SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001

Investigadores

ANDRÉS DAVID BETIN RODRIGUEZ

JHONY ENRIQUE MADERA OSORIO

UNIVERSIDAD DE CARTAGENA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS, 2015

SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001

PROYECTO DE GRADO

GRUPO DE INVESTIGACIÓN GIMÁTICA

Ingeniería del Software

Investigadores

ANDRÉS DAVID BETIN RODRIGUEZ

JHONY ENRIQUE MADERA OSORIO

Tutor

Msc. RAÚL JOSÉ MARTELO GÓMEZ

UNIVERSIDAD DE CARTAGENA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS, 2015

Universidad de Cartagena
Fundada en 1827

Proyecto de Grado: SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001

Autores: ANDRÉS DAVID BETIN RODRIGUEZ

JHONY ENRIQUE MADERA OSORIO

Tutor: RAUL JOSÉ MARTELO GÓMEZ

Nota de Aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, ____ de _____ de 2015

RESUMEN

En este mundo globalizado es necesario que las organizaciones implementen plataformas tecnológicas para soportar la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad de la información que garanticen integridad, disponibilidad y confidencialidad. La implantación de los Sistemas de gestión de la seguridad de la información (SGSI) es una labor fundamental que involucra personas, procesos y recursos de la organización.

Durante el proceso de implantación de un SGSI se pueden generar falencias como falta de conocimiento en el tema de seguridad de la información, tiempo implementado no acorde a los subprocesos en el establecimiento del sistema, documentación mal administrada y ausencia de compromiso por parte de la alta gerencia. Por lo tanto, se requiere un sistema de apoyo para un proceso que enmarcada complejidad, revisiones cíclicas y cuidado en el manejo de todos los informes generados en dicho proceso. Con el propósito de hacer menos tediosa, atenuar las complicaciones abordadas en la implantación y estándares relacionados, de tal forma que se contemple la seguridad en la información.

Para lograrlo, el presente proyecto tiene como objetivo desarrollar un software de apoyo para el proceso de implantación del sistema de gestión de seguridad de la información en organizaciones basado en la norma ISO 27001. El fundamento teórico se centra en definir aspectos relacionados con objetivos, elementos y compromisos de la Seguridad de Información, conceptos y ciclo de vida del SGSI, así como estándares internacionales más destacados en la actualidad.

Con la ejecución del proyecto se obtuvo un informe detallado de los resultados, donde se especificaron estrategias destacadas en cada uno de los modelos de seguridad de la información, estándares y/o normas estudiadas, los cuadros de análisis construidos, y la descripción de características del esquema propuesto. Además, el software que servirá de guía en las organizaciones, anexando los datos relevantes de la prueba de funcionamiento aplicada.

Palabras clave: *Software, información, seguridad, ISO 27001, implantación*.

ABSTRACT

In this globalized world, it is necessary implement technology platforms in the organizations to support the new way of doing business. Using the Internet for this purpose entails the development of information security projects who guarantee integrity, availability and confidentiality. The implementation of information security management systems (ISMS) is a fundamental task that involves people, processes and resources of the organization

During the process of implementation of an ISMS can be generated shortcomings such as lack of knowledge on the subject of information security, implementation of time not according to the subprocesses established in the system, mismanaged documentation and lack of commitment from senior management. Therefore, a support system for a process that framed complexity, cyclical reviews and care in handling all reports generated in this process is required. In order to make it less tedious, mitigate complications contemplated in the related standards and the implementation, so that is contemplated the information security.

To achieve this, the present project has as purpose the development of an support software for the the process of implementing an information security management system on organizations based on the standard ISO 27001. The theoretical foundation is focused in defining aspects of objectives, elements and commitments of Information Security, and life cycle concepts ISMS, as well as more highlights international standards today.

With the implementation of the project a detailed results report was obtained, where outstanding strategies were specified in each of the models of information security, standards and / or studied rules, boxes built analysis and a description of characteristics of the scheme proposed. In addition, the software will guide in organizations, attaching the relevant data of the work test.

Keywords: Software, information, security, ISO 27001, implantation

DEDICATORIA

Este trabajo va dedicado a:

A Dios que nos ha provisto con las herramientas y la fortaleza necesarias para terminar este proyecto.

A nuestros padres que con su amor desinteresado nos han guiado cuando más lo hemos necesitado.

A nuestro docente de la asignatura Proyecto de Grado y a nuestro director de tesis por brindarnos su confianza y su apoyo.

AGRADECIMIENTOS

Este triunfo queremos dedicarlo primeramente a Dios por mostrarnos el camino en los momentos más difíciles y por estar siempre presente en nuestras vidas. Gracias Dios por darnos la fuerza necesaria para la realización de este proyecto.

A nuestras familias por ser el motor principal para seguir adelante. A nuestros padres por esforzarse día a día en darnos la mejor educación para que seamos hombres de bien que contribuyan a construir una mejor sociedad.

También nos gustaría expresar un agradecimiento profundo al Ingeniero Raúl Martelo Gómez, nuestro tutor y guía en esta aventura, el cual mediante de sugerencias, correcciones e indicaciones nos supo llevar por este largo camino.

A nuestros compañeros de clase y amigos quienes siempre a nuestro lado han mostrado su apoyo, permitiéndonos superar las dificultades gracias a sus buenas energías. A nuestros docentes por todas aquellas enseñanzas que nos han llevado a ser mejores personas y mejores profesionales, esperamos sinceramente que Dios les permita ver los frutos de sus enseñanzas en cada uno de nosotros.

A todos ustedes nuestros más sinceros agradecimientos.

CONTENIDO

1. INTRODUCCIÓN 14
2. OBJETIVOS Y ALCANCE 16
2.1 OBJETIVO GENERAL 16
2.2 OBJETIVOS ESPECÍFICOS 16
3. ESTADO DEL ARTE 17
4. MARCO DE TEÓRICO 24
4.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA 24
4.2 ISO 27001 25
4.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) 26
4.3.1 IMPLANTACIÓN DE SGSI 26
4.4 OTRAS NORMAS Y ESTÁNDARES 28
5. METODOLOGÍA 29
5.1 PROCEDIMIENTO 29
5.2 RECOLECCIÓN DE INFORMACIÓN 30
5.2.1 ANÁLISIS DE CONTENIDO: ESTUDIO DE ESTANDAR 31
5.2.2 ENFOQUE DEL PROCESO 31
5.2.3 MODELO DEL PROCESO 32
5.2.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 34
5.2.5 COMPATIBILIDAD CON OTROS SISTEMAS 37
5.3. DELIMITACIÓN DEL PROYECTO 38
5.4 DEFINICIÓN DE MÓDULOS 39
5.4.1 MÓDULO DOCUMENTAL 39
5.4.2 MÓDULO ANÁLISIS DE RIESGOS 43
5.4.3 MODULO ROLES 66
5.4.4 MÓDULO DE ACTIVOS 66
5.4.5 MÓDULO DE REPORTE 67
5.5 ANÁLISIS Y FUNDAMENTOS 69
5.6 ESTRUCTURACIÓN DEL MODELO 76
6. DESARROLLO 82
6.1 MODELO DE DOMINIO 82

6.2 VISTA DE ESCENARIOS 83
6.2.1 CASOS DE USO GESTIÓN DE ROLES 83
6.2.2 CASOS DE USO GESTIÓN DOCUMENTAL 84
6.2.3 CASOS DE USO GESTIÓN DE ACTIVOS 85
6.2.4 CASOS DE USO ANÁLISIS DE RIESGO 86
6.2.5 DESCRIPCIÓN CASOS DE USO 87
6.3 VISTA DE PROCESOS 110
6.3.1 DIAGRAMA DE ACTIVIDADES GESTIÓN DOCUMENTAL 110
6.3.2 DIAGRAMA DE ACTIVIDAD ANÁLISIS DE RIESGOS 111
6.3.3 DIAGRAMA DE ACTIVIDAD GESTIÓN DE ACTIVOS 112
6.3.4 DIAGRAMA DE ACTIVIDAD GESTIÓN DE ROLES 112
6.4 VISTA LÓGICA 113
6.4.1 DIAGRAMA DE CLASE ANÁLISIS DE RIESGOS 113
6.4.2 DIAGRAMA DE CLASE GESTIÓN ACTIVOS 114
6.4.3 DIAGRAMA DE CLASE GESTIÓN DOCUMENTAL 115
6.4.4 DIAGRAMA DE CLASE GESTIÓN ROLES 116
6.5 VISTA FÍSICA 117
6.5.1 DIAGRAMA DE DESPLIEGUE 117
7. EVALUACIÓN Y PRUEBAS DEL SISTEMA 117
7.1 RESULTADOS 127
8. CONCLUSIONES Y RECOMENDACIONES 129
8.1 CONCLUSIONES 129
8.2 RECOMENDACIONES 131
REFERENCIAS 132
ANEXO 1 135
ARTICULO REVISTA SciELO: SOFTWARE PARA GESTIÓN DOCUMENTAL, UN COMPONENTE MODULAR DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 135
ANEXO 2 145
CERTIFICADO PONENCIA: SOFTWARE WEB PARA EL ACOMPAÑAMIENTO EN EL ANÁLISIS Y GESTIÓN DE RIESGOS EN PYMES 145
ANEXO 3 146

CERTIFICADO PONENCIA: INTEGRACIÓN DEL MÓDULO DE AUTOEVALUACIÓN Y GESTIÓN DOCUMENTAL PARA EL CUMPLIMIENTO DE LA NORMA ISO 27001 146

ANEXO 4 147

CERTIFICADO PONENCIA: APLICACIÓN BASADA EN SOFTWARE LIBRE PARA LA AUTOEVALUACIÓN EN EL PROCESO DE IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 147

ANEXO 5 148

SISTEMA DE GESTIÓN DOCUMENTAL BASADO EN DJANGO 148

ANEXO 6 149

SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001 149

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Estructura de metodología SCRUM. (Law, E.L. & Lárusdóttir, M.,2015) 30
Ilustración 2. Modelo de proceso PDCA aplicado por el estándar a los procesos SGSI. Fuente: (Estándar Internacional ISO/IEC 27001, 2005). 33
Ilustración 3. Delimitación del proyecto, componentes que comprende un SGSI. Fuente: Grupo de trabajo 39
Ilustración 4. Modelo gestión documental. Fuente: Grupo de trabajo..... 40
Ilustración 5. Workflow estados de documento. Fuente: Grupo de trabajo 41
Ilustración 6. Interacción con otros módulos. Fuente: Grupo de trabajo 42
Ilustración 7. Versionamiento de documento. Fuente: Grupo de trabajo. 42
Ilustración 8. Modelo generalizado para análisis de riesgos. Fuente: Grupo de trabajo..... 45
Ilustración 9. Modelo de análisis de riesgo. (MAGERIT, 2012) 52
Ilustración 10. Metodología de implantación para certificación en ISO/IEC 27001 69
Ilustración 11. Número de incidentes a nivel mundial. (DATALOSS DB, 2014)..... 70
Ilustración 12. . Incidentes reportados de acuerdo a su clasificación (Foundation, 2013). 71
Ilustración 13. . Distribución de incidentes por tipo de organización afectada (Foundation, 2013)71
Ilustración 14. Incidentes que involucran terceras partes (Foundation, 2013)..... 72
Ilustración 15. Registros que involucran terceras partes (Foundation, 2013)..... 72
Ilustración 16. Motivos para no realizar gestión de riesgos. (ACIS, 2014) 74
Ilustración 17. Cantidad de evaluaciones de riesgos. (ACIS, 2015)..... 74
Ilustración 18. Obstáculos de implementación de la seguridad informática..... 75
Ilustración 19. Fallas e incidentes de seguridad informática. (ACIS, 2014)..... 75
Ilustración 20. Modelo de implantación del SGSI, diseñado como resultado final del proceso. (ACIS, 2014)..... 81
Ilustración 21. Modelo de dominio. 82
Ilustración 22. Casos de uso gestión de roles. 83
Ilustración 23. Casos de uso gestión documental. 84
Ilustración 24. Casos de uso gestión de activo. 85
Ilustración 25. Casos de uso análisis de riesgos..... 86
Ilustración 26. Diagrama de actividad - gestión documental..... 110
Ilustración 27. Diagrama de actividad: análisis de riesgos 111
Ilustración 28. Diagrama de actividad - gestión de activos 112

Ilustración 29. Diagrama de actividad - gestión de roles 112
Ilustración 30. Diagrama de clases análisis de riesgos 113
Ilustración 31. Diagrama de clases gestión activos 114
Ilustración 32. Diagrama de clases gestión documental 115
Ilustración 33. Diagrama de clases gestión roles 116
Ilustración 34. Diagrama de despliegue 117
Ilustración 32. Panel de administrador. 118
Ilustración 33. Cronograma de actividades 119
Ilustración 34. Gestión de actividades 119
Ilustración 35. Detalle de actividad 120
Ilustración 36. Creación de documento 120
Ilustración 37. Gestión de activos 121
Ilustración 38. Enviar a revisión un documento 121
Ilustración 39. Estado de los documentos 121
Ilustración 40. Información básica de proyecto de análisis de riesgos 122
Ilustración 41. Identificación de activos 123
Ilustración 42. Identificación de amenazas 123
Ilustración 43. Valoración de activos 124
Ilustración 44. Valoración de amenazas 124
Ilustración 45. Sesión de valoración activos vs. Amenazas 125
Ilustración 46. Valoración de salvaguardas 125
Ilustración 47. Sesión de valoración amenazas vs. Salvaguardas 126
Ilustración 48. Módulo de reporte 126

ÍNDICE DE TABLAS

Tabla 1. Comparación de otras metodologías de análisis de riesgos. Fuente: Grupo de trabajo ... 54
Tabla 2. Escala de valoración activos. (Veiga, 2009) ... 61
Tabla 3. Caso de Uso: Crear Actividad ... 87
Tabla 4 Caso de Uso: Modificar Actividad ... 88
Tabla 5 Caso de Uso: Eliminar Actividad ... 88
Tabla 6 Caso de Uso: Agregar documentos a una actividad ... 89
Tabla 7 Caso de Uso: Eliminar documentos a una actividad ... 90
Tabla 8 Caso de Uso: Modificar documentos de una actividad ... 91
Tabla 9 Caso de Uso: Versionar documentos de una actividad ... 91
Tabla 10. Caso de Uso: Crear Usuario ... 92
Tabla 11 Caso de Uso: Modificar Usuario ... 93
Tabla 12 Caso de Uso: Desactivar Usuario ... 93
Tabla 13 Caso de Uso: Crear grupo de usuario ... 94
Tabla 14 Caso de Uso: Modificar Grupo de Usuario ... 95
Tabla 15 Caso de Uso: Eliminar grupos de usuario ... 95
Tabla 16 Caso de Uso: Agregar usuarios a grupos ... 96
Tabla 17 Caso de Uso: Remover usuario de grupo ... 97
Tabla 18 Caso de Uso: Agregar permiso a usuario ... 97
Tabla 19 Caso de Uso: Remover permiso a usuario ... 98
Tabla 20 Caso de Uso: Agregar permiso a grupo ... 98
Tabla 21 Caso de Uso: Remover permiso a grupo ... 99
Tabla 22. Caso de Uso: Crear Activo ... 100
Tabla 23 Caso de Uso: Modificar Activo ... 100
Tabla 24 Caso de Uso: Eliminar Activo ... 101
Tabla 25 Caso de Uso: Crear recurso ... 102
Tabla 26 Caso de Uso: Modificar recurso ... 102
Tabla 27 Caso de Uso: Eliminar recurso ... 103
Tabla 28 Caso de Uso: Agregar activo a recurso ... 103
Tabla 29 Caso de Uso: Remover activo a recurso ... 104
Tabla 30. Caso de Uso: Crear Proyecto ... 105
Tabla 31 Caso de Uso: Identificar activos de información ... 105
Tabla 32 Caso de Uso: Identificar amenazas para activos de información ... 106
Tabla 33 Caso de Uso: Valorar activos ... 106
Tabla 34 Caso de Uso: Valorar amenazas ... 107
Tabla 35 Caso de Uso: Valorar salvaguardas ... 108
Tabla 36 Caso de Uso: Valorar activos vs amenazas ... 108
Tabla 37 Caso de Uso: Valorar amenazas vs salvaguardas ... 109
Tabla 38. Participación de ponencias ... 129

1. INTRODUCCIÓN

La información se ha convertido en activo importante de organizaciones (Piattini & Del Peso, 2001), toda vez cuando es completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas. La importancia de la información se fundamenta en la teoría de la organización, la cual se define como un sistema conformado por personas, recursos materiales e información; existe una percepción sobre el concepto de información en la cual se indica que determina "el 'orden y el caos' entre los individuos, los recursos y en la interrelación personas-recursos" (Aja, 2002); por eso, debe considerarse a las organizaciones como sistemas de información.

Sin embargo dichos sistemas a medida que consultan, almacenan y generan información, ponen en riesgo la integridad de la misma; riesgos, que no solo provienen del exterior sino también del interior de la organización (INTECO, 2010). Los virus, gusanos, hackers, phishing e ingenieros sociales, entre otras, son amenazas constantes que atentan contra la información de cualquier organización (Susanto et al, 2011a). Un Hacker, puede causar pérdidas considerables para una organización, tales como, robo de datos de clientes y espiar en la estrategia de negocio en beneficio de competidores (Susanto et al, 2011b).

Como consecuencia, la seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas (Von, B. & Von, R. 2004), sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen unas obligaciones para organizaciones (Susanto & Bin, 2010). Las anteriores obligaciones que se ejercen bajo la seguridad de la información, pueden ser solventadas con la ayuda de un SGSI que permite gestionar con eficacia los activos de información, minimizando posibles riesgos que atenten contra la misma (Broderick, 2006).

El SGSI consiste básicamente en un conjunto de políticas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware y recursos de software (ISO/IEC 27001, 2005); estas políticas, muestran la manera en que los recursos del computador pueden ser utilizados (INTECO, 2010). Adicionalmente, el proceso de implantación de un SGSI aborda

fases de: auditoría inicial, análisis y procesos de flujos de información, análisis y gestión de riesgos y desarrollo del sistema de gestión bajo un modelo PHVA (Planear-Hacer-Verificar-Actuar), que conlleva a dificultades tales como: falta de documentación, administración y organización de la misma, ausencia de roles y responsabilidades, para llevar a cabo las actividades pertinentes para dar cumplimiento a objetivos y alcances del SGSI (Del Rio, 2013).

En este orden de ideas, abordar el proceso de forma tradicional y, las dificultades evidenciadas en cuanto a la documentación que se genera durante este proceso, sugiere la necesidad de buscar soluciones que aborden dicho problema, lo cual se constituye en el objetivo principal de este trabajo. Para lograrlo, se aplica la siguiente estrategia metodológica:

Diseño y aplicación de instrumentos de recolección de información. Búsqueda y apropiación del conocimiento en estándares, normas, o modelos de gestión de buenas prácticas en Seguridad de la Información, destacando las normas internacionales, ISO 27001 e ISO 27002. Posterior construcción de cuadros comparativos y evaluaciones detalladas, que den lugar a modelo conceptual de seguridad, que finalmente, es materializado a través del Software que establece una serie de componentes fundamentales en la implantación de un SGSI. Una vez obtenido el producto software, se realizan pruebas prácticas con datos experimentales, y se documentan los resultados. La implementación del modelo conceptual mencionado, incluye una serie módulos guías para el desarrollo del SGSI, y en particular un módulo de reporte asociado a métricas e indicadores del estado actual de implementación, mostrando graficas de forma sencilla, manejables y facilidad de interpretación; representa no sólo una solución al problema de inseguridad informática enfrentado por las empresas actualmente, debido a la ausencia de principios o intenciones de alto nivel (*Sistemas de gestión de seguridad de la información*) sino, que integra una serie de actividades de carácter documental, descriptivo, analítico y experimental que permitirá a los investigadores la adquisición de amplios conocimientos en el área de seguridad de la información, principalmente, en estándares, modelos o normas internacionales reconocidos mundialmente.

2. OBJETIVOS Y ALCANCE

2.1 OBJETIVO GENERAL

Desarrollar un software de apoyo para el proceso de implantación del sistema de gestión de seguridad de la información en organizaciones basado en la norma ISO 27001.

2.2 OBJETIVOS ESPECÍFICOS

- Construir el estado del arte del proyecto, con base en información relacionada con el proceso de implantación de un SGSI y software de apoyo del mismo, con el fin de obtener un mayor referente teórico y además requerimientos de la herramienta a desarrollar.
- Diseñar un modelo conceptual que permita materializar cada una de las etapas del proceso de implantación del SGSI, apoyado en la norma ISO 27001.
- Desarrollar un software basado en el modelo conceptual construido, ligado a la norma ISO 27001.
- Realizar pruebas con la herramienta desarrollada con datos experimentales para garantizar el correcto funcionamiento del mismo.

3. ESTADO DEL ARTE

La seguridad informática tiene lugar desde los primeros avances de las redes, telecomunicaciones y sistemas computacionales, cuando se detectaron alteraciones desconocidas e inexploradas que fueron poco a poco formando una nube de preocupación en el hombre para salvaguardar la información. Al realizar un breve recorrido por la historia, se rescatan hechos relacionados con el origen de los virus, ataques, códigos maliciosos, hackers y su impacto en este ámbito.

Hacia 1986, dos personajes conocidos como Basit y Amjad descubrieron un código ejecutable en el boot de un disquete, que corría siempre que se reiniciaba el computador con el disco flexible en A; encontrando que éste podía instalarse fácilmente en memoria residente reemplazando un programa almacenado, además de ubicar una copia de sí mismo en cada disquete. Al ser alteraciones desconocidas, las denominaron "virus" por la similitud con los virus biológicos (Virusprot, 2010).

Continuando con importantes acontecimientos como fue el 2 de noviembre de 1988, es llamado por muchos el día que internet se detuvo; aunque en realidad solamente fue el 10% de los equipos conectados a la red conocida hasta entonces (ARPA net). Aunque no fue el primer virus, es considerado el primer gusano que atacó internet, ocasionando de igual manera, el primer ataque de negación de servicio (DOS). En el momento del ataque se estimó que el gusano de Morris infectó alrededor de 6.000 servidores o el 10% de los servidores en Internet, y causó entre los USD$10 millones y USD$ 100 millones en daños y perjuicios. Por otro lado, también logró concientizar en cuanto a la seguridad informática, ya que este evento llevó a la creación del CERT (Computer Emergency Response Team), un equipo de respuesta a emergencias en sistemas computacionales.

Prácticamente desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de forma inevitable, fundamentada en incidentes y falencias mostradas a lo largo de la historia de este medio. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar

mecanismos de protección que reduzcan a un bajo nivel los riesgos asociados a los incidentes de seguridad.

Pero no solo ataques cibernéticos envuelve el tema de la seguridad de la información, cuyo objetivo es mantener la disponibilidad, confidencialidad e integridad de la misma, amenazas por agentes propios de la empresa o desastres naturales alteran este tipo de principios. Por lo tanto, la seguridad de la información aborda todas las atenciones en cuanto a implementación de mecanismos, estrategias o sistemas de gestión. Para atender el problema de la inseguridad, se ha creado distintas normatividades como la ISO 27001 la cual define un sistema de gestión de la seguridad de la información para conocer, gestionar y minimizar todos los riesgos de la misma (INTECO, 2012).

Bajo la inmensa nube de inseguridad en la que se encuentra la información y la garantía de contar con un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. Por lo tanto, la norma ISO 27001 fomenta el propósito de establecer un sistema de gestión de la seguridad de la información que garantiza el conocimiento, apropiación, gestión y disminución de los riesgos de la seguridad de la información por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (ISO27000, 2012).

El estado de estos sistemas de gestión a nivel internacional, relacionados con el propósito de implantar este tipo de sistemas, Ingenia una empresa de servicios de tecnologías de la información, comunicaciones e internet, ha desarrollado una herramienta software que permite la gestión completa de un Departamento de Tecnología de la información (TI) llamada e-PULPO (Plataforma de Unificación Lógica de los Procesos Organizativos) que cumple con dos funcionalidades esenciales para un Departamento de TI: Gestión de requisitos legales y la Gestión de requisitos normativos (SGSI –ISO 27001 e ISO 27002-, SGTI –ISO 20000). Esta plataforma integra un módulo SGSI, enfocado a la primera fase de planificación del mismo, donde permite el manejo de activos, documentación, incidencias, formación, indicadores y las auditorias establecidas por las norma ISO 27001, además de la implementación de controles basado en la norma ISO 27002.

e-PULPO se concentra en la gestión documental, la revisión, control y administración de esta, donde la facilidad, interactividad y los componentes distribuidos de su interfaz gráfica en el componente de gestión documental la hace ser una plataforma eficiente, eficaz y regulada en el cumplimiento de sus funciones. (Ingenia, 2010).

En cuanto a la contra parte de los aportes de esta plataforma, la cual ajusta la normatividad ISO 27001 y 27002, sumado al aspecto legal enfocándose netamente a la gestión documental, teniendo como trabajos futuros la implementación de módulos para el mantenimiento y mejora, además por ser una plataforma que presta servicios crea un factor diferenciante respecto al software de apoyo que acompañará mediante un proceso por etapa la implantación de un SGSI en cualquier organización; no solo en la parte documental, además abordará las fases de planificación, implementación, verificación y mantenimiento, facilitando los procesos posteriores como la certificación.

El proceso de implantación de un SGSI se hace complejo a medida que los procesos y el personal de la empresa empiecen a involucrarse, además la ISO 27001 al ser una norma que contextualiza el ¿Qué? Pero no enmarca el ¿Cómo? Se aplica la normatividad, tanto es la necesidad de esquematizar este proceso de implantación, donde la Universidad central de Chile crean una metodología para implantar un SGSI en PYMES, permitiendo la disminución de tiempo y costos de implementación de un sistema de gestión para estas empresas en el mediano plazo, en conformidad con la norma ISO 27001 dando cumplimiento a las buenas practicas según lo establecido en la norma ISO 27002. Pero el ámbito de aplicación está enmarcada para empresas PYMES, donde los recursos, personal, procesos y el análisis de riesgo, genera menos complejidad y una fuerte incompatibilidad en el momento que dichas empresas empiece a crecer tanto en recursos humanos como tecnológicos. Por lo tanto, la propuesta referente abordará cualquier tipo de organización independientemente de las características que está presente, basándose netamente en la ISO 27001, lo cual facilita la elaboración de una metodología aplicable a todo tipo de empresa (Donders, 2010).

En cuanto a la percepción y la importancia que se le está dando en América Latina a los sistemas de gestión, políticas de seguridad, metodologías y cualquier otro mecanismo o estrategias asociadas a la seguridad de la información, ESET presenta un informe donde se evidencia un acercamiento positivo respecto al 73,8% de las empresas que no pierden la noción de establecer políticas de seguridad, un 38% de contemplar en el presupuesto de la empresa y una necesidad de la no pérdida de datos. (ESET Security Report, 2012).

Las empresas Latinoamericanas, así como entes gubernamentales están en total disposición de salvaguardar la información de todas las amenazas originadas en el entorno, lo cual la manifestación de buenas prácticas de políticas de seguridad informática, planes de seguridad informática, estrategias, metodologías y sistemas de gestión de la seguridad de la información abarcan el crecimiento o valoración de datos estadísticos presentados por la ASCI, ISACA y CSIRT.

En Uruguay figura la propuesta titulada *"Metodología de implantación de un SGSI en un grupo empresarial jerárquico*, la cual presenta un ámbito de aplicación amplio en sentido que alcanza a grupos empresariales y organizaciones donde existe una relación jerárquica o de subordinación, puesto que condiciona la gestión de la información, equivalente a la incorporación como tal de un SGSI. Para el enfoque de estructura jerárquica empresarial, se destaca el objeto de análisis de este trabajo el cual es grupo multiempresarial de relacionamiento vertical o jerárquico. Esta relación que se propaga y afecta las estrategias empresariales, infraestructura compartida, políticas, objetivos, recursos, etc. Por lo que el debido manejo de la información en una estructura jerárquica donde todo la empresa madre comparte procesos de negocio y todo lo relacionado para la continuidad de este. Por lo tanto, *"Debe buscarse una metodología que permita que los SGSI de ambas empresas sean definidos, implantados y gestionados de forma cooperativa, intentando alinear objetivos y prioridades de acuerdo a los intereses del grupo. Esta metodología debe lograr esa cooperación de forma eficaz y eficiente tanto en la búsqueda de recoger las directrices que vienen del SGSI de la empresa jerárquicamente mayor así como también trasladar el feedback y las necesidades de la empresa subordinada"* (Pallas, 2009). Con respecto a los resultados obtenidos, optaron por mantener una metodología mixta en cuanto el manejo y sincronización de los procesos en una estructura jerárquica manteniendo el aspecto legal de la localidad en donde cada miembro del grupo esté ejecutando su SGSI, permitiendo

mantener trabajos futuros enfocados a un sistema de apoyo que permita acoplar e integrar el SGSI de la empresa subordinada y la principal, sin duplicar costos, ni controles y permita el cumplimiento de las políticas establecidas en ambas partes.

De cierta forma la preocupación por la complejidad en cuanto al ámbito de aplicación de la norma ISO 27001 se ha multiplicado, mostrando interés tanto en la búsqueda de mecanismos, como en metodologías para la fácil regulación de la misma.

Para verificación de esas metodologías, políticas de seguridad y temas relacionados con la seguridad de la información, la IV Encuesta latinoamericana de seguridad de la información (2012) basada en una muestra aleatoria de profesionales de tecnologías de información y comunicaciones de Argentina, Colombia, México, Perú, Uruguay, Paraguay entre otros, la cual respondió una encuesta de manera interactiva a través de la página web dispuesta por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), según el análisis desde 2009 hasta 2012, la situación respecto al desarrollo de políticas de seguridad ha avanzado progresivamente comparado con el año anterior 57% de falta de documentación formal y socialización disminuyó a 46.38%, porcentaje que refleja la buenas prácticas y la concientización hacia este ámbito en lo correspondiente al establecimiento de políticas de seguridad y la seguridad de la información (Cano & Saucedo, 2012).

En Colombia para temas relacionados con la gestión de la información, durante el año 2011 más del 70% de las empresas no cuentan con políticas de seguridad definidas formalmente o se encuentran en desarrollo. Es interesante que para este año el 49.3% de la población que contesta la encuesta manifiesta tener una política escrita y aprobada, con un incremento frente al año anterior (2010) de 9.45%. Esto muestra que a las organizaciones les interesa el tema dentro del contexto de la protección de la información como un escenario con incidencia en las estrategias de negocios de la organización. En 2012, en lo referente a los estándares más utilizados para gobernar, gestionar, operar y administrar la seguridad de la información, dicha lista es comandada por ISO 27001, ITIL y Cobit, con un considerable incremento de un 15,95% para ITIL en su uso para las organizaciones (Almanza, 2011).

Entre tanto, ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por

su tamaño como por su actividad. Se calculan aproximadamente 7940 empresas certificadas a nivel mundial 4152 en Japón, 573 en Reino Unido, 112 en Argentina, 24 en Brasil, en comparación con Colombia la cual lleva 14 organizaciones certificadas (ISMS Certificates, 2013).

En relación a la seguridad informática, a nivel nacional, se destaca el proyecto diseñado por el Grupo de Investigación en Informática y Telecomunicaciones de la Universidad Icesi de Cali/Colombia, que desarrollo un Centro de Operaciones de Seguridad Informática, cuyo objetivo es prestar servicios a empresas para las que es muy costoso tener personas y equipos especializados en la gestión a través del sistema SOC Colombia, una herramienta basada en OSSIM (*Open Source Security Information Manager, o Administrador de la Seguridad de la Información de Fuente Abierta*) es un software que permite administrar mantener y monitorear herramientas de seguridad como antivirus, detectores de intrusos, firewalls, analizadores de vulnerabilidades, monitores de red, sniffers etc. Por lo que fue base para la construcción de SOC Colombia, el propósito del proyecto es ofrecer al encargado de la seguridad la capacidad de monitorear el estado de todos sus sistemas informáticos, desde una interfaz amigable (Universia Noticias Colombia, 2009).

Actualmente se evidencia la necesidad de contar con políticas formalmente definidas como parte fundamental del Sistema de Gestión de Seguridad de la Información o esquema establecido. Sin embargo, el interés último está orientado hacia la continuidad de negocio, el cumplimiento de regulaciones y las normativas internas y externas, así como la protección de la reputación de la empresa, lo que proyecta un futuro de altas inversiones. Por otro lado se puede afirmar, según las encuestas nacionales, que las normas o regulaciones nacionales e internacionales fortalecerán los sistemas de gestión, dado el interés manifiesto (Junco, 2009).

A nivel local en relación a la seguridad informática, se destaca el proyecto de grado titulado *"Software de apoyo al proceso de creación y registro de políticas de seguridad informática en organizaciones"* de egresados de la Universidad de Cartagena, con el propósito de armar un esquema para la creación, establecimiento y registro de políticas de seguridad basados en normas y estándares internacionales existentes. Reduciendo la complejidad asociada a la aplicación de estas normas para dicho proceso.

Esta propuesta solo abarca una parte del sistema de gestión de la seguridad de la información, la cual es el establecimiento de políticas de seguridad informática como parte fundamental del mismo, enfocado en el área de la seguridad física, dejando suelta la seguridad lógica como otro de los componentes esenciales de un SGSI. Permitiendo libertad innovadora para la creación de software de apoyo a este tipo de sistema los cuales permitirán el fácil acceso a la certificación de la norma ISO 27001 (Marrugo & Nuñez, 2012).

Desde todas las perspectivas mencionadas con el propósito de mantener los principios fundamentales de la información, tal vez, lo que hace falta no son entidades que brinden servicios de seguridad, sino, crear conciencia de los riesgos a los que están expuestos los sistemas de información crítica, y la disposición de herramientas de apoyo que permitan facilitar la gestión de la seguridad de la información.

4. MARCO DE TEÓRICO

4.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

En el mundo empresarial de hoy, se hace cada vez más necesaria la sistematización de procesos en organizaciones, con el fin de aprovechar todos los beneficios que puede brindar y garantizar un manejo eficaz de la información, el activo más valioso que tienen las empresas. Pues a partir de este se obtienen las ganancias, ya sea por medio de datos estadísticos, estrategias de mercadeo, datos de consumo de un producto, entre otros.

La información según el uso que se le dé, puede ser pública o privada. La primera abarca aquellos datos informativos que se le entregan a los usuarios finales; la segunda es aquella que sólo puede ser visualizada por personal interno de la empresa (Borghello, 2001).

Con esta separación aparece la necesidad de resguardar este elemento tan valioso, tratando que se cumplan ciertas características necesarias como son la integridad, disponibilidad y confidencialidad.

- Integridad: La información se encuentra en constante mantenimiento, ésta sólo debe ser alterable por personal calificado y autorizado para hacerlo. En caso que varíe de forma contraria a lo anterior se está violando la integridad de los datos (Dussan Clavijo, 2006).
- Confidencialidad: La información sólo puede ser manipulada por personal propio de la empresa o autorizado por ésta para dicha labor, en otras palabras, se debe asegurar que sólo la persona correcta acceda (Dussan Clavijo, 2006).
- Disponibilidad: Una vez que se asegura que la información correcta llegue a los destinatarios o usuarios correctos, lo que se debe garantizar es que llegue en el momento oportuno (Dussan Clavijo, 2006).

El cumplimiento de estas características hacen parte de las responsabilidades de la seguridad informática la cual aplica técnicas fundamentales para preservar la información, los diferentes

recursos informáticos con que cuenta la empresa y hacer el sistema lo más seguro posible, implementando un conjunto de Políticas de Seguridad Informática (PSI)

Para efectos del siguiente proyecto, definiremos las Políticas de Seguridad Informática como el conjunto de normas, reglas, procedimientos y prácticas que regulan la información contra la pérdida de confidencialidad, integridad o disponibilidad, de forma accidental o intencionada, garantizando la conservación y buen uso de los recursos informáticos con los que cuenta la empresa.

4.2 ISO 27001

La norma ISO 27001 define como organizar la seguridad de la información en cualquier tipo de empresa. Es posible afirmar que esta norma constituye la base de la gestión de la seguridad de la información. La cual es redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la misma en cualquier organización (Kosutic, 2012).

Apartar de la ISO 27001, muchas organizaciones han tomado esta norma como base para confeccionar las diferentes normatividades en el campo de la protección de datos personales, protección de información, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, entre otros.

Para la implantación del sistema de gestión de la seguridad de la información (SGSI) la norma incorpora el típico PDCA (Plan-Do-Check-Act) que significa "Planificar-Hacer-Controlar-Actuar" con un enfoque de mejora continua. Este ciclo es materializado en la norma en cuatro fases:

- Fase de planificación: Esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y seleccionar los controles adecuados de seguridad (La norma contiene un catálogo de 133 posibles controles).
- Fase de implementación: Esta fase implica la realización de todo lo planificado en la fase anterior.

- Fase de revisión: El objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar el cumplimiento de los objetivos establecidos.
- Fase de mantenimiento y mejora: El objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficiencia del SGSI.

4.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un SGSI se puede definir como el conjunto de estrategias y políticas que engloban la gestión de la seguridad de la información, considerando está el activo más importante y valioso para las organizaciones, a la vez de ser el más vulnerable. Formalmente, según (Huerta, 2004) es un “Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información”. Al, respecto las empresas deben alcanzar y mantener niveles de seguridad exigidos, para lo cual implantan tareas que lo garanticen; su realización comprende la denominada Gestión de la seguridad. De esta forma, la seguridad deja de ser un producto para asumirse como un proceso constante y complejo de controlar. Los SGSI o ISMS por sus siglas en inglés "Information Security Management System" tienen su origen en el estándar para la seguridad de la información ISO/IEC 27001 que establece etapas, elementos, hitos, propósitos y consecuentemente, un proceso claro para la administración organizada y confiable de la seguridad de la información.

4.3.1 IMPLANTACIÓN DE SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requerimientos de seguridad de la Organización. Es estándar más extendido para la definición e implantación de un SGSI es el ISO/IEC 27001:2005.

El SGSI se basa en la aplicación del Ciclo de Deming, o de la mejora continua en el ámbito de la seguridad de la información:

- Planificar: establecer las políticas, objetivos, normas, procesos, procedimientos necesarios para gestionar los riesgos y mejorar la seguridad de la información, de acuerdo a las necesidades y requerimientos de la organización.

- Ejecutar: implantar y operar las políticas, procesos, procedimientos y controles definidos.

- Verificar: evaluar la eficacia y eficiencia de las políticas, procesos, procedimientos y controles para lograr los objetivos de seguridad de la información definidos. Identificar aquellas no conformidades con la planificación realizada.

- Actuar: definir las medidas preventivas y correctivas destinadas a solucionar las no conformidades detectadas, a mejorar el cumplimiento de los requerimientos de seguridad de la información definidos y adaptar el sistema a los cambios internos y externos relevantes.

Un SGSI conforme con el estándar ISO/IEC 27001:2005 consta, fundamentalmente, de los siguientes elementos:

- ✓ Análisis de riesgos
- ✓ Cuerpo normativo, incluyendo:
  - Definición del alcance del SGSI
  - Política de seguridad.
  - Declaración de aplicabilidad, que detalla los controles necesarios para alcanzar los objetivos de seguridad fijados.
  - Procesos de seguridad.
  - Procedimientos de seguridad.
  - Registros de seguridad

- ✓ Asignación de funciones y responsabilidades:
  - Dirección

- Ejecución de procesos y controles
- Revisión del SGSI
- Formación a todos los participantes

4.4 OTRAS NORMAS Y ESTÁNDARES

Como se ha mencionado, el primer fundamento para buenas prácticas de seguridad de la información son los estándares o normas, a partir de éstos se obtiene una orientación hacia el cumplimiento de las mismas. Otros estándares más conocidos y usados en la actualidad son: o COBIT o RFC2196 o TCSEC (Trusted Computer Security, militar, US, 1985). ITSEC (Information Technology Security, europeo, 1991). Common Criteria (internacional, 1986-1988). o ISO/IEC 17799 (Basada en la BS 7799; 1) también llamada ISO 27002 (británico + internacional, 2000). o ISO 27001 (Basada en 7799; 2) Sin embargo, a partir de que ISO 17799 ha sido aceptado como estándar internacional, es el más desarrollado y aplicado en las organizaciones por brindar una guía de buenas prácticas de seguridad (Huerta, 2004). La adaptación española se denomina UNE- ISO/IEC 17799. La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información. De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). A pesar de tratarse de una norma no certificable, recoge la relación de controles a aplicar (o al menos a evaluar) para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma UNE- ISO/IEC 27001 (tiene su origen en UNE 71502, versión española certificable). Entre tanto, ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. Se calculan aproximadamente 23972 empresas certificadas a nivel mundial en el año 2014 (7181 en Japón, 2261 en Reino Unido, 86 en Brasil, 7 en Ecuador, etc.).

5. METODOLOGÍA

5.1 PROCEDIMIENTO

Para cumplir con los objetivos específicos propuestos, y en busca de satisfacer el objetivo general, se propuso el siguiente esquema para cubrir las necesidades del proyecto.

- **Fase I:** Recolección de información.

  El trabajo inicial consistió en la recopilación de información necesaria para la realización de un estado del arte enfocado al estado del Sistema de Gestión de Seguridad de la Información. Con el objetivo de obtener un referente teórico para la toma de requerimientos.

- **Fase II:** Definición y alcance del modelo

  A continuación, se comenzó a dar forma a la aplicación comenzando con la definición del modelo conceptual, a partir de los requerimientos previamente establecidos. Además de determinar el alcance del modelo conceptual y su respectiva complejidad.

- **Fase III:** Desarrollo de la herramienta

  Seleccionando el Framework de trabajo, el lenguaje de programación y la metodología de desarrollo más ajustada a las necesidades. Dando importancia a la realización de los planos de software utilizando el estándar UML. La razón de su escogencia radica en la simplicidad y legibilidad del lenguaje, sin que esto represente pérdida alguna en la expresividad de la información contenida en los planos. Además de esto, UML permite crear modelos de software para aplicaciones bajo cualquier dominio traducibles directamente a código fuente.

  Luego se plasmaron en código fuente todos los planos de software construidos mientras se realizaba paralelamente la documentación del sistema y el manual del usuario.

- **Fase IV:** Pruebas, despliegue y presentación

  En esta fase final, se llevaron a cabo pruebas que nos permitieron decidir si la aplicación funcionaba correctamente. Inicialmente se ejecutaron todas las pruebas unitarias, las cuales se ejecutaron también durante todo el desarrollo de la herramienta, luego se ejecutaron las

pruebas de integración. Una vez finalizado este ciclo. El objetivo de estas pruebas finales era medir la calidad del producto y verificar si cumplía con los objetivos planteados.

La metodología ágil SCRUM, una de las pioneras en el campo de la ingeniería de software y nombrada así debido a su representación pictórica, fue la seleccionada para la realización de la herramienta de apoyo. Fue escogida porque refuerza la noción de trabajar en entornos complejos, además este modelo permite un seguimiento a través de reuniones diarias y mensuales que generan un entregable significativo (Peres, A. L., & Meira, S. L., 2015).

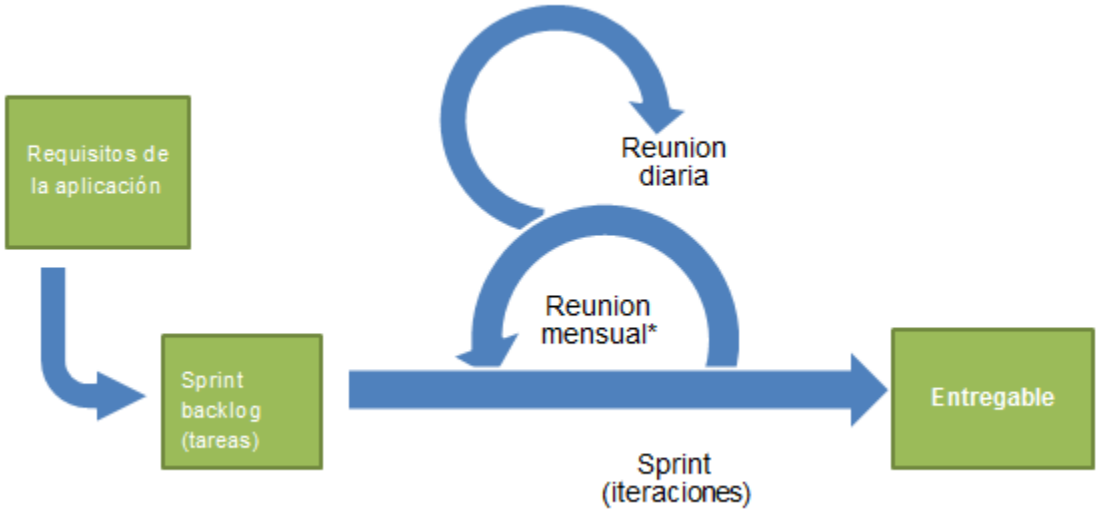


Ilustración 1. Estructura de metodología SCRUM. (Law, E.L. & Lárusdóttir, M.,2015)

5.2 RECOLECCIÓN DE INFORMACIÓN

En este apartado se presenta la información recopilada a través de las Técnicas de recolección de información aplicadas en la etapa de documentación y apropiación de conceptos, estándares y demás.

5.2.1 ANÁLISIS DE CONTENIDO: ESTUDIO DE ESTANDAR

De acuerdo con el objetivo general y la finalidad que conlleva el proceso de implantación de un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO 27001, se hace necesaria la apropiación, aclaración y definición de conceptos referentes al estándar. A continuación se presenta el resultado de análisis de contenido, a partir de artículos, ponencias, informes, reportes estadísticos, documentos de páginas web, consultas a expertos, experiencias materializadas en blog personales, entre otros.

5.2.1.1 ISO 27001

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

El objetivo de esta norma es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Es decir, especifica los requerimientos para implantar ese sistema de gestión y la implementación de los controles de seguridad acorde a las necesidades de las organizaciones.

El diseño e implementación de un SGSI de cualquier organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos, empleados y tamaño y estructura de la organización.

5.2.2 ENFOQUE DEL PROCESO

La ISO 27001 adopta un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
b. Implementar y operar controles para manejar los riesgos de la seguridad de la información.
c. Monitorear y revisar el desempeño y la efectividad del SGSI.
d. Mejoramiento continuo en base a la medición del objetivo.

5.2.3 MODELO DEL PROCESO

Este estándar acoge el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA) como se ilustra en la ilustración 2. Por lo tanto, la ISO 27001 está diseñado para que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado, de este modo abarca todos los tipos de organizaciones.

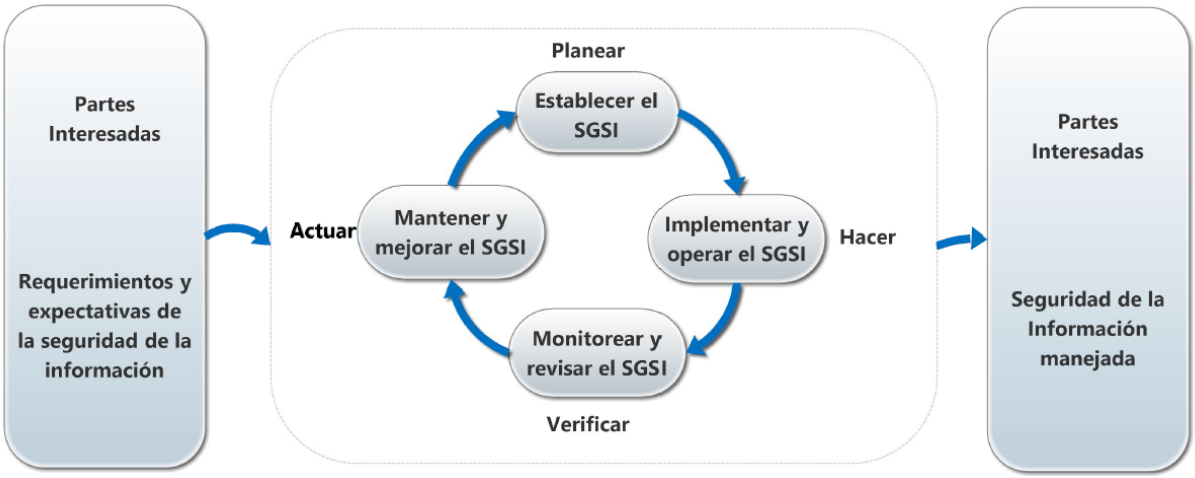


Ilustración 2. Modelo de proceso PDCA aplicado por el estándar a los procesos SGSI. Fuente: (Estándar Internacional ISO/IEC 27001, 2005).

El modelo PDCA refleja un proceso cíclico donde las entradas enfocadas a los requerimientos y expectativas propias de la organización, obtiene como salida la gestión o manejo de la seguridad de información de la misma, pasando por las siguientes etapas:

1. **Establecer el SGSI**
2. **Implementar y operar el SGSI**
3. **Monitorear y revisar el SGSI**
4. **Mantener y mejorar el SGSI**

Por otra parte, es importante mencionar que la gerencia debe proporcionar evidencia de su compromiso en el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI. Así mismo, la organización debe proveer los recursos necesarios y asegurar que todo el personal al que se le asignó responsabilidades definidas en el SGSI sea competente para realizar las tareas.

5.2.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un Sistema de gestión de seguridad de la información (SGSI) es el concepto central sobre el que se construye la ISO 27001. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado, continuo y conocido por toda la organización. Con el fin de garantizar la seguridad de la información, la cual consiste en preservar la confidencialidad (no disposición de la información a entes no autorizados), integridad (mantenimiento y exactitud de la información) y disponibilidad (acceso de la información cuando se requiera), así como como de los sistemas implicados en su tratamiento, dentro de una organización. Por lo tanto, estos tres términos constituyen la base de la seguridad de la información.

Por otra parte, la información junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos

fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

En general, un SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

5.2.4.1 IMPLANTACIÓN

Para establecer y gestionar un SGSI en base a la norma ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

5.2.4.1.1 PLAN (PLANIFICAR): ESTABLECER EL SGSI.

En esta primera fase se realiza un estudio de la situación de la Organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas.

Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello un hito importante dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así

mismo se hace necesario una Gestión para dichos riesgos de cara a reducirlos en la medida de lo posible.

El resultado de este Análisis y Gestión de Riesgos será establecer una serie de prioridades en las tareas a realizar para minimizar dichos riesgos. Puesto que los riesgos nunca van a desaparecer totalmente, es importante que la Dirección de la Organización asuma un riesgo residual, así como las medidas que se van a implantar para reducir al mínimo posible dicho riesgo residual.

5.2.4.1.2 DO (HACER): IMPLEMENTAR Y UTILIZAR EL SGSI.

En esta fase se lleva a cabo la implantación de los controles de seguridad escogidos en la fase anterior. En dicha implantación se instalarán dispositivos físicos (Hardware, Software), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros).

Dentro de esta fase es muy importante dedicar un tiempo a la concienciación y formación del personal de la empresa de cara a que conozcan los controles implantados.

5.2.4.1.3 CHECK (VERIFICAR): MONITOREAR Y REVISAR EL SGSI.

Es importante que la Organización disponga de mecanismos que le permitan evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

5.2.4.1.4 ACT (ACTUAR): MANTENER Y MEJORAR EL SGSI.

En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se

suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se suele esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

Por otra parte, uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene porqué ser toda la organización).

5.2.5 COMPATIBILIDAD CON OTROS SISTEMAS

El SGSI puede estar integrado con otro tipo de sistemas (ISO 9001, ISO 14001…).

La propia norma ISO 27001 incluye en su anexo C una tabla de correspondencias de ISO 27001:2005 con ISO 9001:2000 e ISO 14001:2004 y sus semejanzas en la documentación necesaria, con objeto de facilitar la integración.

Es recomendable integrar los diferentes sistemas, en la medida que sea posible y práctico.

En el caso ideal, es posible llegar a un solo sistema de gestión y control de la actividad de la organización, que se puede auditar en cada momento desde la perspectiva de la seguridad de la información, la calidad, el medio ambiente o cualquier otra.

5.3. DELIMITACIÓN DEL PROYECTO

El proceso de implantación de un SGSI aborda una amplia tarea en cuanto a recursos, políticas, documentación y requerimientos basados en la norma ISO 27001. El desarrollo de este sistema comprende la gestión de diferentes componentes bajo el alcance de cualquier organización. Por lo tanto, la gestión completa de dicho proceso enmarcada en el modelo PDCA, requiere la total fundamentación y realización de componentes que generan el éxito de la misma. Estos componentes requieren dedicación, amplio desarrollo y conformidad con el alcance de la organización.

El proyecto referente se limitará a desarrollar módulos que marcan mayor importancia en el proceso de desarrollo del SGSI. De igual manera, los avances o trabajos futuros tendrán como objetivo complementar lo que requiere todo el ciclo de implantación del mismo.

En efecto, los componentes que se convertirán como productos y apoyaran el proceso de implantación de un SGSI son: un módulo para el análisis de riesgos, en este se fundamenta o aborda el núcleo de un SGSI, el cual permitirá la gestión y seguimiento de Análisis de Riesgos según los requisitos en la materia definidos por la norma ISO 27001; módulo de activos, para la gestión e inventariado de todos los activos de información;; gestión documental, representa el módulo a nivel de producto que enmarca toda la documentación organizada y requerida por la norma referente, por lo que ayuda y mantiene todo material documental a la mano para procesos de auditorías y certificación del sistema de gestión; y un módulo de gestión de roles para mantener compromisos de toda la organización en tareas definidas para el desarrollo del SGSI, además de buscar el apoyo total e incondicional de la alta gerencia en cuanto a procesos de desarrollo del sistema se refiere.

Con un modelo orientado a procesos ejecutado bajo un ciclo PDCA, con características procedimentales que apoyen de inicio a fin todo el proceso de implantación, facilitando el debido proceso y manteniendo la continuidad en el negocio.

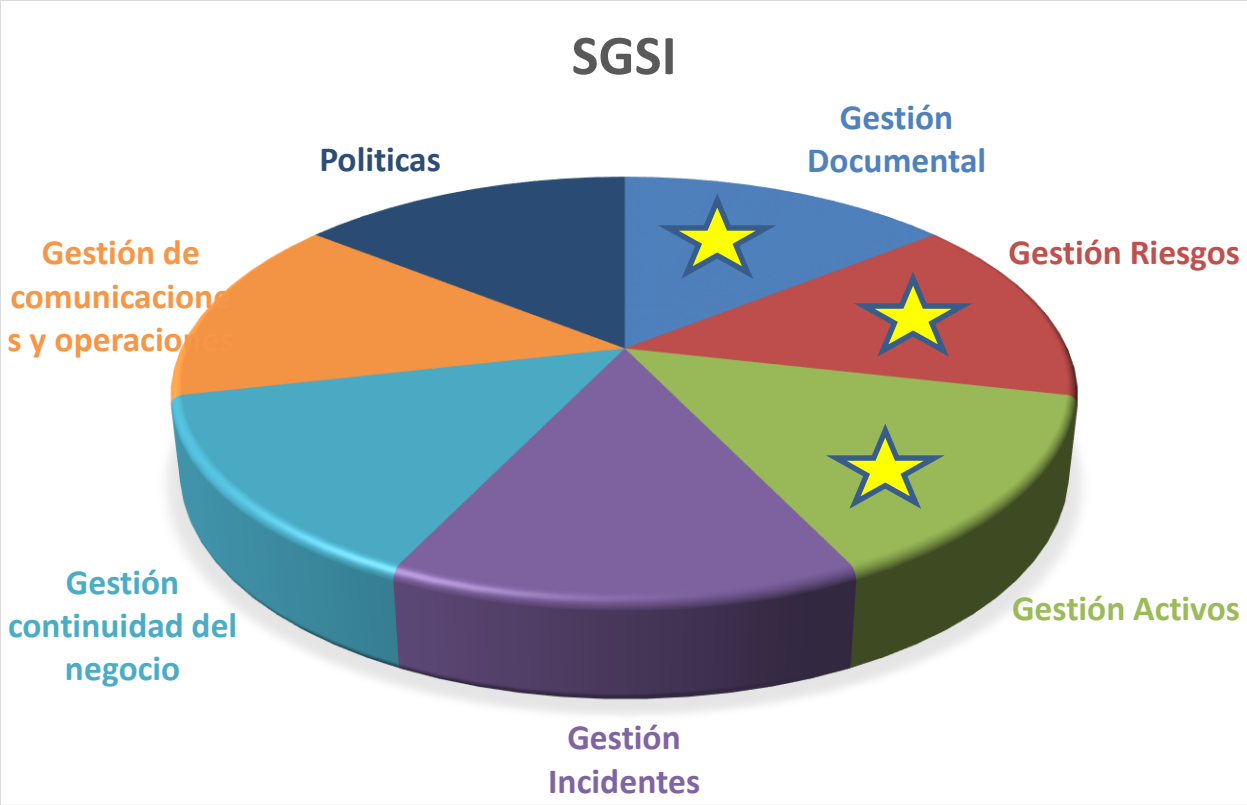


Ilustración 3. Delimitación del proyecto, componentes que comprende un SGSI. Fuente: Grupo de trabajo

5.4 DEFINICIÓN DE MÓDULOS

5.4.1 MÓDULO DOCUMENTAL

El componente gestión documental encargado de llevar el control documental de los procesos asociados a la implantación del SGSI, desde inicio hasta su fase de mantenimiento continúo. La interacción con el Sistema bajo sus fases de desarrollo, implementación, puesta en marcha y mantenimiento es de forma paralela (Ilustración 4).

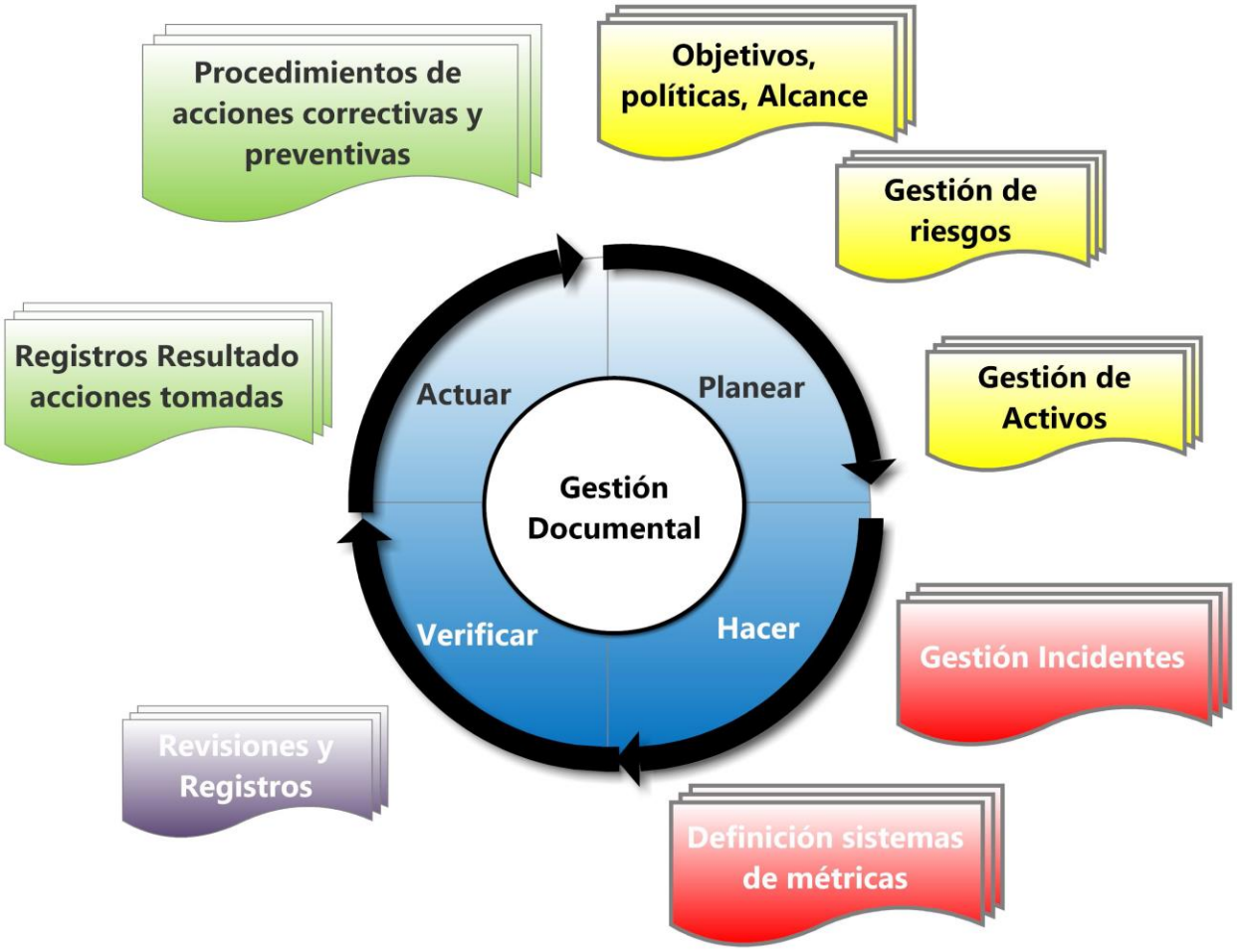


Ilustración 4. Modelo gestión documental. Fuente: Grupo de trabajo

La figura anterior representa la interacción durante el ciclo PHVA del proceso de implantación de un SGSI en las organizaciones. El documento durante este proceso se expone a participar de varios estados siguiendo con la base de modelo de Deming y forzarlo al mejoramiento continuo, la siguiente figura muestra el flujo de estados de un documento durante el proceso de implantación con la herramienta de apoyo:

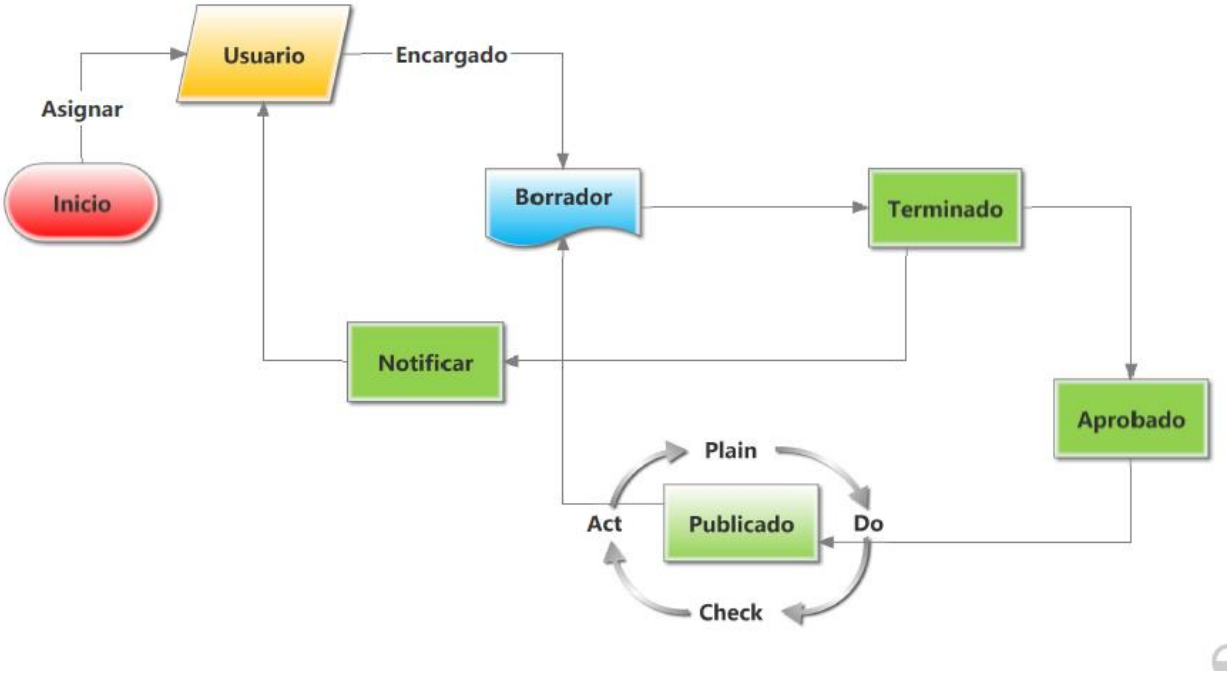


Ilustración 5. Workflow estados de documento. Fuente: Grupo de trabajo

El documento siempre estará asociado a un encargado quien digitará y almacenara el documento en un estado borrador, pasando por un estado de terminando para posterior verificación y publicación, dicho documento podrá devolverse al estad inicial borrador para ser modificado, terminado, aprobado y publicado, con esto se cumple con el modelo de mejoramiento continuo de toda la documentación generada.

5.4.1.1 INTERACCIÓN MODULO GESTIÓN DOCUMENTAL, OTROS MÓDULOS

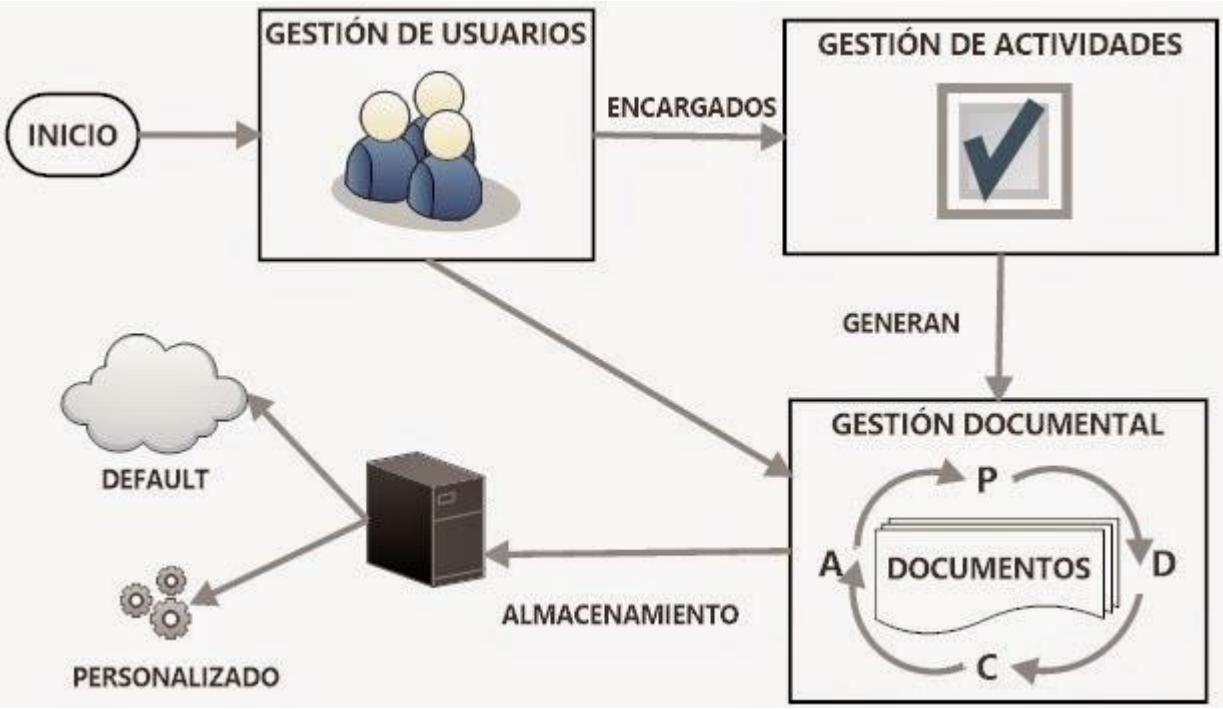


Ilustración 6. Interacción con otros módulos. Fuente: Grupo de trabajo

La anterior figura, representa la interacción donde un usuario es el encargado a partir de una actividad generar una documentación donde su ciclo de vida y mejoramiento continuo está asociado a un almacenamiento personalizado o por defecto.

5.4.1.2 VERSIÓN DE DOCUMENTOS

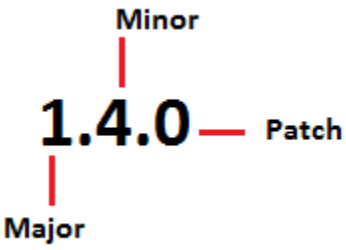


Ilustración 7. Versionamiento de documento. Fuente: Grupo de trabajo.

- **Major**: Incremento cuando el documento pasa de estado **aprobado – publicado**

- **Minor**: Incremento cuando el documento cambia de **cualquier estado** excepto publicado
- **Patch**: Modificaciones que se hacen al documento internamente en **estado borrador**.

5.4.1.3 CARACTERÍSTICAS:

1. Permite identificar el estado de los documentos.
2. Previene la utilización de documentos obsoletos.
3. Compromiso bajo la gestión de roles y asignación de actividades.
4. Garantiza la disponibilidad, accesibilidad y seguimiento a documentos asignados.
5. Permite trabajar bajo procedimientos estrictamente del estándar ISO 27001.
6. Modelo de trabajo cíclico.

5.4.2 MÓDULO ANÁLISIS DE RIESGOS

5.4.2.1 CONCEPTOS GENERALES

A pesar de que existe un elevado número de metodologías de análisis de riesgos de seguridad de la información, que se describen posteriormente en este documento, existe un modelo y unos principios básicos comunes a todas ellas que se describen a continuación.

La base sobre la que se apoyan las metodologías actuales de análisis de riesgo es el cálculo de probabilidades.

5.4.2.1.1 ELEMENTOS DEL MODELO

Las metodologías de análisis de riesgos de seguridad de la información parten de la necesidad de identificar formalmente los elementos a proteger. Estos elementos se recogen en un inventario de activos de información, considerando como tales aquellos elementos que tienen valor para la Organización.

Los activos deben valorarse en función de un conjunto de requerimientos de seguridad. Estos requerimientos varían entre las diferentes metodologías, si bien existe consenso sobre tres de ellas: confidencialidad, integridad y disponibilidad. Esto significa que para cada activo de información debe valorarse de forma independiente el coste que tendría para la Organización una pérdida total de su confidencialidad, de su integridad y de su disponibilidad, así como de los otros requerimientos de seguridad que se consideren en cada caso.

Una vez identificados los activos, deben identificarse las amenazas que pueden causar pérdidas sobre estos activos, teniendo en cuenta los diferentes requerimientos de seguridad. Algunas metodologías especifican un elemento intermedio, las vulnerabilidades, consideradas como las debilidades que hacen que un determinado activo pueda ser vulnerable a una determinada amenaza.

Identificadas las amenazas, debe identificarse las salvaguardas que permiten proteger a los activos de las diferentes amenazas.
La cuantificación de los distintos elementos que forman parte del modelo de análisis de riesgos se aborda en los siguientes apartados.

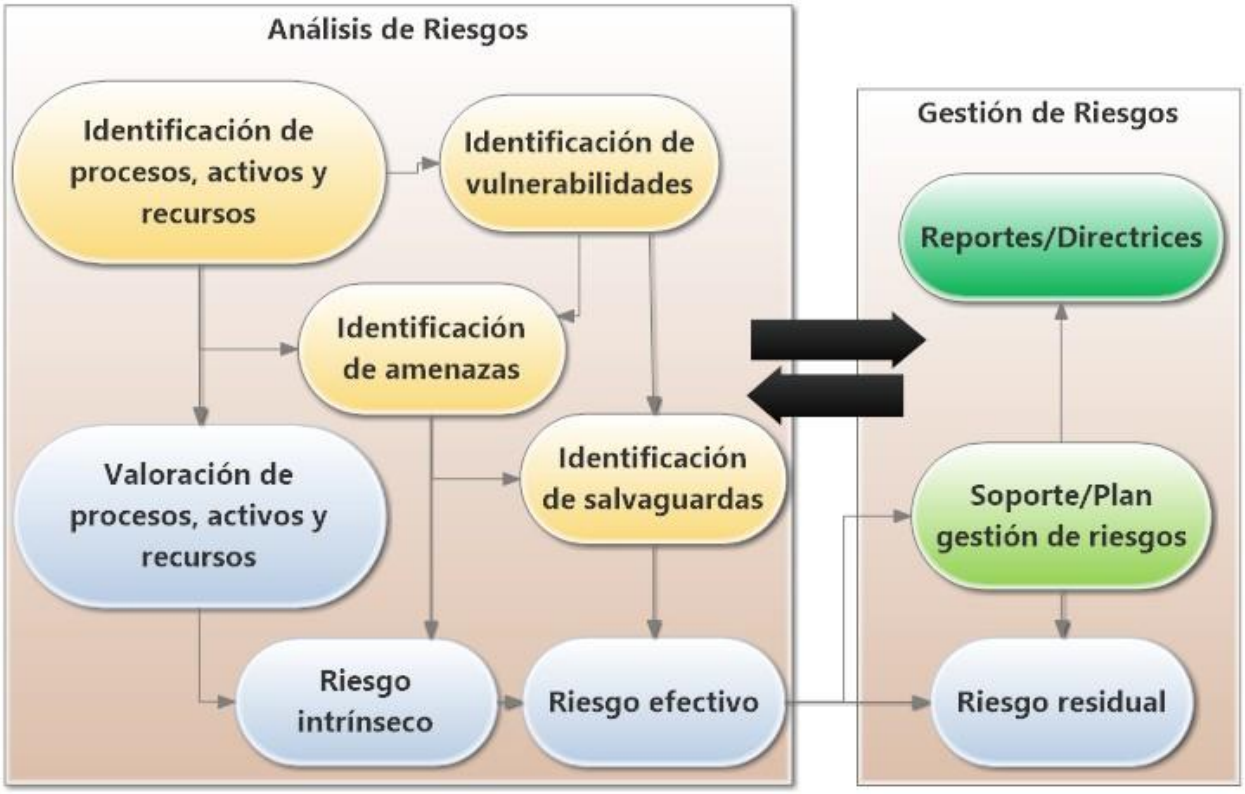


Ilustración 8. Modelo generalizado para análisis de riesgos. Fuente: Grupo de trabajo

5.4.2.1.2 PÉRDIDA ESPERADA (SINGLE LOSS EXPECTANCY – SLE)

Considerando un único activo de información (A), un único requerimiento de seguridad (R) y una única amenaza (T) se puede estimar la pérdida económica esperada en caso de que la amenaza se realice.

Generalmente, la pérdida esperada no se representa en términos absolutos, sino como un porcentaje de degradación referido al valor total del activo para el requerimiento considerado. De esta forma, se puede considerar:

$$SLE(A, R, T) = Valor(A, R) \times Degradación(A, R, T)$$

Dado que la valoración se realiza generalmente respecto a diferentes requerimientos de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, etc.), la pérdida total

debida a la realización de una amenaza sobre un activo se calculará como la suma de las pérdidas en cada requerimiento:

$$SLE(A,T) = \sum_{R} SLE(A,R,T) = \sum_{R} Valor(A,R) \times Degradación\ (A,R,T)$$

Dado que existen diversos activos a los que puede afectar la amenaza considerada, la pérdida esperada total es la suma de la pérdida provocada en cada uno de los activos:

$$SLE(T) = \sum_{A} SLE(A,T) = \sum_{A}\sum_{R} Valor(A,R) \times Degradación(A,R,T)$$

5.4.2.1.3 PÉRDIDA ANUAL ESPERADA (ANNUAL LOSS EXPECTANCY – ALE)

Una vez conocida la pérdida provocada por la realización de cada amenaza, en caso de que ocurra, se debe considerar la probabilidad de que la amenaza se realice efectivamente en el periodo de un año. La pérdida anual esperada provocada por una amenaza puede definirse, como:

$$ALE = P(T) \times SLE(T) = P(T) \times \sum_{A}\sum_{R} Valor(A,R) \times Degradación(A,R,T)$$

La pérdida anual esperada teniendo en cuenta todas las amenazas puede definirse, como:

$$ALE = \sum_{T} P(T) \times SLE(T) = \sum_{T}\left(P(T) \times \sum_{A}\sum_{R} Valor(A,R) \times Degradación(A,R,T)\right)$$

Debido a que existen amenazas para las que se espera más de una ocurrencia anual, el concepto de probabilidad se sustituye por el concepto de frecuencia (Annual Rate of Occurrence – ARO). Por ello, la definición de pérdida anual esperada queda ligeramente modificada como:

$$ALE = \sum_{T} ARO(T) \times SLE(T)$$

$$= \sum_{T} \left(ARO(T) \times \sum_{A} \sum_{R} Valor(A,R) \times Degradación(A,R,T) \right)$$

5.4.2.1.4 CALCULO DEL EFECTO DE SALVAGUARDAS

Las salvaguardas (S) implantadas permiten reducir la frecuencia de ocurrencia de las amenazas o la degradación causada por ellas en caso de realizarse.

Teniendo en cuenta la reducción de la frecuencia, se puede considerar P(S) la probabilidad de que una salvaguarda sea eficaz en la prevención de la ocurrencia de una amenaza determinada. Por tanto, puede considerarse que:

$$P(A/S) = P(A) \times (1 - P(S))$$

Dado el conjunto de salvaguardas implantadas, la probabilidad de ocurrencia puede calcularse como:

$$P(A/S) = P(A) \times \prod_{S} (1 - P(S))$$

Siendo P(S) la probabilidad de que la salvaguarda S sea eficaz mitigando la amenaza A.

Considerando el concepto de frecuencia en lugar del de probabilidad, la frecuencia anual de ocurrencia se puede calcular como:

$$ARO' = ARO \times \prod_{S} (1 - P(S))$$

De forma análoga, se puede calcular la degradación una vez aplicadas las salvaguardas:

$$Degradación(A,R,T)' = Degradación(A,R,T) \times \prod_{S} (1 - I(S))$$

Donde I(S) es la reducción del impacto provocado por la acción de la salvaguarda S.
Por tanto, el cálculo del riesgo residual puede definirse como:

$$ALE = \sum_{T}\Bigg(ARO(T) \times \prod_{S}(1 - P(S) \times \sum_{A}\sum_{R} Valor(A,R) \times Degradación(A,R,T) \times \prod_{S}(1 - I(S))\Bigg)$$

Debido al elevado coste computacional de estos cálculos, algunas metodologías simplifican el cálculo definiendo un porcentaje fijo de reducción de la probabilidad y de la degradación para cada salvaguarda implantada.

5.4.2.1.5 MÉTODOS CUALITATIVOS

Los conceptos desarrollados hasta ahora muestran los principios básicos para un análisis de riesgos cuantitativo, basado en el cálculo de pérdidas en términos monetarios.

La valoración de los diferentes requerimientos de seguridad puede realizarse de forma cuantitativa o cualitativa.

La valoración de los diferentes requerimientos de seguridad puede realizarse de forma cuantitativa o cualitativa.

La **valoración cuantitativa** supone establecer un valor numérico para cada uno de los requerimientos de seguridad. Este valor se calcula en términos de las pérdidas esperadas en caso de incumplimiento de dicho requerimiento. Los principales conceptos de pérdidas a tener en cuenta en una valoración cuantitativa incluyen los siguientes:

- Coste de reposición de los activos y recursos de información perdidos: adquisición, instalación, recuperación, etc.
- Coste de mano de obra invertida en recuperar y/o reponer los activos y recursos de información.

- Lucro cesante debido a la pérdida de ingresos provocada por la parada degradación del funcionamiento de los diferentes procesos afectados.

- Capacidad de operar, debido a la pérdida de confianza de los clientes y proveedores, que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones y penalizaciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos
- Daño a personas.
- Daños medioambientales.
- Daños reputacionales: percepción del mercado, pérdida de clientes, dificultad para acceder al crédito, coste de las campañas de marketing necesarias para recuperar la reputación perdida, etc.
- Valor de los secretos desvelados: secreto industrial, secreto comercial, etc.

La **valoración cualitativa** supone asignar un valor de una escala definida para cada uno de los requerimientos de seguridad. Este valor se calcula en base a un conjunto de características que define cada una de las categorías de la escala, basadas en las descritas para la valoración cuantitativa.
La valoración cuantitativa es más precisa, pero supone un mayor esfuerzo y dificultad, por la necesidad de valorar los distintos conceptos de pérdida en términos generalmente económicos.

Debido a la dificultad y el coste de realizar un análisis cuantitativo, muchas metodologías de análisis de riesgos han desarrollado enfoques cuantitativos, que permiten ubicar el riesgo en una escala de órdenes de magnitud. Este análisis se conoce como análisis cualitativo.

Los principios del análisis cualitativo son los mismos que los del análisis cuantitativo, sustituyendo los cálculos aritméticos por la aplicación de tablas.

5.4.2.1.6 MÉTODO MIXTO

Debido a que los métodos cuantitativos y cualitativos tienen ventajas e inconvenientes, existen alternativas para combinar ambos métodos de forma que se obtengan las mayores ventajas de cada uno. Esos métodos que presentan algunas características de los métodos cuantitativos y otras características de los métodos cualitativos se denominan métodos mixtos.

5.4.2.1.7 MAGERIT

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Administraciones Pública.
La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 3.0, publicada en 2012.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública Española.

Dispone de una herramienta de soporte, PILAR II (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

La metodología consta de tres volúmenes:

Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.

Volumen II – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:

- Tipos de activos
- Dimensiones y criterios de valoración

- Amenazas
- Salvaguardas

Volumen III – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:

- Técnicas específicas para el análisis de riesgos:
  - Análisis mediante tablas
  - Análisis algorítmico
  - Árboles de ataque
- Técnicas generales
  - Análisis coste-beneficio
  - Diagramas de flujo de datos (DFD)
  - Diagramas de procesos
  - Técnicas gráficas
  - Planificación de proyectos
  - Sesiones de trabajo: entrevistas, reuniones y presentaciones
  - Valoración Delphi

La metodología MAGERIT se puede resumir gráficamente :

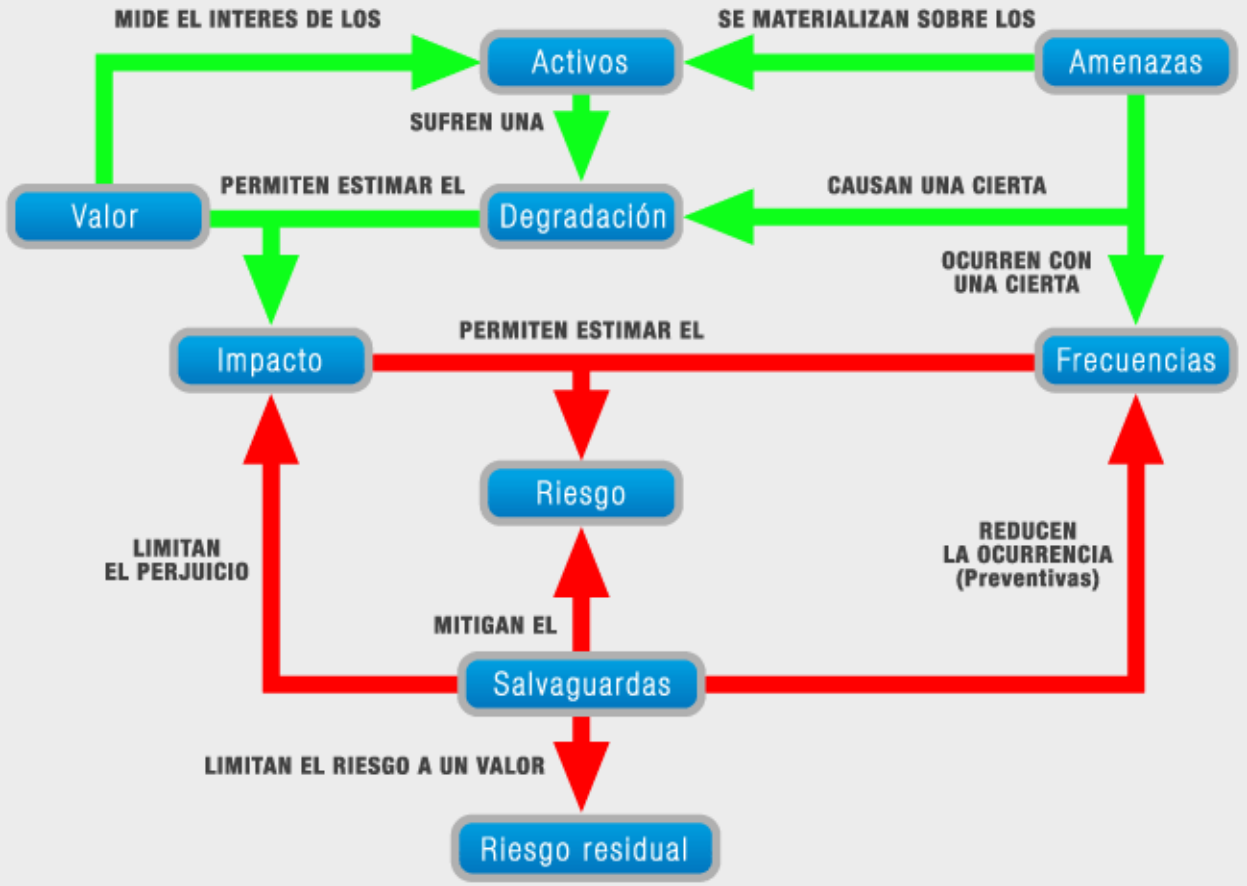


Ilustración 9. Modelo de análisis de riesgo. (MAGERIT, 2012)

Nombre	**Origen**			
	Descripción	**Organización**	**País**	**Año**
ISO TR 13335:2004	Tecnología de la información – Guías para la gestión de la seguridad de las TI	ISO – International Organization for Standardization	**Suiza**	**2004**
ISO 27005:2013	Tecnologías de la información – Técnicas de seguridad –	ISO	**Suiza**	**2013**

	Gestión del riesgo de seguridad de la información			
UNE 71504:2008	Metodología de análisis y gestión de riesgos para los sistemas de información	AENOR – Asociación Española de Normalización y Certificación	**España**	**2008**
BS 7799-3:2006	Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la gestión de riesgos de seguridad de la información	BSI – British Standards Institution	**Reino Unido**	**2006**
AS/NZS 4360:2004	Gestión de riesgos	AS/NZ – Australian Standards / New Zealand Standards	**Australia / Nueva Zelanda**	**2004**
MAGERIT	Metodología de análisis y gestión de riesgos de IT	Ministerio de Administraciones Públicas	**España**	**2012**
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Universidad de Carnegie Mellon	**Estados Unidos**	**2001 - 2007**
CRAMM	CCTA Risk analysis and Management	CCTA – Central Computing and Telecommunications	**Reino Unido**	**2003**

	Method	Agency		
NIST SP 800 – 30	Guis de gestión de riesgos para sistemas de tecnología de nformación	NIST – National Institute of Standards and Technology	**Estados Unidos**	**2002**
IRAM	Information Risk Analysis Methodologies	ISF – Information Security Forum	**Reino Unido**	**2006**
CORAS	Construct a platform for Risk Analysis of Security critical systems	SINTEF y otros	**Noruega**	**2001-2007**
SOMAP	Security Officers Management & Analysis Project	SOMAP.org	**Suiza**	**Beta4**
FAIR	Factor Analysis of Information Risk	Risk Management Insight	**Estados Unidos**	**2005**

Tabla 1. Comparación de otras metodologías de análisis de riesgos. Fuente: Grupo de trabajo

5.4.2.2 DEFINICIÓN DEL MODELO

Teniendo en cuenta las distintas metodologías disponibles para hacer el análisis de riesgos, se decidió desarrollar una metodología adaptada específicamente a las necesidades de la Organización.

Las características deseables del módulo a desarrollar son los siguientes:

- ✓ Basada en estándares, para aprovechar conocimiento y herramientas y permitir la realización de comparaciones con otras organizaciones.

- ✓ Sencillez y facilidad de uso, tanto en el momento de la primera implantación como en el mantenimiento.

- ✓ Enfocada a los procesos de negocio y de soporte de la Organización.

- ✓ Modular y adaptable, que pueda adaptarse a diferentes entornos.

- ✓ Objetiva, los resultados no deben depender de quién aplique el módulo de análisis de riesgos ni de cómo lo haga.

Dadas las características deseables para el modulo, se han desarrollado unos principios para su desarrollo:

- ✓ Metodología mixta, con entrada de datos cualitativa, para facilitar la comunicación entre las distintas partes que deben participar en el análisis y métodos de cálculo cuantitativos para aprovechar la mayor eficiencia computacional y mayor precisión en los resultados.
- ✓ Eliminación de los elementos que aporten menor valor en la consecución de los objetivos, en aras de mayor facilidad de uso y claridad.
- ✓ Que disponga de diversos inventarios de tipos de activos, amenazas y salvaguardas, de modo que se pueda utilizar con sencillez y que se pueda adaptar fácilmente a distintas necesidades y objetivos del análisis.

- ✓ Que disponga de una herramienta de soporte específica que facilite la entrada de datos y la realización de los cálculos.

- ✓ Que disponga de todos los elementos habituales que permiten dotar de objetividad al proceso: acuerdo entre varios expertos, definición de baremos objetivos de valoración y proporcionar ejemplos con valores de referencia reales.

5.4.2.3 FASES DE MODELO

En primer lugar, el modelo diferencia dos fases diferenciadas:

Análisis de riesgos, que comprende la obtención de información referente a procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas.

Gestión de riesgos, que comprende la definición de la estrategia a seguir para ajustar el nivel de riesgo a los requerimientos de la Organización.

En este modelo se distinguen por colores tres tipos de elementos:

- Inventario de activos, vulnerabilidades, amenazas y salvaguardas.
- Valoración de activos, vulnerabilidades, amenazas y salvaguardas para la obtención del riesgo intrínseco, efectivo y residual.
- Plan de gestión del riesgo.

Por último, el modelo especifica que el análisis de riesgos debe considerarse un ciclo por el que, tras la gestión del riesgo se sitúa una nueva iteración del análisis de riesgos que permite obtener la evolución de los procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas y de esta forma reajustar permanentemente el nivel de riesgo a los requerimientos de la Organización.

5.4.2.3.1 VALORACIÓN DE ACTIVOS

Se considera **activo de información** a toda aquella información que tiene valor para la Organización en la medida en que le permite el cumplimiento de sus objetivos.
En oposición, los **recursos de la información** tienen un valor intrínseco generalmente despreciable para la Organización, y son necesarios en la medida en que permiten el manejo de los activos de información.

Los activos de información son intangibles, esto es, la tarea no consiste en identificar aplicaciones ficheros o bases de datos sino la información que se utiliza en el proceso desde un punto de vista conceptual.

Para facilitar un método sistemático para la identificación de los activos de información existen dos enfoques que pueden utilizarse independiente o conjuntamente:

- Enfoque **top-down** (de arriba abajo), que consiste en inferir los activos de información relacionados con los procesos a partir de la descripción de los procesos.

- Enfoque **bottom-up** (de abajo arriba), que consiste en identificar las principales aplicaciones, ficheros y bases de datos utilizados por el proceso y conceptualizar la información que almacenan y procesan. En este enfoque no se debe olvidar la importancia de la información no automatizada que pueda ser relevante para el análisis y que en función del alcance definido, puede formar parte del alcance del análisis de riesgos.

Para cada activo de información identificado se debe registrar, al menos, la siguiente información:

- ✓ Nombre del activo de información.
- ✓ Descripción del contenido del activo de información.

- ✓ Descripción del uso que se da a esta información en el contexto del proceso considerado y de otros procesos que puedan estar relacionados.
- ✓ Recursos de información que se utilizan para procesar y almacenar el activo de información.

Una vez inventariados los activos de información es necesario identificar y documentar el valor que su seguridad representa para la Organización. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes teniendo en cuenta el alcance y el objetivo definido para el análisis de riesgos.

El valor que tienen los activos de información para la Organización en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de esta metodología, requerimientos de seguridad.

La valoración se deberá realizar mediante una ponderación de las pérdidas ocasionadas para la Organización en caso de que se pierda, debido a la realización de una amenaza, cada uno de los requerimientos de seguridad definidos para los diferentes activos de información.

En aras de la adaptabilidad, la metodología no define un conjunto de requerimientos de seguridad cerrado a utilizar, que deberá definirse para cada análisis, si bien, a título orientativo, se proponen los siguientes requerimientos de seguridad que pueden valorarse al definir los requerimientos a considerar, procedentes de diversas metodologías:

- ✓ Confidencialidad (generalmente aceptado)
- ✓ Integridad (generalmente aceptado)
- ✓ Disponibilidad (generalmente aceptado)
- ✓ Trazabilidad - Responsabilidad – Auditabilidad
- ✓ Autenticidad - No repudio
- ✓ Fiabilidad
- ✓ Efectividad
- ✓ Eficiencia

- ✓ Cumplimiento
- ✓ Mal uso
- ✓ Divulgación

La valoración de la disponibilidad requiere considerar el impacto en función de distintos tiempos de indisponibilidad. Para simplificar el modelo y homogeneizar el tratamiento de los diferentes requerimientos de seguridad sólo se considera el impacto en caso de indisponibilidad indefinida, por tanto, en caso de superarse el Tiempo Objetivo de Recuperación (RTO - Recovery Time Objective) o el Punto Objetivo de Recuperación (RPO – Recovery Point Objective) (MAGERIT, 2012).

Conviene destacar que los distintos requerimientos de seguridad no son totalmente independientes entre sí, existiendo algunos requerimientos para los que se espera una elevada correlación. Algunos ejemplos de estas correlaciones son:

- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar accesos no autorizados a la información.

- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar modificaciones no autorizadas de la información.

- Un requerimiento elevado de disponibilidad se espera que generalmente lleve asociado un elevado requerimiento de integridad, debido a que el impacto entre no disponer de información para la ejecución de un proceso y que la información disponible no sea fiable, será generalmente similar.

- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que acceden a la información.

- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que modifican la información.

- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de datos, debido a que el impacto de utilizar datos no fiables y utilizar datos no auténticos será, en muchos casos, similar.

La metodología a emplear en este proyecto utiliza una valoración de activos cualitativa, si bien a cada valor de la escala se le asigna un valor cuantitativo fijo. Esto permite utilizar los métodos de cálculo del riesgo cuantitativos, que aportan mayor precisión que los cualitativos. La escala cualitativa deberá determinarse en función del entorno, si bien no deberá ser lineal, sino exponencial, para facilitar la diferenciación de los riesgos más importantes [JONES05A].

La metodología no define una escala determinada a utilizar en la valoración, recomendándose utilizar escalas de entre 3 y 10 valores, en función de las necesidades de cada análisis de riesgos.

La escala por defecto tiene 5 niveles:

Criterios de valoración		**Valores**				
		Critico (10)	**Alto (5)**	**Medio (2)**	**Bajo (1)**	**Nulo (0)**
Estrategia de la organización		Imposibilidad de seguir la estrategia fijada	Impacto grave sobre la estrategia	Impacto moderado sobre la estrategia	Impacto leve sobre la estrategia	No afecta a la estrategia de la organización
Operaciones	Daños personales	Pérdida de varias vidas	Pérdida de una vida	Lesiones graves a una o varias vidas	Daños leves a una o varias personas	No afecta a la seguridad de las personas

	Orden publico	Alteración sería del orden publico	Manifestaciones o presiones significativas	Protestas puntuales	Generación de malestar	No afecta el orden publico
	Actividad de la organización	Interrupción permanente de las actividades	Interrupción prolongada de las actividades	Interrupción breve de las actividades	Entorpecimiento de las actividades	No afecta a la actividad organizacional
Operaciones	Intereses comerciales	Interés muy grande para la competencia	Alto interés para la competencia	Interés moderado para la competencia	Bajo Interés para competencia	Sin interés para la competencia
	Impacto sobre terceros	Grave impacto para muchos terceros	Grave impacto para pocos terceros.	Grave impacto para un tercero	Impacto moderado para un tercero	Impacto leve para un tercero
Relaciones Internacionales		Impacto en las relaciones internacionales	Impacto en las relaciones a nivel diplomático	Impacto en las relaciones internacionales	Impacto leve en las relaciones internacionales	No tiene impacto en las relaciones internacionales
Obligaciones legales y reglamentaciones		Deficiencias excepcionales grave de la ley	Incumplimiento grave de las obligaciones contractuales.	Incumplimiento moderado de las obligaciones contractuales	Incumplimiento leve de obligaciones contractuales	Sin impacto sobre el cumplimiento

Tabla 2. Escala de valoración activos. (Veiga, 2009)

5.4.2.3.2 VALORACIÓN DE VULNERABILIDADES

La metodología no considera explícitamente el concepto de vulnerabilidad. Este concepto queda reflejado en el hecho de que no todas las amenazas son aplicables a todos los recursos. Por tanto, la consideración de que una amenaza pueda afectar a un recurso supone la posibilidad de que el activo pueda tener vulnerabilidades ante esa amenaza.

5.4.2.3.3 VALORACIÓN AMENAZAS

Una amenaza es cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información, y, por extensión, a los activos de información que dicho recurso soporta.

Para la valoración de las amenazas es necesario estimar un ratio anual de ocurrencia y un porcentaje de degradación para cada uno de los requerimientos de seguridad definidos.

Para la estimación de la frecuencia cabe diferenciar las amenazas intencionadas de las fortuitas.
El modulo proporciona un inventario clasificado de amenazas basado en el suministrado por la Metodología MAGERIT.

5.4.2.3.4 CALCULO DE RIESGO INTRÍNSECO

Se considera que el riesgo intrínseco es la pérdida anual esperada considerando que no existe ninguna salvaguarda que proteja los recursos de información de sus amenazas.
La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información.
- La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.

De acuerdo con las definiciones ya vistas en la introducción, el riesgo intrínseco de los activos de información puede definirse como:

$$Riesgo_A = \sum_T \left(ARO(T) \times \sum_R (Valor(A,R) \times Degradación(R,T)) \right)$$

Donde:

- A representa el activo de información a considerar.
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis.
- T representa cada una de las amenazas del activo información.

5.4.2.3.5 VALORACIÓN DE SALVAGUARDAS

Las salvaguardas son las medidas establecidas por la Organización para mitigar sus riesgos. Las salvaguardas pueden reducir la probabilidad de éxito de una amenaza reduciendo, por tanto, su frecuencia y/o reducir el impacto en caso de producirse.

La eficacia de una salvaguarda para una determinada amenaza y activo de información se mide en el porcentaje de reducción de la probabilidad y el impacto. Teniendo en cuenta una escala a partir del **nivel de madurez de la implantación**, que define en qué medida se puede confiar en el funcionamiento adecuado de la salvaguarda según sus especificaciones. En la determinación del nivel de madurez se considera el modelo CMM (Capability Maturity Model), que define los siguientes niveles de madurez aplicables a cualquier proceso o control:

- **Nivel 0 (Inexistente):** La salvaguarda no se ha implantado.
- **Nivel 1 (Inicial):** La implantación de la salvaguarda depende de la iniciativa de personas individuales, por lo que no se puede garantizar su aplicación de forma consistente ni en todos los casos.
- **Nivel 2 (Repetible):** La salvaguarda se aplica de forma generalizada debido al conocimiento de todos los interesados de su necesidad y de su funcionamiento, pero no se ha llevado a cabo una formalización que asegure la aplicación de forma consistente ni que la aplicación de la medida se mantendrá a lo largo del tiempo al cambiar las personas responsables.

- **Nivel 3 (Formalizado):** La aplicación de la salvaguarda está formalmente documentada en políticas, procedimientos, guías, estándares, cuadernos de carga, definiciones de puestos, etc. Esta formalización asegura que la salvaguarda se aplicará de forma generalizada y consistente y se mantendrá independientemente de las personas responsables.
- **Nivel 4 (Gestionado):** La aplicación de la salvaguarda se monitoriza y se revisa periódicamente. Esta monitorización y revisión permite detectar cualquier desviación en la aplicación de la salvaguarda, garantizando su funcionamiento permanente.
- **Nivel 5 (Optimizado):** La monitorización y la revisión de la salvaguarda se utiliza para introducir mejoras que permitan aumentar la eficacia a lo largo del tiempo.

5.4.2.3.6 CALCULO DE RIESGO EFECTIVO

Se considera que el riesgo efectivo es la pérdida anual esperada considerando el efecto de las salvaguardas actualmente implantadas para proteger a los recursos de información de sus amenazas.

La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información.
- La exposición de los activos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.
- La eficacia de las salvaguardas para reducir la frecuencia o el impacto de las amenazas, teniendo en cuenta la medida en que están implantadas.

De acuerdo con las definiciones ya vistas en la introducción, el riesgo efectivo de los activos de información puede definirse como:

$$Riesgo_A = \sum_T \left(\left(ARO(T) \times \prod_S (1 - P(S,T,A)) \right) \times \sum_R \left(Valor(A,R) \times Degradación(R,T) \times \prod_S (1 - I(S,T,A,R)) \right) \right)$$

Donde:

- A representa el activo a considerar.
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis.
- T representa cada una de las amenazas del activo.
- P(S, T, A) representa la probabilidad con la que la salvaguarda S podrá prevenir la realización de la amenaza T sobre el activo A. A su vez, P(S) se calcula en función de la eficacia de la salvaguarda y de su grado de implantación:

P(S, T, A) □□Probabilidad (S, T, B) x Implantación (S, A)

I(S) representa la reducción del impacto de la amenaza T sobre el activo A. A su vez, I(S) se calcula en función de la eficacia de la salvaguarda y de su grado de implantación, para cada uno de los requerimientos de seguridad: I(S, T, A, R) □□Reducción del impacto (S, T, A) x Implantación (S, B).

5.4.2.3.7 CALCULO DE RIESGO RESIDUAL

Se considera que el riesgo residual es la pérdida anual esperada considerando el efecto de las salvaguardas actualmente implantadas para proteger a los recursos de información de sus amenazas más las salvaguardas consideradas en el plan de acción definido.

$$Riesgo\ residual = Riesgo\ Intrinseco - Riesgo\ Efectivo$$

5.4.3 MODULO ROLES

Modulo gestión de roles se encargar de definir la administración de los usuarios, grupos de usuarios, permisos, autenticación y autorización para el acceso a la aplicación.

- Modelo de seguridad positiva: "todo aquello que no está explícitamente permitido, está prohibido". Define lo que está permitido, y rechaza todo lo demás, permite el acceso a recursos o funciones específicas autorizadas.
- Los usuarios y grupos de usuario acceden a recursos con un rol.
- Roles
  - **Lectura**: permite listar y detalles de los objetos.
  - **Escritura**: crear, editar y listar objetos.
  - **Usuario**: crear, editar, listar y eliminar objetos.
  - **Administrador**: acciones que requieren un mayor nivel de permiso.

5.4.4 MÓDULO DE ACTIVOS

Activo de información, cualquier información valiosa o necesaria para que la organización cumpla sus objetivos.

Módulo de activos dispone de un repositorio de tipos de activos, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
Los datos que se almacenarán de los activos de información son:

- Identificador de activo de información.
- Nombre del activo de información.
- Descripción del activo de información.

- Responsables del activo de información.
- Tipo de activo de información.

Recurso de información Cualquier elemento empleado en el tratamiento de activos de información.

De la misma forma para recursos de información:

- Identificador de recurso de información
- Nombre del recurso de información.
- Descripción del recurso de información.
- Tipo de recurso
- Propietario del recurso de información.
- Activos que soporta

5.4.5 MÓDULO DE REPORTE

Informes y gráficos con los resultados de los análisis realizados. Estos informes serán:

- **Riesgo intrínseco**
  - ✓ Listado del riesgo intrínseco por activo.
  - ✓ Listado del riesgo intrínseco por activo desglosado por requerimiento de seguridad
  - ✓ Gráfico de barras de riesgo intrínseco por activo.
  - ✓ Gráfico de barras de riesgo intrínseco por activo desglosado por requerimiento de seguridad.
  - ✓ Mapa de riesgos por activos, sobre la matriz de activos (por filas) y requerimientos de seguridad
  - ✓ Mapa de riesgos por activos, sobre la matriz de activos (por filas) y requerimientos de seguridad (por columnas), con un código semafórico cuyos umbrales serán configurables por el usuario en la propia pantalla, utilizando por defecto los percentiles 33 y 66.
  - ✓ Mapa de riesgos por activos, con las amenazas.

- **Riesgo efectivo**
  - ✓ Las mismas gráficas e informes que con el riesgo intrínseco.
  - ✓ Gráfico de radar con la implantación de las salvaguardas (media).
  - ✓ Gráfico de radar con la implantación de las salvaguardas (desglosado).

- **Riesgo residual**
  - ✓ Las mismas gráficas que con el riesgo efectivo, para cada escenario.
  - ✓ Gráfico de radar con la implantación de las salvaguardas en cada escenario.

5.5 ANÁLISIS Y FUNDAMENTOS

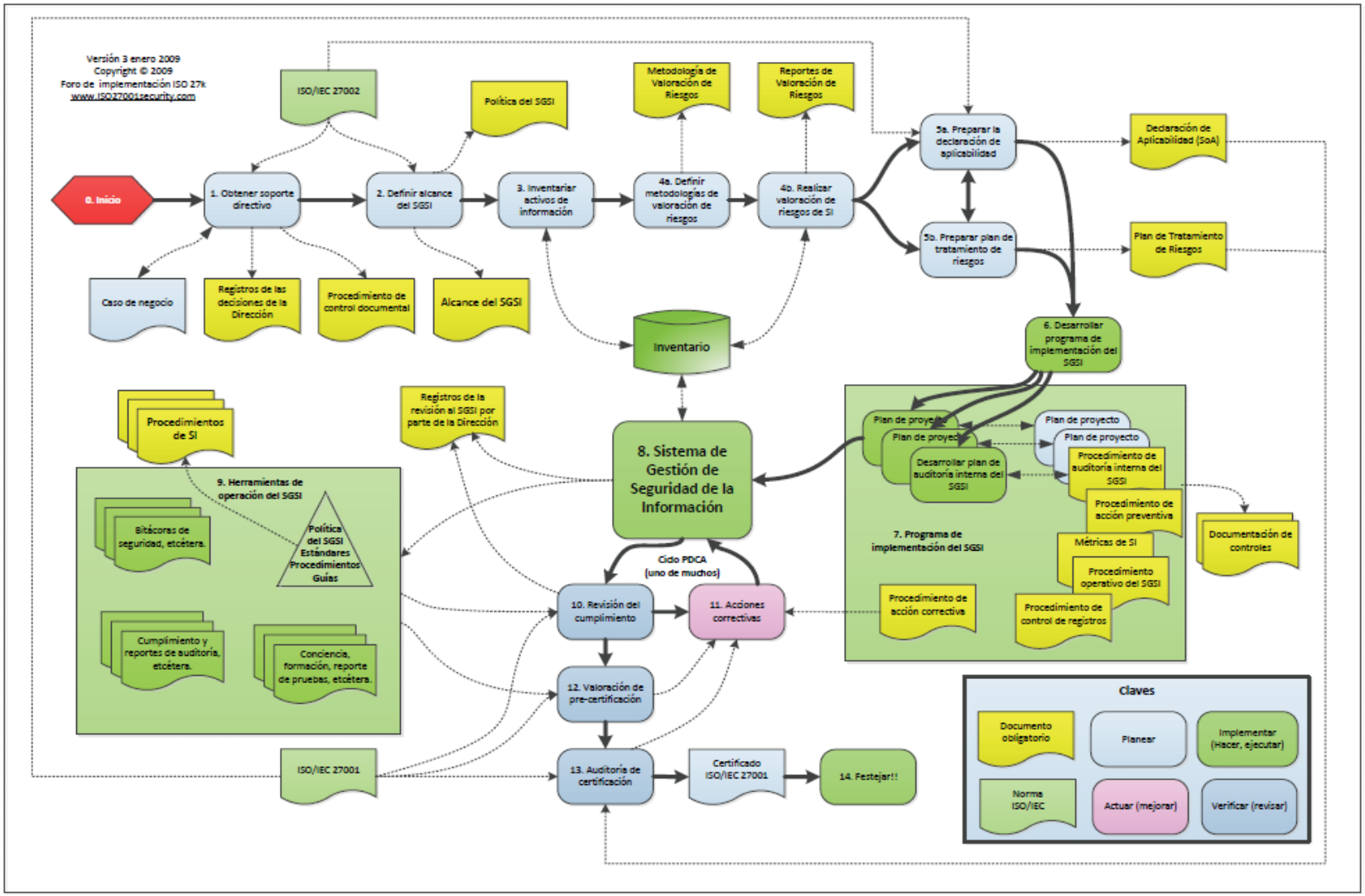


Ilustración 10. Metodología de implantación para certificación en ISO/IEC 27001

El diagrama anterior, representa los requerimientos de la ISO enfocado a la implantación del SGSI para cualquier organización, de esta forma y bajo el cumplimento de las exigencias, dicha organización puede iniciar proceso de certificación; antes debe tener un historial de por lo menos 3 meses de funcionamiento demostrable para inicio del debido proceso.

5.5.1. BASE DE DATOS DATALOSS DB – REPORTE MUNDIAL

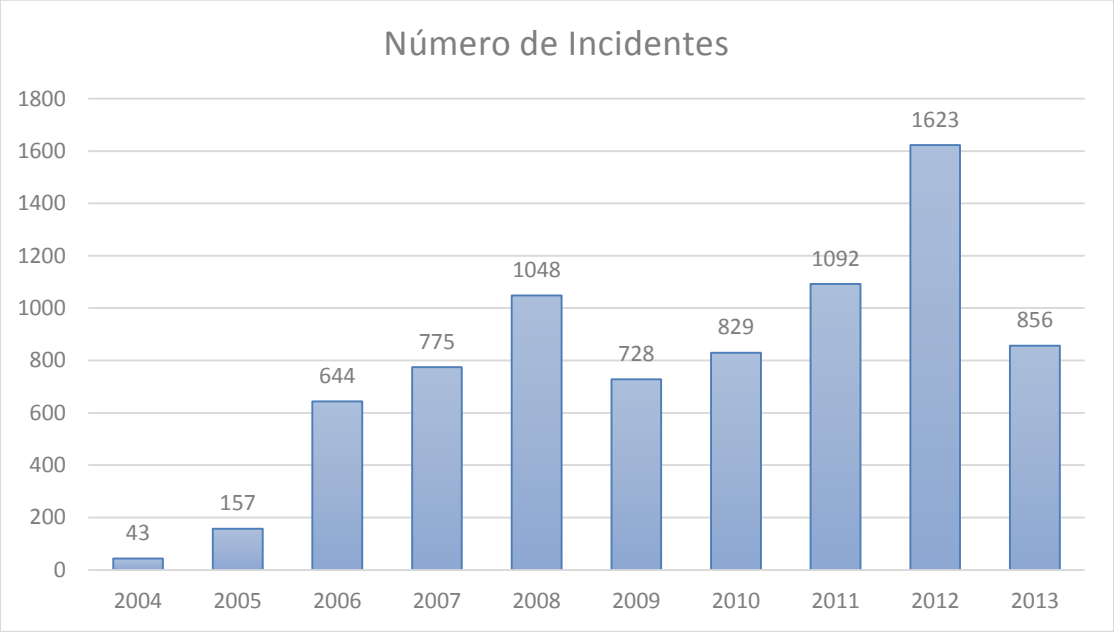


Ilustración 11. Número de incidentes a nivel mundial. (DATALOSS DB, 2014)

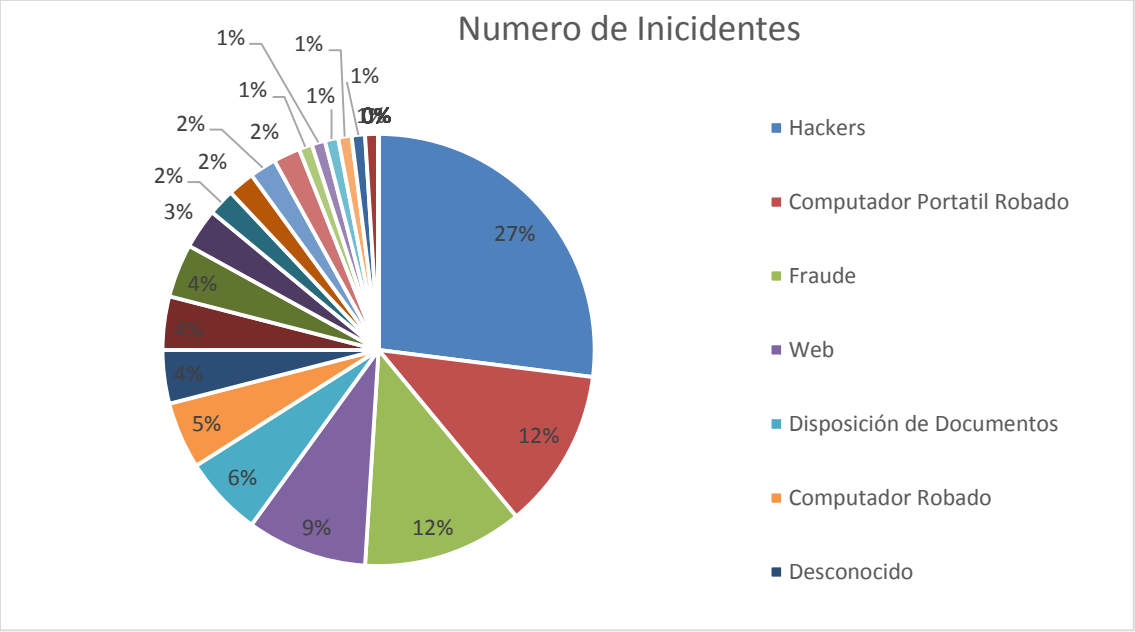


Ilustración 12. . Incidentes reportados de acuerdo a su clasificación (Foundation, 2013).

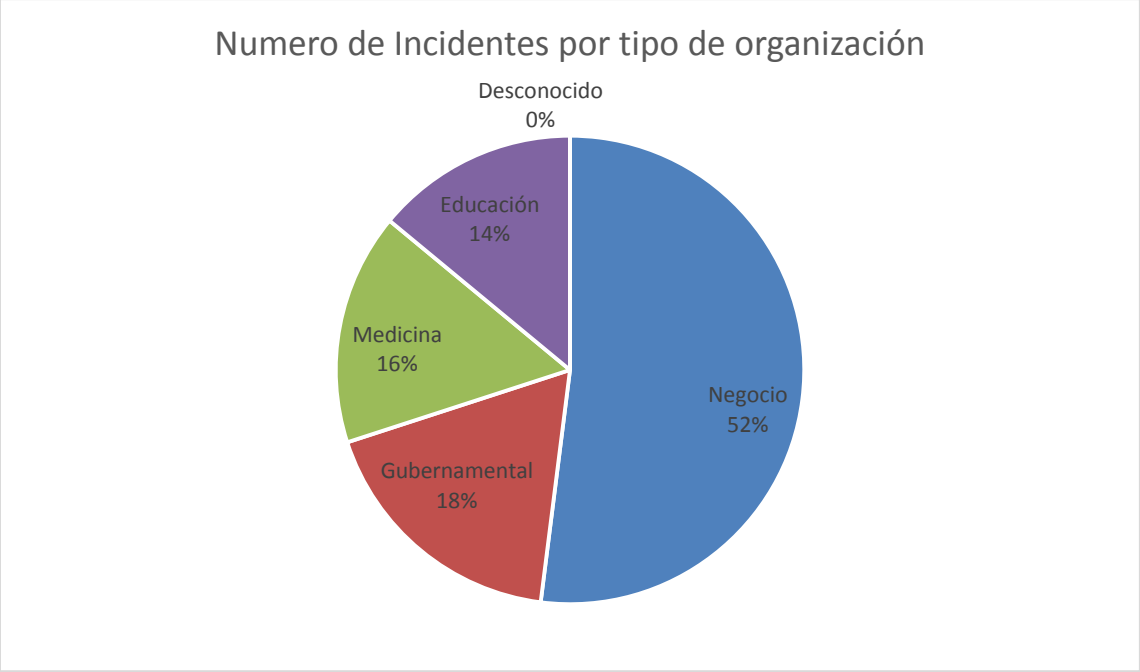


Ilustración 13. . Distribución de incidentes por tipo de organización afectada (Foundation, 2013)

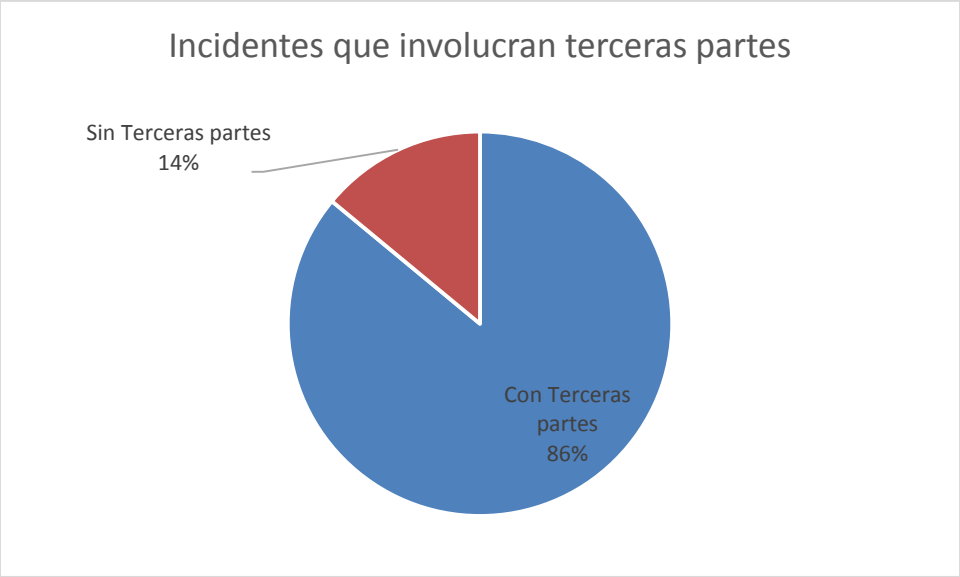


Ilustración 14. Incidentes que involucran terceras partes (Foundation, 2013)

Ilustración 15. Registros que involucran terceras partes (Foundation, 2013)

5.5.2 ANÁLISIS GRÁFICOS

Para 2013 según los tipos de incidentes:

Hacker fue el incidente con mayor porcentaje de ocurrencia con un 27%, es decir, el caso más frecuente en las empresas fue el ataque de 'ciberdelincuentes' (Hacker) a falta de gestión de la seguridad y evaluaciones de riesgos en las mismas.

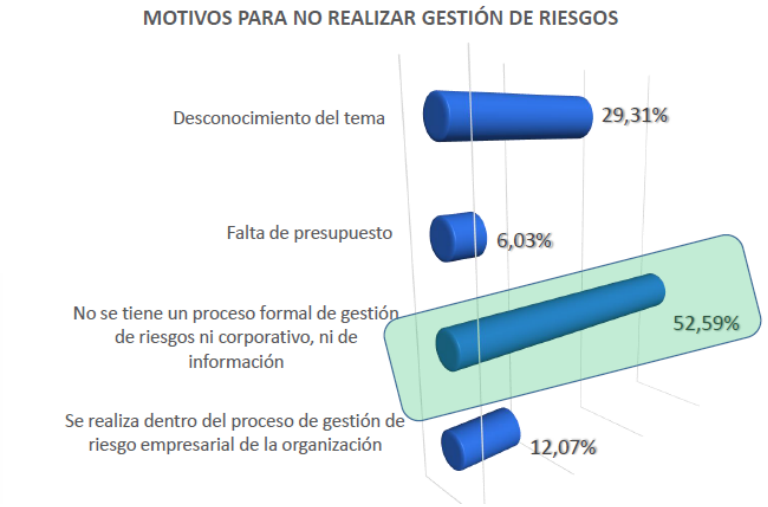
Seguido del ***Ordenador portátil robado*** con porcentaje de 18%, es decir, el segundo caso más frecuente en las empresas para este año fue el robo de los portátiles a raíz de fallas en el acceso físico a las instalaciones.

Las figuras 6 y 7 destacan una tendencia que indica que los incidentes de pérdida de datos que involucran a terceros, en promedio, resultan en un mayor número de registros perdidos que los incidentes que no implican a terceros. Esto puede ser el resultado del tipo de datos manejados por terceros, el proceso de transferencia de los datos entre las organizaciones u otra hipótesis, mayormente todos especulativos, pues existen pocos datos para establecer una causa tan dominante.

5.5.3 ESTADÍSTICAS Y TENDENCIAS EN COLOMBIA Y PAISES DE LATINOAMERICA

La V Encuesta Latinoamericana de seguridad de la información, ACIS 2013, contó con la participación de 240 participantes de 15 países. Los resultados estadísticos más relevantes para el proyecto, son ilustrados en los gráficos siguientes:

Estándares y buenas prácticas de seguridad y Motivos para no realizar gestión de riesgos



ESTÁNDARES Y BUENAS PRÁCTICAS	2009	2013
ISO 27001	45.80%	58.33%
Common Criteria	5.20%	3.75%
Cobit 4.1	23.40%	31.25%
Magerit	5.20%	4.58%
Octave	2.30%	2.50%
Guías del NIST (National Institute of Standards and Technology) USA	12.30%	12.92%
Guías de la ENISA (European Network of Information Security Agency)	2.30%	1.67%
OSSTM - Open Standard Security Testing Model	7.50%	5.00%
ISM3 - Information Security Management Maturiy Model	3.90%	1.67%
ITIL	26.90%	32.08%
No se consideran	37.70%	28.75%
Otra;Top 20 de fallas de seguridad del SANS, ISO 17799. BS 259999, Cobit 5.0, NTC 5254, OWASP, ISSAF, PCI-DSS, MCIIEF, SOX, N24360, SARO, Comunicación A4609, Propias, Circular 052	7.10%	9.17%

Ilustración 16. Motivos para no realizar gestión de riesgos. (ACIS, 2014)

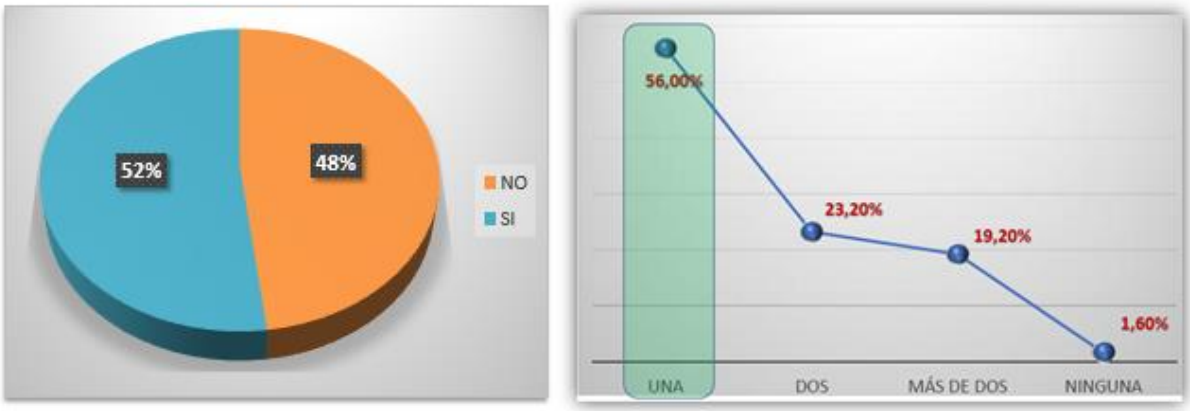


Ilustración 17. Cantidad de evaluaciones de riesgos. (ACIS, 2015)

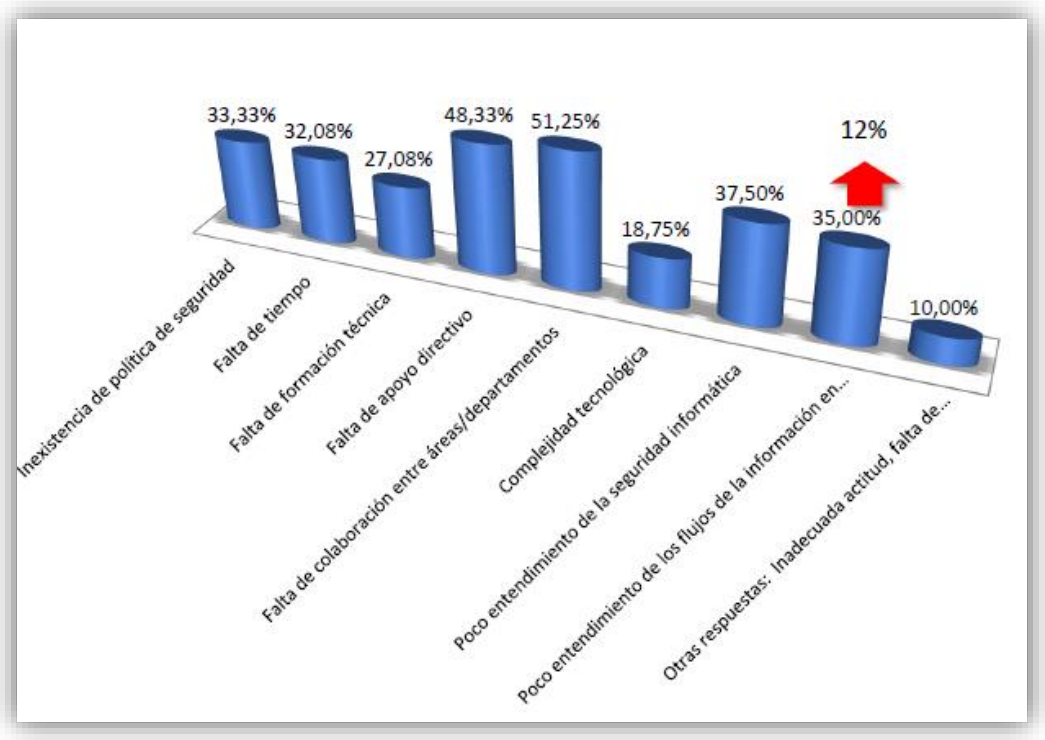


Ilustración 18. Obstáculos de implementación de la seguridad informática.

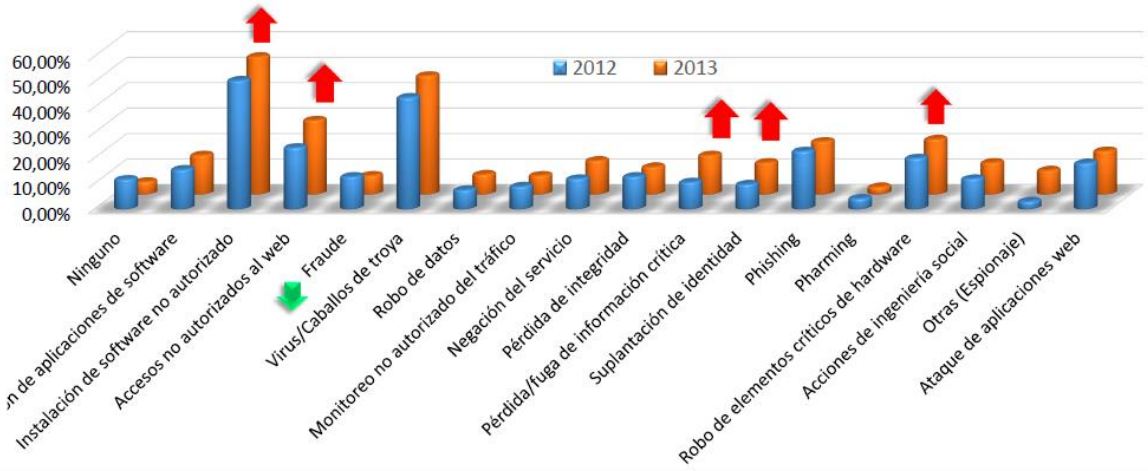


Ilustración 19. Fallas e incidentes de seguridad informática. (ACIS, 2014)

La encuesta revela que la ISO 27001 es el estándar más aplicado seguido de ITIL y Cobit 4.1. La falta de colaboración entre las áreas/departamentos es el principal obstáculo para implementar SI en las organizaciones del año 2013, con un incremento de un 9.59% en relación al anterior, y en segundo lugar la falta de apoyo directivo con 13.06%. Sin dejar de mencionar el aumento considerable de "poco entendimiento de los flujos de información en la organización" con un respectivo 12% comparado con el año anterior (2013), dejando en evidencia la falta de conocimiento en el área de la seguridad de la información, la poca concientización y manejo de la misma, por lo que retrasan procesos implantación de SGSI enfocados en la continuidad del negocio, manteniendo la disponibilidad, confidencialidad e integridad de la información.

Por otra parte, siguiendo el núcleo fundamental de los SGSI se mantiene casi que un equilibrio en cuanto a la existencia de procesos de evaluación de riesgos, en la encuesta un 52% afirma tener procesos de evaluación de riesgos. Además la cantidad de evalución de riesgos procesadas durante el año, el 56% solo hacen una evaluación de riesgos.

La mayor concentración en un proceso de implantación de un SGSI está coordinada por la gestión de riesgos, y los motivos por la no realización de la misma; se centra en "no se tiene proceso formal de riesgo ni cooperativo ni de información". Finalmente, se muestra un leve incremento de políticas en desarrollo, y un importante crecimiento en políticas formalmente definidas.

En consecuencia, el desconocimiento total que se tiene de los riesgos a los cuales la organización se encuentran expuestas, conllevan a una poca gestión de aquellos activos involucrados directa o indirectamente con la información de la misma.

5.6 ESTRUCTURACIÓN DEL MODELO

La dinámica actual de las organizaciones exige de éstas un aprendizaje permanente para mantener los altos niveles actuales de operación y aumentar la capacidad de reacción ante las eventualidades en el desarrollo de sus negocios (Cano J. J., Aprendiendo de la Inseguridad Informática, 2010). Paralelamente, la inseguridad informática evoluciona y propone nuevos retos a las empresas que se manifiestan en variables humanas, técnicas o procedimentales, impactando los activos más importantes para las organizaciones.

De esta forma, se hace necesario que las empresas implementen medidas de seguridad que le permitan establecer una línea estratégica de continuidad en el futuro, basándose en la norma ISO 27001 con el cumplimiento de todos sus requerimientos.

El modelo de referencia del proceso de implantación diseñado como resultado de las investigaciones, es una forma de lograr este objetivo; porque reúne características y elementos estratégicamente adaptados e integrados, fundamentados en la problemática preestablecida y los requerimientos actuales, desde una perspectiva de alcance y necesidad de la organización.

Más adelante, la figura 27 muestra el esquema propuesto, estructurado de la siguiente forma:

Objetivo: Ofrecer guías para el desarrollo de componentes requeridos en el proceso de implantación de un SGSI, vinculando las metas del negocio con las tecnologías de información de la organización.

Enfoque: Modelo orientado a procesos, que adopta un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. Manteniendo prioridad en la autoevaluación, gestión documental, gestión de riesgos, gestión de activos y gestión de roles.

Modelo de proceso: Cuatro etapas comprenden el modelo de proceso, las cuales están basadas y organizadas de acuerdo al orden de trabajo del PDCA; al cumplirse la última, se pueden reiniciar las actividades, convirtiéndose en un el ciclo de trabajo. Debido al proceso que comprende la ISO 27001.

Sin embargo, antes de abordar el recorrido por las etapas, el modelo incluye un módulo de autoevaluación para conocer, establecer y evaluar el estado de la organización en materia de seguridad de la información. No es posible continuar la aplicación del modelo sin haber culminado este paso.

Luego de finalizar la autoevaluación, se continúa con el proceso:

Planear:

En el momento de implementar la autoevaluación de la organización, se procederá a mostrar los requerimientos que establece la norma ISO 27001 de forma guiada para su debido desarrollo.

Estos requerimientos se establecen como actividades relacionadas con:

- Definición del alcance del SGSI
- Definición de políticas de seguridad
- Inventariar activos de información, apoyado bajo el módulo de gestión de activos.
- Definir metodología de evaluación de riesgos
    - Para este caso se tiene un módulo de gestión de riesgos, el cual permitirá realizar todas las actividades que conlleven a identificación, análisis, evaluación y valoración de los mismos. Dicho análisis de riesgo se llevará a cabo a través de la metodología MAGERIT.
- Aplicación de controles

En la medida que se desarrollen estas actividades, se genera documentación la cual se mantendrá en control documental bajo riendas de la gestión de documentos, permitiendo mantener centralizada toda la información y documentos fundamentales del proceso de implantación de un SGSI, así mismo como la presentación, organización, versión y estado de aprobación de los documentos anexos.

Hacer:

En esta etapa, el SGSI se encuentra en estado de implementación donde se ejecuta todo lo planificado en la etapa anterior. Por lo tanto, en esta fase se generarán indicadores, recomendaciones y falencias del sistema de gestión que se está poniendo en marcha, así pues, a través de métricas se medirá la eficiencia del mismo obteniendo resultados reproducibles y comparables.

Por otra parte, en esta etapa se recolectará informes de incidentes, guiará en aspectos como tratamiento de riesgos manifestado en la gestión de riesgos para definir e implantar dicho tratamiento. Permitiendo alcanzar los objetivos de los controles establecido en la planificación.

Monitorear:

A través de la gestión de roles y el control documental desde el inicio del proceso ayudará a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos

tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.

En esta etapa:

- Se procede a ejecutar procedimientos de monitorización y revisión para:
    - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
    - Identificar brechas e incidentes de seguridad.
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Revisión del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas y registros generados de las mismas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Actuar:

- Mostrar registro de mejoras identificadas.
- Notificar para la realización de las acciones preventivas y correctivas adecuadas.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Actuar lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Aunque no necesariamente es un ciclo secuencial, debido al modelo planteado modularizado se puede hacer actividades de implementación cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

En la siguiente grafica se muestra el modelo enmarcado en un proceso cíclico desarrollado por módulos enfocados en la gestión de componentes del proceso de implantación de un SGSI.

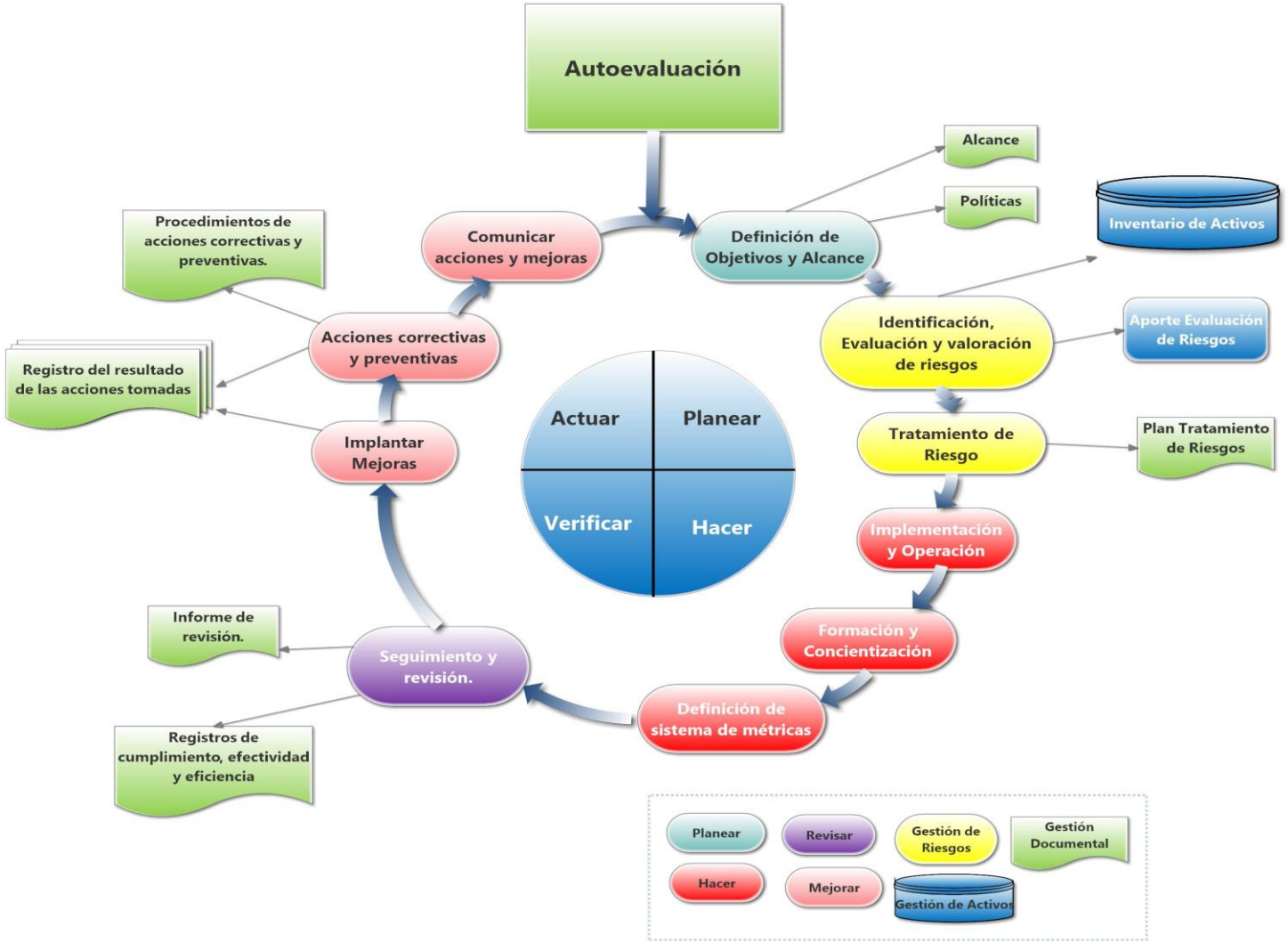


Ilustración 20. Modelo de implantación del SGSI, diseñado como resultado final del proceso. (ACIS, 2014)

6. DESARROLLO

6.1 MODELO DE DOMINIO

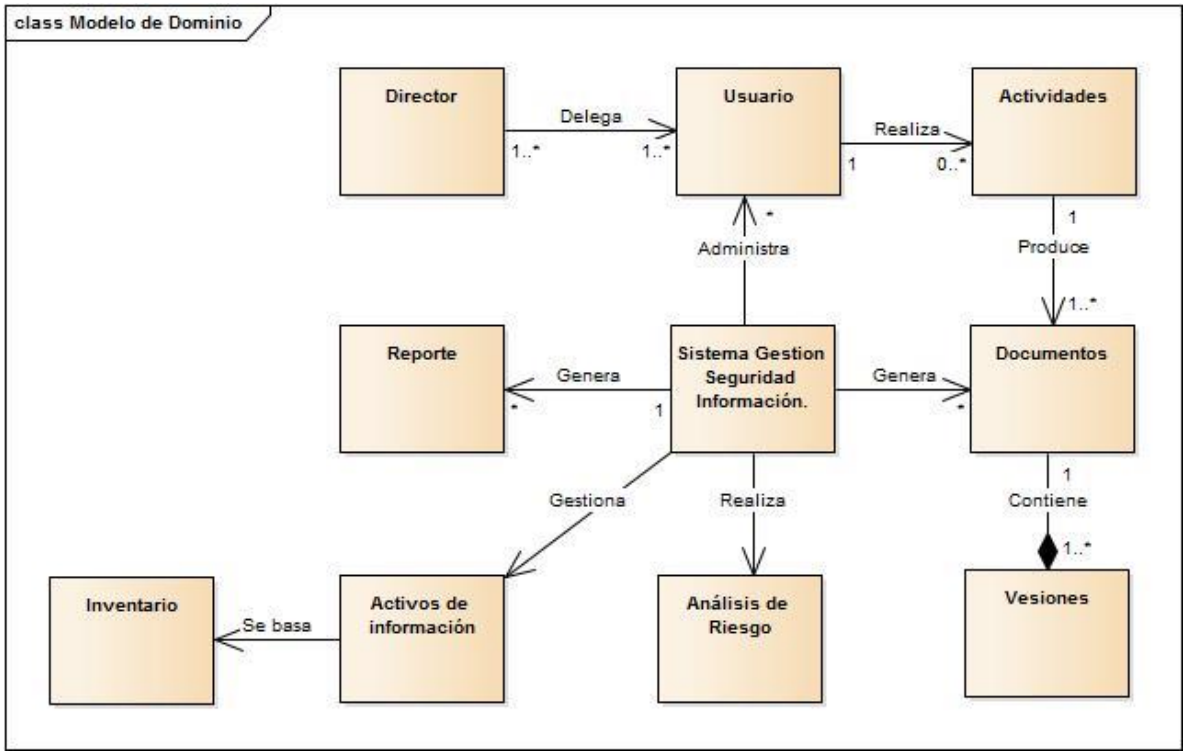


Ilustración 21. Modelo de dominio.

6.2 VISTA DE ESCENARIOS

6.2.1 CASOS DE USO GESTIÓN DE ROLES

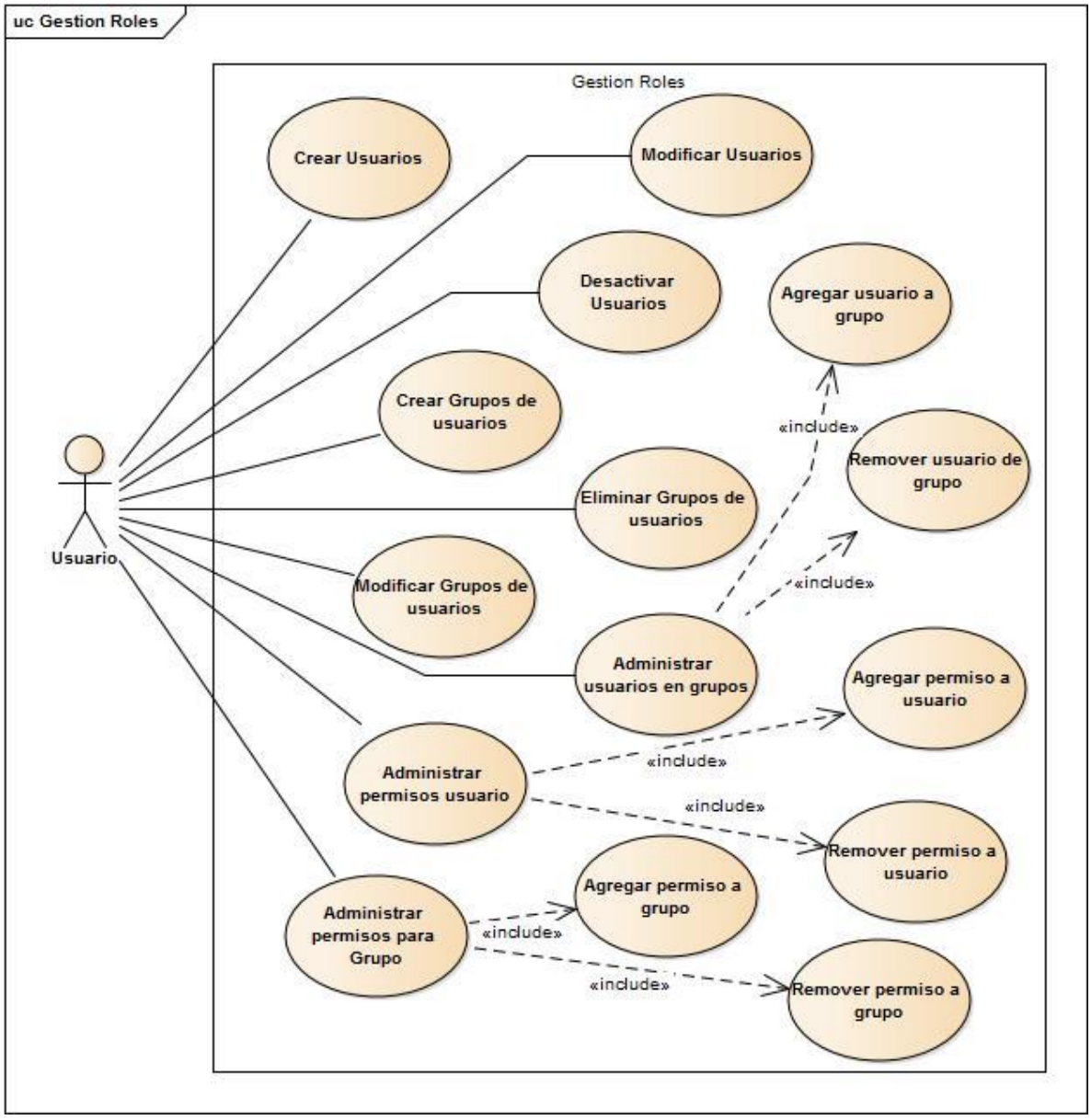


Ilustración 22. Casos de uso gestión de roles.

6.2.2 CASOS DE USO GESTIÓN DOCUMENTAL

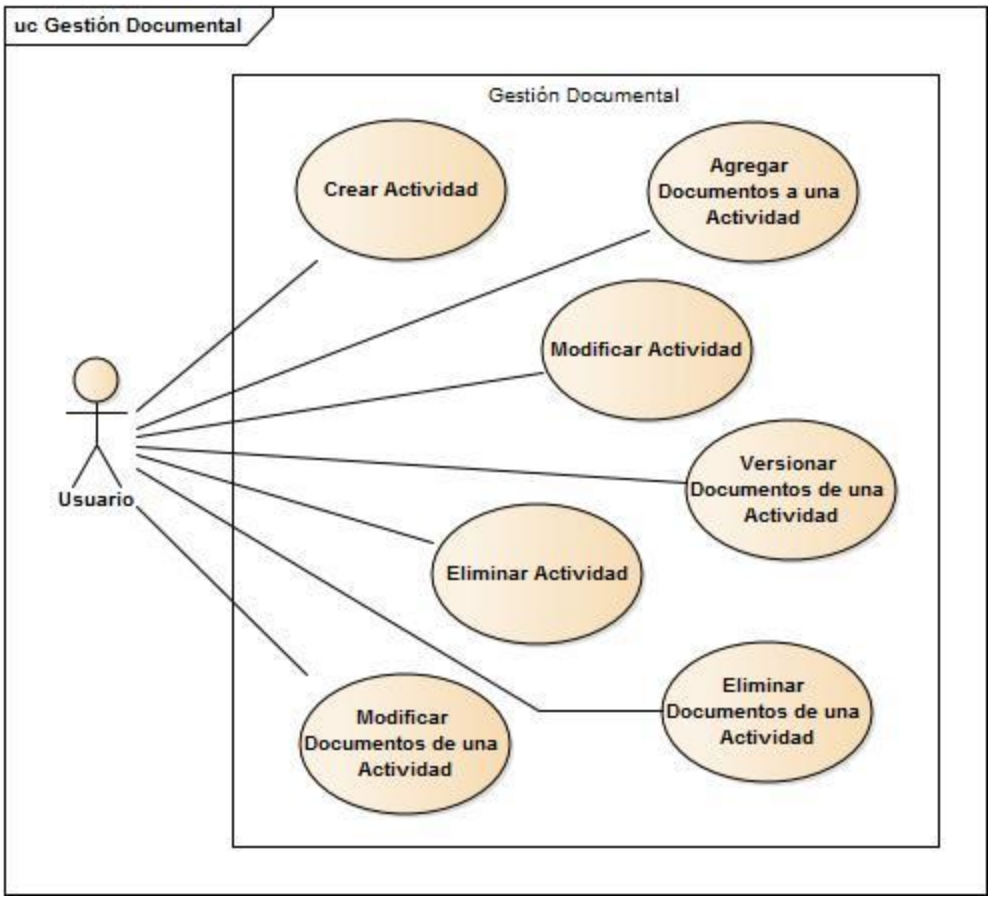


Ilustración 23. Casos de uso gestión documental.

6.2.3 CASOS DE USO GESTIÓN DE ACTIVOS

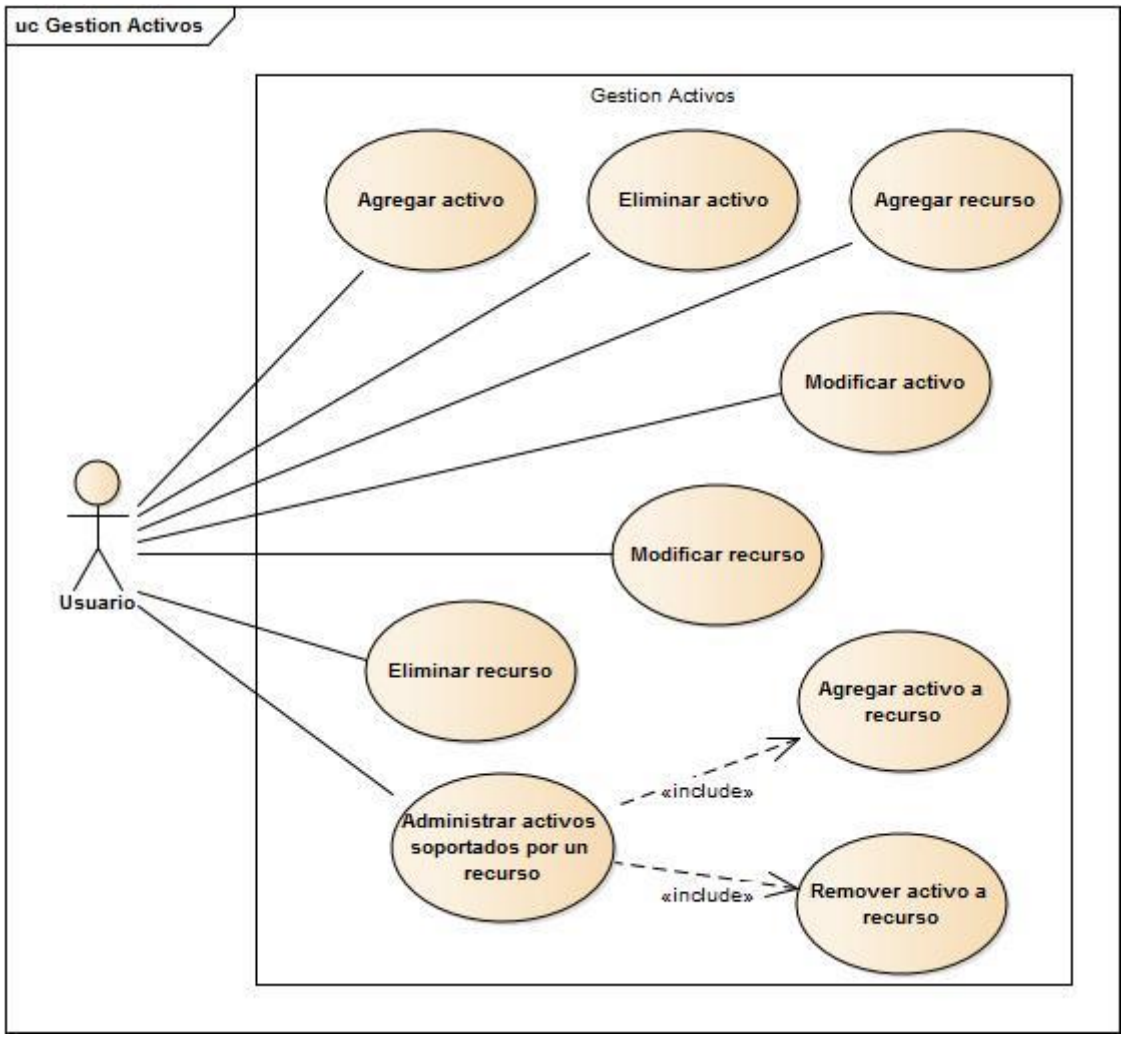


Ilustración 24. Casos de uso gestión de activo.

6.2.4 CASOS DE USO ANÁLISIS DE RIESGO

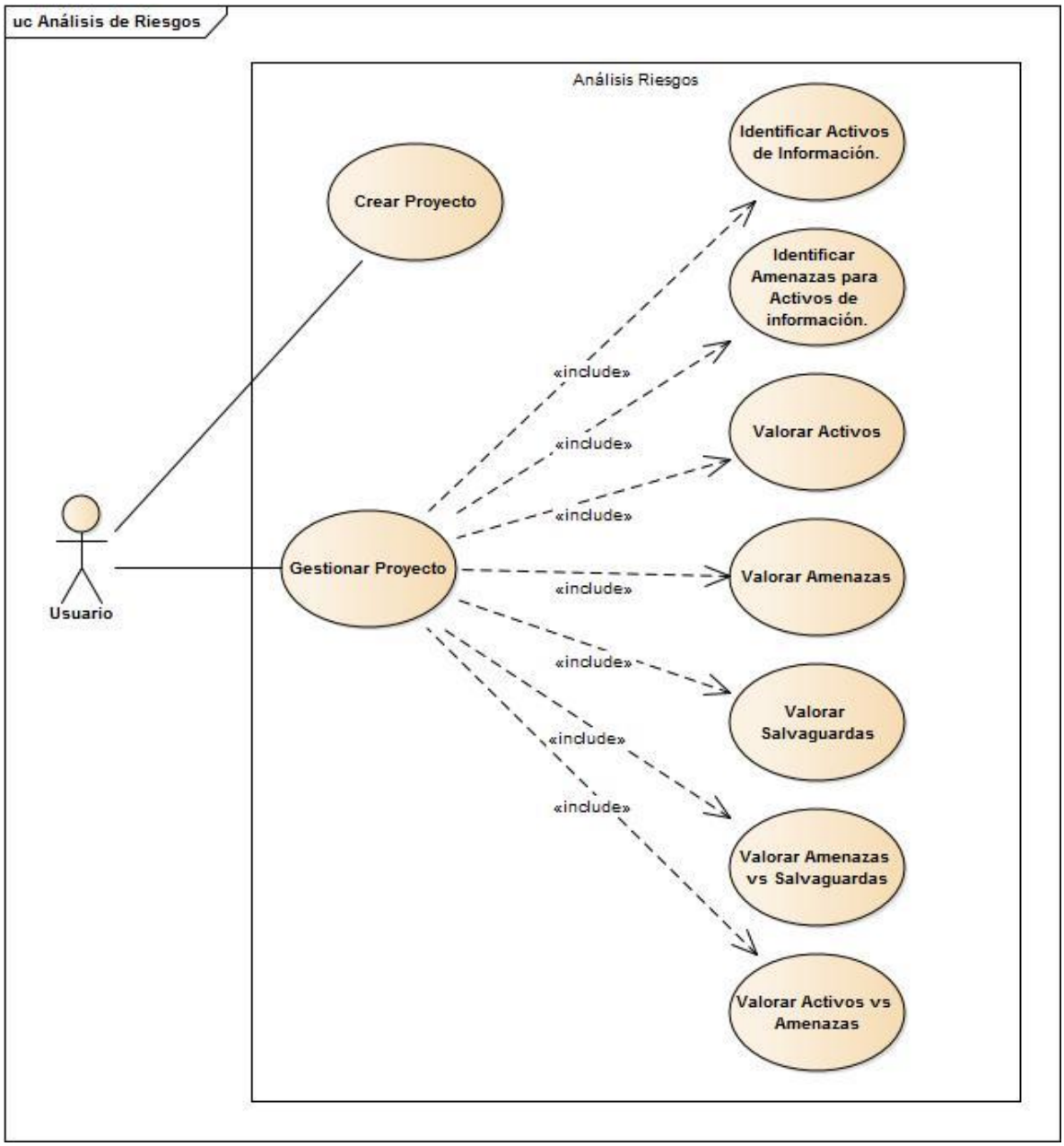


Ilustración 25. Casos de uso análisis de riesgos.

Casos de uso gestión documental

6.2.5 DESCRIPCIÓN CASOS DE USO

Caso de Uso	CREAR ACTIVIDAD
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	Ninguna
Garantías de éxito	El usuario podrá crear una actividad
Flujo Básico	1. El usuario solicita crear una actividad. 2. El sistema retorna el formulario para creación de actividad. 3. El usuario llena la información correspondiente a la actividad a crear. 4. El usuario selecciona guardar información. 5. El sistema notifica que la actividad ha sido creada.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario crear una actividad
Temas abiertos	Ninguno

Tabla 3. Caso de Uso: Crear Actividad

Caso de Uso	MODIFICAR ACTIVIDAD
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada
Garantías de éxito	El usuario podrá modificar una actividad
Flujo Básico	1. El usuario solicita modificar una actividad. 2. El sistema retorna el formulario para modificación de actividad. 3. El usuario llena la información correspondiente a la actividad a modificar. 4. El usuario selecciona guardar información. 5. El sistema notifica que la actividad ha sido modificada.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo

	5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario modificar los datos de una actividad
Temas abiertos	Ninguno

Tabla 4 Caso de Uso: Modificar Actividad

Caso de Uso	**ELIMINAR ACTIVIDAD**
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada
Garantías de éxito	El usuario podrá eliminar una actividad
Flujo Básico	1. El usuario solicita eliminar una actividad. 2. El sistema solicita confirmación de la acción. 3. El usuario selecciona eliminar actividad. 4. El sistema notifica que la actividad ha sido eliminada.
Flujo Alternativo:	3.a El usuario selecciona cancelar eliminación de actividad 3.a.1 El sistema oculta la ventana de eliminación de actividad
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario eliminar una actividad
Temas abiertos	Ninguno

Tabla 5 Caso de Uso: Eliminar Actividad

Caso de Uso	**AGREGAR DOCUMENTOS A UNA ACTIVIDAD**
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada
Garantías de éxito	El usuario podrá agregar documentos a una actividad
Flujo Básico	1. El usuario selecciona una actividad. 2. El sistema retorna los detalles de la

	actividad 3. El usuario solicita agregar un documento 4. El sistema retorna el formulario para creación de documento. 5. El usuario llena la información correspondiente al documento a modificar. 6. El usuario selecciona guardar información. 7. El sistema notifica que el documento ha sido agregado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 4.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 4.a.1 El sistema notifica el fallo 7.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 7.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Los documentos adjuntos deben ser de tipo Imagen (jpeg, jpg, png), documento de Word, Excel, PowerPoint o PDF.
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un usuario solicite agregar un documento a una actividad
Temas abiertos	Ninguno

Tabla 6 Caso de Uso: Agregar documentos a una actividad

Caso de Uso	**ELIMINAR DOCUMENTOS DE UNA ACTIVIDAD**
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada • El documento debe estar creado
Garantías de éxito	El usuario podrá eliminar documentos asociados a una actividad
Flujo Básico	1. El usuario selecciona una actividad. 2. El sistema retorna los detalles de la actividad 3. El usuario solicita eliminar un documento 4. El sistema solicita confirmación de la acción. 5. El usuario selecciona eliminar el documento. 6. El sistema notifica que el documento ha

	sido eliminado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a El usuario selecciona cancelar eliminación de documento 5.a.1 El sistema oculta la ventana de eliminación de documento
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario eliminar un documento de una actividad
Temas abiertos	Ninguno

Tabla 7 Caso de Uso: Eliminar documentos a una actividad

Caso de Uso	**MODIFICAR DOCUMENTOS DE UNA ACTIVIDAD**
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada • El documento debe estar creado
Garantías de éxito	El usuario podrá modificar documentos asociados a una actividad
Flujo Básico	1. El usuario selecciona una actividad. 2. El sistema retorna los detalles de la actividad 3. El usuario solicita modificar un documento 4. El sistema retorna el formulario para edición de documento. 5. El usuario llena la información correspondiente al documento a modificar, además de una observación referente al cambio 6. El usuario selecciona guardar información. 7. El sistema modifica la versión del documento automáticamente 8. El sistema notifica que el documento ha sido modificado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 4.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 4.a.1 El sistema notifica el fallo 7.a La información suministrada por el usuario

	contiene datos inválidos o campos requeridos que no han sido llenados 7.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Los documentos adjuntos deben ser de tipo Imagen (jpeg, jpg, png), documento de Word, Excel, PowerPoint o PDF.
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario modificar datos de un documento.
Temas abiertos	Ninguno

Tabla 8 Caso de Uso: Modificar documentos de una actividad

Caso de Uso	**VERSIONAR DOCUMENTOS DE UNA ACTIVIDAD**
Actor Principal:	Usuario
Personal Involucrado:	Usuarios asociados a la actividad
Precondiciones	• La actividad debe estar creada • El documento debe estar creado
Garantías de éxito	El usuario podrá versionar documentos asociados a una actividad
Flujo Básico	1. El usuario selecciona una actividad. 2. El sistema retorna los detalles de la actividad 3. El usuario solicita acción de versionamiento de un documento (verificar, revisar, aprobar, publicar) 4. El usuario agrega observaciones a la acción 5. El sistema modifica la versión del documento. 6. El sistema notifica que la versión del documento ha sido modificado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a El usuario no agrega observaciones 5.a.1 El sistema notifica al usuario que el campo observación es requerido
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un usuario solicite modificar el estado de un documento en una actividad
Temas abiertos	Ninguno

Tabla 9 Caso de Uso: Versionar documentos de una actividad

Caso de Uso	CREAR USUARIO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener permiso para agregar cuentas de usuario
Garantías de éxito	El usuario podrá crear una cuenta para ingreso al sistema.
Flujo Básico	1. El usuario solicita crear una cuenta para ingresar al sistema. 2. El sistema retorna el formulario para creación de usuario. 3. El usuario llena la información correspondiente a la cuenta a crear. 4. El usuario selecciona guardar información. 5. El sistema notifica que la cuenta ha sido creada.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se necesite crear un usuario
Temas abiertos	Ninguno

Tabla 10. Caso de Uso: Crear Usuario

Caso de Uso	MODIFICAR USUARIO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe estar creado • El usuario debe tener permiso para modificar cuentas de usuario
Garantías de éxito	El usuario podrá modificar los datos de una cuenta para ingreso al sistema.
Flujo Básico	1. El usuario solicita modificar una cuenta para ingresar al sistema. 2. El sistema retorna el formulario para modificación de usuario. 3. El usuario llena la información correspondiente a la cuenta a crear. 4. El usuario selecciona guardar información.

	5. El sistema notifica que la cuenta ha sido modificada.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se necesite modificar los datos de una cuenta de usuario
Temas abiertos	Ninguno

Tabla 11 Caso de Uso: Modificar Usuario

Caso de Uso	**DESACTIVAR USUARIO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe estar creado • El usuario debe tener permiso para desactivar cuentas de usuario
Garantías de éxito	El usuario podrá desactivar cuentas para ingreso al sistema.
Flujo Básico	1. El usuario solicita desactivar una cuenta para ingresar al sistema. 2. El sistema solicita confirmación de la acción. 3. El usuario confirma la desactivación de la cuenta. 4. El sistema notifica que la cuenta ha sido desactivada.
Flujo Alternativo:	3.El usuario selecciona cancelar desactivación de la cuenta 3.a.1 El sistema oculta la ventana de desactivación de usuario
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un usuario no necesite ingresar al sistema.
Temas abiertos	Ninguno

Tabla 12 Caso de Uso: Desactivar Usuario

Caso de Uso	CREAR GRUPO DE USUARIO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener permiso para agregar grupos de usuario
Garantías de éxito	El usuario podrá crear un grupo de usuario para agrupar permisos.
Flujo Básico	1. El usuario solicita crear un grupo de usuario. 2. El sistema retorna el formulario para creación de grupo de usuario. 3. El usuario llena la información correspondiente al grupo de usuarios. 4. El usuario selecciona guardar información. 5. El sistema notifica que la creación ha sido exitosa
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se necesite crear un grupo de usuario para agrupar permisos
Temas abiertos	Ninguno

Tabla 13 Caso de Uso: Crear grupo de usuario

Caso de Uso	MODIFICAR GRUPOS DE USUARIO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El grupo debe estar creado • El usuario debe tener permiso para modificar grupos de usuario
Garantías de éxito	El usuario podrá modificar los datos de un grupo de usuario.
Flujo Básico	1. El usuario solicita modificar un grupo de usuarios. 2. El sistema retorna el formulario para modificación de grupo de usuario. 3. El usuario llena la información correspondiente al grupo de usuario. 4. El usuario selecciona guardar información.

	5. El sistema notifica que la modificación ha sido exitosa.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se necesite modificar los datos de un grupo de usuario
Temas abiertos	Ninguno

Tabla 14 Caso de Uso: Modificar Grupo de Usuario

Caso de Uso	**ELIMINAR GRUPOS DE USUARIO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El grupo debe estar creado • El usuario debe tener permiso para eliminar grupos de usuario
Garantías de éxito	El usuario podrá eliminar grupos de usuario.
Flujo Básico	1. El usuario solicita eliminar un grupo de usuario. 2. El sistema solicita confirmación de la acción. 3. El usuario confirma la eliminación del registro. 4. El sistema notifica que el grupo de usuario ha sido eliminado.
Flujo Alternativo:	3.a El usuario selecciona cancelar eliminación 3.a.1 El sistema oculta la ventana de eliminación de grupo de usuario
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un usuario no sea requerido
Temas abiertos	Ninguno

Tabla 15 Caso de Uso: Eliminar grupos de usuario

Caso de Uso	AGREGAR USUARIO A GRUPO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener permiso para administrar grupos de usuario • El grupo de usuarios debe estar creado • La cuenta a agregar debe estar registrada
Garantías de éxito	El usuario podrá modificar los usuarios que conforman un grupo de usuarios
Flujo Básico	1. El usuario selecciona un grupo. 2. El sistema muestra una ventana con la interfaz para agregar usuarios. 3. El usuario selecciona la cuenta a agregar. 4. El sistema relaciona el grupo con el usuario. 5. El sistema notifica que la cuenta ha sido agregada.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un usuario requiera permisos que se encuentran relacionados a un grupo.
Temas abiertos	Ninguno

Tabla 16 Caso de Uso: Agregar usuarios a grupos

Caso de Uso	REMOVER USUARIO DE GRUPO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener permiso para administrar grupos de usuario • El grupo de usuarios debe estar creado • La cuenta a remover debe estar registrada y asociada al grupo.
Garantías de éxito	El usuario podrá modificar los usuarios que conforman un grupo de usuarios
Flujo Básico	1. El usuario selecciona un grupo. 2. El sistema muestra una ventana con la interfaz con las cuentas asociadas al grupo. 3. El usuario selecciona la cuenta a remover. 4. El sistema elimina la relación entre el grupo y el usuario. 5. El sistema notifica que la cuenta ha sido removida.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo

Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se deba remover permisos generales, contenidos en un grupo, a un usuario.
Temas abiertos	Ninguno

Tabla 17 Caso de Uso: Remover usuario de grupo

Caso de Uso	**AGREGAR PERMISO A USUARIO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener acceso a la administración de permisos.
Garantías de éxito	El usuario podrá modificar los permisos asociados directamente a un usuario
Flujo Básico	1. El usuario selecciona una cuenta. 2. El sistema muestra una ventana con la interfaz para agregar permisos. 3. El usuario agrega el permiso y define un rol. 4. El sistema relaciona la cuenta con el permiso. 5. El sistema notifica que el permiso ha sido agregado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que una cuenta de usuario requiera permisos.
Temas abiertos	Ninguno

Tabla 18 Caso de Uso: Agregar permiso a usuario

Caso de Uso	**REMOVER PERMISO A USUARIO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener acceso a la administración de permisos.
Garantías de éxito	El usuario podrá modificar los permisos asociados directamente a un usuario
Flujo Básico	1. El usuario selecciona una cuenta. 2. El sistema muestra una ventana con los permisos asociados a una cuenta. 3. El usuario selecciona el permiso a remover.

	4. El sistema elimina la relación de la cuenta con el permiso. 5. El sistema notifica que el permiso ha sido removido.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que una cuenta de usuario requiera que se le eliminen permisos.
Temas abiertos	Ninguno

Tabla 19 Caso de Uso: Remover permiso a usuario

Caso de Uso	**AGREGAR PERMISO A GRUPO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener acceso a la administración de permisos.
Garantías de éxito	El usuario podrá modificar los permisos asociados a un grupo
Flujo Básico	1. El usuario selecciona un grupo. 2. El sistema muestra una ventana con la interfaz para agregar permisos. 3. El usuario agrega el permiso y define un rol. 4. El sistema relaciona el grupo con el permiso. 5. El sistema notifica que el permiso ha sido agregado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un grupo requiera permisos.
Temas abiertos	Ninguno

Tabla 20 Caso de Uso: Agregar permiso a grupo

Caso de Uso	REMOVER PERMISO A GRUPO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El usuario debe tener acceso a la administración de permisos.
Garantías de éxito	El usuario podrá modificar los permisos asociados a un grupo
Flujo Básico	1. El usuario selecciona un grupo. 2. El sistema muestra una ventana con los permisos asociados al grupo seleccionado. 3. El usuario selecciona el permiso a remover. 4. El sistema elimina la relación del grupo con el permiso. 5. El sistema notifica que el permiso ha sido removido.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un grupo requiera que se le eliminen permisos.
Temas abiertos	Ninguno

Tabla 21 Caso de Uso: Remover permiso a grupo

Caso de Uso	CREAR ACTIVO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• Las dependencias de activo deben estar creadas
Garantías de éxito	El usuario podrá crear un activo
Flujo Básico	1. El usuario solicita crear un activo. 2. El sistema retorna el formulario para creación de activo. 3. El usuario llena la información correspondiente al activo a crear. 4. El usuario selecciona guardar información. 5. El sistema notifica que el activo ha sido creado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que

	debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario crear un activo
Temas abiertos	Ninguno

Tabla 22. Caso de Uso: Crear Activo

Caso de Uso	**MODIFICAR ACTIVO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El activo debe estar creado • Las dependencias de activo deben estar creadas
Garantías de éxito	El usuario podrá modificar un activo
Flujo Básico	1. El usuario solicita modificar un activo. 2. El sistema retorna el formulario para modificación de activo. 3. El usuario llena la información correspondiente al activo a modificar. 4. El usuario selecciona guardar información. 5. El sistema notifica que el activo ha sido modificado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario modificar los datos de un recurso
Temas abiertos	Ninguno

Tabla 23 Caso de Uso: Modificar Activo

Caso de Uso	ELIMINAR ACTIVO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El activo debe estar creado • El activo no debe ser dependencia de otro.
Garantías de éxito	El usuario podrá eliminar un activo
Flujo Básico	1. El usuario solicita eliminar un activo. 2. El sistema solicita confirmación de la acción. 3. El usuario selecciona eliminar activo. 4. El sistema valida que el activo no sea dependencia de otros activos. 5. El sistema notifica que la actividad ha sido eliminada.
Flujo Alternativo:	3.a El usuario selecciona cancelar eliminación del activo 3.a.1 El sistema oculta la ventana de eliminación de activo 4.a El activo pertenece a las dependencias de otros activos 4.a.1 El sistema notifica que el activo no puede ser eliminado
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario eliminar un activo
Temas abiertos	Ninguno

Tabla 24 Caso de Uso: Eliminar Activo

Caso de Uso	CREAR RECURSO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	Ninguna
Garantías de éxito	El usuario podrá crear un recurso
Flujo Básico	1. El usuario solicita crear un recurso. 2. El sistema retorna el formulario para creación de recurso. 3. El usuario llena la información correspondiente al recurso a crear. 4. El usuario selecciona guardar información. 5. El sistema notifica que el recurso ha sido creado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario

	contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario crear un recurso
Temas abiertos	Ninguno

Tabla 25 Caso de Uso: Crear recurso

Caso de Uso	**MODIFICAR RECURSO**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El recurso debe estar creado
Garantías de éxito	El usuario podrá modificar un recurso
Flujo Básico	1. El usuario solicita modificar un recurso. 2. El sistema retorna el formulario para modificación de recurso. 3. El usuario llena la información correspondiente al recurso a modificar. 4. El usuario selecciona guardar información. 5. El sistema notifica que el recurso ha sido modificado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario modificar los datos de un recurso
Temas abiertos	Ninguno

Tabla 26 Caso de Uso: Modificar recurso

Caso de Uso	ELIMINAR RECURSO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El recurso debe estar creado
Garantías de éxito	El usuario podrá eliminar un activo
Flujo Básico	1. El usuario solicita eliminar un recurso. 2. El sistema solicita confirmación de la acción. 3. El usuario selecciona eliminar recurso. 4. El sistema notifica que la actividad ha sido eliminada.
Flujo Alternativo:	3.a El usuario selecciona cancelar eliminación del recurso 3.a.1 El sistema oculta la ventana de eliminación de recurso
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario eliminar un recurso
Temas abiertos	Ninguno

Tabla 27 Caso de Uso: Eliminar recurso

Caso de Uso	AGREGAR ACTIVO A RECURSO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El recurso debe estar creado • El activo debe estar creado
Garantías de éxito	El usuario podrá modificar los activos soportados por un recurso
Flujo Básico	1. El usuario selecciona un recurso. 2. El sistema muestra una ventana con la interfaz para agregar activos. 3. El usuario agrega el activo. 4. El sistema relaciona el recurso con el activo. 5. El sistema notifica que el activo ha sido agregado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un recurso soporte un nuevo activo.
Temas abiertos	Ninguno

Tabla 28 Caso de Uso: Agregar activo a recurso

Caso de Uso	REMOVER ACTIVO A RECURSO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El recurso debe estar creado • El activo debe estar relacionado con el recurso
Garantías de éxito	El usuario podrá modificar los activos soportados por un recurso
Flujo Básico	1. El usuario selecciona un recurso. 2. El sistema muestra una ventana con los activos asociados a un recurso. 3. El usuario selecciona el activo a remover. 4. El sistema elimina la relación del recurso con el activo. 5. El sistema notifica que el activo ha sido removido.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que un recurso deja de soportar un activo.
Temas abiertos	Ninguno

Tabla 29 Caso de Uso: Remover activo a recurso

Caso de Uso	CREAR PROYECTO
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	Ninguna
Garantías de éxito	El usuario podrá crear un proyecto
Flujo Básico	1. El usuario solicita crear un proyecto. 2. El sistema retorna el formulario para creación de proyecto. 3. El usuario llena la información correspondiente al proyecto a crear. 4. El usuario selecciona guardar información. 5. El sistema notifica que el proyecto ha sido creado.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo 5.a La información suministrada por el usuario contiene datos inválidos o campos requeridos que no han sido llenados 5.a.1 El sistema notifica al usuario que

	debe corregir los campos
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que sea necesario crear un proyecto
Temas abiertos	Ninguno

Tabla 30. Caso de Uso: Crear Proyecto

Caso de Uso	**IDENTIFICAR ACTIVOS DE INFORMACIÓN**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	Deben existir activos de información.
Garantías de éxito	El usuario podrá identificar los activos de información que pertenecen a su proyecto
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de activos disponibles. 3. El usuario selecciona los activos que pertenecen al proyecto. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la información referente a un proyecto
Temas abiertos	Ninguno

Tabla 31 Caso de Uso: Identificar activos de información

Caso de Uso	**IDENTIFICAR AMENAZAS PARA ACTIVOS DE INFORMACIÓN**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	El proyecto debe estar creado
Garantías de éxito	El usuario podrá identificar las amenazas de información que pertenecen a su proyecto
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de amenazas disponibles. 3. El usuario selecciona las amenazas que pueden afectar al proyecto. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.

Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifiquen las amenazas referentes a un proyecto
Temas abiertos	Ninguno

Tabla 32 Caso de Uso: Identificar amenazas para activos de información

Caso de Uso	**VALORAR ACTIVOS**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El proyecto debe estar creado • Se debe realizar la identificación de activos
Garantías de éxito	El usuario podrá valorar a partir de cada requerimiento de seguridad los activos de información que pertenecen a su proyecto
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de activos de información referentes al proyecto. 3. El usuario valora cada uno de los activos a partir de cada requerimiento de seguridad. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la valoración de activos referente a un proyecto
Temas abiertos	Ninguno

Tabla 33 Caso de Uso: Valorar activos

Caso de Uso	VALORAR AMENAZAS
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El proyecto debe estar creado • Se debe realizar la identificación de amenazas
Garantías de éxito	El usuario podrá valorar la frecuencia de ocurrencia para cada amenaza que pueda afectar su proyecto
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de amenazas referentes al proyecto. 3. El usuario valora cada una las amenazas, asignándoles una frecuencia de ocurrencia. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la valoración de amenazas referente a un proyecto
Temas abiertos	Ninguno

Tabla 34 Caso de Uso: Valorar amenazas

Caso de Uso	VALORAR SALVAGUARDAS
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	El proyecto debe estar creado
Garantías de éxito	El usuario podrá valorar salvaguardas o controles a partir de su nivel de su efectividad y nivel de valoración. Además definir si aplica o no para su proyecto
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de controles. 3. El usuario asigna un nivel de efectividad y madurez para cada salvaguarda. Es posible especificar que no aplica el control. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno

Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la valoración de salvaguardas referente a un proyecto
Temas abiertos	Ninguno

Tabla 35 Caso de Uso: Valorar salvaguardas

Caso de Uso	**VALORAR ACTIVOS VS AMENAZAS**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El proyecto debe estar creado • Se debe realizar la valoración de activos • Se debe realizar la valoración de amenazas
Garantías de éxito	El usuario podrá valorar cada activo contra sus posibles amenazas y definir la degradación que sufre a partir de cada requerimiento de seguridad
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna lista de activos. 3. El usuario asocia amenazas al activo 4. El usuario asigna un porcentaje de degradación para cada amenaza. 5. El usuario selecciona guardar información. 6. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la valoración de activo a partir de amenazas en un proyecto
Temas abiertos	Ninguno

Tabla 36 Caso de Uso: Valorar activos vs amenazas

Caso de Uso	**VALORAR AMENAZAS VS SALVAGUARDAS**
Actor Principal:	Usuario
Personal Involucrado:	Ninguno
Precondiciones	• El proyecto debe estar creado • Se debe realizar la valoración de salvaguardas
Garantías de éxito	El usuario podrá definir que salvaguarda debe utilizar para cada una de las amenazas relacionadas con el proyecto.
Flujo Básico	1. El usuario selecciona un proyecto. 2. El sistema retorna la lista de amenazas

	relacionadas con el proyecto. 3. El usuario asocia salvaguardas a cada amenaza. 4. El usuario selecciona guardar información. 5. El sistema notifica que los datos han sido actualizados.
Flujo Alternativo:	2.a La conexión falla, causando pérdida de paquetes entre el aplicativo y el servidor 2.a.1 El sistema notifica el fallo
Requisitos Especiales:	Ninguno
Lista de tecnologías y variaciones de datos	Ninguno
Frecuencia	Cada vez que se modifique la valoración de activo a partir de amenazas en un proyecto
Temas abiertos	Ninguno

Tabla 37 Caso de Uso: Valorar amenazas vs salvaguardas

6.3 VISTA DE PROCESOS

6.3.1 DIAGRAMA DE ACTIVIDADES GESTIÓN DOCUMENTAL

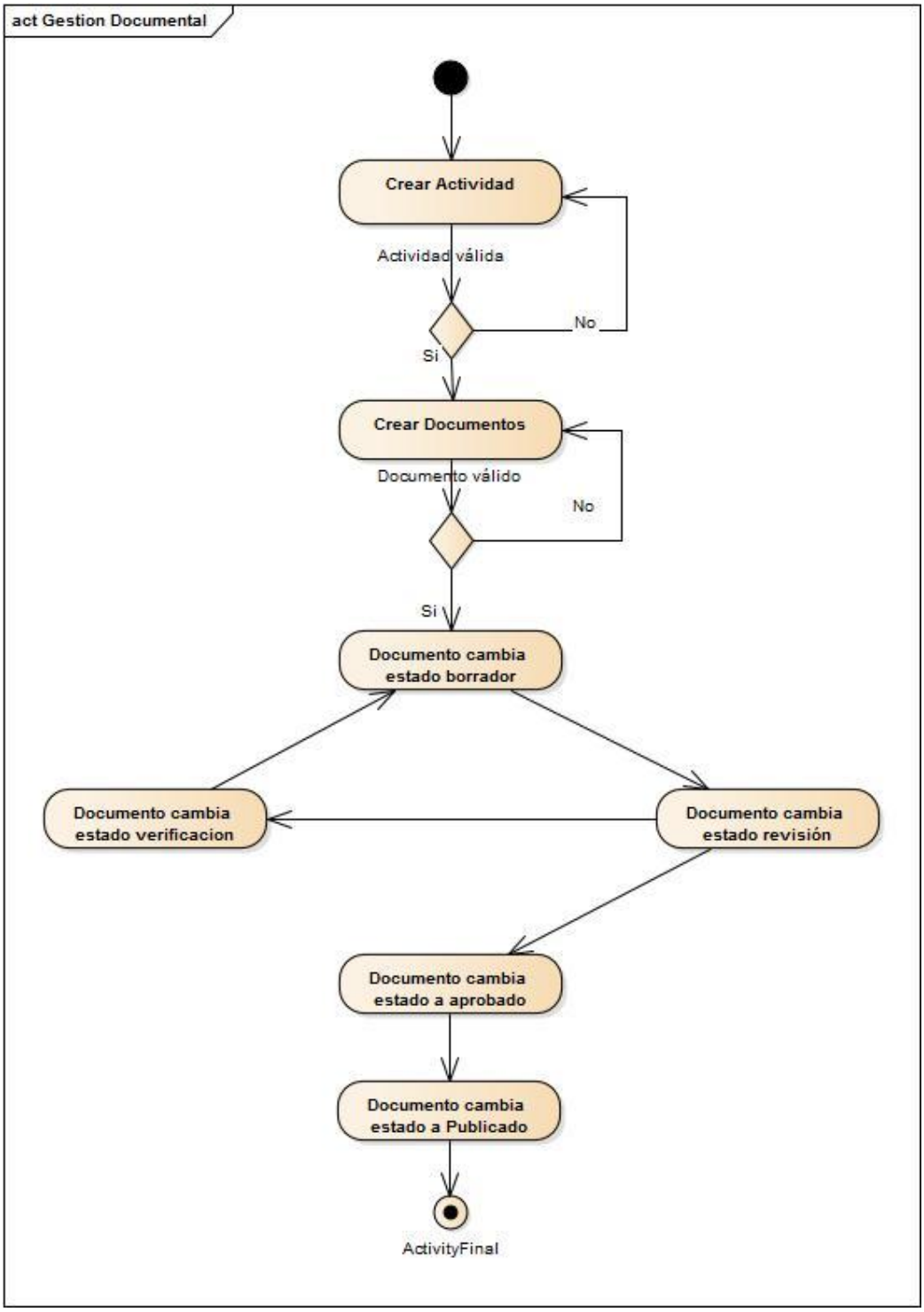


Ilustración 26. Diagrama de actividad - gestión documental

6.3.2 DIAGRAMA DE ACTIVIDAD ANÁLISIS DE RIESGOS

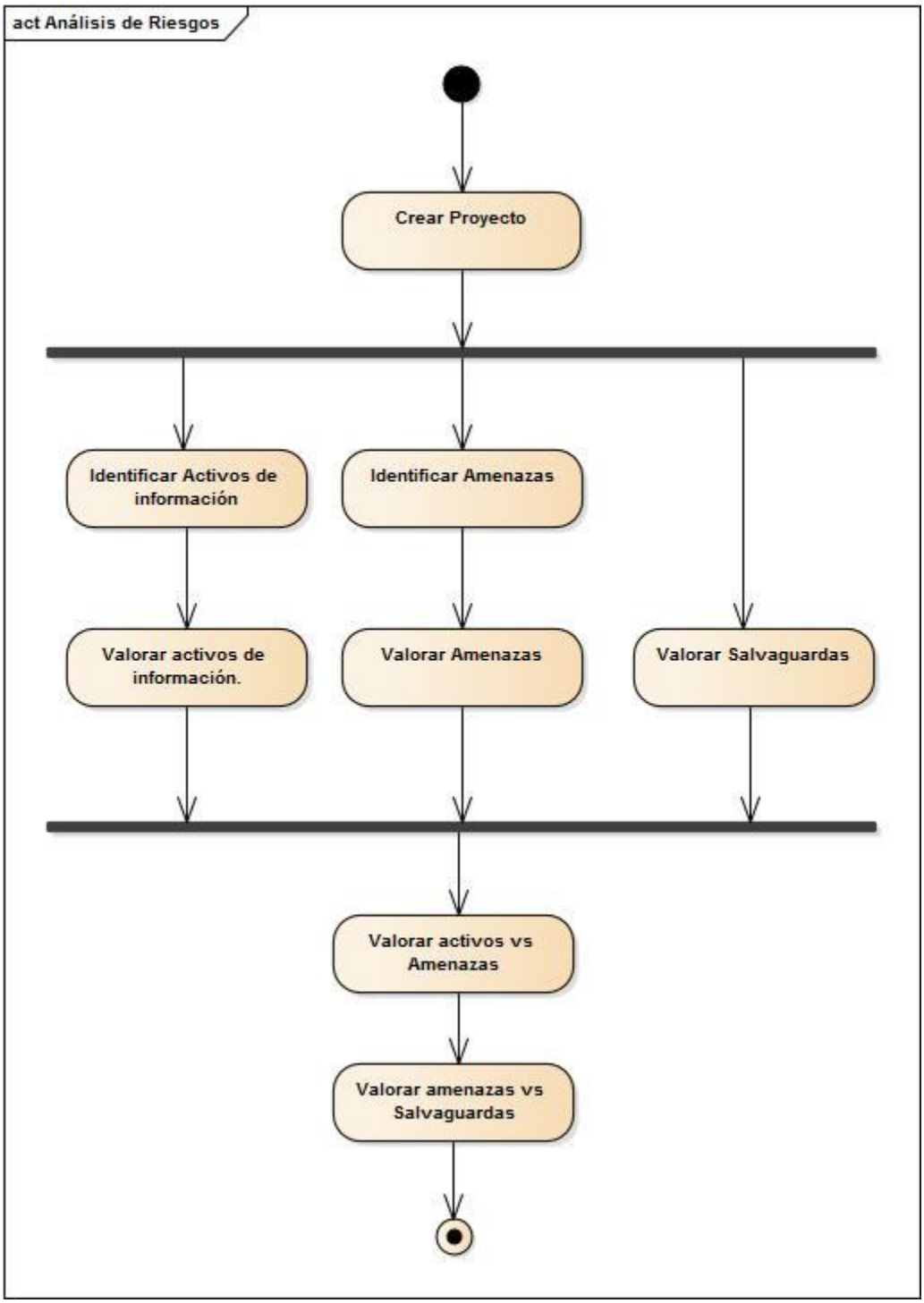


Ilustración 27. Diagrama de actividad: análisis de riesgos

6.3.3 DIAGRAMA DE ACTIVIDAD GESTIÓN DE ACTIVOS

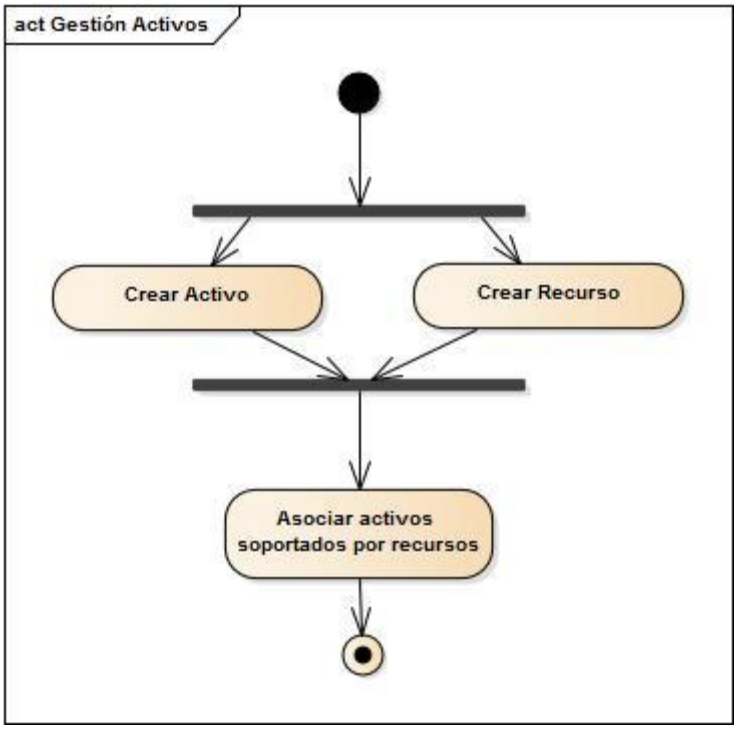


Ilustración 28. Diagrama de actividad - gestión de activos

6.3.4 DIAGRAMA DE ACTIVIDAD GESTIÓN DE ROLES

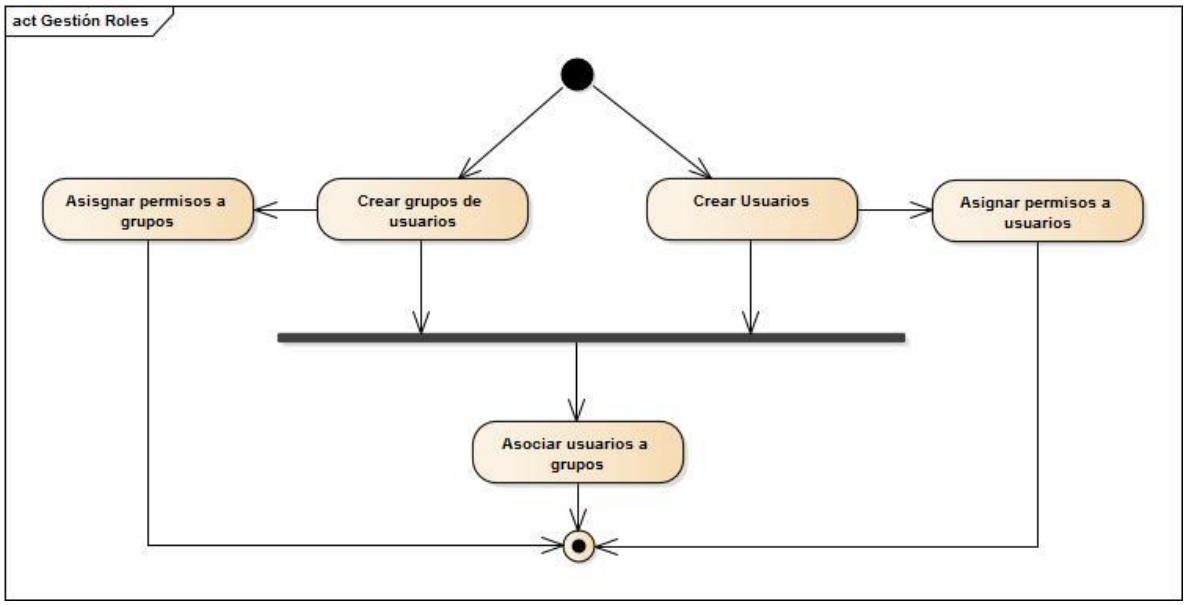


Ilustración 29. Diagrama de actividad - gestión de roles

6.4 VISTA LÓGICA

6.4.1 DIAGRAMA DE CLASE ANÁLISIS DE RIESGOS

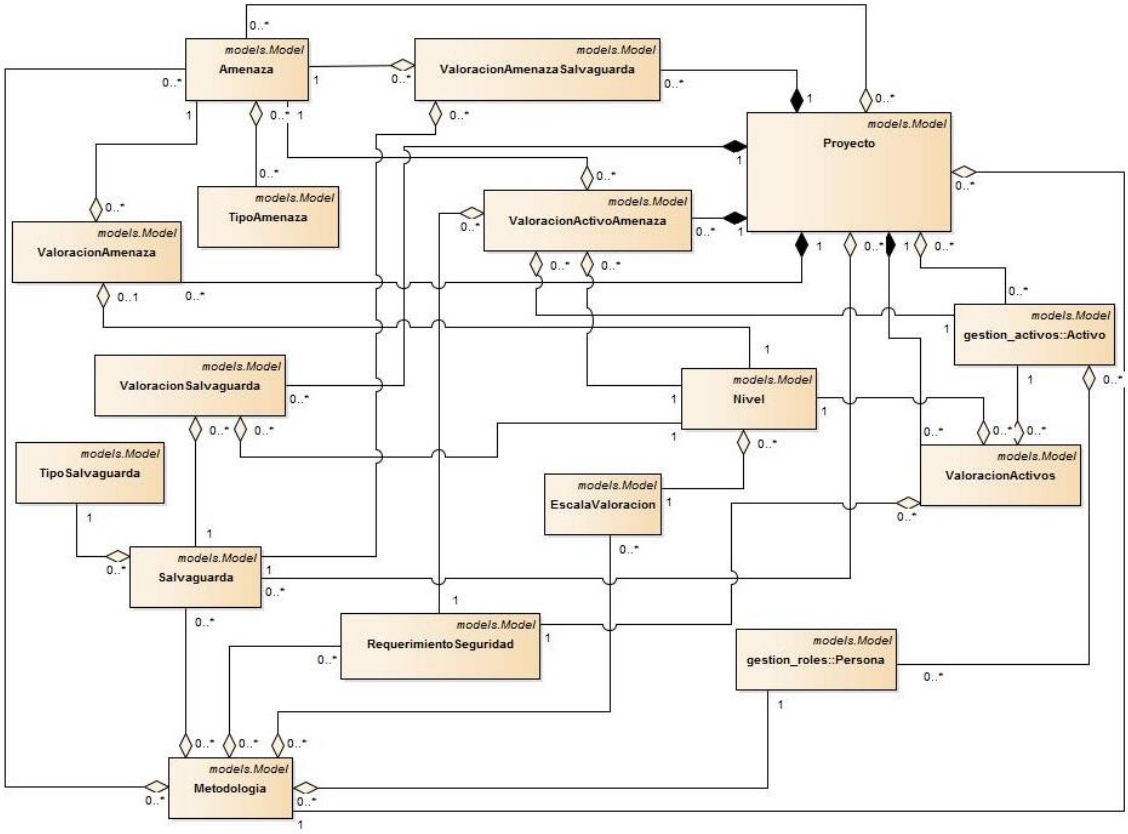


Ilustración 30. Diagrama de clases análisis de riesgos

6.4.2 DIAGRAMA DE CLASE GESTIÓN ACTIVOS

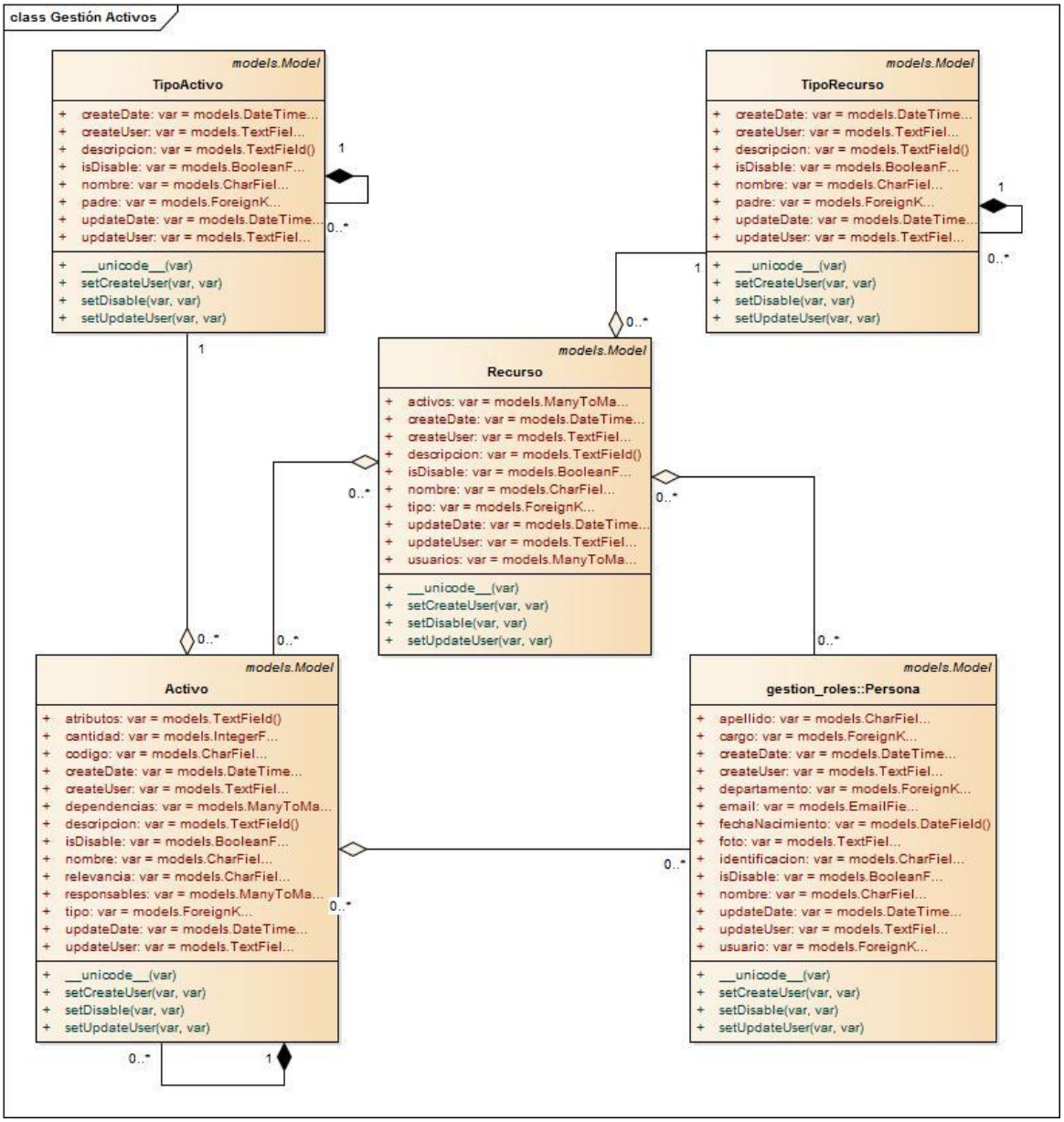


Ilustración 31. Diagrama de clases gestión activos

6.4.3 DIAGRAMA DE CLASE GESTIÓN DOCUMENTAL

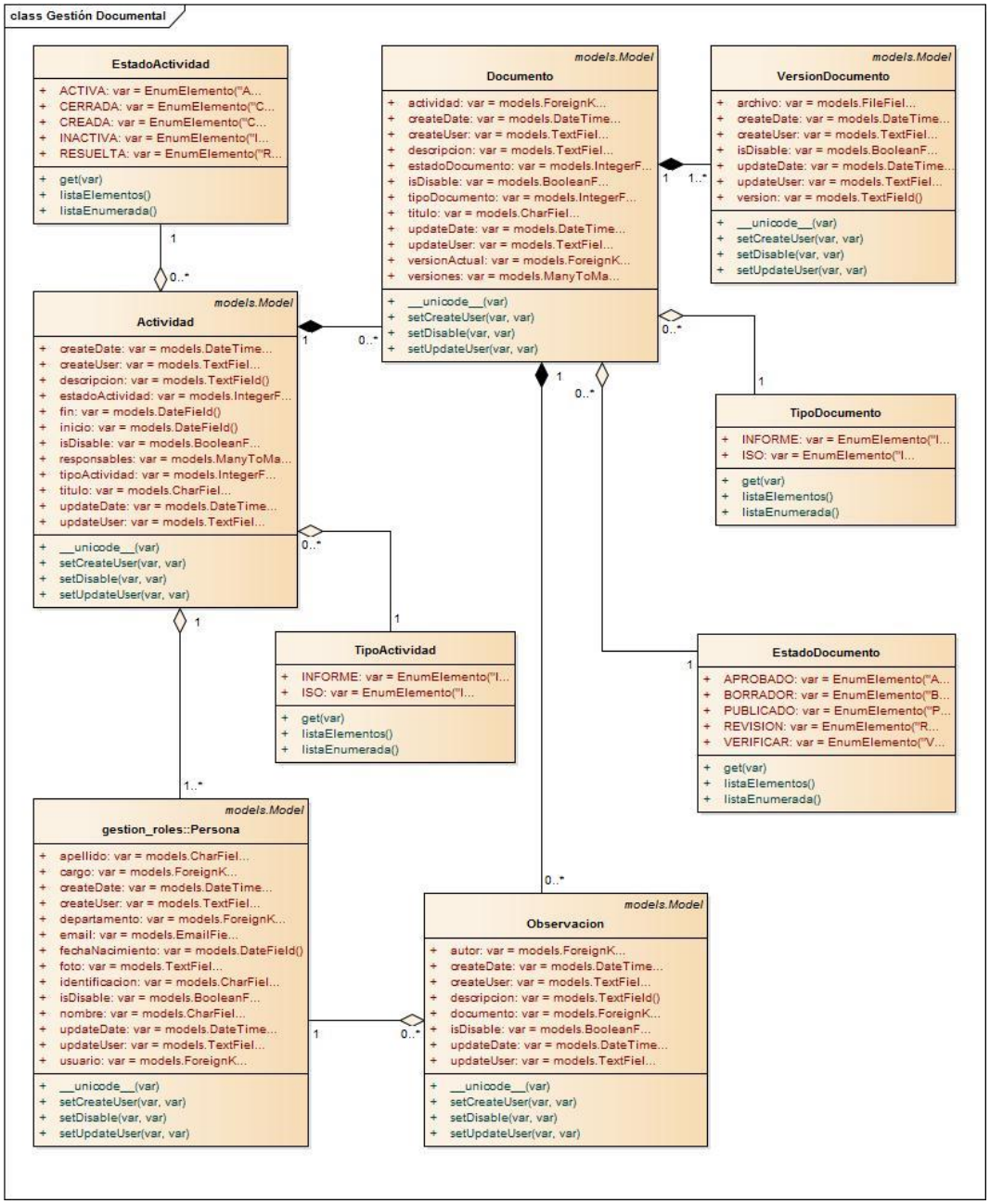


Ilustración 32. Diagrama de clases gestión documental

6.4.4 DIAGRAMA DE CLASE GESTIÓN ROLES

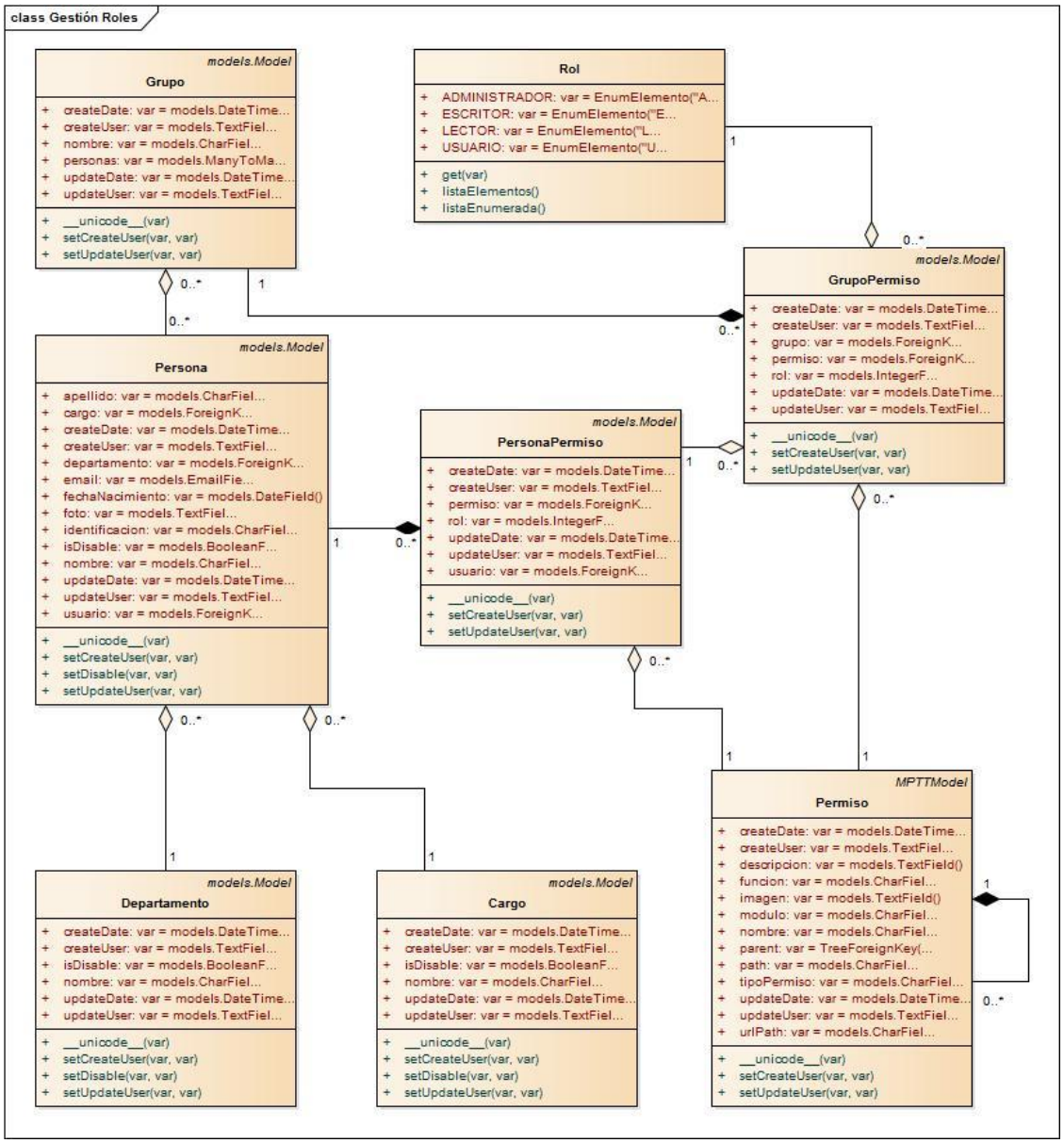


Ilustración 33. Diagrama de clases gestión roles

6.5 VISTA FÍSICA

6.5.1 DIAGRAMA DE DESPLIEGUE

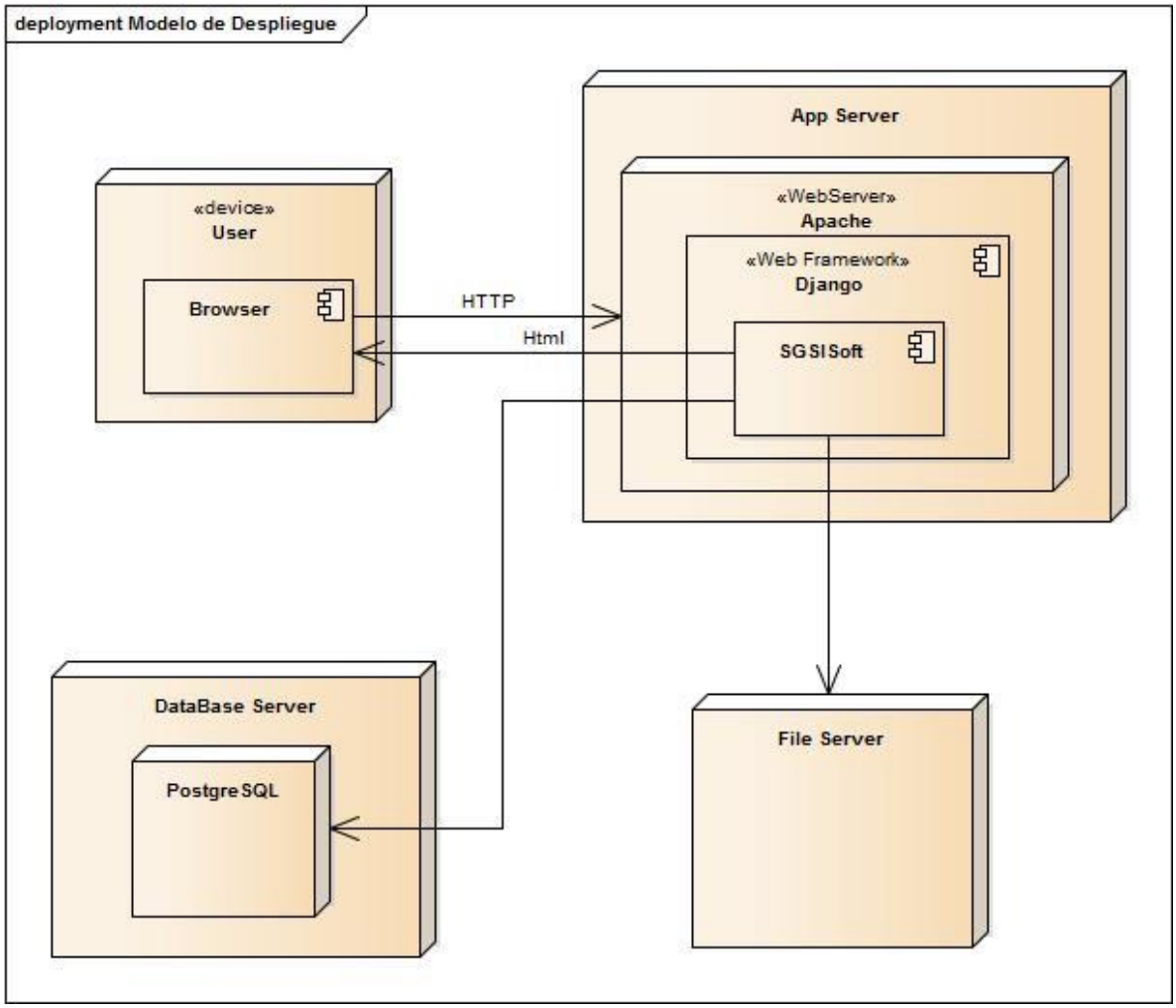


Ilustración 34. Diagrama de despliegue

7. EVALUACIÓN Y PRUEBAS DEL SISTEMA

La etapa de prueba, consistió en ejecutar todas las pruebas unitarias y funcionales de la aplicación, tomar datos experimentales para corroborar el buen funcionamiento de todos los módulos. Los resultados se pueden apreciar en las siguientes imágenes alusivas y representativas de cada componente del software de apoyo al proceso de implantación de un SGSI.

En la aplicación se manejan dos roles principales, usuario y administrador quien este último se encarga de las asignaciones y revisiones de actividades relacionadas con todo el enfoque colaborativo al proceso de implantación. La ilustración 32, muestra el panel de administración donde acciones de gestión como activos, recursos, documentos, riesgos, reportes y seguimiento a los mismos.

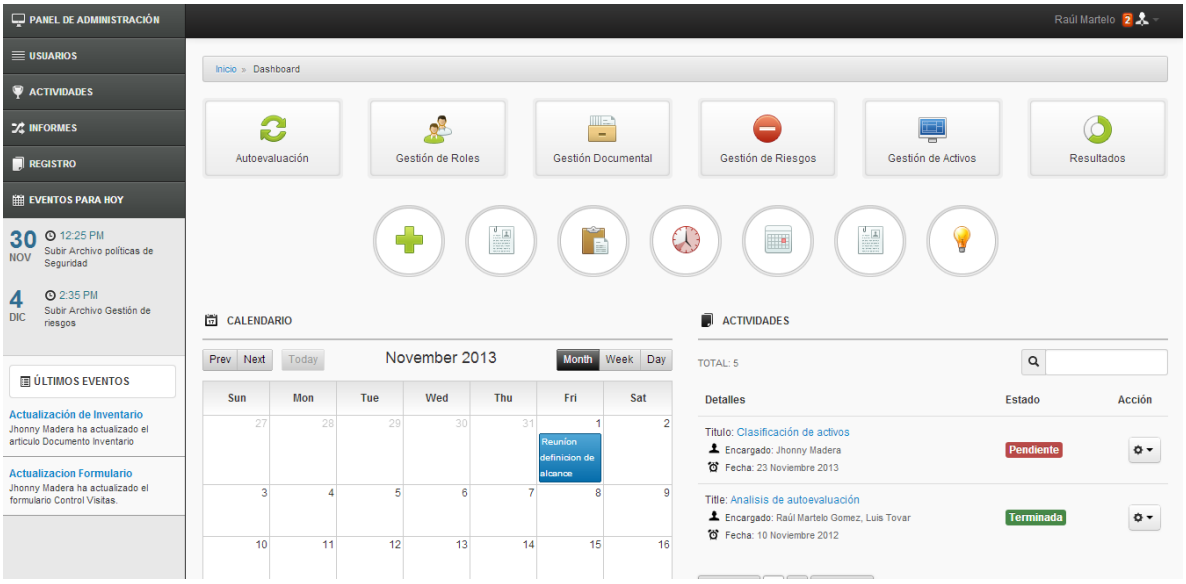


Ilustración 35. Panel de administrador.

Por otra parte, las ilustraciones 33, 34 y 35 representan la gestión de las actividades que luego son convertidas en productos como documentos. La ilustración 33, es el calendario donde se desglosan todas las actividades del usuario conectado.

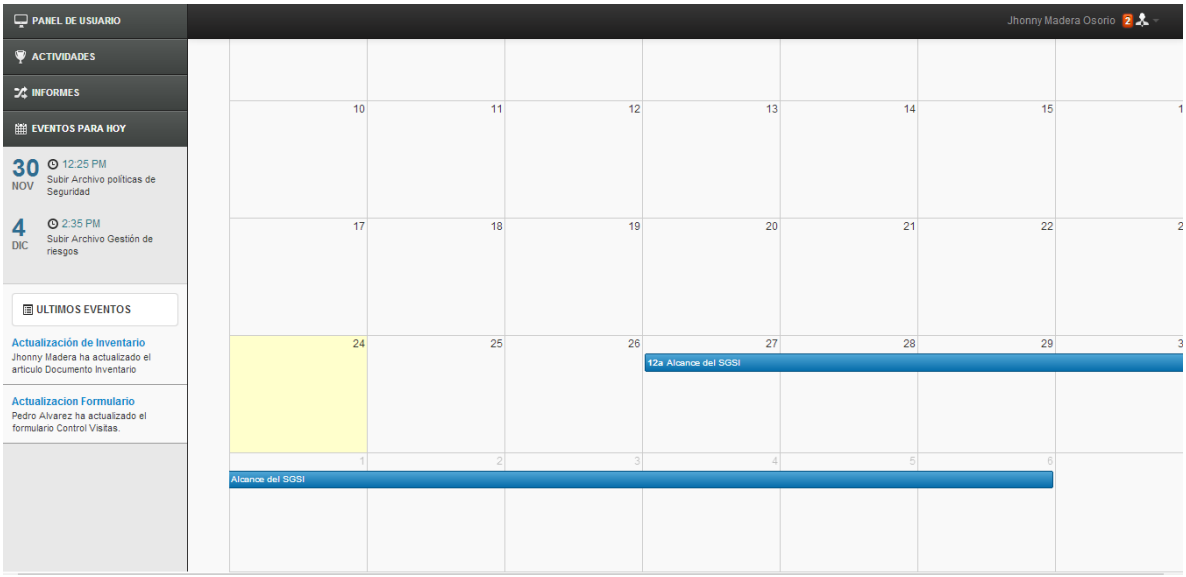


Ilustración 36. Cronograma de actividades

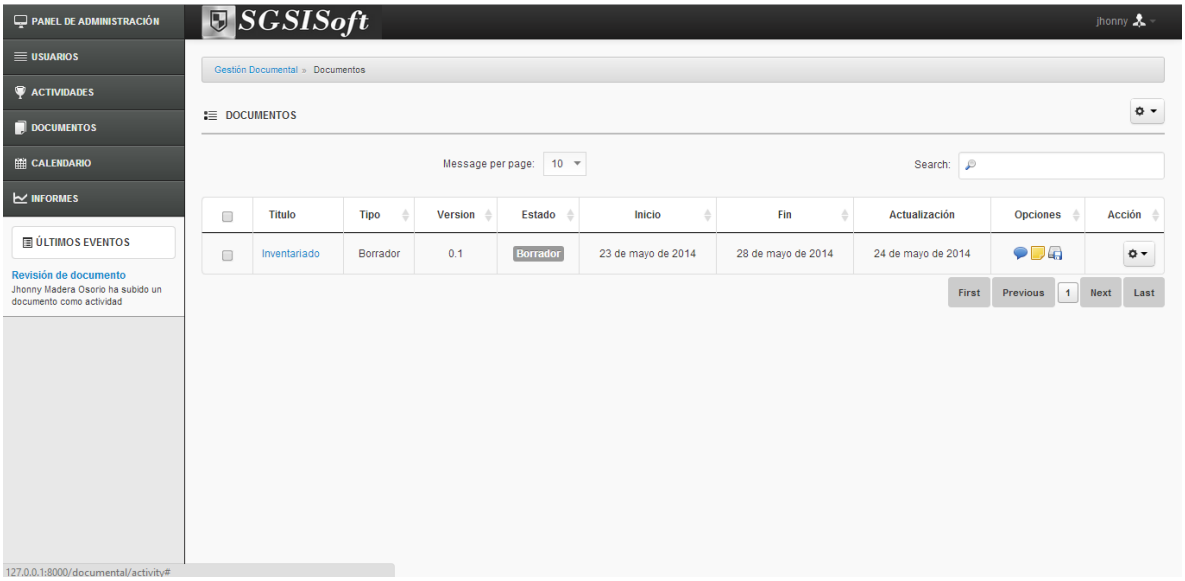


Ilustración 37. Gestión de actividades

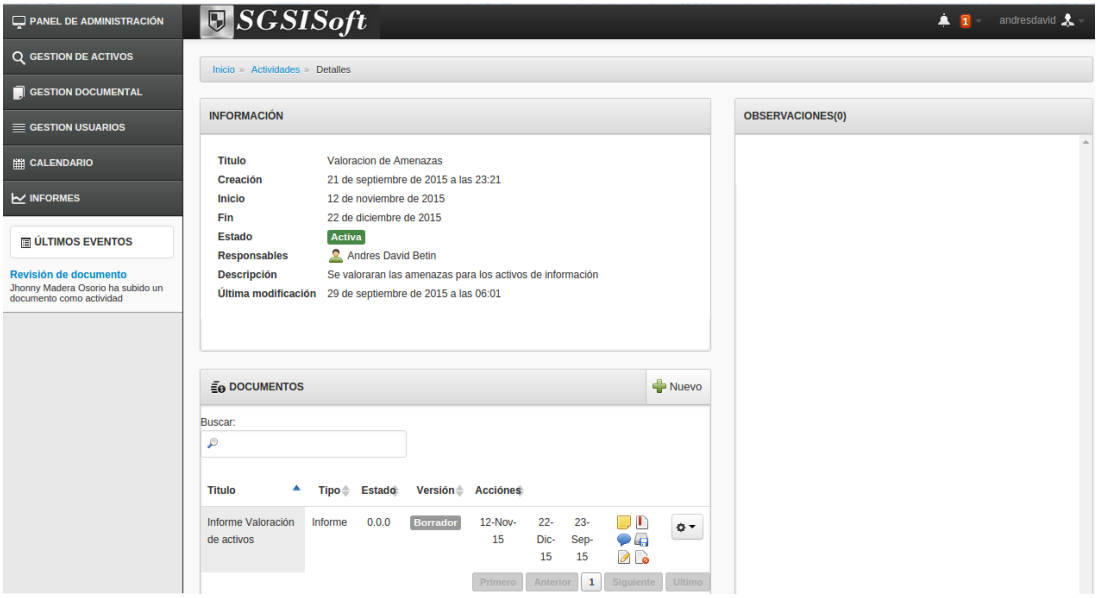


Ilustración 38. Detalle de actividad

La mayoria de actividades generan documentación, la ilustración 36 muestra la subida y creacion de documento, ingresando campos importacntes como “tipo de documento” que porteriomente permitira relaizar ua agrupación para saber el estado de los documentos requeridos por la norma ISO 27001. El resto de ilustraciones muestran el detalle, estados y sguimiento total de los documentos almacenados.

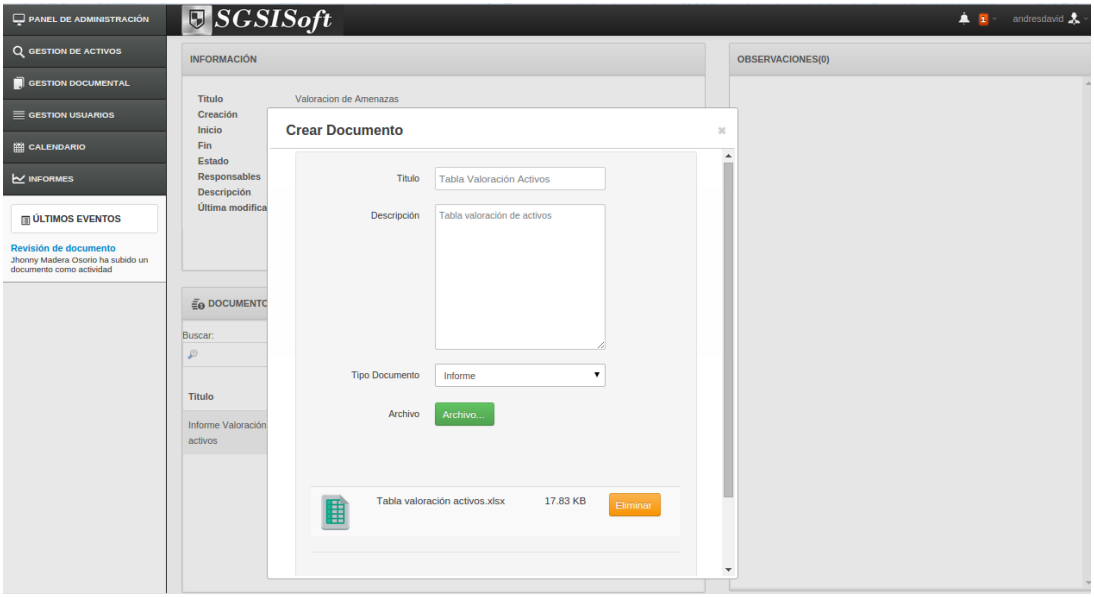


Ilustración 39. Creación de documento

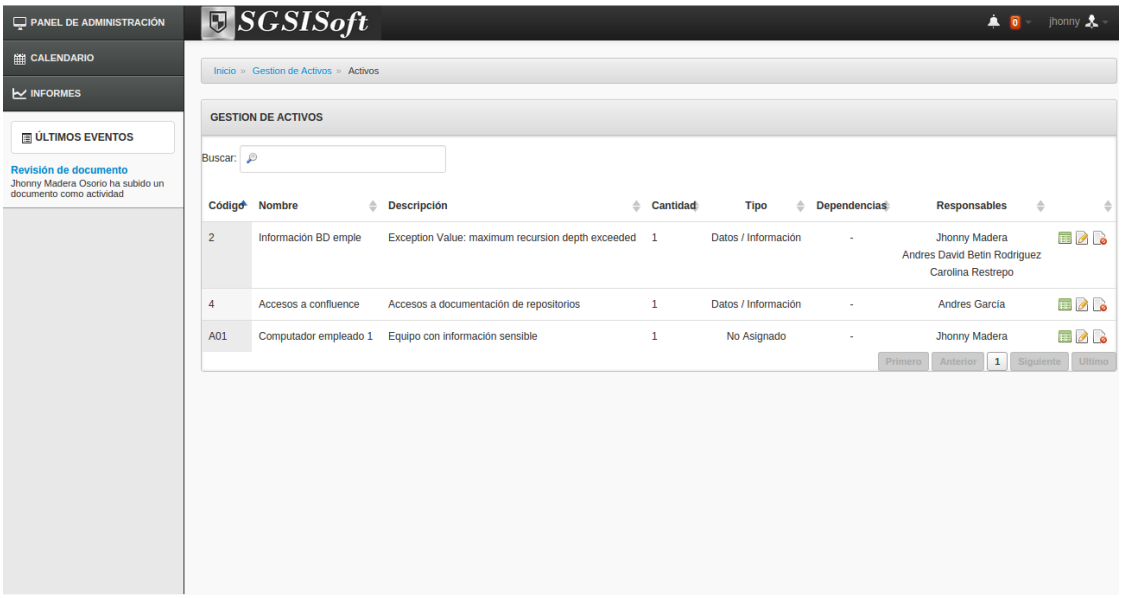


Ilustración 40. Gestión de activos

Ilustración 41. Enviar a revisión un documento

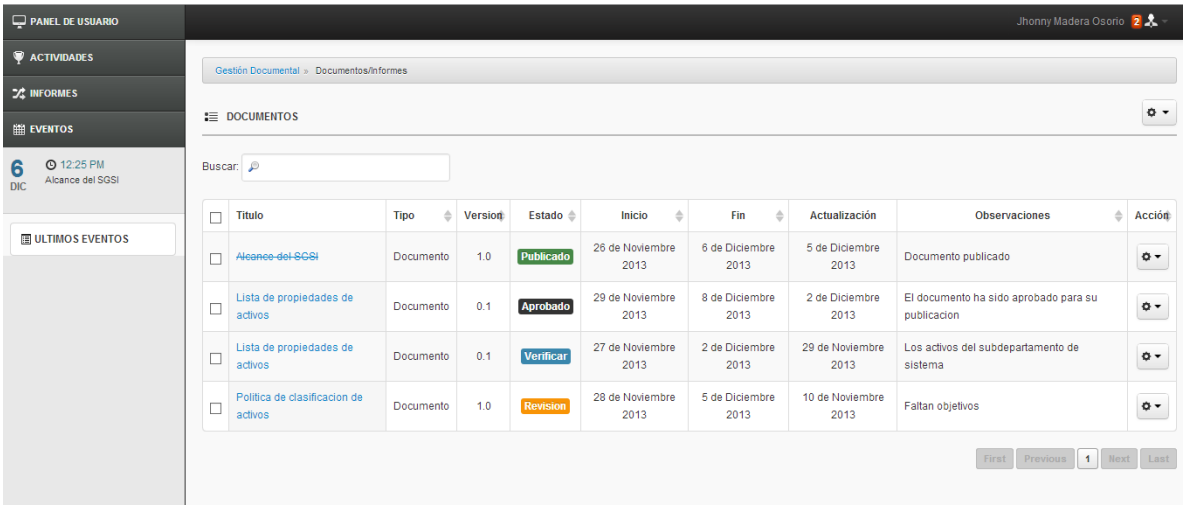


Ilustración 42. Estado de los documentos

Para un analisis de riesgo se ideó realizar proyectos que vayan acorde a los objetivos y alcance del mismo, la creación de este implica digitar campos utiles para un plan de riesgo al final de todo el proceso, por lo tanto, la información básica va relacionado con los objetivos, alcance descripcón y metodología de analisis de riesgos, que permitirá asociar el proyecto a crear con un inventario de activos, amennazas y salvaguardas. (Ilustración 40)

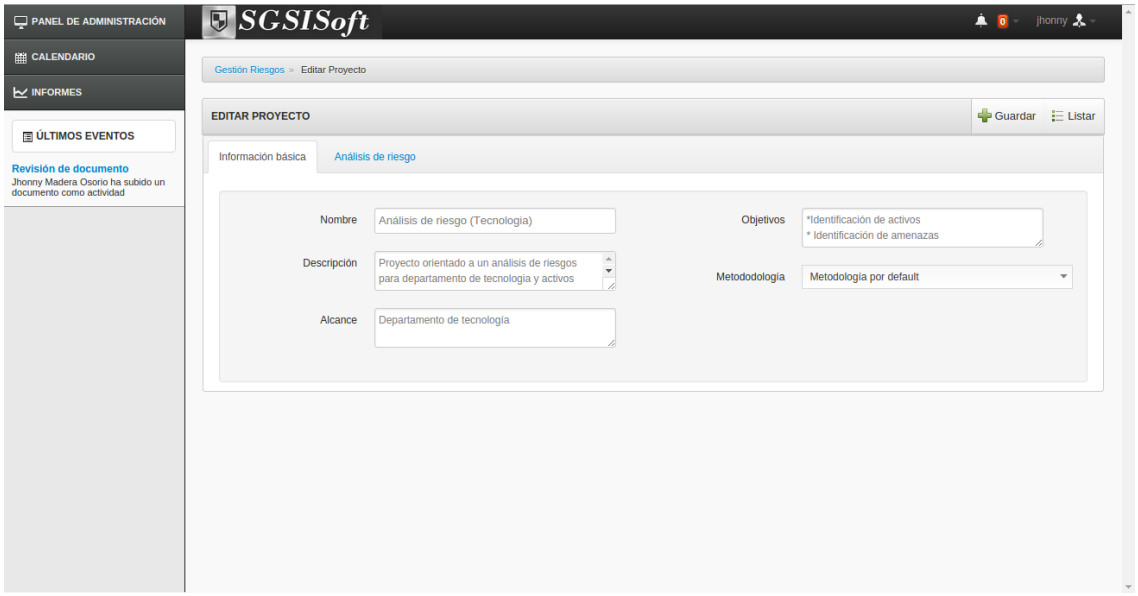


Ilustración 43. Información básica de proyecto de análisis de riesgos

Luego de creado el proyecto se procede a la identificación y valoración de activos, amenazas y salvaguardas, para la recolección de datos y posterior valoración de activos vs. Amenaza frente a los requerimientos de seguridad seleccionados en la metodología.

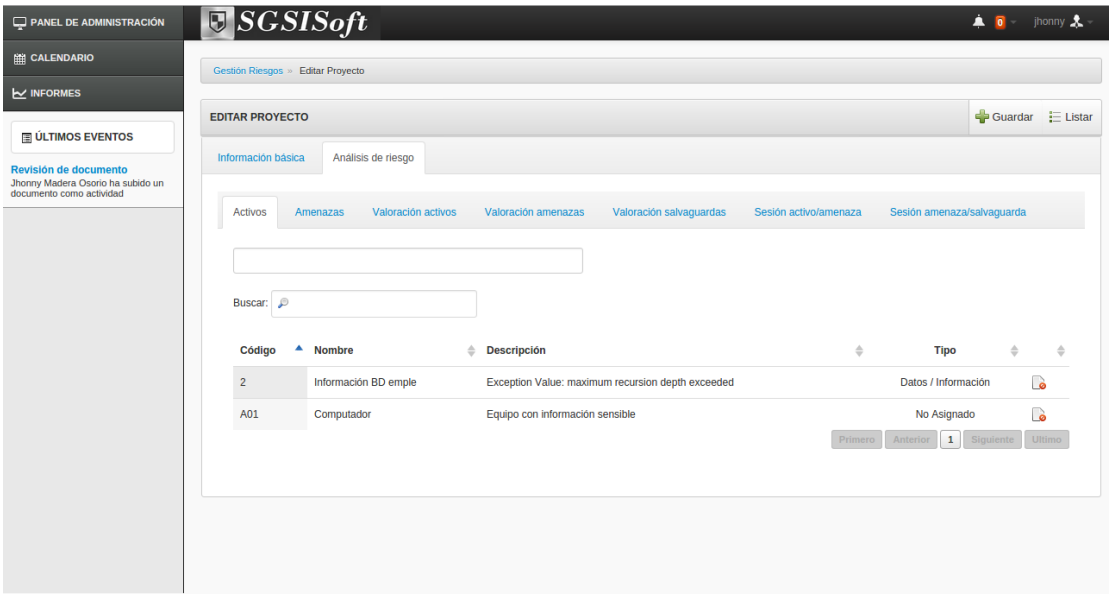


Ilustración 44. Identificación de activos

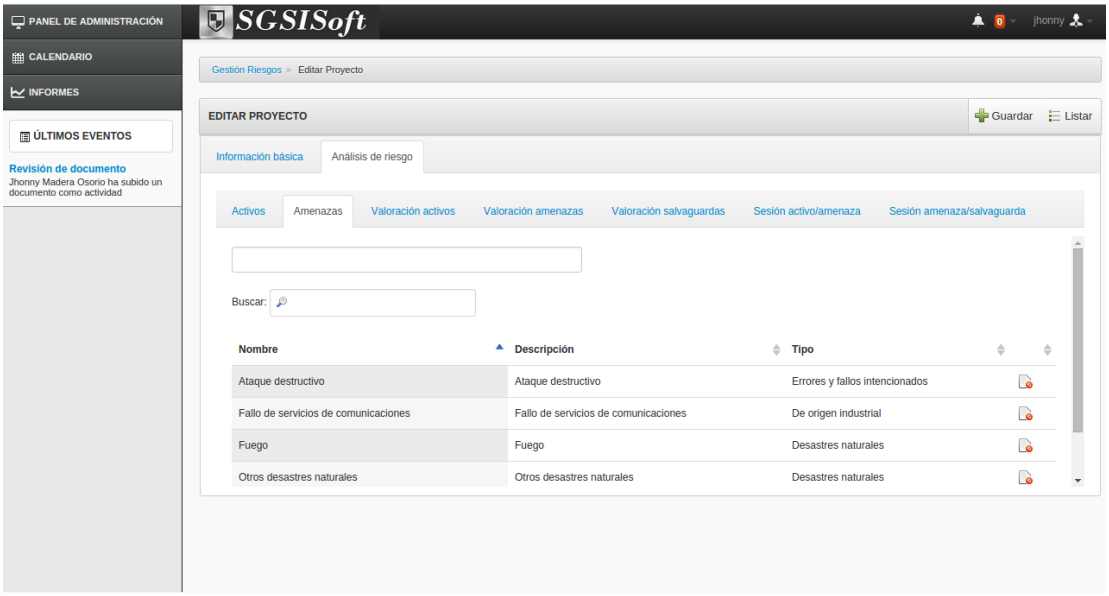


Ilustración 45. Identificación de amenazas

Las valoraciones de los activos, amenazas y salvagudars se realiza a traves de escalas de valoración que a su vez se encuentran como convenciones los valores a ingresar en cada items de valoración.

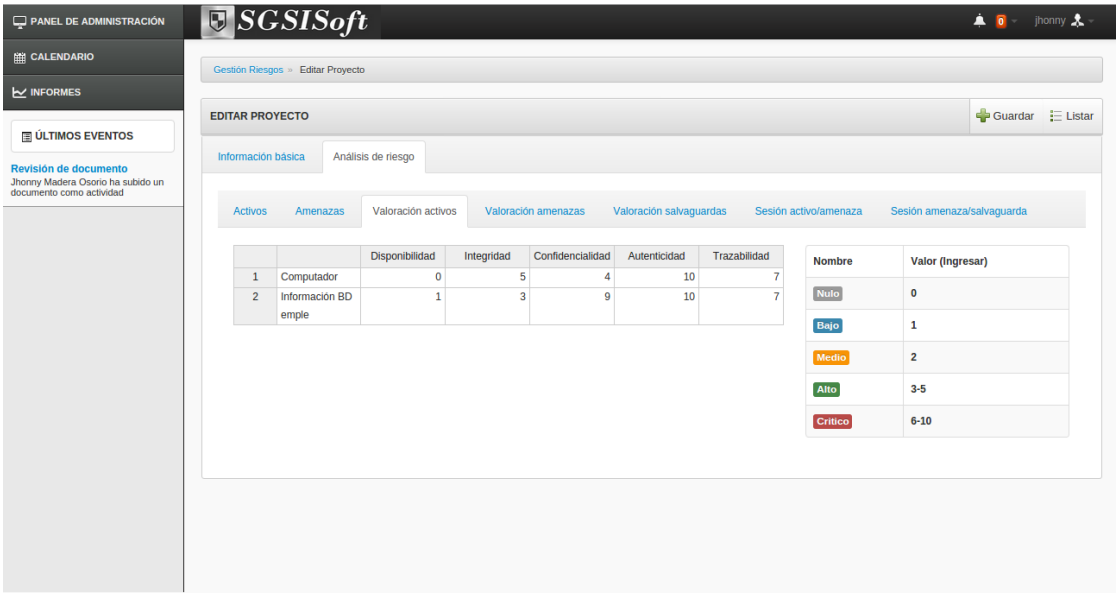


Ilustración 46. Valoración de activos

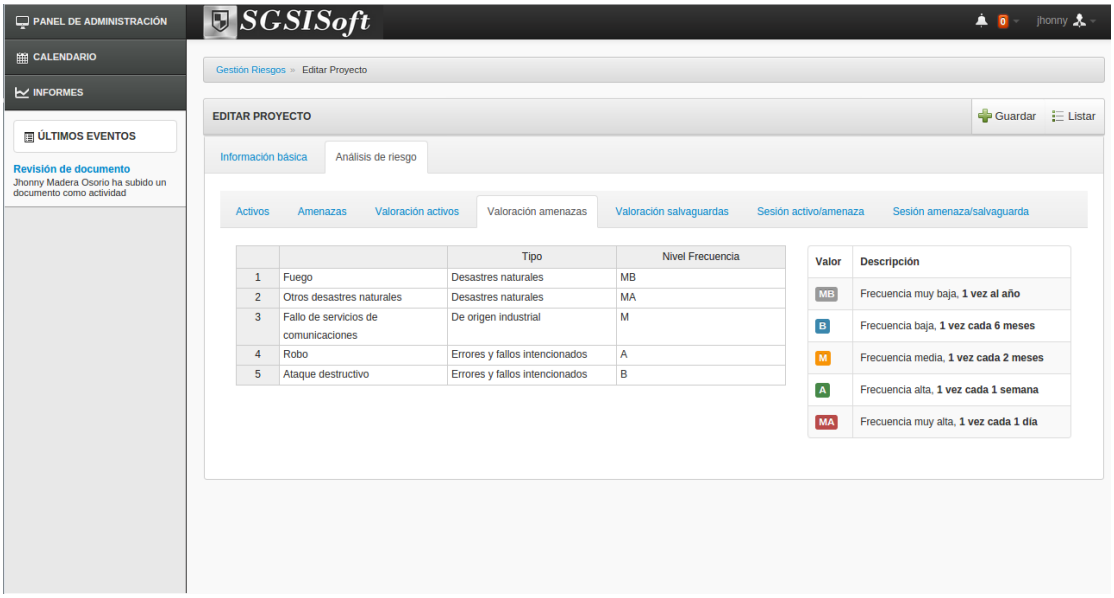


Ilustración 47. Valoración de amenazas

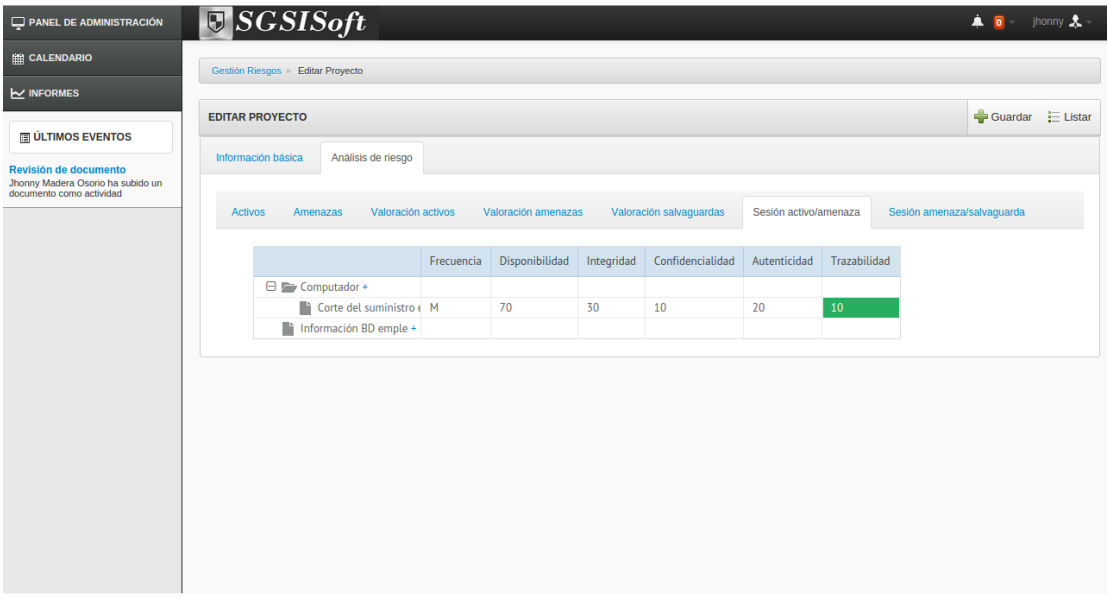


Ilustración 48. Sesión de valoración activos vs. Amenazas

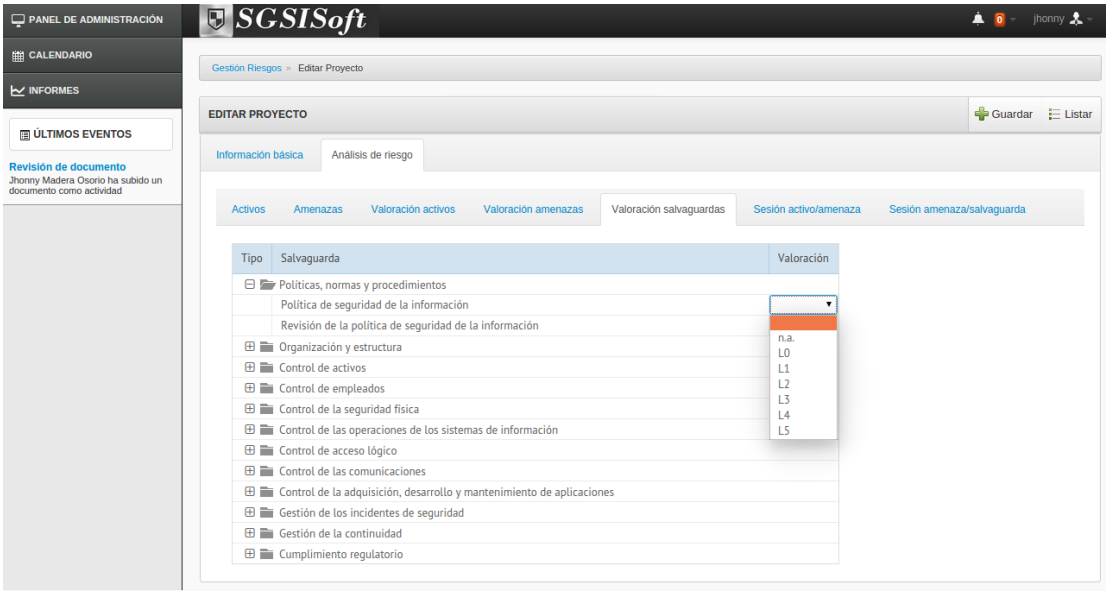


Ilustración 49. Valoración de salvaguardas

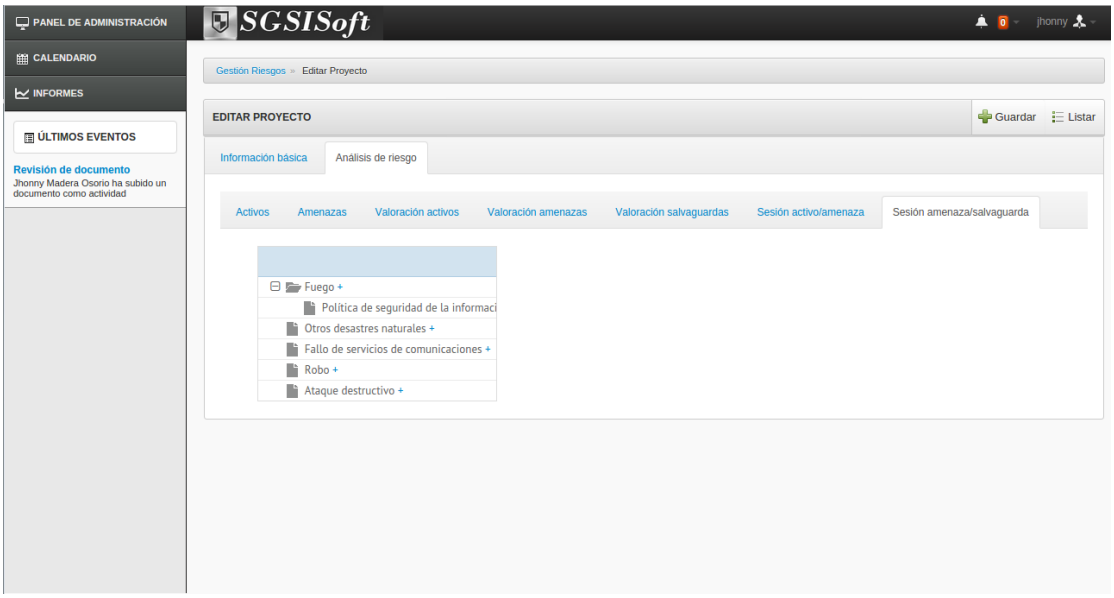


Ilustración 50. Sesión de valoración amenazas vs. Salvaguardas

El módulo de reporte figura reportes asociados a los proyectos de análisis de riesgos. En la ilustración 48 se aprecia El impacto ocasionado por las distintas amenazas que pueden degradar el activo en cada requerimiento de seguridad.

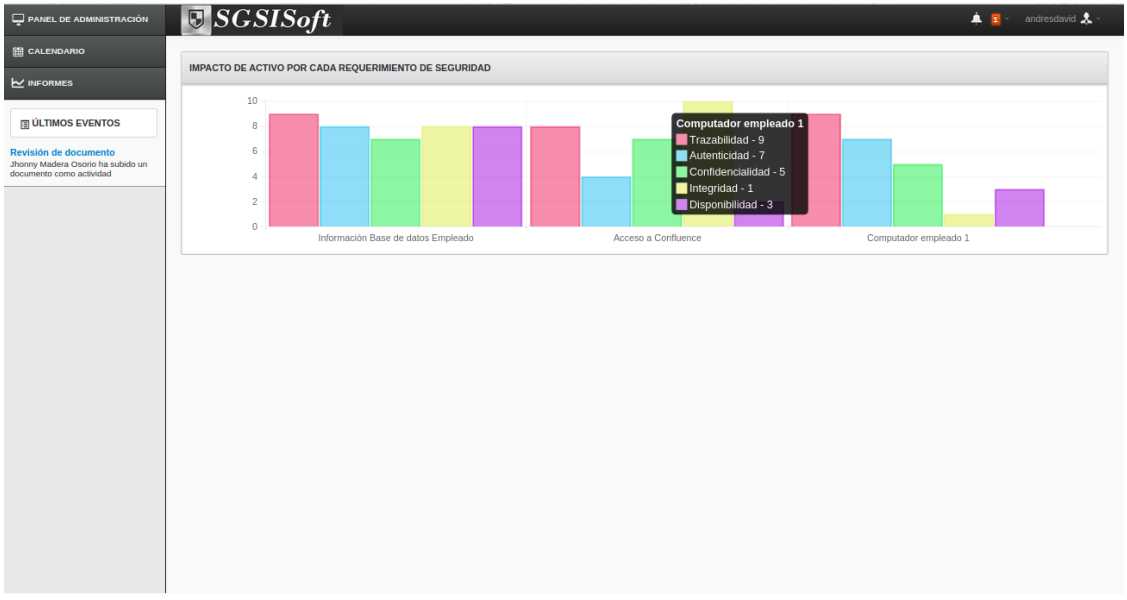


Ilustración 51. Módulo de reporte

7.1 RESULTADOS

En relación a los objetivos del proyecto, los resultados obtenidos con la ejecución del mismo son los siguientes: La construcción de un completo referente teórico, que engloba desde seguridad información hasta los estándares a ser estudiados, como parte del estado del arte y marco de requerimientos de la herramienta a desarrollar. Contacto y comunicación virtual con el Dr. Luis Enrique Sánchez Crespo de España, (Universidad de las Fuerzas Armadas (Ecuador)), asesor en el proceso de investigación. Se aplicaron y diseñaron formatos de técnicas de recolección de información (TRI): Análisis de Contenido y Observación no estructurada; el análisis de los resultados delimitó el proyecto hacia la implementación de etapas fundamentales para el proceso de implantación del SGSI. Dado la complejidad que manifiesta el desarrollo de un proyecto certificable. Delimitado el proyecto, como parte inicial del diseño del esquema o modelo, se realizó la selección de estándares internacionales de seguridad de la información más aplicados, se identificaron aspectos comunes que los caracterizan y permiten describir sus fines y forma de trabajar. Posteriormente se adecuaron para construir el modelo basado en MAGERIT y PILAR, en la medida en que se analizó como se comportaba la norma en un mismo sentido. De esta forma se conocieron ventajas y desventajas. El desarrollo de la sección de Metodología, corresponde a la descripción de las estrategias técnicas y teóricas aplicables al esquema requerido para el desarrollo del software de gestión. La teoría de la dualidad constituyó el fundamento para la definición de la metodología a aplicar en la selección de características y elementos componentes del modelo. Sobre la base de las consideraciones anteriores, se realizó la investigación, extracción, clasificación y depuración de los datos de reportes mundiales sobre los incidentes de seguridad física realizados por la Open Security Foundation mediante la base de datos DatalossDB14. Igualmente, se revisaron estadísticas y tendencias en Colombia y Latinoamérica. Como resultado de estos razonamientos se establecieron los criterios de evaluación de los estándares, asignando una valoración, de acuerdo a la escala planteada; así de seleccionaron y adaptaron características y elementos de COBIT, PILAR, ISO 27001 y MAGERIT, que permitieron estructurar el esquema de solución propuesto en la investigación (sección 5.2.3). Se diseñó la arquitectura del software que corresponde a la implementación del modelo de gestión, a través de modelos

en herramientas I-CASE, que representan las diferentes funcionalidades de la herramienta, siguiendo el modelo 4+1 vistas, y el patrón de diseño software MVC. El consolidado final de la investigación, es el presente documento (destacando la sección 5.2.3 de estructuración del modelo), donde se plasman los resultados teóricos y prácticos. La publicación del articulo para la revista SciELO: **Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)** Vol. 26 Nº 2 2015 y la participación en las ponencias:

Ponencia	Evento	Lugar	Año	Autores
Software Web para el Acompañamiento en el Análisis y Gestión de Riesgos en Pymes	Encuentro Internacional de Investigadores en Administración	Cali	2014	Raúl José Martelo Gómez, David Franco Borré y Jhonny Enrique Madera Osorio.
Integración del Módulo de Autoevaluación y Gestión Documental para el cumplimiento de la Norma ISO 27001	Encuentro Internacional de Investigadores en Administración	Cali	2014	Raúl José Martelo Gómez, Jhonny Enrique Madera Osorio y Andrés David Betin Rodríguez
Aplicación Basada en Software Libre para la Autoevaluación en el Proceso de Implantación de un Sistema de Gestión de Seguridad de la Información	Festival Latinoamericano de Software Libre	Cartagena	2014	Raúl José Martelo Gómez, Natividad Villabona, Jhonny Enrique Madera Osorio y Andrés Betin Rodríguez
Sistema de Gestión Documental basado en Django	Festival Latinoamericano de Software Libre	Cartagena	2014	Raúl José Martelo Gómez, Natividad Villabona, Jhonny Enrique Madera Osorio y Andrés Betin Rodríguez
Software de Apoyo Para el Proceso de Implantación Del	Encuentro Internacional de Investigadores en	Santa Marta	2013	Raúl José Martelo Gómez, Jhonny Enrique Madera

Sistema de Gestión de Seguridad de la Información en Organizaciones Basado en la Norma ISO 27001	Administración			Osorio y Luis Carlos Tovar Garrido

Tabla 38. Participación de ponencias

8. CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

La misma historia se ha encargado de mostrar las numerosas pérdidas de información ocasionadas por la falta de seguridad. De allí el origen de numerosos modelos, metodologías, estándares o normas elaboradas con el fin de dar pautas para mantener la confidencialidad, integridad y disponibilidad de la información; sin embargo, la aplicación de éstos, ha sido una tarea difícilmente asumida por las organizaciones, dada su complejidad.

Así mismo, las metodologías y normas existentes relacionadas con los SGSI no aclaran sus ámbitos de aplicación, resultando una amalgama de normas de compleja aplicación. Esto reduce su posible implantación a las grandes corporaciones; así como la implantación en organizaciones PYMES donde la falta de madurez, desconocimiento total de la seguridad de la información y la ausencia de compromiso, por considerar el desarrollo de los SGSI como proyectos de gran envergadura, establecen evidencias para la necesidad de implementar herramientas de apoyo para el establecimiento de políticas, sistemas y esquemas de seguridad informática en las organizaciones.

El proceso de implantación implica compromiso por parte de toda la organización, por lo tanto involucrar solo el departamento de las Tecnologías de información y comunicaciones (TIC), no conlleva al éxito de la implantación de los SGSI. Es necesario que se asignen los roles y tareas correspondientes a cada uno de los empleados de la empresa. Todos y cada

uno de los empleados están ligados a participar activamente en el desarrollo del sistema de gestión, debido a que de una u otra manera la información es accesible para el personal interno en distintos niveles de sensibilidad.

El compromiso total en el momento de implantar un SGSI debe tener sus raíces enfocadas en la alta gerencia, al mantener esta parte de la organización conectada con el desarrollo del proyecto, se pretende minimizar la dependencia y la manera de ver este proceso como responsabilidad del departamento de las TIC. De tal manera, no se implica el éxito de la implantación del SGSI debido a factores esenciales para determinado logro como la ausencia de la gestión de riesgos, siendo esta el núcleo fundamental del SGSI, la cual permite conocer los riesgos a los cuales se encuentra expuesta la organización, y a través del análisis de los mismos establecer el tratamiento que se considere más adecuado. Algunas organizaciones describen un "análisis de riesgos", donde sólo han evaluado subjetivamente algunas amenazas sobre los activos que más conocen, sin tener una idea clara de su valor y por otro lado sin conformar la totalidad de los activos de la organización o al menos del proceso evaluado. Por lo tanto saber que nos puede pasar y las consecuencias que generaría ese suceso, son aspectos claves al momento de definir una buena estrategia de seguridad. (Del Rio, 2013).

En este sentido, la estructuración de los módulos de apoyo propuestos como parte de solución en el presente proyecto, estuvo marcada por investigaciones amplias que además de confirmar la complejidad asociada a la selección y aplicación de estándares, permitieron responder a los objetivos planteados, a través de diferentes métodos, como la dualidad de la seguridad informática, técnicas formales de recolección de información, el análisis estadístico de informes, y la determinación de criterios de evaluación de estándares para la consolidación de los módulos. Respecto al enfoque dual, es pertinente concluir que, ha sido factor clave para el desarrollo de muchos conceptos que hoy en día son esenciales para el avance no sólo de la tecnología sino de la seguridad información, porque se presenta como una manera complementaria de comprender los elementos, relaciones y efectos de la seguridad de información en el contexto de una realidad cambiante y dinámica. Convirtiéndose en una estrategia que permite trascender a la par de los posibles avances que puedan generar amenazas a nuestros sistemas. Por lo tanto, el modelo de apoyo para la implantación del SGSI, es una

herramienta con fundamentos sólidos, que ofrece pautas a partir de módulos funcionales soportados en los requerimientos del mercado y elementos de estándares internacionales, proyectados en las etapas, orden de trabajo del modelo, alineación estratégica aplicada, análisis de riesgos, sugerencias específicas, documentación metodológica, revisión frecuente, manejo de correcciones y trabajo en Ciclo. Cabe destacar que la definición de los estándares de seguridad estudiados es muy general, lo que limitó en cierto momento la determinación de criterios de comparación y evaluación de éstos, para construir un esquema que respondiera a los requerimientos de seguridad de la información detectados en estudios preliminares.

El trabajo desarrollado fue una experiencia enriquecedora no sólo a nivel profesional sino personal; los miembros del equipo se integraron para realizar tareas de recolección de información, análisis de datos, construcción de conceptos, comprensión y aplicación de teorías, entre otros, que permitieron el intercambio de conocimientos, destrezas y valores humanos, además del fortalecimiento del nivel intelectual. El producto final constituye un modelo conceptual que describe procesos y pautas a apoyar el proceso de implantación del Sistema de Gestión de Seguridad de la Información. Acompañado del sistema software como implementación del mismo y herramienta de facilitación y consolidación de metas.

8.2 RECOMENDACIONES

Tomando como precedente los resultados planteados, se recomienda seguir trabajando en la consolidación del Macro proyecto. Lo que implica completar la parte de apoyo en los módulos de gestión de continuidad del negocio, gestión de incidentes, gestión de comunicaciones y operaciones, y proceso de autoevaluación, dado que esta investigación se delimitó a la gestión de activos, documentos, usuarios y análisis de riesgos. Las bases teóricas adelantadas en el proyecto, pueden agilizar su implementación.

La utilización del modelo y la aplicación, requiere de tiempo y dedicación. Por lo que se sugiere asignar una persona que cumpla el rol de Consultor o Usuario encargado de las tareas, para lograr una implementación adecuada.

REFERENCIAS

Almanza, A.R. (2011). Encuesta seguridad informática en Colombia tendencias 2011-2012.ACIS.

Asociación Colombiana de Ingenieros de Sistemas. (2013). ACIS. Recuperado el 28 de febrero de 2013, de ACIS: www.acis.org.co.

Borghello, C. F. (Septiembre de 2010). Seguridad Informática, sus implicancias e implementación. Universidad Tecnológica Nacional.

Camelo, L. (2013, Marzo 28). Dificultades en la implementación de un SGSI [en línea]. Mensaje enviado a ccamelozing@hotmail.com [2013, Abril 2]

Cano, J.J. & Saucedo, G.M (2012). IV Encuesta Latinoamericana de seguridad de la información tendencias 2012.ACIS.

Del Rio, M. (2011). *Deficiencias más comunes en los SGSI basados en la ISO 27001*. Recuperado el 20 de septiembre de 2013, http://www.securitybydefault.com/2011/08/deficiencias-mas-comunes-en-los-sgsi.html

Donders, E. J. (2010). Formulación de un modelo electrónico y una metodología que permitan diseñar, implantar y mantener un plan de Sistema de Gestión de Seguridad de la Información para PYMES: e-SGSI. Tesis de maestría, Universidad Central de Chile, Santiago, Chile.

Dussan Clavijo, C. A. (2006). Políticas de seguridad informática. Unilibre Cali.

ESET. (2012). ESET Security Report Latinoamérica 2012.ESET.

Foundation, O. S. (2014). DataLossDB Open Security Foundation. Recuperado el 14 de 09 de 2014, de DataLossDB Database - 2014 yearly report: http://datalossdb.org/

González, M. (2010). Seguridad de la información, de asignatura pendiente a activo empresarial. Revisado el dia 10 de abril 2013 de: http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=591

Huerta, A. V. (2004). El Sistema de Gestión de Políticas de Seguridad de la Información. Valencia.

Huerta, A. V. (2004). *El Sistema de Gestión de Políticas de Seguridad de la Información.* Valencia.

Ingenia. (2010). Recuperado el 28 de Abril de 2013 de https://www.e-pulpo.es/

INTECO. Sistema de gestión de la seguridad informática. Obtenido de INTECO: http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/index.html.

ISO/IEC 27001:2005. *Information technology – Security techniques - Information security management system implementation guidance*. Recuperado el 20 de septiembre de 2013, http://web.bryant.edu/~commtech/guidelines/iso27001.pdf.

Kusotic D. (Productor). (2010). What is ISO 27001? (Video). Croacia.

L, Paul. (2002). How to Deal With Resistance to Change. Recuperado el 22 de octubre de 2013, http://hbr.org/1969/01/how-to-deal-with-resistance-to-change

Law, E. L. C., & Lárusdóttir, M. K. (2015). Whose Experience Do We Care About? Analysis of the Fitness of Scrum and Kanban to User Experience.*International Journal of Human-Computer Interaction*, *31*(9), 584-602.

Linares, S., & Paredes, I. (2007). IS2ME Seguridad de la Información a la Mediana Empresa.

Marrugo, Y. & Núñez, R. (2012). Software de apoyo al proceso de creación y registro de políticas de seguridad informática en organizaciones. Tesis de grado no publicada, Universidad de Cartagena, Cartagena de Indias, Colombia.

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Tesis de Maestría, Universidad de la Republica, Montevideo, Uruguay.

Peres, A. L., & Meira, S. L. (2015, June). Towards a framework that promotes integration between the UX design and SCRUM, Aligned to CMMI. In*Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on* (pp. 1-4). IEEE.

Susanto, H. & Bin, F. Multimedia Information Security Architecture. @ IEEE. 2010.

Susanto, H., Almunawar, M. N. & Chee, Y. I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains. Journal of Computer, Asian Transaction. July 2011.

Universia Noticias Colombia. (22 de enero de 2009). Universia. Recuperado el 2 de febrero de 2011, de Universia, red de Universidades, red de Oportunidades: http://noticias.universia.net.co/publicaciones/noticia/2009/01/22/239003/seguridad-informatica-es-realidad-colombia-gracias-proyecto-investigacion-icesi.html

Virusprot. (2010). Recuperado el 20 de Agosto de 2010, de Virusprot: www.virusprot.com

ANEXO 1

ARTICULO REVISTA SciELO: SOFTWARE PARA GESTIÓN DOCUMENTAL, UN COMPONENTE MODULAR DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Andrés D. Betín, Jhonny E. Madera y Raúl J. Martelo

Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA, Avenida del Consulado, Calle 30, No. 48 – 152, Cartagena-Colombia.(e-mail: abetinr@unicartagena.edu.co , jmaderao@unicartagena.edu.co, rmartelog1@unicartagena.edu.co)

RESUMEN

El objetivo principal de este trabajo consistió en desarrollar un software para garantizar el control de los documentos generados a partir del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI); dicho software permite recepcionar, administrar y organizar la documentación generada en el proceso de implantación del SGSI y como valor agregado, se dispone: gestión y seguimiento al encargado en desarrollar el documento asignado. Para soportar dicho software, se diseñó e implementó un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. Lo anterior, produjo como resultado un módulo para gestión documental que permite el control de documentos por parte de la organización participante en el proceso de implantación de un SGSI.

Palabras claves: software, información, seguridad, ISO 27001, documentación.

SOFTWARE TO DOCUMENT MANAGEMENT, A MODULAR COMPONENT OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

ABSTRACT

The main objective with this paper, it was to develop a software to ensure generated document control based on the implantation process on an Information Security Management System (ISMS); this software allows to receive, manage and organize the documents generated on the process of implantation of ISMS. As added value is: management and monitoring of the person in charge of developing the assigned document. To support this software, it was designed and implemented a model that defines management actions necessary to approval, reviews, updates, states and legible documents through the life cycle of ISMS. As a result, it was created a document management module that allows the control on documents, which handle the organization involved in the implementing process of ISMS.

Keywords: software, information, security, ISO 27001, documentation.

INTRODUCCIÓN

La información se ha convertido en activo importante de organizaciones (Piattini & Del Peso, 2001), toda vez cuando es completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas. La importancia de la información se fundamenta en la teoría de la organización, la cual se define como un sistema conformado por personas, recursos materiales e información; existe una percepción sobre el concepto de información en la cual se indica que determina "el 'orden y el caos' entre los individuos, los recursos y en la interrelación personas-recursos" (Aja, 2002); por eso, debe considerarse a las organizaciones como sistemas de información.

Sin embargo dichos sistemas a medida que consultan, almacenan y generan información, ponen en riesgo la integridad de la misma; riesgos, que no solo provienen del exterior sino también del interior de la organización (INTECO, 2010). Los virus, gusanos, hackers, phishing e ingenieros sociales, entre otras, son amenazas constantes que atentan contra la

información de cualquier organización (Susanto et al, 2011a). Un Hacker, puede causar pérdidas considerables para una organización, tales como, robo de datos de clientes y espiar en la estrategia de negocio en beneficio de competidores (Susanto et al, 2011b).

Como consecuencia, la seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas (Von, B. & Von, R. 2004), sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen unas obligaciones para organizaciones (Susanto & Bin, 2010). Las anteriores obligaciones que se ejercen bajo la seguridad de la información, pueden ser solventadas con la ayuda de un SGSI que permite gestionar con eficacia los activos de información, minimizando posibles riesgos que atenten contra la misma (Broderick, 2006).

El SGSI consiste básicamente en un conjunto de políticas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware y recursos de software (ISO/IEC 27001, 2005); estas políticas, muestran la manera en que los recursos del computador pueden ser utilizados (INTECO, 2010). Adicionalmente, el proceso de implantación de un SGSI aborda fases de: auditoría inicial, análisis y procesos de flujos de información, análisis y gestión de riesgos y desarrollo del sistema de gestión bajo un modelo PHVA (Planear-Hacer-Verificar-Actuar), que conlleva a dificultades tales como: falta de documentación, administración y organización de la misma, ausencia de roles y responsabilidades, para llevar a cabo las actividades pertinentes para dar cumplimiento a objetivos y alcances del SGSI (Del Rio, 2013).

En este orden de ideas, abordar el proceso de forma tradicional y, las dificultades evidenciadas en cuanto a la documentación que se genera durante este proceso, sugiere la necesidad de buscar una pronta solución, lo cual se constituye en el objetivo principal de este trabajo.

Para alcanzar el objetivo mencionado anteriormente, se desarrolló un software que enmarca la consecución de los requerimientos y actividades que conforman la debida documentación del SGSI. Como principal resultado, se obtiene un módulo de gestión

documental que permite ejercer un control de documentos y asignación de actividades para miembros del grupo de implantación del SGSI, que facilita la recepción, administración, mantenimiento y estado de la documentación obtenida en el desarrollo del mismo.

TRABAJOS RELACIONADOS

Los Sistemas de Gestión de la Seguridad de la Información bajo los requerimientos que exige la norma ISO 27001, constituyen la base para la gestión de la seguridad de la información; dicha norma, define un SGSI que garantiza el conocimiento, apropiación, gestión y disminución de riesgos de seguridad de la información para la organización, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías (Calder, 2006).

Ahora bien, la necesidad que se ha generado para implantar un SGSI (Cano, J. & Saucedo, G.M., 2013), la problemática que ejerce el proceso tradicional, así como la descentralización y desorganización de la información generada, más la complejidad del desarrollo del SGSI, ha permitido innovar, construir, validar herramientas y modelos que aborden el proceso de implantación del SGSI de principio a fin, bajo el cumplimiento de actividades que lo requieren y la gestión documental de la misma.

De esta forma propuestas como e-PULPO, plataforma que integra un módulo SGSI, enfocado a la primera fase de planificación del mismo, permite el manejo de activos, documentación, incidencias, formación, indicadores y auditorías establecidas por la norma ISO 27001, además de la implementación de controles basado en la norma ISO 27002; e-PULPO se concentra en la gestión documental, la revisión, control y administración de ésta, de manera que la facilidad, interactividad y los componentes distribuidos de su interfaz gráfica del módulo gestión documental, la hace ser una plataforma eficiente, eficaz y regulada en el cumplimiento de sus funciones. (Ingenia, 2010).

Por otro lado, Gesconsultor herramienta que integra 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 (Gesconsultor, 2013). En el mismo sentido, la plataforma GlobalSGSI permite la gestión integral de la norma 27001 y cumple con el ciclo completo de la misma, desde las fases de inicio y planificación del proyecto hasta el mantenimiento y mejora continua, pasando por el análisis de riesgos, el cuadro de mandos e implantación de procedimientos (GlobalSGSI, 2013).

Respecto a metodologías que no han sido materializadas en software, pero que aportan debido a su aplicación en pequeñas y medianas empresas (PYMES), Linares y Paredes (2007), publican Metodología en español para implantación de seguridad de la información para este tipo de empresas, la cual surge como solución y aproximación para el camino a seguir hacia la implementación de la seguridad de la información, en empresas cuyo modelo de seguridad aún no es maduro y desean acometer la labor de implantación de la seguridad de la información y de su sistema de gestión, asociado de una forma eficiente, eficaz y práctica, de forma que permita disminuir el riesgo de la organización a corto plazo, a la vez que se inicie el camino hacia el cumplimiento de los estándares deseados. Por otro lado, María Eugenia Corti (2010) propuso una metodología que permite la disminución de tiempo y costos de implementación de un sistema de gestión para estas empresas en el mediano plazo, en conformidad con la norma ISO 27001 dando cumplimiento a las buenas prácticas según lo establecido en la norma ISO 27002.

MODELO PLANTEADO

En esta sección, se presenta el modelo propuesto para solventar problemas efectuados durante el proceso de implantación de un SGSI, que pueden ser generados por la poca gestión documental. La siguiente figura presenta el modelo conceptual planteado:

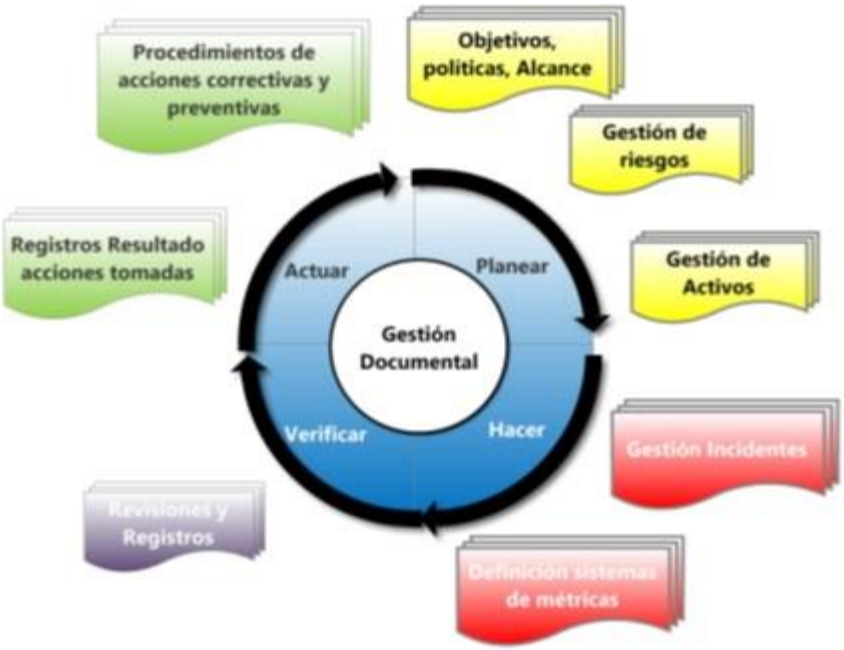


Fig. 1: Modelo conceptual gestión documental. Fuente: Grupo de trabajo basado en ISO 27001.

En la figura de arriba se aprecia un modelo complementario de gestión que reúne características y elementos (estratégicamente adaptados e integrados), fundamentados en la problemática preestablecida y requerimientos actuales, desde una perspectiva de organización, administración y control documental de procedimientos referentes del proceso de implantación del SGSI en la organización. Este modelo permite ejecutar procedimientos documentados durante el ciclo de desarrollo del SGSI y, gestionar documentos generados a partir de módulos o actividades de cada etapa del debido proceso.

Los requerimientos funcionales generados a partir del anterior modelo fueron los siguientes:

Manejo roles de usuarios, Asignación de actividades, Documentos versionados, Actualización de documentos, Gestión de estados de documentos, Notificaciones de actividades y Manejo de calendario.

Así con el fin de atender los requerimientos funcionales expuestos anteriormente, la siguiente imagen representa el panel de ejecución y módulos de apoyo para el componente de gestión documental:

Fig. 2: Panel de administración.

Como se aprecia en la figura anterior, la investigación fue planificada para gestionar procesos relevantes en el desarrollo de un SGSI, enfocándose en el control documental durante el ciclo de vida de dicho proceso. De esta forma, con un modelo orientado a procesos ejecutado bajo un ciclo PHVA, implementa características procedimentales que apoyan de inicio a fin el proceso de implantación, facilitando el debido proceso y manteniendo la continuidad en el negocio, esto, brindado a través de un software que contribuye a la flexibilidad, portabilidad, facilidad de uso e integridad, con módulos de apoyo al cumplimiento de las metas del proceso de implantación de un SGSI.

RESULTADOS

Con el fin de dar cumplimento al objetivo principal de este artículo, se desarrolló un módulo de gestión documental para control de documentos generados durante el proceso de implantación de un SGSI. Este módulo garantiza la organización, versión, apoyo y

accesibilidad al material documental para procesos de auditorías y certificación del sistema de gestión. Además, permite un seguimiento exhaustivo para cada documento, creado a partir de actividades asignadas a usuarios partícipes de este proceso. Estos documentos pasan por distintos estados que definen el ciclo PDCA y un proceso secuencial, que continúa de un estado borrador, revisión, verificación, aprobado, hasta que sea publicado para un grupo seleccionado por el administrador del sistema o, en su defecto, el encargado del desarrollo del SGSI.

La figura 3, muestra los estados del documento y las características que permiten una gestión eficiente en cuanto a seguimiento, mantenimiento, facilidad y control documental durante todo el proceso.

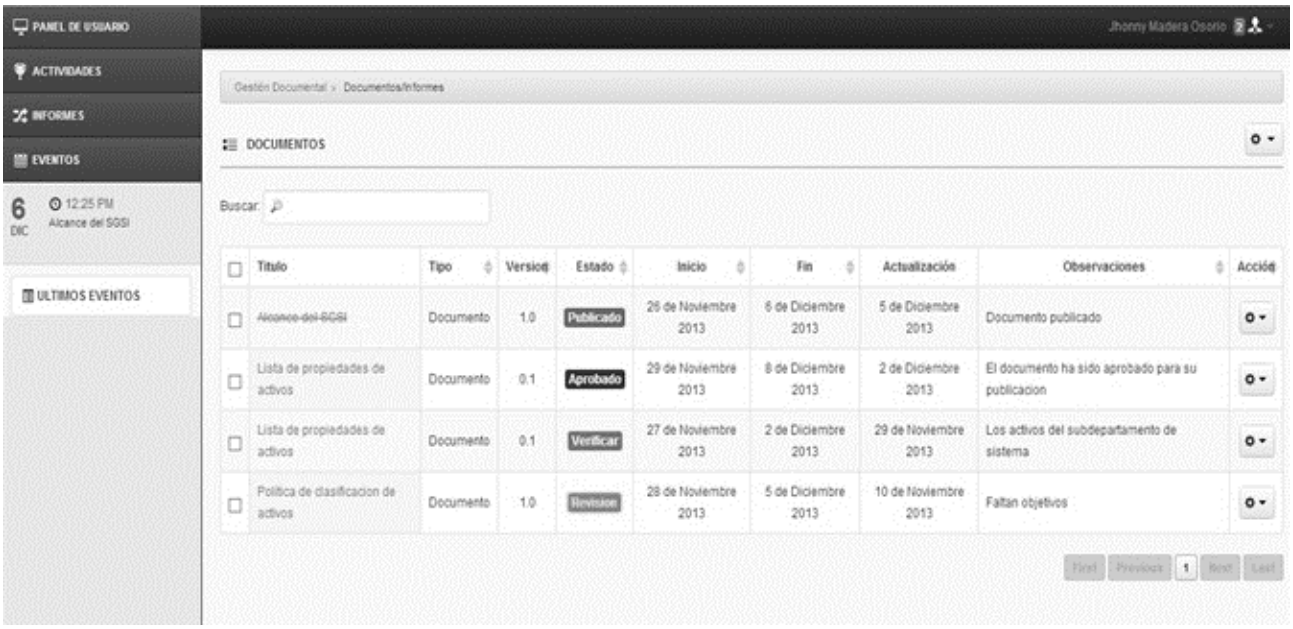


Fig. 3: Gestión documental.

CONCLUSIONES

De los resultados obtenidos, se pueden anunciar las siguientes conclusiones sobre el modelo y la herramienta que lo soporta: 1) Permite identificar el estado de los documentos; 2) Previene la utilización de documentos obsoletos; 3) Compromiso bajo la gestión de roles y asignación de actividades; 4) Garantiza la disponibilidad, accesibilidad y seguimiento a

documentos asignados; 5) Permite trabajar bajo procedimientos estrictamente del estándar ISO 27001; y 6) Modelo de trabajo cíclico.

REFERENCIAS

Aja Quiroga, L. (2002). Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. Acimed, 10(5), 7-8.

Broderick, J. S. (2006). ISMS, security standards and security regulations. information security technical report, 11(1), 26-31.

Calder, A. (2006). Implementing information security based on ISO 27001/ISO 17799: a management guide. J. Van Bon (Ed.). Van Haren Publishing.

Cano, J. & Saucedo. G. M. (2013) Encuesta Latinoamericana de Seguridad de la Información 2013. ACIS.

Corti, M. E. (2010). Metodologías para la implantación de SGSI.

Del Rio, M. (2011). Deficiencias más comunes en los SGSI basados en la ISO 27001. Recuperado el 20 de septiembre de 2013, http://www.securitybydefault.com/2011/08/deficiencias-mas-comunes-en-los-sgsi.html

GesConsultor. (2013). Recuperado el 25 de Noviembre de 2013 de http://www.gesconsultor.com/

GloblalSGSI. (2013). Recuperado el 12 de Noviembre de 2013 de http://www.globalsgsi.com/

Ingenia. (2010). Recuperado el 28 de Abril de 2013 de https://www.e-pulpo.es/

INTECO. Sistema de gestión de la seguridad informática. Obtenido de INTECO: http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/index.html.

ISO/IEC 27001:2005. Information technology – Security techniques - Information security management system implementation guidance. Recuperado el 20 de septiembre de 2013, http://web.bryant.edu/~commtech/guidelines/iso27001.pdf.

Linares, S., & Paredes, I. (2007). IS2ME Seguridad de la Información a la Mediana Empresa.

Piattini, M., & Del Peso, E. (2001). Auditoría Informática. Un enfoque práctico. RA-MA, Madrid, 245.

Susanto, H. & Bin, F. Multimedia Information Security Architecture. @ IEEE. 2010.

Susanto, H., Almunawar, M. N. & Chee, Y. I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains. Journal of Computer, Asian Transaction. July 2011.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.

Von, B. & Von, R. 2004. The 10 deadly sins of Information Security Management. Computer & Security 23(2004) 371- 376. Elsevier Science Ltd.

ANEXO 2

CERTIFICADO PONENCIA: SOFTWARE WEB PARA EL ACOMPAÑAMIENTO EN EL ANÁLISIS Y GESTIÓN DE RIESGOS EN PYMES

ENCUENTRO Internacional de INVESTIGADORES en ADMINISTRACIÓN 2014
Facultad de Ciencias de la Administración - Universidad del Valle

La Universidad del Valle
y
La Universidad Externado de Colombia

Certifican que la ponencia titulada

Software Web Para el Acompañamiento en el Análisis y Gestión de Riesgos en Pymes.

Cuyos autores son

Raul Jose Martelo Gomez, David Franco Borré, Jhonny Enrique Madera Osorio

Fue presentada en el marco del

Encuentro Internacional de Investigadores en Administración 2014

Realizado en la ciudad de Santiago de Cali, los días 19 y 20 de noviembre de 2014

Carlos Eduardo Cobo Oliveros
Decano
Facultad de Ciencias de la Administración
Universidad del Valle

Alejandro Beltrán Duque
Decano
Facultad de Administración de Empresas
Universidad Externado de Colombia

Santiago de Cali, noviembre de 2014

ANEXO 3

CERTIFICADO PONENCIA: INTEGRACIÓN DEL MÓDULO DE AUTOEVALUACIÓN Y GESTIÓN DOCUMENTAL PARA EL CUMPLIMIENTO DE LA NORMA ISO 27001

ENCUENTRO Internacional de INVESTIGADORES en ADMINISTRACIÓN 2014
Facultad de Ciencias de la Administración - Universidad del Valle

La Universidad del Valle
y
La Universidad Externado de Colombia

Certifican que la ponencia titulada

Integración Del Módulo de Autoevaluación y Gestión Documental Para el Cumplimiento de la Norma Iso 27001.

Cuyos autores son

Raul Jose Martelo Gomez, Jhonny Enrique Madera Osorio, Andres David Betin Rodriguez

Fue presentada en el marco del

Encuentro Internacional de Investigadores en Administración 2014

Realizado en la ciudad de Santiago de Cali, los días 19 y 20 de noviembre de 2014

Carlos Eduardo Cobo Oliveros
Decano
Facultad de Ciencias de la Administración
Universidad del Valle

Alejandro Beltrán Duque
Decano
Facultad de Administración de Empresas
Universidad Externado de Colombia

Santiago de Cali, noviembre de 2014

ANEXO 4

CERTIFICADO PONENCIA: APLICACIÓN BASADA EN SOFTWARE LIBRE PARA LA AUTOEVALUACIÓN EN EL PROCESO DE IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

RedTIC
Red de Tecnologías de la Información y el Conocimiento

CERTIFICADO DE PARTICIPACIÓN
EVENTOS ACADÉMICOS REDTIC

El suscrito Coordinador del FLISOL 2014, hace constar que **NATIVIDAD VILLABONA, RAUL JOSE MARTELO GOMEZ, ANDRES BETIN y JHONNY MADERA** participaron en calidad de ***PONENTES*** a nombre de la Universidad de Cartagena con la conferencia titulada **"APLICACIÓN BASADA EN SOFTWARE LIBRE PARA LA AUTOEVALUACION EN EL PROCESO DE IMPLANTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION"** en el Festival Latinoamericano de Software Libre 2014, realizado en la ciudad de Cartagena de indias el día 10 de Mayo de 2014.

Para constancia se firma a solicitud del interesado a los VEINTÍUN (21) días del mes de JULIO de 2014.

Atentamente,

RedTIC
Red de Tecnologías de la Información y el Conocimiento
Nit: 900.414.105-6

STALIN CHAPUEL TRELLO
Director General de RedTIC

CARTAGENA
La Matuna, Edificio Monroy Oficina 205
servicios@redtic.org +57 (5) 660 6501

WWW.REDTIC.ORG

ANEXO 5

SISTEMA DE GESTIÓN DOCUMENTAL BASADO EN DJANGO

RedTIC
Red de Tecnologías de la Información y el Conocimiento

CERTIFICADO DE PARTICIPACIÓN
EVENTOS ACADÉMICOS REDTIC

El suscrito Coordinador del FLISOL 2014, hace constar que **NATIVIDAD VILLABONA, RAUL JOSE MARTELO GOMEZ, ANDRES BETIN y JHONNY MADERA.** participaron en calidad de ***PONENTES*** a nombre de la Universidad de Cartagena con la conferencia titulada ***"SISTEMA DE GESTION DOCUMENTAL BASADO EN DJANGO."*** en el Festival Latinoamericano de Software Libre 2014, realizado en la ciudad de Cartagena de indias el día 10 de Mayo de 2014.

Para constancia se firma a solicitud del interesado a los VEINTÍUN (21) días del mes de JULIO de 2014.

Atentamente,

RedTIC Red de Tecnologías de la Información y el conocimiento
Nit: 900.544.132 - 0

STALIN CHAPUEL TELLO
Director General de RedTIC

CARTAGENA
La Matuna. Edificio Monroy Oficina 205
servicios@redtic.org +57 (5) 660 6501

WWW.REDTIC.ORG

ANEXO 6

SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001

Universidad Externado de Colombia
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

Facultad de Ciencias De la Administración
Universidad del Valle

FACULTAD DE CIENCIAS EMPRESARIALES Y ECONÓMICAS
Programa de Administración de Empresas

ENCUENTRO Internacional de INVESTIGADORES en ADMINISTRACIÓN 2013

CERTIFICAN QUE LA PONENCIA TITULADA

Software de Apoyo Para el Proceso de Implantación Del Sistema de Gestión de Seguridad de la Información en Organizaciones Basado en la Norma Iso 27001

Cuyos autores fueron:

Jhonny Enrique Madera Osorio, Luis Carlos Tovar Garrido, Raul Jose Martelo Gomez

Fue presentada en marco del Encuentro Internacional de Investigadores en Administración 2013, realizado los días 26 y 27 de noviembre de 2013.

Santa Marta, Colombia. Noviembre 27 de 2013.

ALEJANDRO BELTRÁN DUQUE
Decano de la Facultad Ciencias Administración de Empresas - Universidad Externado de Colombia

CARLOS EDUARDO COBO OLIVEROS
Decano de la Facultad Ciencias de la Administración - Universidad del Valle

EDWIN CHACÓN VELÁSQUEZ
Decano de la Facultad de Ciencias Empresariales y Económicas - Universidad del Magdalena