activos?			X		
¿Los informes gráficos presentados por la aplicación son sencillos de entender?		X			
¿La aplicación ofrece mecanismos para la interpretación de datos en los informes presentados?		X			
¿Pueden exportarse archivos a diferentes formatos de forma intuitiva?	X				

Comentarios:

- En el perfil administrador los menús parecen desordenados dado que se cargan los botones de gestión de usuarios.

- Los informes gráficos de los procesos cargan las abreviaciones del nombre del proceso pero no se muestra ninguna convención al respecto.

German Augusto Perez

Asesor TI Seguridad

Ministerio de Comercio Industria y Turismo

SASGSI					
PREGUNTA	5	4	3	2	1
¿El proceso de autenticación es sencillo?	X				
¿La accesibilidad de las diferentes pantallas funciona de forma fácil y correcta?	X				
¿La información es verídica al momento de realizar las respectivas búsquedas?			X		
¿El proceso de carga de archivos es sencillo?		X			
¿La creación, modificación y eliminación de cuentas o usuarios es intuitiva?	X				
¿La respuesta del Software es suficiente, acertada?		X			
¿La consulta de procesos es sencilla y confiable?		X			
¿La consulta de controles es sencilla y confiable?		X			
¿La consulta de activos es sencilla y confiable?		X			
¿La consulta de reuniones es sencilla?		X			
¿Se identifica fácilmente el proceso para la asignación de riesgos a los activos?			X		
¿Los informes gráficos presentados por la aplicación son sencillos de entender?	X				
¿La aplicación ofrece mecanismos para la interpretación de datos en los informes presentados?	X				
¿Pueden exportarse archivos a diferentes formatos de forma intuitiva?			X		

Comentarios:

- En la consultas puede agregarse una ayuda en línea para que el usuario identifique más fácilmente el proceso.
- Pueden agregarse más estilos a nivel visual para que hagan más amigable la herramienta.

Juan Daniel Valero Duran

Ingeniero de Sistemas -Especialista en Desarrollo de Software

Ministerio de Comercio Industria y Turismo

SASGSI					
PREGUNTA	5	4	3	2	1
¿El proceso de autenticación es sencillo?	X				
¿La accesibilidad de las diferentes pantallas funciona de forma fácil y correcta?			X		
¿La información es verídica al momento de realizar las respectivas búsquedas?	X				
¿El proceso de carga de archivos es sencillo?		X			
¿La creación, modificación y eliminación de cuentas o usuarios es intuitiva?		X			
¿La respuesta del Software es suficiente, acertada?		X			
¿La consulta de procesos es sencilla y confiable?	X				
¿La consulta de controles es sencilla y confiable?	X				
¿La consulta de activos es sencilla y confiable?	X				
¿La consulta de reuniones es sencilla?	X				
¿Se identifica fácilmente el proceso para la asignación de riesgos a los activos?			X		
¿Los informes gráficos presentados por la aplicación son sencillos de entender?	X				
¿La aplicación ofrece mecanismos para la interpretación de datos en los informes presentados?	X				
¿Pueden exportarse archivos a diferentes formatos de forma intuitiva?		X			

Comentarios:

- La información de algunas de las consultas es elevada.
- En las opciones de exportación se incluyó tipos de archivos que no son comunes como el cssv, estos pueden confundir al usuario
- Las pantallas que se refieren a los activos no son claras.

Hans Lwver Carlosama

Técnico de apoyo a la Ventanilla Única de Comercio Exterior (VUCE)

Ministerio de Comercio, Industria y Turismos