Gobierno y Modelado de la Seguridad de la Información en las Organizaciones

Universidad Carlos III de Madrid

Escuela Politécnica de Madrid

Ingeniería Técnica en Informática de Gestión

2011

Autor: Sandra Ontoria Gonzalo

Tutor: Antonio Folgueras Marcos

AGRADECIMIENTOS

Debo agradecer de manera especial y sincera al Profesor Antonio Folgueras Marcos el gran apoyo que me ha mostrado a lo largo de este proyecto. Por haberme transmitido una gran confianza en mi trabajo y por haberme orientado su gran conocimiento en esta área con entusiasmo.

A mis padres por haberme concienciado tras muchos años en que la educación es el pilar del ser humano, brindando la oportunidad de optar a la realización de una carrera. A mi hermano Jesús, ya que fue mi guía a la hora de elegir esta titulación con la cual me siento totalmente identificada. A mi hermano Rubén, cuñadas, sobrinas y resto de familia por haberme transmitido una gran comprensión y ánimos.

A mis compañeros de carrera porque ha sido todo un lujo avanzar a lo largo de este gran camino, juntos, aprendiendo unos de otros.

A todos mis amigos y compañeros de trabajo que durante esta última fase me han apoyado tanto.

Gracias a todos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

1.1 Descripción del proyecto

En este proyecto se estudia el entorno de Gobierno de Seguridad de la Información, con la finalidad de establecer un análisis y diseño de un Sistema de Gobierno de Seguridad de la Información.

El entorno de Gobierno se centra en la normativa ISO 27000, aplicando modelos de procesos como Cobit e ITIL, modelos de madurez y métricas para garantizar la Seguridad de la Información a alto nivel, bajo la normativa legal vigente.

Asimismo, se van a analizar las herramientas de mercado orientadas a Gestión de la Seguridad, con el objetivo de obtener una parte de los requisitos funcionales de partida a considerar en el diseño que se llevará a cabo en este proyecto.

Se detallarán los requisitos de Gobierno de Seguridad de la Información mediante casos de uso y diagramas, con el fin de obtener un modelo de un Sistema de Gestión de Seguridad de la Información. El modelo es aplicado a un modelo de simulación que permita predecir los resultados de aplicar unas decisiones de Gobierno de la Seguridad TI en los sistemas de información de la organización.

Por último, se llevará a cabo un catalogo de datos específicos a alimentar en las entidades del modelo diseñado.

El Gobierno de la Seguridad TI es una parte del Gobierno Corporativo de las TI que a la vez es una parte del Gobierno Corporativo de las Organizaciones. Ello es debido a que los aspectos de las TI son transversales a toda la organización e intervienen en el valor que aportan las organizaciones, pero esta aportación al valor es en conjunción con el resto de las unidades y departamentos de la organización y cualquier aspecto de mejora ha de abordarse de manera corporativa. Por motivos de simplificación se denomina Gobierno de la Seguridad TI, aunque la filosofía de la propuesta sería denominarlo Gobierno Corporativo de la Seguridad TI. A continuación se incluyen varias definiciones de Gobierno de la Seguridad TI:

DEFINICIONES GOBIERNO SEGURIDAD TI

El Gobierno de Seguridad está compuesto por un conjunto de responsabilidades y practicas llevadas a cabo mediante la junta ejecutiva con el objetivo de proporcionar la dirección estratégica, asegurando que los objetivos se logran, cerciorándose de que los riesgos se gestionan de manera adecuada y asegurando que los recursos de la empresa son usados responsablemente - *IT Governance Institute.*

El Gobierno de Seguridad de la Información es un subconjunto de Gobierno de la Empresa que proporciona la dirección estratégica, asegura que los objetivos se logran, gestiona los riesgos adecuadamente, asigna responsabilidades a los recursos de la organización, y supervisa el éxito o el fracaso del programa de seguridad de la empresa - *Information Security Governance*

De manera casi general las definiciones mostradas de Gobierno de la Seguridad incorporan: Ser parte de un gobierno más amplio, ser una actividad realizada a nivel ejecutivo, ayuda a definir el camino y los objetivos estratégicos y se compone de: asignar recursos, controlar la ejecución y asignar responsabilidades.

El Gobierno de Seguridad de la Información es un factor crítico por el empleo creciente de redes sociales e internet en las organizaciones, donde puede recaer mucha información de alto grado de confidencialidad de las personas y de las organizaciones. La seguridad es un proceso “top down” (arriba / abajo) y “down top” (abajo / arriba) en donde intervienen tres niveles: estratégico, táctico y operativo. Un buen comienzo ha de ser establecer las directrices estratégicas (Gobierno de la Seguridad TI), las cuales ayudaran a determinar y seleccionar los métodos y estándares de Seguridad más aplicables para llevar a cabo la gestión y la operación de la Seguridad TI.

En el entorno existen múltiples normas, estándares y mejores prácticas con propuestas relativas a la ejecución de la seguridad de las TI: definición de políticas, definición de procesos, definición de controles y acciones, etc. El problema es que tanta disparidad de información con un elevado número de amenazas crecientes hace complicado tener una imagen simple de las fortalezas y debilidades de las organizaciones así como de los planes de acción estratégicos a ejecutar. Por ello, se presenta el siguiente proyecto.

El partir de las directrices estratégicas (Gobierno de la Seguridad TIC), ayudará a determinar y seleccionar los métodos y estándares de Seguridad más aplicables para llevar a cabo la gestión y la operación de la Seguridad TI en función de las necesidades de la organización. No entender los requerimientos claves de seguridad de la

organización y empezar a implantar medidas de mucho detalle, conllevara costes elevados y resultados cuestionados.

1.2 Objetivos del Modelo de Gobierno de la Seguridad TI

Con el fin de contemplar en el presente proyecto los propósitos de un Gobierno de Seguridad de la Información se han de contemplar los siguientes objetivos:

- → Realizar un estudio del entorno de Seguridad de la Información, el cual comprende principalmente los estándares de Seguridad de la Información: ISO 27000, junto con los modelos de procesos como son ITIL, Cobit y Margarit, el reglamento vigente en cuanto a protección de la información, y los modelos de madurez y métricas que afecten al Gobierno de Seguridad de la Información.
- → Analizar los beneficios y aspectos de mejora de las herramientas software comerciales de Gestión de Seguridad de la Información que cubran en gran parte las consideraciones internas, como los factores influyentes del entorno.
- → Tras las áreas de mejora detectadas, realizar un Análisis y un Diseño de un Sistema de Gobierno de Seguridad de la Información con los requisitos obtenidos y seleccionados de las herramientas de mercado. El modelo propuesto ha de contemplar los requisitos de Gobierno de la Seguridad considerando la normativa ISO 27000, junto con los marcos legales, las buenas prácticas, los modelos, métodos y las métricas de la bibliografía existentes al respecto.
- → Proponer un modelo de simulación sobre el Gobierno de la Seguridad TI.
- → Llevar a cabo una planificación y una estimación de los puntos de función para obtener una aproximación del presupuesto del proyecto y recursos necesarios para la implementación.
- → Definir un catalogo de datos maestros con los que una herramienta de Gobierno de Seguridad de la Información debería comenzar.

1.3 Marco general de Seguridad de la información

El objetivo de Seguridad de la Información, según la ISO 27001, consiste en diseñar, implementar y mantener un Sistema de Gestión de Seguridad de la Información

mediante un conjunto coherente de procesos para la gestión eficaz de acceso a la información, garantizando así la confidencialidad, la integridad y la disponibilidad de los activos de información, minimizando los riesgos de seguridad de la información en la TI.

El diseño de un Sistema de Gestión de Seguridad de la Información contempla las actividades de establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información, junto con su debida documentación.

Los requisitos de seguridad de la información que el sistema certifica son:

- → Descripción y garantía de los elementos de configuración de la empresa.
- → Gestión y mitigación de los riesgos de seguridad de la información.
- → Las políticas de seguridad junto con sus propiedades y garantías.
- → Las medidas de seguridad son inspeccionadas periódicamente.

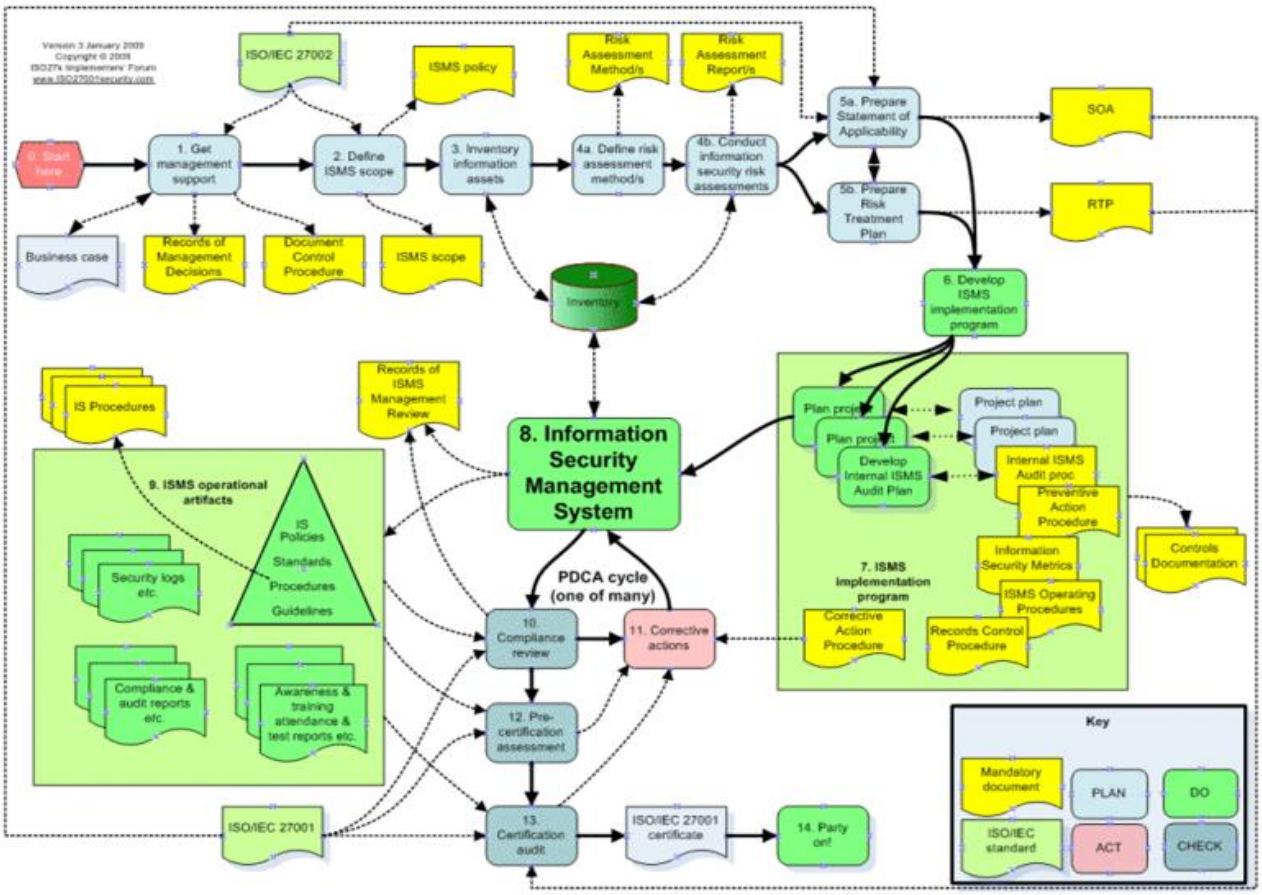


Figura 1. Sistema de Gestión de Seguridad de la Información.

Como con todos los procesos de gestión, un Sistema de Gestión de Seguridad de la Información debe seguir siendo eficaz y eficiente en un largo plazo, la adaptación a los cambios en la organización interna y del medio ambiente externo. El modelo

propuesto es de Gobierno de la Seguridad TI por lo que solo contempla los aspectos más ejecutivos de la gestión TI. La ISO / IEC 27001, como el resto de las normas de calidad, incorpora el típico "Plan-Do-Check-Act" (PDCA) enfoque de Deming a la mejora continua. Al ser crítico y al incorporarse la mejora continua en el modelo de Gobierno de la Seguridad TI se explica a continuación:

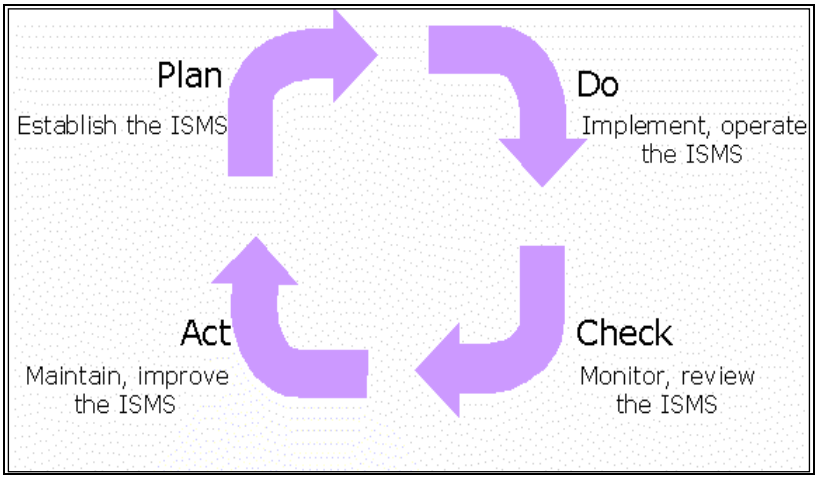


Figura 2. Proceso de Gestión. Plan-Do-Check-Act

Plan (Establecer el SGSI): En esta etapa se define el alcance del SGSI en términos de negocio, organización, localización, activos y tecnologías. Implica, establecer la política ISMS, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- → Debe ser aprobada por la dirección una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización, alineada con el contexto estratégico de gestión de riesgos y criterios de evaluación de los mismos. Considerando los requerimientos legales o contractuales relativos a seguridad.
- → Se establece una metodología de evaluación del riesgo, además de definir los criterios de aceptación del riesgo. Existen numerosas metodologías estandarizadas para la evaluación de riesgos que serán analizadas, aunque es aceptable definir una propia.
- → En esta fase se realiza la identificación de riesgos mediante la identificación de los activos que están dentro del alcance del SGSI y sus responsables directos, la identificación de las amenazas en relación a los activos, la identificación de las vulnerabilidades que puedan ser aprovechadas por dichas amenazas, la

identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- → Los riesgos han de ser analizados y evaluados, en base al impacto que provocaría en el negocio un fallo de seguridad que supongo pérdida de confidencialidad, integridad o disponibilidad de un activo de información, la probabilidad de ocurrencia de un fallo en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados, según los criterios determinar la aceptación del riesgo.
- → Para el tratamiento del riesgo se han de seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- → En la declaración de aplicabilidad se incluye los objetivos de control y controles seleccionados y los motivos para su elección, los objetivos de control y controles que actualmente ya están implantados, los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión.

Do (Implementar y operar el ISMS): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos. Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

- → Se define un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información, y se implementa el plan junto con los controles.
- → Para obtener los resultados de eficacia de los controles se especifica el sistema de métricas.
- → Se implantan procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check (Monitorizar y revisar el ISMS): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión. - Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- → La organización deberá ejecutar procedimientos de monitorización y revisión para detectar a tiempo los errores en el procesamiento de la información, identificar brechas e incidentes de seguridad, ayudar 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, detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores, determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- → Se revisara regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- → Se verificara la efectividad de los controles para ver si cumple con los requisitos de seguridad.
- → Se revisara 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.
- → Se realizaran periódicamente auditorías internas del SGSI en intervalos planificados.
- → Se revisara por parte de la dirección periódicamente el SGSI para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- → Se actualizaran los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- → Se registraran acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act (Mantener y mejorar el ISMS): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS. Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS.

- → La organización deberá implantar regularmente las mejoras identificadas en el SGSI, realizando las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

- → Comunicara las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- → Asegurar que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Un SGSI puede ser implementado como un sistema de información específico que se ocupa de un área de negocio en particular, o puede ser implementado como un sistema que abarque todas las participaciones de toda la organización.

[IT Risk Control Matrices Resources. (2008). Consultado el 1 de Julio 2010. http://www.riskmatrices.com/]

1.3.1 Riesgos y Amenazas

ISM se enfrenta a muchos retos que debe cumplir en el establecimiento de una política de seguridad de la información adecuada, con un apoyo eficaz del proceso y de los controles.

Los riesgos han llevado a la necesidad de proteger los sistemas y servicios. La diferencia es determinada por factores internos y externos, incluyendo el uso generalizado de la tecnología, la creciente complejidad e interconectividad de los sistemas.

Esto significa que hay nuevas áreas de riesgo que podrían tener un impacto significativo en las operaciones críticas de negocio, tales como:

- → Aumento de los requisitos de disponibilidad y robustez.
- → El mal uso y abuso de los sistemas de información que afectan a la intimidad y los valores éticos
- → Peligros externos de los hackers, obstrucción del servicio, ataques de virus, extorsión, espionaje industrial y captura de información de la organización o datos privados.
- → La falta de compromiso de la empresa a los procesos y procedimientos de ISM, y la falta de información adecuada sobre los planes y estrategias futuras

- → La falta de compromiso de la alta dirección o la falta de recursos y / o el presupuesto para el proceso de ISM
- → Los procesos se centran demasiado en las cuestiones de tecnología y no lo suficiente en los servicios de TI y las necesidades y prioridades de la empresa
- → Evaluación de riesgos y la gestión se lleva a cabo de forma aislada y no en relación con Gestión de la disponibilidad y ITSCM

1.3.2 Controles de Seguridad

El Administrador de Seguridad de la Información debe contemplar la seguridad de la información como parte integrante de todos los servicios y sistemas, y como un proceso que necesita ser continuamente administrado mediante un conjunto de controles de seguridad. El modelo de Gobierno también los contempla aunque los agrupa en grupos de controles.

El conjunto de controles de seguridad deben estar destinados a aplicar la política de seguridad de la información minimizando todas las amenazas reconocidas e identificadas. Los grupos de controles serán más rentables si se incluye en el diseño de todas las áreas de servicio.

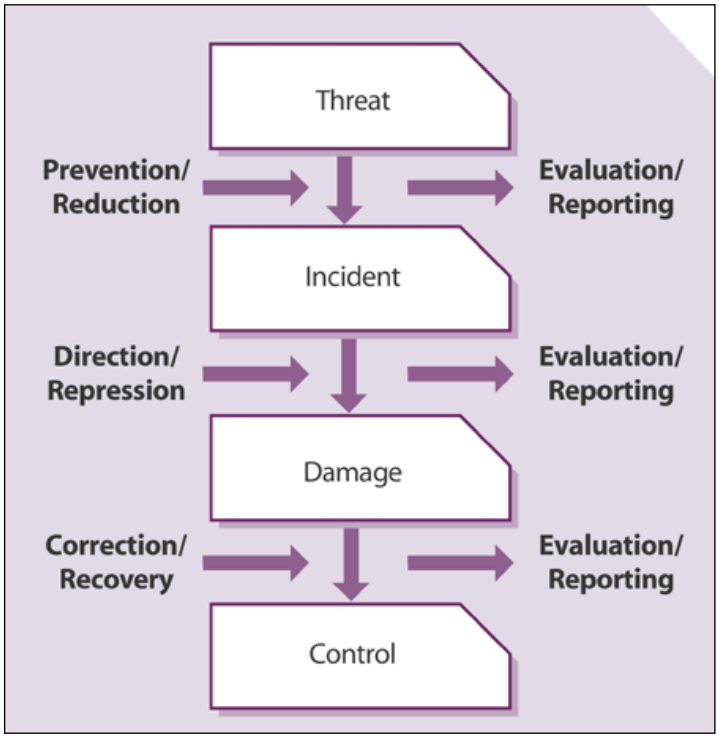


Figura 3. Etapas de detección de Controles

La definición de las etapas consiste en que al comienzo hay un riesgo de que una amenaza se materialice. Una amenaza puede ser cualquier cosa que interrumpa el proceso de negocio o tiene un impacto negativo sobre el negocio. Cuando una amenaza se materializa, se habla de un incidente de seguridad. Este incidente de seguridad puede causar daños a la información o a los activos, que tiene que ser reparado o corregido.

Los controles tienen una determinada agrupación. Las medidas se seleccionaran para cada una de estas etapas dependiendo de la importancia atribuida a la información.

[Sharon Taylor, Vernon Lloyd, Colin Rudd. (2007). ITIL V3. Service Design. OGC (Office of Govemment Commerce)]

1.4 Alcance del proyecto

El proyecto se enfocara hacia un marco de Gobierno de Seguridad de la Información y para ello, aunque nos basemos en estándares de gestión solamente requerimos los aspectos ejecutivos o con importancia estratégica.

Comencemos explicando el alcance de un Sistema de Gestión de la Seguridad de la Información. El Sistema de Gestión dentro de Seguridad de la Información en una organización contempla la gestión de los riesgos empresariales que le atañen y su forma de reducir y/o mitigar impactos adversos a un nivel aceptable mediante el establecimiento de un programa amplio y conciso en seguridad de la información y el uso efectivo de recursos cuya guía principal sean los objetivos del negocio.

El Sistema de Gestión de la Seguridad de la Información (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.

Un SGSI identifica los riesgos a los que está sometida la información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida, que se revisa y mejora constantemente.

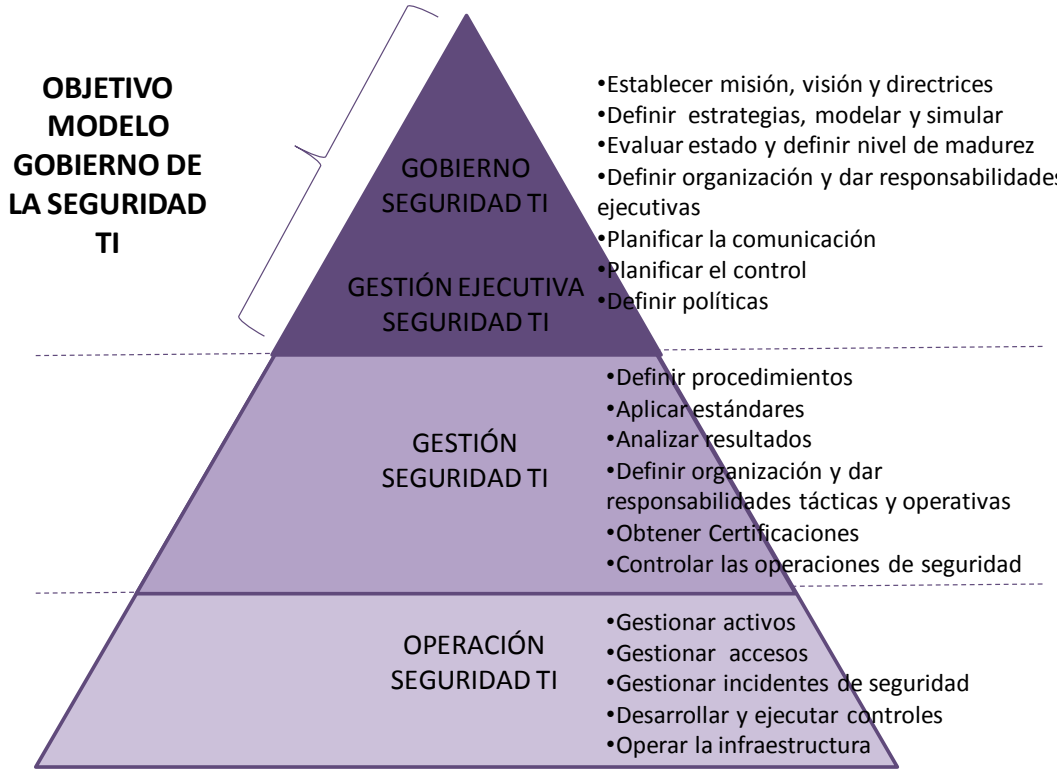


Figura 4. Pirámide de Gestión de Seguridad de la Información

Tal y como se muestra en la figura 4, aquellas actividades de corte ejecutivo y que dan las directrices para la gestión y la operación son las tenidas en cuenta en el modelo de Gobierno de la Seguridad TI propuesto. Estas actividades son detalladas en sus correspondientes requisitos en el apartado 4 del diseño conceptual.

1.5 Estructura del documento

La memoria de este diseño está compuesta de portada, prólogo, índice general, índice de figuras, índice de tablas, nueve apartados, glosario de acrónimos y abreviaturas empleadas.

A continuación se muestra una breve descripción de todos los apartados de la memoria.

- → **Introducción:** Comienza con una breve descripción, y objetivos del Modelo de Gobierno de la Seguridad TI, después un marco general donde se describe la situación de la Gestión de Seguridad y el alcance del proyecto, y por último la estructura de la memoria que es este punto.
- → **Estado del arte:** Comienza con un análisis general de cómo debe de ser una buena Gestión de Seguridad de la información. Después se analizarán estándares,

modelos de trabajo de mejores prácticas y normativa legal como son Normativa ISO 27000, ITIL, COBIT, MARGERIT y Ley Orgánica de Protección de datos.

- → **Herramientas de Gestión de Seguridad de la Información:** Con la posterior comparativa entre ellas y la selección de los requisitos esenciales de Gobierno de la Seguridad TI para basarse en la realización del presente diseño (solución a medida seleccionando los requisitos del estado del arte y de las herramientas empleadas).
- → **Solución Tecnológica Propuesta:** Se detalla la arquitectura sobre la que se implementaría y mantendría el sistema de Gobierno de Seguridad definido en el proyecto, y la vía de acceso para el usuario final.
- → **Diseño Conceptual:** En este apartado se realiza el análisis de un sistema de Gobierno de Seguridad de la Información. Comienza con la descripción de los usuarios y los requisitos, junto con los casos de uso en formato extendido.
- → **Diseño Funcional:** Para su documentación se emplean diagramas UML. Comienza con el diagrama de clases y posteriormente los de secuencia, estado y por último el diagrama relacional de la base de datos.
- → **Modelo de simulación de un Sistema de Gobierno de Seguridad TI:** Se muestra el modelo de simulación dinámico del Gobierno de la Seguridad TI que emplea la herramienta Vensim.
- → **Análisis económico:** En este punto se realiza el análisis económico de un sistema de Gobierno de Seguridad de la Información, con su planificación. Contemplando el cálculo de los puntos de función, como guía para establecer el coste de la implementación del proyecto y posibles recursos.
- → **Aportaciones de un gobierno de seguridad de la información:** Aquí se detallaran las aportaciones de un Gobierno de Seguridad de la Información para la TI y las conclusiones personales del proyecto.
- → **Referencias:** Bibliografía y recursos de internet usados para el desarrollo de este proyecto.

2 ESTADO DEL ARTE

2.1 Objetivos de la Gestión de Seguridad de la Información

No existe mucha bibliografía sobre el Gobierno de la Seguridad de la Información, por lo que en el estado del arte nos centramos en modelos y estándares de Gestión de la Seguridad de la Información.

El principal objetivo de la Gestión de Seguridad de la Información es aplicar un SGSI o Information Security Management System, es decir, un sistema de gestión basado en un enfoque sistemático de riesgos empresariales. SGSI es un sistema diseñado para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información. Se trata de un método de organización para la seguridad de la información. SGSI es un sistema de documentación que certifique que:

- → Las políticas de seguridad junto con sus propiedades y garantías están en su lugar.
- → Los riesgos de seguridad de la información son gestionados y mitigados.
- → Los activos de información en su empresa se describen y garantizan.
- → La adhesión a las medidas de seguridad son inspeccionados periódicamente.

SGSI puede ser implementado como un sistema de información específico que se ocupa de un área de negocio en particular, o puede ser implementado como un sistema que abarque todas las áreas de toda la organización. En cualquier caso, SGSI generalmente implica recursos que abarcan desde la gestión a los usuarios y personal del departamento TI, y suele afectar a todos los activos TI: conocimiento, información, hardware, software y documentación. Al no haber muchas referencias sobre el Gobierno de la Seguridad TI y al estar muy relacionado las referencias mostradas son tanto de Gestión de la Seguridad como de Gobierno de la Seguridad TI.

Tabla 1. Referencias consideradas en el estado del arte

AREA	CobiT (Control Objectives for Information and Related Technology	ITIL (Information Technology Infrastructure Library)	ISO 27000

	)		
Funciones	Mapeo de procesos TI	Mapeo de la Gestión de Niveles de Servicio de TI	Marco de referencia de seguridad de la Información
Áreas	4 Procesos y 34 dominios	9 Procesos	10 Dominios
Creador	ISACA	OGC (Office of Government Commerce)	ISO (International Organization for Standardization)
¿Para qué se implementa?	Auditoria de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quiénes lo evalúan?	Compañías de contabilidad, Compañías de consultoría en TI	Compañías de consultoría en TI	Compañías de Consultoría en TI, Empresas de Seguridad, Consultores de seguridad en redes

2.2 Normativa 27000

2.2.1 Serie ISO/IEC JTC 27000

La Organización Internacional para la Estandarización o ISO, nacida en febrero de 1947, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional. ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotécnica) conforman un sistema especializado para los estándares mundiales. En el desarrollo de Normas Internacionales ISO o IEC participan organismos nacionales como miembros de comités técnicos, establecidos por la

organización para tratar con los casos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

Mediante el uso de la familia SGSI de las normas, las organizaciones pueden desarrollar y aplicar un marco para la Gestión de la Seguridad de sus activos de información y prepararse para una evaluación independiente de su SGSI aplicado a la protección de la información, como información financiera, la propiedad intelectual, y el empleo de detalles o información confiada a ellos por los clientes o de terceros.

La familia de normas de SGSI se destina a ayudar a las organizaciones de todos los tipos y tamaños para aplicar y operar un SGSI. La familia de SGSI de las normas consiste en las siguientes Normas Internacionales:

- → **ISO / IEC 27000:2009,** Información general y de vocabulario.
- → **ISO / IEC 27001:2005,** Requisitos.
- → **ISO/IEC 27002:2005,** Código de prácticas de gestión de la información de seguridad.
- → **ISO/IEC 27003,** Guía de implementación.
- → **ISO/IEC 27004,** Indicadores de rendimiento.
- → **ISO / IEC 27005:2008,** Gestión de riesgos de Información de seguridad.
- → **ISO / IEC 27006:2007,** Requisitos para organismos que presten servicios de auditoría y certificación de sistemas de Gestión de Seguridad de la Información.
- → **ISO / IEC 27007,** Directrices para los sistemas de gestión de la información de auditoría de seguridad.
- → **ISO / IEC 27011,** Directrices de gestión de información de seguridad para las organizaciones de telecomunicaciones con sede en la norma ISO / IEC 27002.

2.2.2 ISO / IEC 27001:2005

Este estándar provee un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS. La adopción del ISMS debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requisitos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un proceso. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

Este estándar internacional adopta también el modelo "Plan-Do-Check-Act" (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y se ha mencionado previamente.

Los requisitos de este estándar internacional, son genéricos y aplicables a la totalidad de las organizaciones. Las cláusulas son las siguientes:

- → Information Security Management System (ISMS).
- → Responsabilidades de la Administración.
- → Auditoría Interna del ISMS.
- → Administración de las revisiones del ISMS.
- → Mejoras del ISMS.

2.2.2.1 Information Security Management System

Los requisitos generales son los siguientes:

- → La organización establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documento ISMS en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos.
- → Para este propósito el proceso está basado en el modelo PDCA.
- → La organización llevará a cabo acciones para eliminar las causas que no estén conformes con los requisitos del ISMS, con la finalidad de evitar la recurrencia de los mismos.
- → El anexo A de esta norma propone una detallada tabla de los controles, los cuales quedan agrupados.
- → Documentación a considerar.
- → Procedimientos más importantes:
  - → Control de documentos.
  - → De registro. Debería existir un procedimiento general, y dentro del mismo, algunos específicos como son:

- De actividad (informes, autorizaciones de acceso, auditorías, cambios, permisos temporales, bajas, etc.) de mejoras y decisiones que afectan al ISMS.
- Respuesta a incidentes de seguridad.
- Detección de eventos de seguridad.
- Recolección y centralización de eventos de seguridad.
- Revisión del ISMS (Periódica e inhabitual).
- Revisión y medición de la efectividad de los controles.

→ Todos los documentos requeridos por el ISMS serán protegidos y controlados.

2.2.2.2 Responsabilidades de administración

La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:

→ Establecimiento de la política del ISMS
→ Asegurar el establecimiento de los objetivos y planes del ISMS.
→ Establecer roles y responsabilidades para la seguridad de la información.
→ Comunicar y concienciar a la organización sobre la importancia y apoyo necesario de los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.
→ Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el ISMS.
→ Decidir los criterios de aceptación de riesgos y los niveles de los mismos.
→ Asegurar que las auditorías internas del ISMS, sean llevadas a cabo y a su vez, la administración revise el ISMS.

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el ISMS sea competente, y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria.

2.2.2.3 Auditoría interna del ISMS

La organización realizará auditorías internas al ISMS en intervalos planificados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de

conformidad a esta norma, y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

La responsabilidad y requisitos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento.

2.2.2.4 Administración de las revisiones del ISMS

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el ISMS incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, como se mencionó en el punto anterior serán claramente documentados y los mismos darán origen a esta actividad. Esta actividad está constituida por la revisión de entradas y la de salidas, y dará como resultado el documento correspondiente.

2.2.2.5 Mejoras del ISMS

La organización deberá mejorar continuamente la eficiencia del ISMS a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

2.2.3 ISO / IEC 27002:2005

La norma ISO 27002 es un código de prácticas para la seguridad de la información. Básicamente describe cientos de posibles controles y mecanismos de control, que pueden ser aplicadas, en teoría, con sujeción a la orientación proporcionada en la norma ISO 27001.

La norma establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la Gestión de Seguridad de la Información dentro de una organización. Los controles reales que figuran en la norma están destinados a atender las necesidades específicas a través de una evaluación de riesgo. La norma tiene también por objeto proporcionar una guía para el desarrollo de normas de seguridad de la organización y prácticas de gestión eficaz de seguridad.

2.2.4 ISO / IEC 27003

El objetivo es proporcionar ayuda y orientación en la implementación de un ISMS. Esto incluirá la atención en el método PDCA, con respecto al establecimiento, la revisión de la aplicación y la mejora en sí del SGSI.

2.2.5 ISO / IEC 27004

La norma ISO 27004 es el número oficial de la nueva norma que abarca la seguridad de medición de gestión de información y métricas. Su objetivo es ayudar a una organización a establecer la efectividad de su aplicación SGSI, que abarca la evaluación de los resultados.

2.2.6 ISO / IEC 27005:2008

ISO 27005 abarca la gestión de información de riesgo. La norma establece directrices para la Gestión de Riesgos de Seguridad de la Información (ISRM) en una organización, en particular el apoyo a las exigencias de un sistema de información de gestión de seguridad definidas por la norma ISO 27001.

2.2.7 ISO / IEC 27006:2007

Este es el estándar que ofrece las directrices para la acreditación de las organizaciones que ofrecen la certificación y el registro con respecto a un SGSI.

Los capítulos de la norma son los siguientes: Ámbito de aplicación, referencias; Condiciones; Principios; Requisitos generales, requisitos estructurales; necesidades de recursos; los requisitos de información; Sistema de Gestión de Requisitos.

2.2.8 ISO / IEC 27007

La norma ISO 27007 ofrecerá orientación para auditar un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001. Su uso está previsto principalmente por organismos de certificación acreditados y similares.

2.2.9 ISO / IEC 27011

La propia norma establece directrices y principios para iniciar, implementar, mantener y mejorar la Gestión de Seguridad de la Información (ISM) de las

organizaciones de telecomunicaciones basado en la norma ISO 27002. Sus objetivos son ofrecer orientación práctica especialmente adecuada para las organizaciones de telecomunicaciones.

2.3 Modelos de procesos de gestión de la seguridad informática

2.3.1 ITIL: Conceptos y procesos fundamentales

Las prácticas comerciales prudentes exigen que los procesos de TI y las iniciativas se alineen con los procesos de negocio y objetivos. Esto es crítico cuando se trata de seguridad de la información, que debe estar estrechamente alineado con la seguridad del negocio y sus necesidades. Todas las organizaciones TI de proveedor de servicios deben asegurarse de que tienen una política de ISM y los controles de seguridad necesarios para vigilar y hacer cumplir las políticas.

La política de seguridad debe analizar cada aspecto de la estrategia, con su correspondiente gestión de control y riesgos. Además, la parte de gestión debe incluir las normas, procedimientos y directrices como apoyo a las políticas de seguridad de la información. A nivel global, debe adoptar una seguridad eficaz basada en la estructura de la organización y vinculada a los objetivos, estrategias y planes de negocio. Y por último, es necesaria una formación basada en la estrategia y el plan de seguridad.

La política debe cubrir todas las áreas de seguridad y debe incluir:

- → El uso y abuso de los activos de la política de TI
- → Una política de control de acceso
- → Una política de control de contraseña
- → Una política de e-mail
- → Una política de Internet
- → Una política de lucha contra virus
- → Una política de clasificación de la información
- → Una política de clasificación de documentos
- → Una política de acceso remoto
- → Una política en materia de acceso proveedor de servicios de TI, la información y los componentes.
- → Una política de enajenación de bienes.

El cumplimiento de esta política debe ser contemplado en todos los acuerdos SLR, SLAs y contratos.

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (Information Technology Infrastructure Library), es un marco de trabajo de buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

No es posible certificar una organización o sistema de gestión conforme a ITIL, pero una organización que haya implementado las guías de ITIL sobre Gestión de los Servicios de TI puede lograr certificarse bajo la ISO/IEC 20000.

El 26 de junio de 2007 se presenta la tercera versión de este código de buenas prácticas. ITIL 3 eleva las TI a un nivel estratégico.

ITIL se basa en el ciclo de vida de la gestión del servicio según se muestra en la siguiente ilustración:

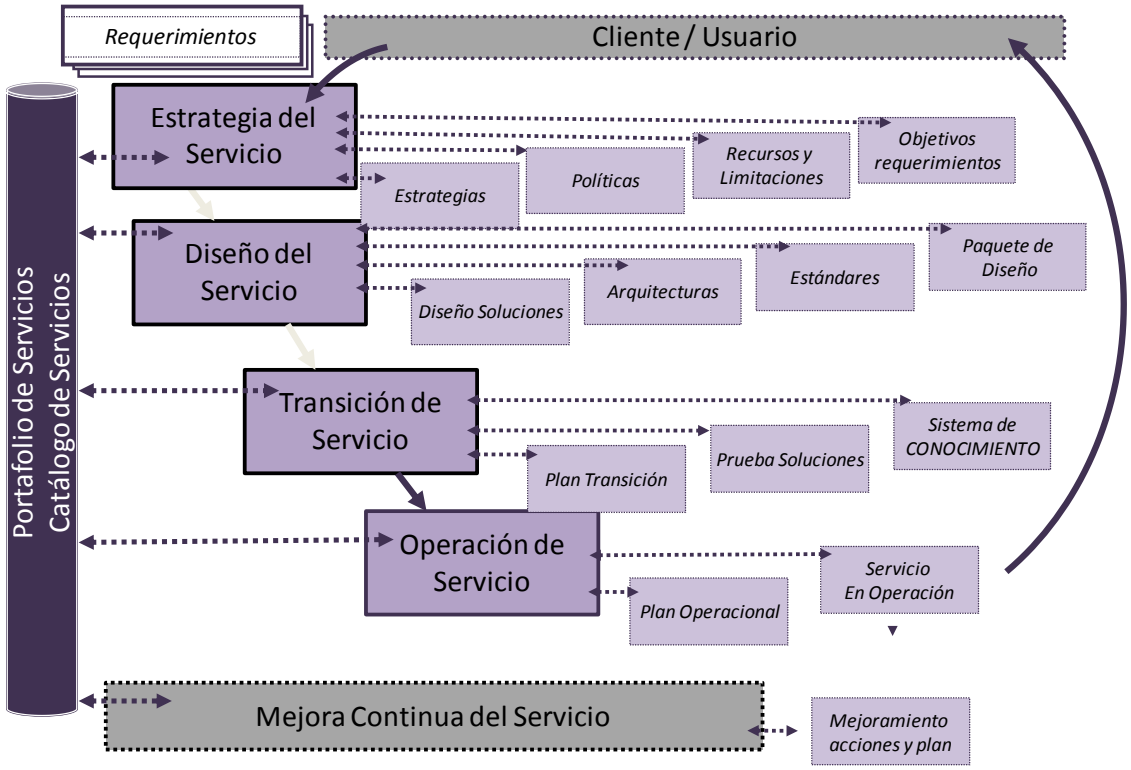


Figura 5. ITIL. Ciclo de vida de la gestión del servicio

Los cinco libros de ITIL v5 y sus temas basados en el ciclo de vida de la gestión del servicio son:

Estrategia del Servicio:

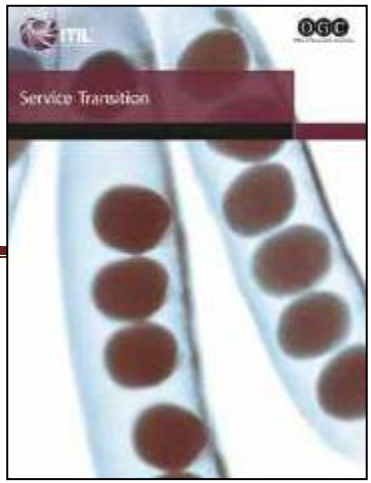
Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente tomando en cuenta la real factibilidad de su puesta en marcha. Así mismo, se analizan posibles mejoras para servicios ya existentes. Se verifican los contratos en base a las nuevas ofertas de proveedores antiguos y posibles nuevos proveedores, lo que incluye la renovación o revocación de los contratos vigentes.

→ Gestión del Portafolio de Servicios:
→ Gestión Financiera:
→ Gestión de la Demanda, modelos de la actividad del negocio:

Diseño del Servicio:

Una vez identificado un posible servicio el siguiente paso consiste en analizar su viabilidad. Para ello, se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Para la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc.), la infraestructura y software a implementar.

→ Gestión Catálogo de Servicio
→ Gestión de Niveles de Servicio
→ Gestión de la Capacidad
→ Gestión de la Disponibilidad
→ Gestión de la Continuidad de Servicio
→ Gestión de la Seguridad de la Información
→ Gestión de Proveedores



Transición del Servicio:

Antes de poner en marcha el servicio se deben realizar pruebas. Para ello se analiza la información disponible acerca del nivel real de capacitación de los usuarios, estado de la infraestructura, recursos IT disponibles, entre otros. Luego se prepara un escenario para realizar pruebas, se replican las bases de datos, se preparan planes de rollback (reversión) y se realizan las pruebas. Luego, de ello se limpia el escenario hasta el punto de partida y se analizan los resultados, de los cuales dependerá la implementación del servicio. En la evaluación se comparan las expectativas con los resultados reales.

→ Planeación de Soporte de Transición
→ Gestión de Cambios
→ Gestión de Activos y Configuración
→ Gestión de Liberación y Despliegue
→ Validación y Pruebas de Servicio
→ Evaluación
→ Gestión del Conocimiento

Operación del Servicio:

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio.

→ Gestión de Incidentes
→ Gestión de Eventos
→ Gestión de Cumplimiento de Requerimientos
→ Gestión de Problemas
→ Gestión de Accesos

Mejora Continua del Servicio:

Se utilizan herramientas de medición y feedback para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, etc. Para ello, se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios.

→ Definir qué se debe mejorar.

→ Definir qué se puede mejorar
→ Hacerse de datos
→ Procesar los datos e información
→ Analizar los datos
→ Usar info/definir acciones
→ Implementar acciones

ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la Information Services Procurement Library (ISPL, 'Biblioteca de adquisición de servicios de información'), la Application Services Library (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, Dynamic Systems Development Method), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con el gobierno de tecnologías de la información mediante COBIT (Control Objectives for Information and related Technology). Por su importancia en los temas de seguridad en los siguientes apartados se resumen cuatro procesos de ITIL v3 relacionados con la gestión de la seguridad (gestión de la seguridad de la información, gestión de la configuración y acuerdo de niveles de servicio) y operación de la seguridad (gestión de acceso).

2.3.1.1 Gestión de la Seguridad de la Información

El objetivo del proceso de ISM consiste en alinear la seguridad de TI con la seguridad del negocio, y asegurar que la seguridad de la información se administra con eficacia en todos los servicios y actividades de gestión de servicio.

ISM debe ser considerado en el marco de gobierno corporativo general. El gobierno corporativo es el conjunto de responsabilidades y las prácticas ejercidas por el equipo directivo y la gerencia ejecutiva, con el objetivo de proporcionar dirección estratégica, asegurando alcanzar los objetivos, determinar que los riesgos se están gestionando correctamente y verificar que los recursos de la empresa utilizan los sistemas con eficacia.

El propósito de ISM es proporcionar un enfoque para todos los aspectos de seguridad de TI y gestionar todas las actividades de seguridad de TI.

El término 'Información' se usa como un término general que incluye los almacenes de datos, bases de datos y metadatos. El objetivo de la seguridad de la información es proteger los intereses de aquellos que dependen de la información, y los sistemas y las comunicaciones que brindan la información, de cualquier daño resultante de fallos de disponibilidad, confidencialidad e integridad.

El proceso de ISM debe ser foco de todas las cuestiones de seguridad de TI, y debe asegurarse de que una política de seguridad de la información es producida, mantenida y cumplida, en lo referente al uso y mal uso de todos los sistemas y servicios. ISM tiene que comprender toda la TI y el entorno de seguridad para empresas, incluyendo:

- → Políticas y planes de seguridad del negocio.
- → El funcionamiento del negocio actual y sus requisitos de seguridad.
- → Los planes futuros de negocios y los requisitos.
- → Requisitos legislativos.
- → Obligaciones y responsabilidades en materia de seguridad definidas en los SLA
- → La empresa y los riesgos de TI y su gestión.

Establecer todo esto permitirá a ISM garantizar que todos los aspectos de seguridad actuales y futuras y los riesgos del negocio son gestionados de forma rentable.

El proceso de ISM debe incluir:

- → La producción, mantenimiento, distribución y ejecución de una Política de Seguridad de la Información, y el soporte a las mismas.
- → Comprender los requisitos de seguridad actuales y futuros de la empresa, y la actual Política de Seguridad negocio.
- → Implementación de un conjunto de controles de seguridad que dan soporte a las políticas de seguridad de la información y gestionan los riesgos asociados con el acceso a los servicios, información y sistemas.
- → Documentación de todos los controles de seguridad, junto con la operación y mantenimiento de los controles, y sus riesgos asociados.
- → Gestión de proveedores y contratos de acceso a los sistemas y servicios, en conjunto con Gestión de Proveedores.
- → Gestión de todas las violaciones de la seguridad e incidentes relacionados con todos los sistemas y servicios.
- → La mejora de los controles de seguridad proactiva, y la gestión de riesgo para la seguridad y la reducción de riesgos de seguridad.
- → Integración de los aspectos de seguridad en todos los demás procesos de IT SM.

Para lograr un gobierno de seguridad de la información eficaz, la gerencia debe establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) para guiar el desarrollo y gestión de un programa de información de seguridad integral que apoya los objetivos de negocio.

El desarrollo de los procesos de Gestión de Seguridad de la Información, junto con los métodos, herramientas y técnicas, constituyen la estrategia de seguridad. El administrador de seguridad debe garantizar que las tecnologías, productos y servicios están en su lugar y que la política general se ha desarrollado y publicado. El encargado de la seguridad es responsable también de la arquitectura de la seguridad, la autenticación, autorización, administración y recuperación.

La estrategia de seguridad también debe considerar cómo se van a integrar las buenas prácticas de seguridad en todas las áreas del negocio. La formación y la sensibilización son vitales en la estrategia global, la seguridad es la más débil a menudo en la fase del usuario final. Es aquí, también, donde existe una necesidad de desarrollar métodos y procesos que permiten a las políticas y a las normas ser más fáciles de seguir y aplicar.

2.3.1.2 Gestión de acceso

Gestión de Accesos es el proceso que otorga a los usuarios autorizados el derecho a utilizar un servicio, mientras que restringe el acceso a usuarios no autorizados. Se basa en ser capaz de identificar con precisión a los usuarios autorizados y luego administrar su capacidad para acceder a los servicios requeridos, y actualización de los permisos de acceso.

Gestión de Accesos depende de la Gestión de Disponibilidad y la Gestión de Seguridad de la Información, permitiendo gestionar a la organización la confidencialidad, disponibilidad e integridad de los datos de la organización y la propiedad intelectual.

La Gestión de Accesos garantiza que los usuarios tienen derecho a utilizar un servicio, pero no garantiza que este acceso está disponible en todos los tiempos acordados, éste es proporcionado por Gestión de la Disponibilidad.

Gestión de Accesos es un proceso que se ejecuta conjuntamente por todos los técnicos y las funciones de administración de aplicaciones. Sin embargo, puede ser iniciado por una solicitud de servicio a través del Service Desk.

En este sentido, Monitorización y Control de Acceso debe ser incluido en las actividades de supervisión de todos los técnicos y las funciones de administración de aplicaciones y todos los procesos del Servicio Operacional.

El valor añadido del proceso de Gestión de Accesos es el siguiente:

- → El acceso controlado a los servicios asegura que la organización es capaz de mantener más eficazmente la confidencialidad de su información.
- → Los empleados tienen el nivel adecuado de acceso para ejecutar su trabajo con eficacia.
- → Hay menos probabilidad de incurrir en errores de entrada de datos o en el uso de un servicio fundamental por un usuario no cualificado (por ejemplo, sistemas de control de producción)
- → Mejora la capacidad de auditar el uso de los servicios y rastrear el uso indebido de los servicios.
- → La posibilidad más fácil de revocar los derechos de acceso cuando sea necesario, una consideración importante de seguridad.
- → Puede ser necesario para el cumplimiento normativo (por ejemplo, SOX, HIPAA, COBIT).

2.3.1.3 Gestión de la configuración

La Infraestructura de TI consiste en elementos de configuración (CI). Un CI es un elemento documentado de la infraestructura de TI, tal como hardware, software, alojamiento, personas y documentación (Categoría).

El factor primordial al decidir tanto el rango, como el detalle es la información necesaria para gestionar el servicio, al margen del coste o dificultad de obtener y mantener esos datos.

Antes de que el diseño e implantación de una CMDB se lleve a cabo, se debe decidir acerca de qué parte de la infraestructura de TI será controlada por la Gestión de Configuración. Aparte de esto, el rango se puede recoger de la determinación del Acuerdo de Nivel de Servicio.

Con la subdivisión en niveles, se crea una jerarquía de componentes y unidades. Se toman decisiones sobre qué son Cl's principales y en cuántos niveles estos Cl's deben ser detallados. El nivel más alto es la infraestructura de TI. El nivel útil más bajo es el nivel donde todavía sea posible llevar control. La instancia de un CI en la CMDB sólo es efectiva cuando el control sobre el CI y la información que conlleva sean útiles para otros procesos de ITIL.

2.3.1.4 Acuerdos de Niveles de Servicio

La actividad de Gestión de Seguridad de la Información puede ser desencadenada por muchos acontecimientos como modificaciones o nuevas directrices de gobierno

corporativo, de negocios de Política de Seguridad, de los procesos de gestión corporativa de riesgos, nuevas necesidades de la empresa o cambios o actualización de servicios, de acuerdos, tales como las SLR, SLA, OLA o de los contratos. Por revisión de planes de negocio y las estrategias de TI, o por análisis del diseño. Debido a las brechas de seguridad de componentes o advertencias, eventos y alertas. Como consecuencia de actividades periódicas, como la revisión o la presentación de informes. Por la detección o la notificación de un cambio de riesgo o impacto de un proceso de negocios, un servicio de TI o un componente. Por las solicitudes de otras áreas, en particular, el SLM aporta beneficios a los problemas de seguridad.

Los principales objetivos del proceso de Gestión de Seguridad deben proporcionar un valor para el dinero de los contratos, y garantizar que todos los objetivos en la consolidación de contratos y los acuerdos se ajustan a las necesidades empresariales y los objetivos acordados dentro de los SLA. La gestión de acuerdos es llevada a cabo a través del proceso de Gestión del Cambio, para garantizar que cualquier impacto se evalúa.

En ITIL un SLA se define como un acuerdo por escrito entre un proveedor de servicios y los clientes de los niveles de servicio acordados para un servicio. Los SLA`s deben ser revisados periódicamente para asegurar que el rendimiento se ajusta a los niveles de servicio que se han acordado.

2.3.2 Cobit

El estándar Cobit (Control Objectives for Information and related Technology) ofrece un conjunto de mejores prácticas para la gestión de los sistemas de información de las organizaciones.

El objetivo principal de Cobit consiste en proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos con tal de:

- → Asegurar el buen gobierno, protegiendo los intereses de los stakeholders (clientes, accionistas, empleados, etc.)
- → Garantizar el cumplimiento normativo del sector al que pertenezca la organización.
- → Mejorar la eficacia y eficiencia de los procesos y actividades de la organización.
- → Garantizar la confidencialidad, integridad y disponibilidad de la información.

Cobit clasifica los procesos de negocio relacionados con las Tecnologías de la Información en 4 dominios:

- → Planificación y Organización
- → Adquisición e Implementación
- → Entrega y Soporte
- → Supervisión y Evaluación

Por otra parte, la organización dispone de recursos (aplicaciones, información, infraestructura y personas) que son utilizados por los procesos para cubrir los requisitos del negocio:

- → Efectividad (cumplimiento de objetivos)
- → Eficiencia (consecución de los objetivos con el máximo aprovechamiento de los recursos)
- → Confidencialidad
- → Integridad
- → Disponibilidad
- → Cumplimiento regulatorio
- → Fiabilidad

Cabe destacar que Cobit también ofrece mecanismos para la medición de las capacidades de los procesos con objeto de conseguir una mejora continua. Para ello, proporciona indicaciones para valorar la madurez en función de la misma clasificación utilizada por estándares como ISO 15504:

- → Nivel 0 – Proceso incompleto: El proceso no existe o no cumple con los objetivos
- → Nivel 1 – Proceso ejecutado
- → Nivel 2 – Proceso gestionado: el proceso no solo se encuentra en funcionamiento, sino que es planificado, monitorizado y ajustado.
- → Nivel 3 – Proceso definido: el proceso, los recursos, los roles y responsabilidades se encuentran documentados y formalizado.
- → Nivel 4 – Proceso predecible: se han definido técnicas de medición de resultados y controles.
- → Nivel 5 – Proceso optimizado: todos los cambios son verificados para determinar el impacto, se han definido mecanismos para la mejora continua, etc.

En general, gran parte de los puntos que se exponen a continuación pueden ser mapeados a los controles definidos en el estándar ISO 27002.

- → Planificación y Organización

→ Adquisición e Implementación
→ Entrega y Soporte
→ Supervisión y Evaluación

El marco general de Cobit se muestra en la siguiente ilustración.

Tabla 2. Procesos de Cobit

Planear y Organizar	Entregar y Dar Soporte
PO1 Definir un Plan Estratégico de TI	AI1 Identificar soluciones automatizadas
PO2 Definir la Arquitectura de la Información	AI2 Adquirir y mantener software aplicativo
PO3 Determinar la Dirección Tecnológica	AI3 Adquirir y mantener infraestructura tecnológica
PO4 Definir los Procesos, Organización y Relaciones de TI	AI4 Facilitar la operación y el uso
PO5 Administrar la Inversión en TI	AI5 Adquirir recursos de TI
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	AI6 Administrar cambios
PO7 Administrar Recursos Humanos de TI	AI7 Instalar y acreditar soluciones y cambios
PO8 Administrar la Calidad	
PO9 Evaluar y Administrar los Riesgos de TI	
PO10 Administrar Proyectos	
Adquirir e Implementar	**Monitorear y Evaluar**
DS1 Definir y administrar los niveles de servicio	ME1 Monitorear y Evaluar el Desempeño de TI Gobierno de TI
DS2 Administrar los servicios de terceros	ME2 Monitorear y Evaluar el Control Interno
DS3 Administrar el desempeño y la capacidad	ME3 Garantizar el Cumplimiento Regulatorio
DS4 Garantizar la continuidad del servicio	ME4 Proporcionar Gobierno de TI
DS5 Garantizar la seguridad de los sistemas	
DS6 Identificar y asignar costos	
DS7 Educar y entrenar a los usuarios	
DS8 Administrar la mesa de servicio y los incidentes	
DS9 Administrar la configuración	
DS10 Administrar los problemas	
DS11 Administrar los datos	
DS12 Administrar el ambiente físico	
DS13 Administrar las operaciones	

La entrega y soporte de servicios se encuentran constituidos por diversos procesos orientados a asegurar la eficacia y eficiencia de los sistemas de información. En concreto el proceso DS5 se basa en garantizar la seguridad de los sistemas: gestión de identidades, gestión de usuarios, monitorización y tests de seguridad, protecciones de seguridad, prevención y corrección de software malicioso, seguridad de la red, intercambio de datos sensibles. El proceso está compuesto por:

- → **DS5.1 Administración de la Seguridad de TI:** Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
- → **DS5.2 Plan de Seguridad de TI:** Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.
- → **DS5.3 Administración de Identidad:** Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas, y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.
- → **DS5.4 Administración de Cuentas del Usuario:** Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse

a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

- → **DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad:** Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.
- → **DS5.6 Definición de Incidente de Seguridad:** Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.
- → **DS5.7 Protección de la Tecnología de Seguridad**: Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.
- → **DS5.8 Administración de Llaves Criptográficas:** Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de claves criptográficas estén implantadas, para garantizar la protección de las claves contra modificaciones y divulgación no autorizadas.
- → **DS5.9 Prevención, Detección y Corrección de Software Malicioso:** Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).
- → **DS5.10 Seguridad de la Red:** Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
- → **DS5.11 Intercambio de Datos Sensitivos:** Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

El proceso DS5 tiene como entradas los siguientes resultados de los procesos:

- → PO2. Clasificacion de datos asignados mediante la definición de la Arquitectura de Información.
- → PO3 Estándares de tecnología a través de la determinación de la Dirección Tecnológica.
- → PO9 Evaluación de riesgo por el proceso Evaluar y Administra los Riesgos de TI.
- → AI2 Especificaciones de controles de seguridad en las aplicaciones gracias al proceso de Adquirir y Mantener Software Aplicativo.
- → DS1 OLAs como salida del proceso de Definir y Administrar los Niveles de Servicio.

Y los procesos dependientes de DS5 son:

- → DS8 Administrar los Servicios e Incidentes a través de los Requerimientos específicos de entrenamiento sobre conciencia de seguridad.
- → DS7 Educar y Entrenar a los Usuarios gracias a los Reportes de desempeño del proceso.
- → ME1 Monitorear y Evaluar el Desempeño de TI con los Cambios de seguridad requeridos.
- → AI6 Administrar cambios a través de los Cambios de seguridad requeridos.
- → P09 Evaluar y Administra los Riesgos de TI mediante las Amenazas y vulnerabilidades de seguridad.

A continuación, se muestra una imagen que representa el proceso DS5 con los procesos relacionados, y los valores de entrada y salida:

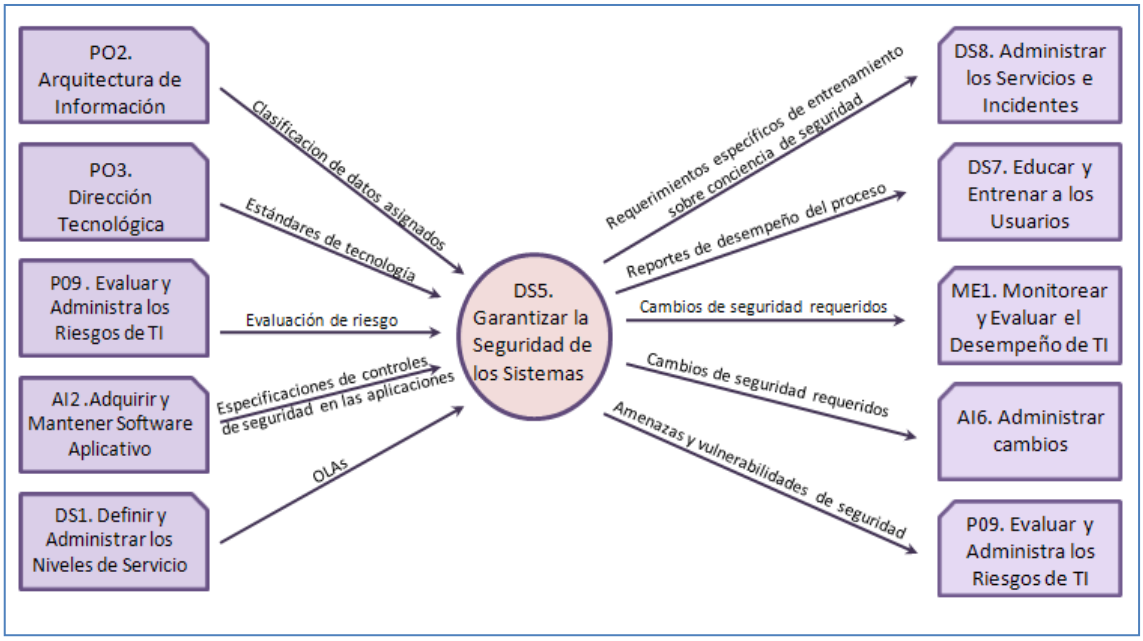


Figura 6. Cobit Proceso DS5 y sus relaciones con procesos anteriores y posteriores

2.3.3 MAGERIT II

El análisis de riesgos propuesto por MAGERIT II es una aproximación metódica que permite determinar el riesgo siguiendo unos pasos:

- → Determinar los activos relevantes para la Organización
- → Determinar a qué amenazas están expuestos aquellos activos
- → Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- → Valorar dichos activos en función del coste que supondría para la Organización recuperarse ante un problema de disponibilidad, integridad, confidencialidad o autenticidad
- → Valorar las amenazas potenciales.
- → Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

El método propuesto por MAGERIT II da cumplimiento en lo establecido en la ISO 13335, en el epígrafe 4.2.1.d Identificar Riesgos, 4.2.1.e Analizar y evaluar riesgos de la ISO /IEC 27001:2005 , y además garantiza conformidad respecto los estándares.

2.4 Conformidad Legal

2.4.1 LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Es una Ley Orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

2.5 Modelos de Madurez de Seguridad de la Información

Los modelos de madurez o de capacidad permiten ayudar a las organizaciones a definir sus procesos, a evaluar su calidad y a mejorar a lo largo del tiempo. El ámbito de la seguridad, al requerir esfuerzos importantes que afectan a varias áreas, existen varios modelos de madurez de alcance internacional y que se han estudiado para definir el modelo de madurez a emplear en el modelo de Gobierno de la Seguridad TI propuesto. A modo simplificado en la figura continua se muestran diferentes estados por los que pasa la seguridad de la información TI en las organizaciones dependiendo del nivel de experiencia en que nos encontremos.

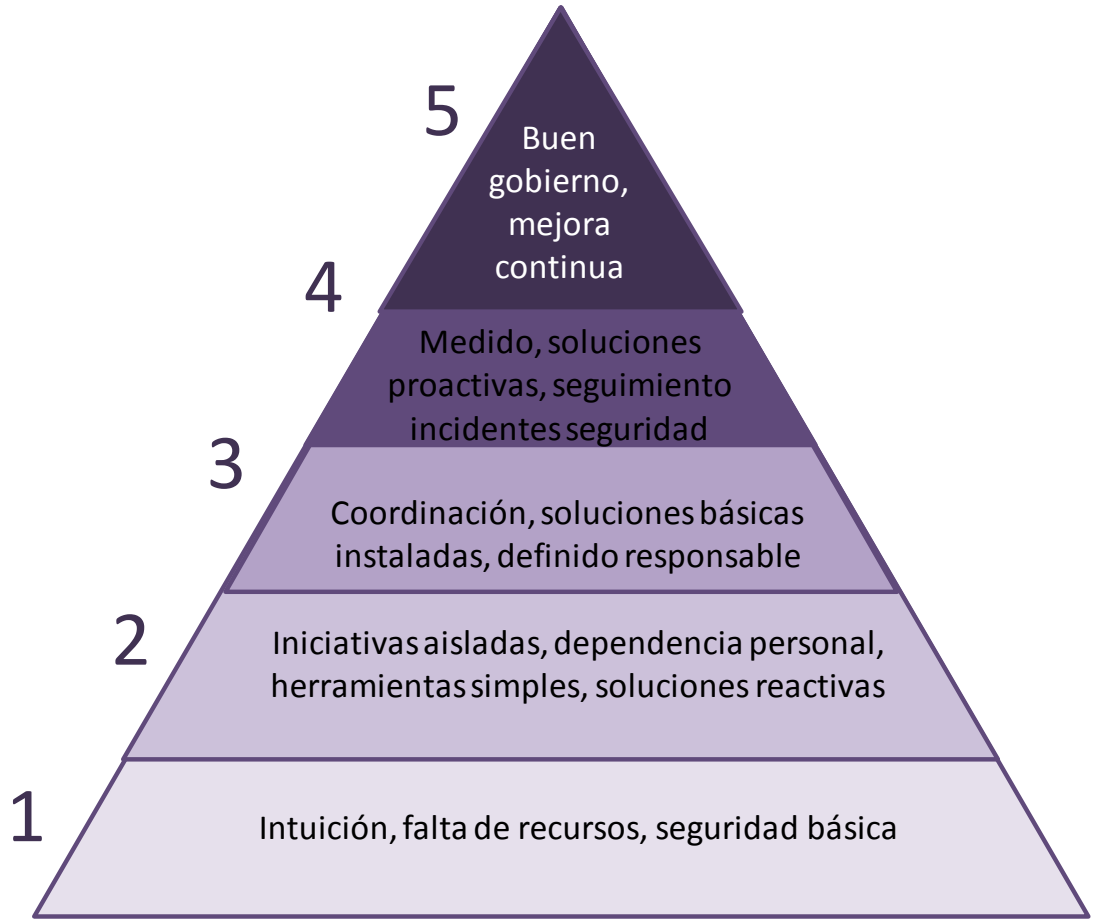


Figura 7. Ejemplo de niveles de madurez en el área de seguridad

Uno de los modelos de madurez relativos a la seguridad que se encuentran más completos y evolucionados es el "Systems Security Engineering Capability Maturity Model" desarrollado por Carnegie Mellon University. El modelo de madurez de "Information Security Management Maturity Model" (ISM3) introduce tres niveles de responsabilidad de la gestión (strategic management, tactical management and operational management) y una serie de procesos con información de cómo llegar a cubrir los objetivos y sus principales entradas y salidas. En la tabla continua se muestran los modelos de madurez relativos a la seguridad TI analizados (los niveles se han dejado en inglés para mantener la versión inicial).

Tabla 3. Modelos de Madurez de la Seguridad analizados

	PRINCIPALES CARACTERÍSTICAS	**NIVELES DE MADUREZ**
Systems Security engineering Capability Maturity	El System Security Engineering Capability Maturity Model describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de	Performed informally, planned and tracked, well defined, quantitatively controlled and

Model (SSE-CMM) or ISO/IEC 21827	sistemas. Define 22 áreas para cada una de las cuales se puede alcanzar un nivel en función del cumplimiento de unas "características comunes". Existen 11 áreas de procesos de ingeniería y otras 11 dedicadas a la gestión de proyectos y organización.	continuously improving
Information Security Management Maturity Level - ISM3	Focalizado en nivel de cumplimiento de procesos comunes de seguridad de la información. Proporciona métricas, responsabilidades y principales metodologías relacionadas.	Undefined, defined, managed, controlled and optimized
Building Security In Maturity Model (BSIMM)	BSIMM describes a number of activities that any large organization can put into practice. The activities are described in terms of the SSF, which identifies twelve practices grouped into four domains. Associated with each activity is an objective.	Level 1, level 2 y level 3.
Citigroup Information Security Evaluation Model - Citi-ISEM	Citi-ISEM is a five-level model based on Information Security sound practices and the concepts of Prevention, Detection and Verification. ISEM sets Information Security goals and monitors status, defines a set of controls for assessing and compensating for vulnerabilities, provides a means for classifying risk, assists in determining the nature of threats and provides tools for impact assessment and analysis and recommends solutions.	Complacency, acknowledgment, integration, common practice and continuous improvement.
Gartner´s Security Model	Modelo simplificado que sigue una curva en “s” empezando en temas estratégicos de la seguridad y terminando en la mejora continua.	Blissfull ignorance, awareness phase, corrective phase and operations excellence phase.
Community Cyber Maturity Model (CSMM)	The Community Cyber Security Maturity Model provides a structure which communities and states can use to determine their level of preparedness and to create a plan to improve their security posture and enhance their chances of successfully preventing or detecting and responding to a cyber attack.	Security Aware, Process Development, Information Enabled, Tactics Development, Full Security Operational Capability

NIST PRISMA Enhancement	Presenta un nivel de madurez en cinco niveles en nueve áreas procedentes de las 17 familias de control de NIST SP 800-53.	Policy, procedures, implemented, tested, integreted.
Generic Security Maturity Model (SMM) by MM Lessing	Define un modelo de madurez genérico tras analizar las mejores prácticas y su enlace con sus correspondientes niveles de madurez.	Blind trusting, repeteable, defined, amanged and maintenace.

A continuación, y a modo de ejemplo, se detallan algo más el modelo ISM3 y el modelo de madurez del ITGI.

2.5.1 ISM3

El Modelo de Madurez de la Gestión de la Seguridad de la Información (ISMMM o ISM3, del inglés Information Security Management Maturity Model) ofrece un enfoque para especificar, implementar, operar y evaluar sistemas ISM, y se basa en las siguientes pautas:

- → Está diseñado para ser aplicable a cualquier organización independientemente de su tamaño.
- → Puede usarse para mejorar los sistemas ISM de la organización, resaltando diferencias entre el nivel actual y el nivel deseado de madurez.
- → Emplea un enfoque cuantitativo para evaluar la madurez del sistema ISM de una organización y su ambiente de control de seguridad de la información.
- → Puede ser útil como una guía para priorizar inversiones. Comparando los objetivos de seguridad y los objetivos de madurez, el análisis del nivel de madurez puede ayudar a determinar si una organización debería estar gastando más o menos en seguridad de la información.

ISM3 define la madurez en términos de procesos ISM y tres amplios niveles de responsabilidad de gestión. Se utilizan cuatro modelos conceptuales:

- → El Modelo de Gestión de la Seguridad de Información: proporciona un marco para identificar los procesos principales en un sistema ISM y evaluar su madurez.
- → El Modelo Organizativo: proporciona una visión basada en responsabilidades de una organización.
- → El Modelo de Sistema de Información: proporciona una manera de describir los componentes principales de los sistemas de información.

→ El Modelo de Seguridad Contextual: permite a una organización preparar su propia definición de seguridad ajustada al ambiente y misión de la organización.

Es importante destacar que muchas amenazas de las organizaciones caen fuera del alcance de la gestión de sistemas de información. Tales incidentes son de origen interno, y a menudo incluyen errores, o acciones maliciosas o fraudulentas de los empleados. Tales incidentes incluyen:

→ Error Humano;
→ Incompetencia;
→ Fraude;
→ Corrupción.

Estos incidentes caen fuera del alcance de ISM3 porque ISM3 busca evidencia de la existencia de procesos, no de resultados; los resultados son responsabilidad de la gestión.

En cualquier caso, el uso de la Transparencia, el Particionado, la Supervisión, la Rotación y la Separación de Responsabilidades (TPSRSR), en procesos ISM y procesos no ISM puede ayudar a proteger a la organización y a los sistemas de información de este tipo de incidentes.

2.5.2 IT Governance Institute

El Instituto de Gobierno de TI (ITGITM), del inglés IT Governance Institute (ITGITM) ofrece las pautas para lograr un gobierno eficaz de seguridad de la información, a través de la gerencia mediante un marco para guiar el desarrollo y el mantenimiento de un programa de seguridad de la información global. El marco de gobierno general de seguridad de la información se compone de:

→ Metodologías de gestión de riesgos de seguridad de la información.
→ Una estrategia de seguridad integral explícitamente vinculada con las empresas y objetivos de TI.
→ Una estructura de seguridad de la organización efectiva.
→ Una estrategia de seguridad que habla sobre el valor de la información protegida y entrega.
→ Políticas de seguridad que se ocupan de cada aspecto de la estrategia, control y regulación.
→ Un conjunto completo de estándares de seguridad para cada política para asegurar que la política cumple los procedimientos y directrices.

- → Observación de los procesos institucionales para garantizar el cumplimiento y proporcionar comentarios sobre la eficacia y la mitigación de riesgo.
- → Un proceso para asegurar una evaluación continua y la actualización de las políticas de seguridad, normas, procedimientos y riesgos.

El programa de seguridad se basa en las siguientes pautas:

- → Desarrollo y mantenimiento de las políticas de seguridad.
- → Asignación de roles, responsabilidades, autoridad y rendición de cuentas.
- → Desarrollo y mantenimiento de un marco de seguridad y control que se compone de normas, medidas, prácticas y procedimientos.
- → Evaluaciones periódicas de los riesgos y los análisis de impacto sobre las empresas.
- → Clasificación y asignación de la propiedad de los activos de información.
- → Adecuada, efectiva y pruebas de controles a las personas, procesos y tecnología.
- → Integración de la seguridad en todos los procesos de la organización.
- → Procesos para monitorear los elementos de seguridad.
- → Gestión de incidencias de seguridad de la información.
- → Procesos de identidad y gestión de acceso para los usuarios y proveedores de la información.
- → Monitorización y métricas de rendimiento de seguridad.
- → La educación de todos los usuarios, administradores y miembros del equipo respecto a los requisitos de seguridad de la información.
- → Evaluaciones anuales de seguridad de la información e informes.
- → Plan de medidas correctivas para corregir las deficiencias de seguridad de la información.
- → Formación en el funcionamiento de los procesos de seguridad.
- → Desarrollo y evaluación de los planes para continuar el negocio en caso de interrupción o un desastre.

El objetivo de seguridad se cumple cuando:

- → La información está disponible y para utilizar cuando sea necesario, y los sistemas que la proporcionan puede resistir o recuperarse de los ataques (disponibilidad).
- → La información es observada por o revelada sólo a aquellos que tienen la necesidad de saber (confidencialidad).
- → La información no está protegida contra modificaciones no autorizadas (integridad).
- → Las transacciones comerciales, así como el intercambio de información entre la empresas o con los socios externos se puede confiar (autenticidad y no repudio).

Los resultados esperados de la Gestión de Seguridad de la Información son:

- → Alineación estratégica de seguridad de la información con la estrategia de negocio para apoyar los objetivos de la organización.
- → Gestión de riesgos mediante la ejecución de las medidas adecuadas para gestionar y mitigar los riesgos y reducir los impactos potenciales sobre los recursos de información a una nivel aceptable
- → Gestión de los recursos mediante la utilización de los conocimientos y la información de seguridad infraestructura eficiente y eficaz.
- → Indicadores de rendimiento, monitorización y presentación de informes mediante métricas de gobierno de seguridad para garantizar que la organización logra los objetivos.
- → Optimización de las inversiones de Seguridad de la Información garantizando los objetivos

Se recomienda cuatro prácticas esenciales:

- → Identificar los líderes de seguridad de la información
- → Garantizar la eficacia de la política de la información de seguridad mediante la revisión y aprobación.
- → Asignar la seguridad de la información a un comité.

2.6 Métricas de madurez

En el caso de violaciones graves de seguridad o incidentes, es necesaria una evaluación para determinar qué error en los procesos hubo, qué lo provocó y cómo se puede prevenir en el futuro. Todas las infracciones de la seguridad y los incidentes de seguridad deben ser estudiados con el fin de obtener una imagen completa de la eficacia de las medidas de seguridad en su conjunto. Un procedimiento de presentación de informes de incidentes de seguridad es necesario para poder evaluar la eficacia y la eficiencia de las medidas de seguridad actual.

2.6.1 COBIT

Las métricas óptimas de Cobit aplicadas a seguridad de la información se detallan a continuación, distribuidas en los cuatro dominios: planificación y organización, adquisición e implementación, entrega y apoyo, seguimiento y evaluación.

2.6.1.1 Planificación y Organización

→ PO5 Administrar la Inversión en TI:

- Asignaciones presupuestarias para la seguridad (programas operativos, los nuevos programas, apreciación)

→ PO7 Administrar Recursos Humanos de TI

- % Evaluaciones de los responsables del Sistema de Seguridad del desempeño en el trabajo y cumplimiento.
- % De definiciones de roles, responsabilidades y certificadores.

→ PO9 Evaluar y Administrar los Riesgos de TI. Se basa en métricas que cuantifican lo que la organización sabe, y no sabe, sobre la naturaleza del riesgo inherente a su infraestructura, la gente, y la información. Las métricas son:

- % Activos críticos /funciones que residen en sistemas compatibles.
- % Activos críticos/ funciones de revisión de los riesgos de seguridad física.
- % Activos críticos/ funciones con un coste estimado de compromiso.
- % Activos críticos/ funciones de evaluación de riesgos documentadas.
- % Activos críticos/ funciones con planes de mitigación de riesgos documentadas.

2.6.1.2 Desarrollo y Mantenimiento

Se basa en métricas de administración de la entrega y mantenimiento de las actividades de control del día a día que comprenden operaciones de seguridad:

→ AI1 Identificar soluciones automatizadas:

- % Cobertura de los controles de confidencialidad de datos intercambiados con los clientes / socios.
- % Cobertura de los controles de integridad de datos intercambiados con los clientes / socios.
- % De nuevos sistemas con consultas de seguridad.

→ AI4 Facilitar la operación y el uso:

- % Sistemas de información con políticas operativas y controles.
- % Principales unidades de negocio con procedimientos operaciones alineados a controles.

→ AI7 Instalar y acreditar soluciones y cambios basados en la acreditación y certificación de los sistemas de la información:

- % Acreditados y clientes.
- % Sistemas con acreditaciones de seguridad.
- % Sistemas con certificaciones de seguridad.
- % Sistemas de información con los costes de seguridad integrada.

2.6.1.3 Adquisición e Implementación

→ DS2 Administrar los servicios de terceros:

- % Aplicaciones a terceros examinados con éxito dentro de los estándares del servicio.
- % Acuerdos con partner/terceros con requisitos de seguridad documentados.
- % Acuerdos con terceros que requieren validación externa de los procesos.
- % Usuarios de terceros cuyos privilegios están revisados.

→ DS5 Garantizar la seguridad de los sistemas:

- % Usuarios con acceso autorizado al sistema.
- % Usuarios con acceso autorizado a software de seguridad.
- % Empleados con multitud de privilegios revisados
- % Empleados obsoletos con multitud de privilegios revisados.

- % Activos con roles asignados.
- % Roles, aplicaciones y funciones de sistemas en producción.
- % Sistemas con políticas implementadas de bloqueo de cuentas.
- % Sistemas/Aplicaciones con políticas de verificación de contraseñas.
- % Directorios de cuentas obsoletas o deshabilitadas.
- % Cuentas de usuarios inactivas por política
- % Cuentas de usuarios antiguos deshabilitadas por política.

→ DS11 Administrar los datos:

- % Backup para terceros.
- % Backup entregado satisfactoriamente.

2.6.1.4 Monitorización se basa en la medición de las actividades de control

→ ME1 Monitorear y Evaluar el Desempeño de TI Gobierno de TI:

- % Sistemas con monitorización de eventos y logs de actividad
- % Sistemas de cara al cliente e Internet con monitorización de eventos y logs de actividad.
- % Sistemas monitorizados para las desviaciones de configuraciones aprobadas.

→ ME2 Monitorear y Evaluar el Control Interno:

- % Sistemas críticos revisados el cumplimiento de los controles.
- % Relaciones con terceros revisadas de cumplimiento
- % Sistemas con al menos una deficiencia grave.

→ ME3 Garantizar el Cumplimiento Regulatorio:

- % Requisitos externos claves para cumplir la auditoría externa.
- % Revisiones de cumplimiento de seguridad de las debilidades más importantes

2.6.2 ITIL

Las métricas óptimas de ITIL aplicadas a Seguridad de la Información se detallan a continuación, distribuidas en los cinco dominios: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio.

Los Indicadores Clave de Rendimiento ITIL (KPI's) se utilizan para evaluar si los procesos de una organización de TI funcionan según las expectativas. Los principales PKI´s basados en Gobierno de Seguridad de la Información son los siguientes:

2.6.2.1 Diseño del Servicio

→ Gestión de la Disponibilidad:

- Índice de resistencia a la disponibilidad. Resistencia de nuestra infraestructura hacia la protección de servicios. Fórmula: 1- (Número total de incidencias con impacto/ Número total de incidencias)
- Madurez del proceso de Gestión de Disponibilidad. Mide el grado en que cumplimos las mejores prácticas de Gestión de Disponibilidad. Fórmula: Madurez del proceso de Gestión de Disponibilidad.
- Índice de vulnerabilidad de la seguridad. Mide el grado de vulnerabilidad ante amenazas de seguridad. Fórmula: Número de incidencias relacionadas con la seguridad/ Número total de incidencias.
- Índice de mejora continúa de la disponibilidad. Mide la proactividad con la que se busca mejorar el servicio de disponibilidad. Fórmula: 1-(Número de servicios no cubiertos por el plan de disponibilidad/ Número de servicios en el catálogo de servicios)

→ Gestión de la Seguridad de la Información:

- Cantidad de medidas preventivas implementadas. Mide la Cantidad de medidas de seguridad preventivas implementadas como respuesta a amenazas de seguridad identificadas. Fórmula: Número total de medidas preventivas.
- Duración de la implementación de medidas preventivas implementadas. Duración desde la identificación de una amenaza de seguridad hasta la implementación de una contramedida adecuada. Fórmula: Tiempo medio de la implementación de las medidas.
- Cantidad de incidentes graves de la seguridad. Cantidad de incidentes de seguridad identificados, clasificados por categoría de gravedad. Fórmula: Número de incidente graves / Número total de incidencias / peticiones
- Cantidad de periodos de inactividad de servicio relacionados con la seguridad. Cantidad de incidentes de seguridad que causan interrupciones de servicio o disponibilidad reducida.

- Cantidad de pruebas de seguridad. Cantidad de pruebas y adiestramientos de seguridad llevados a cabo. Fórmula: Número total de pruebas de seguridad.
- Cantidad de defectos identificados durante las pruebas de seguridad. Cantidad de defectos identificados en los mecanismos de seguridad durante las pruebas. Fórmula: Numero de defectos / Número total de pruebas de seguridad.

2.6.2.2 Transición del Servicio

→ Gestión de Cambios:

- Tasa de eficiencia de los cambios. Mide la eficiencia a la hora de gestionar los cambios. Fórmula: Número total de cambios implementados / Número total de cambios.
- Tasa de éxitos de cambios. Mide la efectividad a la hora de gestionar los cambios. Fórmula: 1- (Número de cambios fallidos/ Número total de cambios implementados)
- Tasa de cambios replanificados. Mide la eficiencia de implementar cambios en el tiempo estipulado. Fórmula: Número de cambios replanificados / Número total de cambios.
- Tiempo medio de proceso por cambio (días). Mide el tiempo medio en que se tarda realizar un cambio. Fórmula: Tiempo medio de proceso por cambio (días)
- Tasa de cambios no autorizados. Porcentaje de cambios que se saltaron el proceso de gestión de cambios. Fórmula: Número de cambios no autorizados detectados/ Número total de cambios implementados.
- Tasa de incidencias provocadas por el cambio. Porcentaje de cambios que provocaron incidencias. Fórmula: Número de cambios que han provocado incidencias/ Número total de cambios implementados.
- Madurez del proceso de Gestión de Cambios. Mide en qué grado se cumplen las mejores prácticas de Gestión de Cambios. Fórmula: Madurez del proceso de Gestión de Cambios.

→ Gestión de Activos y Configuración:

- Tasa de acierto de la CMDB. Mide la precisión de la información contenida en la CMDB. Fórmula: 1- (Numero de errores en los CI descubiertos/ Número total de CIs en la CMDB)

- Número de incidencias relacionadas con información incorrecta de un CI. Mide el número de incidencias causadas debido a una información imprecisa de la CMDB. Fórmula: Número de incidencias relacionadas con un información incorrecta de un CI.
- Número de cambios erróneos relacionados con una información incorrecta de un CI. Mide el número de cambios que fallaron debido a una información imprecisa de la CMDB. Fórmula: Número de cambios erróneos relacionados con una información incorrecta de un CI.
- Madurez del proceso de Gestión de la configuración. Mide si se está ejecutando el proceso de una manera adecuada o no. Fórmula: Madurez del proceso de Gestión de la Configuración.
- Tasa de CMDB. Mide qué porcentaje de la infraestructura está comprendida en la CMDB. Fórmula: 1- (Número de servicios operados con una información incompleta de sus CIs/ Número de de servicios incluidos dentro del Catalogo de servicios)
- Tasa de propiedad de los CIs. Mide qué parte de la infraestructura no tiene asignado un propietario. Fórmula: 1- (Número de servicios operados con una información incompleta de sus CIs/ Número total de CIs en la CMDB)

→ Gestión de Liberación y Despliegue:

- Tasa de eficiencia de las entregas. Mide la eficiencia a la hora de manejar las entregas. Fórmula: Número total de entregas implementadas/ Número total de entregas
- Tasa de éxitos de entregas. Mide la efectividad a la hora de manejar las entregas. Fórmula: 1- (Número de entregas fallidas/ Número total de entregas implementadas)
- Tasa de entregas replanificadas. Mide la eficiencia de implementar entregas en el tiempo estipulado. Fórmula: Número de entregas replanificadas/ Número total de entregas.
- Tasa de entregas defectuosas. Mide el porcentaje de entregas que causaron incidencias. Fórmula: Número de entregas que han provocado incidencias/ Número total de entregas implementadas.
- Madurez del proceso de Gestión de Entregas. Mide en qué grado cumplimos las mejores prácticas de Gestión de la Entrega. Fórmula: Madurez del proceso de Gestión de la Entrega

2.6.2.3 Operación del Servicio

→ Gestión de Incidentes:

- Número total de incidencias. Número de incidencias que ocurren dentro de la infraestructura. Fórmula: (Número total de incidencias / peticiones).
- Número de incidencias con prioridad alta. Número de incidencias de prioridad alta que han ocurrido. Fórmula: Número de incidencias con prioridad alta.
- Tasa de resolución de incidencias. Mide el porcentaje de resolución de incidencias de negocio. Fórmula: Número de incidencias / peticiones resueltas dentro de los SLAs/ (Número total de incidencias / peticiones)
- Tiempo medio de resolución de incidencias con prioridad alta (horas). Mide la rapidez resolviendo incidencias. Fórmula: Tiempo medio para resolver incidencias con prioridad alta (horas)
- Madurez del proceso de Gestión de Incidencias. Mide en qué grado cumplimos las mejores prácticas de Gestión de Incidencias. Fórmula: Madurez del proceso de Gestión de Incidencias
- Tiempo medio de resolución de incidencias. Mide el tiempo habitual en la resolución de una incidencia desde su apertura hasta al cierre.

→ Gestión de Problemas:

- Tasa de repeticiones de Incidencias. Mide la efectividad previniendo la repetición de incidencias. Fórmula: Número de incidencias repetidas/ Número total de incidencias.
- Número de problemas graves. Mide cuantos problemas graves se han producido en la infraestructura. Fórmula: Número de problemas graves.
- Tasa de resolución de problemas. Porcentaje de problemas solucionados. Fórmula: Número total de problemas eliminados (Control del Error)/ Número total de problemas encolados.
- Tasa de Soluciones Temporales. Porcentaje del número de soluciones temporales que se han implementado por problema. Fórmula: Número de Errores Conocidos (Causa raíz conocida y solución temporal propuesta)/ Número de incidencias repetidas.

- Tiempo medio de resolución de problemas con prioridad alta (días). Mide la rapidez resolviendo problemas. Fórmula: Tiempo medio de resolución de problemas – gran prioridad (días).
- Madurez del proceso de Gestión de Problemas. Mide el grado en que cumplimos las mejores prácticas de Gestión de Problemas. Fórmula: Madurez del proceso de Gestión de Problemas

→ Gestión de Accesos

- Número total de solicitudes de acceso. Número de solicitudes de acceso, solicitud de servicio, RFC, etc. que se dan dentro de la infraestructura. Fórmula: Número total de solicitudes de acceso.
- Las instancias de acceso concedidas, por el servicio, usuario, departamento, etc.
- Las instancias de acceso concedidas por el departamento o la concesión de derechos individuales.
- Número de incidentes que requieren un restablecimiento de los derechos de acceso.
- Número de incidentes causados por la configuración de acceso incorrecto.

3 HERRAMIENTAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1 La Gestión de Seguridad de la Información

El proceso de un Sistema de Gestión de Seguridad de la Información requiere de un medio para diseñar el Plan de Gestión de Riesgos. Por ello, a continuación se detallan las herramientas de mercado que contienen mayor funcionalidad para cubrir un Plan de Gestión de Seguridad de la Información.

Las herramientas analizadas son:

- → STREAM Integrated Risk Manager (Acuity)
- → EAR/ Pilar. El Centro Criptológico Nacional ha patrocinado el desarrollo de la herramienta comercial, que está siendo ampliamente utilizada en la administración pública española.
- → G&SGSI (Sigea)
- → Proteus (InfoGov)
- → RiskVision OpenGRC (Agilance)
- → RSA Archer eGRC Solutions
- → Brabeion Polaris IT GRC Management Suite
- → Modulo Risk Manager (Modulo)
- → RSAM
- → Control Compliance Suite y Security Information Manager (Symantec)

3.2 Características de las Herramientas

3.2.1 STREAM Integrated Risk Manager (Acuity)

STREAM es una solución amplia, altamente configurable y sencilla de utilizar de software de gestión de riesgos. Automatiza los procesos complejos involucrados en la gestión de cumplimiento.

Figura 8. Principales áreas de Stream

Características principales:

- → Evaluaciones de riesgo
- → Auditorías, cuadros de mando e informes, junto con una extensa gestión de métricas.
- → Cumplimiento de controles y asignación.
- → Gestión de Riesgos.
- → Gestión de Incidentes.
- → Identificación de Problemas en base al histórico.
- → Gestión de Normas ISO 27001.
- → Gestión de Amenazas y Vulnerabilidades.

→ Gestión de Mejoras y Seguimiento.

[STREAM Integrated Risk Manager (Acuity). Consultado el 30 de Septiembre 2010. http://www.acuityrm.com/]

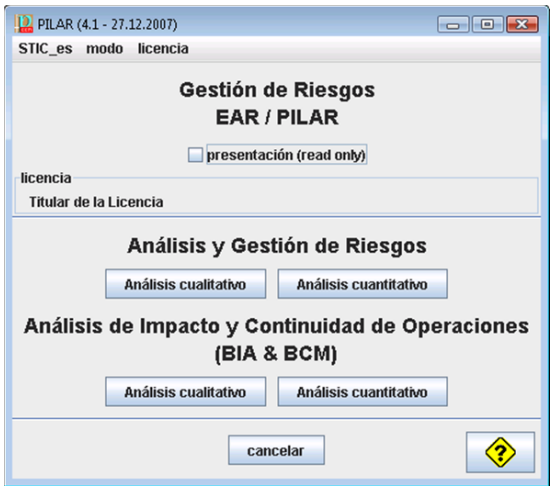
3.2.2 EAR/Pilar

Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

→ Esquema Nacional de Seguridad.

→ ISO/IEC 27002:2005.



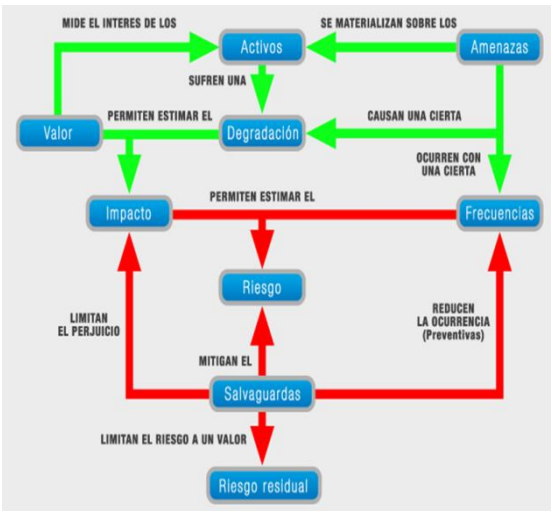


Figura 9. Principales áreas de EAR/Pilar

Características principales:

- → Evaluaciones de Riesgo y Riesgo Residual.
- → Auditorías e informes.
- → Gestión de Riesgos.
- → Gestión de Normas y procedimientos de Seguridad, y personalización de Políticas y Leyes.
- → Bibliotecas que incluyen clases de activos, amenazas típicas, una política de seguridad y procedimientos estándar de seguridad
- → Gestión de Planes de Continuidad mediante Backup y planes de recuperación de desastres.
- → Gestión de Amenazas y Vulnerabilidades.

[EAR/Pilar. Consultado el 1 de Octubre 2010. http://www.ar-tools.com/]

3.2.3 G&SGSI (Sigea)

G&SGSI es un software destinado a realizar un Análisis de Riesgos de Seguridad necesario para la certificación de un Sistema de Gestión de Seguridad de la Información , bajo las normas UNE 71502 e ISO 27001.

GxSGSI incluye un componente de simulación de fallos, mediante el cual puede generar, de manera ficticia, un fallo en cualquiera de los equipos del sistema de información con el fin de analizar las amenazas y vulnerabilidades que lo afectan o podrían afectar y detectar el número y coste de las contramedidas necesarias.

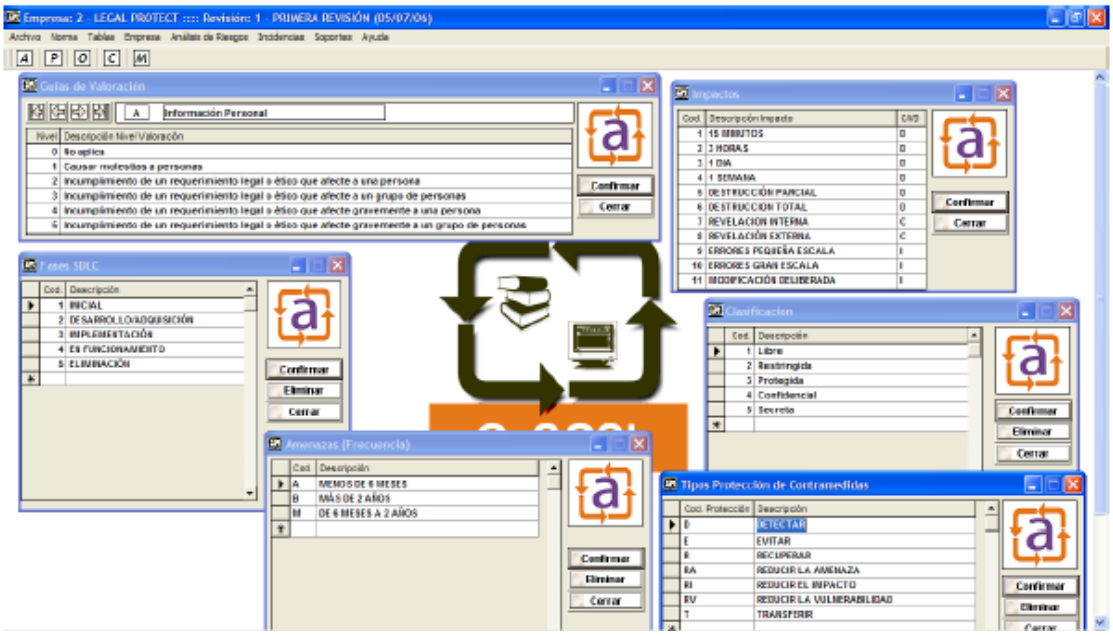


Figura 10. Principales áreas de G&SGSI

Características principales:

- → Gestión de Políticas y Normativa Legal.
- → Evaluaciones del Riesgo Residual e Intrínseco.
- → Auditorías. Genera todos los informes requeridos en una auditoría de certificación ISO 27001.
- → Cumplimiento de controles. Incorpora un inventario de activos y árboles de dependencia.
- → Gestión de Riesgos.
- → Gestión de Incidentes.
- → Gestión de Amenazas y Vulnerabilidades.
- → Gestión de Planes de Continuidad.

3.2.4 Proteus (InfoGov)

Proteus ® Enterprise ™ es una suite de productos en línea para analizar, gestionar y medir el cumplimiento de estándares corporativos y permite crear y administrar un SGSI según la norma BS ISO / IEC 27001. Proteus ® Manager ™ y Proteus ® ™ RISKview son herramientas de software de Administración de Información, están diseñados para ser utilizados en combinación con el software Proteus ®.

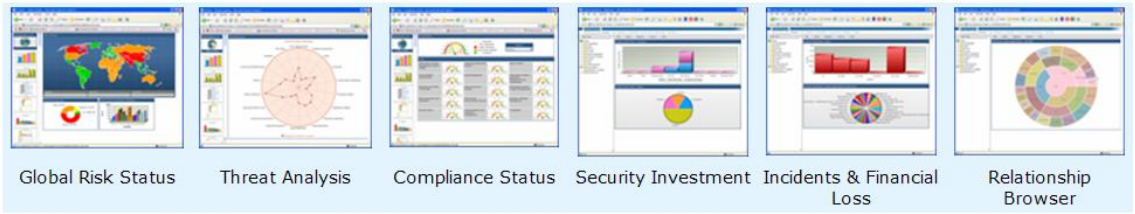


Figura 11. Principales áreas de Proteus

Características principales:

- → Evaluaciones de riesgo gracias a una gestión de activos incorporada.
- → Auditorías e Informes con Business Objects.
- → Cumplimiento de controles mediante un formato gráfico en tiempo real.
- → Gestión de Riesgos y Riesgos Residuales.
- → Gestión de Incidentes.
- → Seguimiento de Problemas y Soluciones.
- → Gestión de Amenazas y Vulnerabilidades.
- → Gestión de Normas ISO 27001.
- → Gestión de Planes de Continuidad.

[Infogov. The leader in Web-based IT Governance, Risk, Compliance and Fraud Management. (2009). Consultado en Agosto y Octubre 2010. http://www.infogov.co.uk/]

3.2.5 RiskVision OpenGRC (Agiliance)

La tecnología RiskVision se basa en un innovador diseño OpenGRC ™, con la infraestructura configurable, extensible y escalable. La aplicación incluyen un motor de informes, una asignación dinámica de riesgo y el motor de la agregación, un motor de cálculo de riesgo, un motor de flujo de trabajo flexible, un motor de colaboración, una AppBuilder para configurar las aplicaciones, el diseño de ventanas DashBuilder, y un marco de integración con el formato que mantienen I/O entre Microsoft Word, Excel y SharePoint, SQL y la API de servicios web para la mayoría de las aplicaciones, bases de datos, archivos y sistemas y más de 30 conectores.

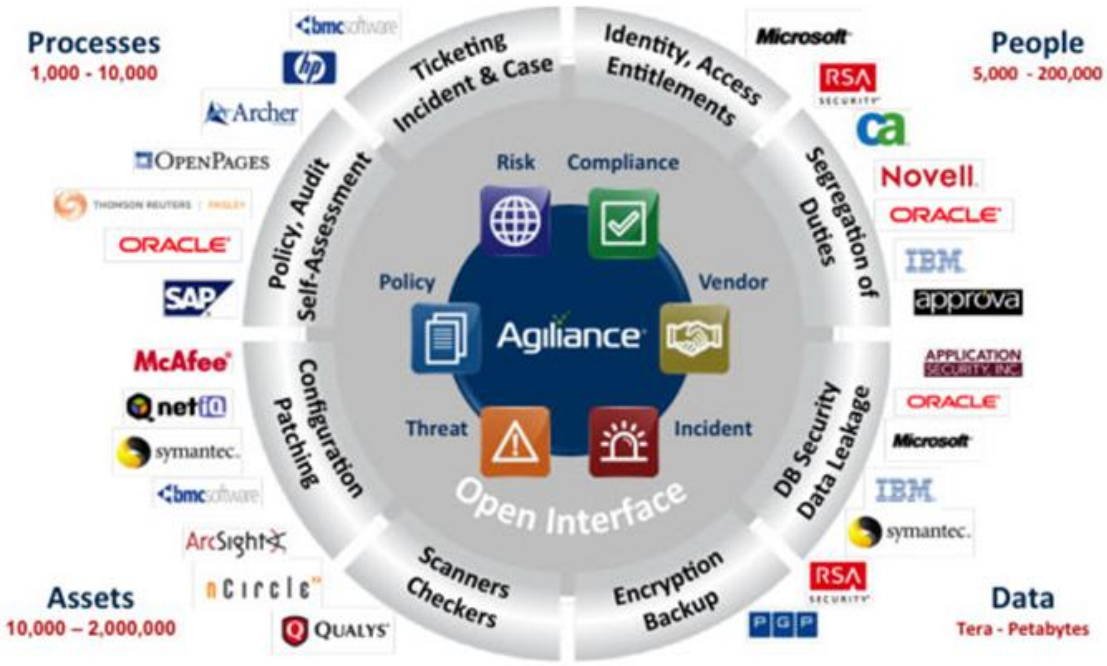


Figura 12. Principales áreas de RiskVision

Características principales:

- → Evaluaciones de riesgo
- → Auditorías. Hacer cumplir las políticas iniciales y establece periodos de revisión y aprobación de las políticas. Evalúa los controles.
- → Cumplimiento de controles. Establece automatizar la clasificación de activos con la evaluación de la clasificación y asignar dinámicamente lo controles en base a dicha clasificación. Incluyo, informa y mide sobre el cumplimiento de las leyes y las políticas internas.
- → Gestión de Riesgos. Permite identificar y analizar los numerosos riesgos que pueden afectar a la organización. Incluye crear y supervisar indicadores clave de riesgo y seguimiento de tendencias.
- → Gestión de Incidentes. Incorpora un riguroso proceso de respuesta a incidentes, incluyendo una recopilación de datos, investigación, evaluación de riesgos, recuperación, aprobación, revisión y presentación de informes.
- → Gestión de Políticas. Permite Crear y hacer cumplir la política de normalización y las plantillas de política de normalización, y administrar la excepción del ciclo de vida de la política, incluyendo solicitud, revisión, aprobación y autorización.

→ Gestión de Amenazas y Vulnerabilidades. Permite la identificación, correlación, evaluación, corrección y presentación de informes de vulnerabilidades, indicando automáticamente los activos vulnerables y la información sobre las amenazas. También, calcula dinámicamente la puntuación de la amenaza y el impacto de negocio basado en la criticidad de los activos y la criticidad amenaza.

[PRiskVision OpenGRC (Agiliance). Consultado el 4 de Octubre 2010. http://www.agiliance.com/products/platform.html]

3.2.6 RSA Archer eGRC Solutions

RSA Archer eGRC Solutions permite construir un gobierno de riesgo y cumplimiento (eGRC) de programas en TI, finanzas, operaciones y ámbitos jurídicos.

Con RSA Archer se puede gestionar los riesgos, demostrar el cumplimiento, automatizar procesos de negocio, y ganar visibilidad en el riesgo corporativo y controles de seguridad.

Figura 13. Principales áreas de RSA Archer eGRC Solutions

Características principales:

- → Evaluaciones de riesgo en base a los activos, ya que incluye un repositorio con el detalle de estos.
- → Auditorías. Incluye planificación, programación, asignación de prioridades en al riesgo, la dotación de personal, la gestión de los procedimientos de auditoría y seguimiento de los esfuerzos.
- → Cumplimiento de controles, incluye la opción de importación de controles.
- → Gestión de Riesgos. Identificación de Riesgo, junto con indicadores y vías de comunicación.
- → Gestión de Incidentes. Esta solución basada en web permite capturar eventos que pueden derivar en incidentes, evaluar la criticidad incidente, y asignar los miembros del equipo de respuesta en función del impacto de negocio y los requisitos reglamentarios
- → Gestión de Políticas. La herramienta ofrece una infraestructura centralizada para la creación de políticas, normas y procedimientos de control y asignación a los objetivos corporativos, reglamentos, directrices de la industria y las mejores prácticas. Permite comunicar las políticas en toda la empresa, la aceptación, evaluar la comprensión y gestión de excepciones.
- → Gestión de Amenazas y Vulnerabilidades. Proporciona un repositorio consolidado de datos de amenazas, información clara de las actividades para remediar la amenaza, y un proceso de gestión de amenazas consistente.
- → El Plan de Continuidad proporciona un enfoque centralizado y automatizado para la planificación de recuperación de desastres y continuidad del negocio, lo que le permite responder rápidamente en situaciones de crisis para proteger sus operaciones en curso. Combina la continuidad del negocio y recuperación ante desastres.

[RSA Archer eGRC Solutions. Consultado el 4 de Octubre 2010. http://www.archer.com/solutions/index.html]

3.2.7 Brabeion Polaris IT GRC Management Suite

Polaris Brabeion IT GRC Suite de Administración incorpora una Gestión de Gobierno de riesgos y cumplimiento de perfiles efectivos, para crear la alineación a través de una

política de la empresa correspondiente, los procedimientos y el marco de los controles y reducir los costos, los despidos y las exposiciones con las evaluaciones y auditorías automatizadas.

Brabeion es propulsado por un motor de contenido gracias a una alianza estratégica con PricewaterhouseCoopers. Y otras alianzas estratégicas como E & Y, IT Governance Institute, Microsoft, NetIQ y Oracle permiten a los clientes aprovechar las tecnologías existentes, el contenido y la experiencia de las mejores prácticas de implementación.

Características principales:

- → Evaluaciones de riesgo
- → Auditorías.
- → Cumplimiento de controles
- → Gestión de Riesgos.
- → Gestión de Incidentes.
- → Seguimiento de Problemas y Soluciones.
- → Gestión de Políticas, en consonancia con los objetivos de negocio y los mandatos legislativos
- → Gestión de Amenazas y Vulnerabilidades.
- → Gestión de Planes de Continuidad con el fin de simplificar el mantenimiento y la recuperación rápida de la información y los procedimientos.

[Brabeion Polaris IT GRC Management Suite. Consultado el 4 de Octubre 2010. http://www.networkproductsguide.com/best/2008/Brabeion_Software.html]

3.2.8 Modulo Risk Manager (Modulo)

Módulo Risk Manager permite la gestión de riesgos, evalúa el cumplimiento de los reglamentos y normas aplicables. El análisis de riesgos se realiza mediante una metodología estructurada sobre la base de prácticas internacionalmente reconocidas de gestión de riesgos.

La gestión de riesgos se realiza a través de un ciclo de gestión de riesgo integrado por los siguientes pasos: Inventario de captura, análisis, evaluación y tratamiento.

Características principales:

- → Evaluaciones de riesgo. Ofrece un perfil de riesgo de acuerdo al impacto potencial de cada activo y la importancia. Permite obtener informes filtrados por tipo de activo, perímetros, procesos de negocio y las amenazas.
- → Auditorías.
- → Cumplimiento de controles. También incorpora gestión controles innecesarios eliminando así los costos redundantes. Incluyendo una base de conocimiento con más de 11.000 controles.
- → Gestión de Riesgos. Incluye evaluación de leyes, reglamentos, normas y directrices que marcan la pauta para la Gobierno y Cumplimiento.
- → Gestión de Amenazas y Vulnerabilidades. Monitorea amenazas de la infraestructura tecnológica, procesos de negocio, gente y distribución geográfica
- → Gestión de Planes de Continuidad con el fin de simplificar el mantenimiento y la recuperación rápida de la información y los procedimientos.

[Modulo Risk Manager (Modulo). Consultado el 5 de Octubre 2010. http://www.modulo.com/risk-manager]

3.2.9 RSAM

Rsam es una plataforma de Gobierno, Riesgo y Cumplimiento (GRC) que integra la criticidad de negocios, la evaluación de los datos reglamentarios y las vulnerabilidades, permitiendo a las organizaciones empresariales ganar una gran visibilidad de riesgo, la supervisión y la garantía.

El resultado es un proceso de gestión de riesgos repetible y sostenible que reduzca los costos, mejore el rendimiento del negocio, y proporcione una visibilidad amplia de riesgos empresariales.

Características principales:

- → Evaluaciones de riesgo de requisitos y evaluación de cumplimiento. Incluye encuestas personalizadas, flujo de trabajo dinámico, notificación por correo electrónico automatizado e informes interactivos. Las evaluaciones se centran en la evaluación de los activos individuales que representan cierto nivel de criticidad para la organización. El objetivo de la evaluación del Riesgo es encontrar estos objetos, calcular su criticidad y riesgo, registrar sus vulnerabilidades y controles, y la puntuación de ellos.

- → Auditorías. Permite la Auto-evaluación antes de la auditoría in situ mediante la distribución de cuestionarios y listas de control de auditoría para los auditados, reduciendo considerablemente el tiempo durante la auditoría. También, se puede realizar un seguimiento e informar sobre las pruebas o programar y controlar las pruebas periódicas y planes de acción.
- → Cumplimiento de controles. Rsam elimina las redundancias en el cumplimiento de los requisitos y gestiona las excepciones de las políticas y una evaluación de los controles activos.
- → Gestión de Riesgos. Se combina la criticidad de negocios, la evaluación de los datos reglamentarios, y las vulnerabilidades en un marco de riesgo centralizada para el seguimiento de todos los riesgos y controles
- → Gestión de Incidentes. Proceso crítico que ofrece una organización con la capacidad de detectar y solucionar los incidentes y, a continuación directa de los recursos adecuados para resolverlos lo antes posible
- → Seguimiento de Problemas y Soluciones. Incorpora un repositorio de información.
- → Gestión de excepción de Políticas.
- → Gestión de Amenazas y Vulnerabilidades. La evaluación del riesgo de una vulnerabilidad permite priorizar de manera inteligente (mediante la criticidad de los activos, los requisitos de cumplimiento, amenazas, etc.) y solucionar vulnerabilidades descubiertas.

[RSAM. Consultado el 5 de Octubre 2010. http://www.rsam.com/RsamPlatform.htm]

3.2.10 Control Compliance Suite y Security Information Manager (Symantec)

Control Compliance Suite Symantec es la solución integral y completamente automática que administra todos los aspectos del cumplimiento y los riesgos de TI a un menor costo y con menor complejidad. Control Compliance Suite ofrece contenido listo para usar de varias normativas del sector, evaluación automática de controles técnicos y de procedimientos, con elaboración centralizada de informes mediante paneles de control según la función e integración con otras soluciones de seguridad de Symantec.

Características principales:

- → Definición y administración de políticas
- → Evaluación de la eficacia de los controles en el cumplimiento de las políticas.
- → Identificación de las vulnerabilidades críticas en los servidores, las aplicaciones web, las bases de datos y los sistemas de control no administrados más confidenciales.
- → Informes sobre el nivel de cumplimiento y riesgos generales con informes y paneles de control dinámico y basado en Web. Integración de los controles técnicos, de datos y de procedimientos con evidencia de sistemas externos.
- → Identificación de las amenazas desde dispositivos administrados y no administrados
- → Diferenciación entre amenazas reales y posibles vulnerabilidades con calificación avanzada de riesgos.
- → Paneles de control dinámicos y basados en Web que comunican los datos más importantes a las múltiples partes interesadas de la organización y ofrecen visibilidad completa del nivel de cumplimiento y los riesgos de TI.
- → Comunicación de los resultados fácilmente mediante la impresión, exportación o envío por correo electrónico de vínculos a tableros de control.
- → Priorización de las tareas de evaluación y reparación para los activos de TI según los datos almacenados en éstos.

Security Information Manager permite ejecutar procesos documentados y repetibles de respuesta ante amenazas para la seguridad e implementar el cumplimiento de políticas de TI mediante soluciones integradas de respuesta ante incidentes y administración de registros. Symantec Security Information Manager está diseñado para brindar protección anticipada, lo que ayuda a las organizaciones a demostrar el cumplimiento y reducir los riesgos generales para la seguridad.

Características principales:

- → Integración con Active Directory. Permite el acceso a usuarios del AD haciendo más rápida y fiable la autenticación de usuarios y disminuyendo los gastos de administración.
- → Recolectores universales y personalizados de administración de registros. Permite aumentar el alcance de los datos de seguridad incluidos en las colecciones de inteligencia.
- → Más de 150 plantillas de elaboración de informes para automatizar, analizar y entregar pruebas de cumplimiento: SOX, ISO 27001, PCI-DSS, HIPAA, Informes, NERC, UK-DPA.

[Symantec. Consultado el 6 de Octubre 2010. http://www.symantec.com]

3.3 Análisis comparativo y conclusiones

A continuación, se detallan las diversas funcionalidades de las herramientas seleccionadas. Como se ha mencionado previamente el estudio es para determinar los requisitos a considerar en el diseño a medida de la Solución de Gobierno propuesta, dado que principalmente las herramientas analizadas tratan de aspectos de gestión:

	Sw 1	Sw 2	Sw 3	Sw 4	Sw 5	Sw 6	Sw 7	Sw 8	Sw 9	Sw 10
Definición y Administración de Políticas	x	x	x	x	√	√	√	√	√	√
Definición de Vulnerabilidades	√	√	√	√	√	√	x	√	√	√
Gestión de Amenazas	√	x	√	x	√	√	x	√	√	√
Análisis de Impacto De negocio	x	√	x	x	x	√	x	√	x	√
Inventario de activo y evaluación	√	√	√	√	√	√	x	√	√	√
Identificación de riesgos	√	√	√	√	√	√	√	√	√	x
Análisis de riesgos	√	√	√	√	√	√	√	√	√	√
Tratamiento de riesgo	√	√	√	√	√	√	√	√	√	√
Aceptación de riesgo	√	√	√	√	√	√	√	√	√	√
Priorización del Riesgo	√				√	√	√	√	√	√

Cumplimiento de controles	√	√	x	√	√	√	√	√	√	√
Métricas e Indicadores claves de riesgos	√	x	x	x	√	√	x	x	x	x
Desarrollo de control	√	x	x	√	√	√	√	√	√	√
Gestión de incidencias e informes	√	x	√	√	√	√	x	x	√	x
Eventos	√	√	√	√	√	√	x	x	√	x
Plan de Continuidad	√	√	√	√	x	√	x	√	x	x
Auditoria remota	√	x	x	√	√	√	√	√	√	x
Informes	√	√	√		√	√	√	√	√	√
Medios de comunicación	√	√	√	√	x	√	√	√	√	√
País de Origen	Reino Unido	España	España	Reino Unido						
Cobertura	Todo el mundo	Local	Todo el mundo	Local	Todo el mundo	Todo el mundo	Todo el mundo	Todo el mundo	Todo el mundo	Todo el mundo
Precio	5.500 €	1.500 €	5.500 €	4.500 €				Licencia por tipo de organización y cantidad de asset.		Licencias 1120€ Control + 24.650€ Security Information
Soporte					√	√	√	√	√	√
Escalabilidad	√	x	x	√						√

Figura 14. Análisis comparativo de Herramientas

En la siguiente tabla se muestran valoradas las funcionalidades contempladas en las herramientas de Gestión de Seguridad de la Información. En la columna Pesos se ha establecido un valor de mayor importancia a menor en función de la funcionalidad en cuestión.

	Pesos	Sw 1	Sw 2	Sw 3	Sw 4	Sw 5	Sw 6	Sw 7	Sw 8	Sw 9	Sw 10
Definición y Administración de Políticas	4	0	0	0	0	4	4	4	4	4	4
Definición de Vulnerabilidades	3	3	3	3	3	3	3	0	3	3	3
Gestión de Amenazas	3	3	0	3	0	3	3	0	3	3	3
Análisis de Impacto De negocio	3	0	3	0	0	0	3	0	3	0	3
Inventario de activo y evaluación	4	4	4	4	4	4	4	0	4	4	4
Identificacion de riesgos	3	3	3	3	3	3	3	3	3	3	0
Analisis de riesgos	3	3	3	3	3	3	3	3	3	3	3
Tratamiento de riesgo	4	4	4	4	4	4	4	4	4	4	4
Aceptación de riesgo	3	3	3	3	3	3	3	3	3	3	3
Priorizacion del Riesgo	3	3	0	0	0	3	3	3	3	3	3
Cumplimiento de controles	3	3	3	0	3	3	3	3	3	3	3
Metricas e Indicadores claves de riesgos	2	2	0	0	0	2	2	0	0	0	0
Desarrollo de control	2	2	0	0	2	2	2	2	2	2	2
Gestion de incidencias e informes	2	2	0	2	2	2	2	0	0	2	0
Eventos	2	2	2	2	2	2	2	0	0	2	0
Plan de Continuidad	1	1	1	1	1	0	1	0	1	0	0
Auditoria remota	1	1	0	0	1	1	1	1	1	1	0
Informes	2	2	2	2	0	2	2	2	2	2	2

Medios de comunicación	1	1	1	1	1	0	1	1	1	1	1
TOTAL VALOR TI:	42	32	31	32	44	49	29	43	43	38	
Cobertura	3	3	0	3	0	3	3	3	3	3	3
Soporte	2	0	0	0	0	2	2	2	2	2	2
Escalabilidad	1	1	0	0	1	1	1	1	1	1	1
TOTAL ASPECTOS TECNOLOGICOS:	4	0	3	1	6	6	6	6	6	6	

Figura 15. Análisis de pesos comparativo de Herramientas

El Diagrama Tecnología-Valor-Riesgo muestra gráficamente la funcionalidad de las herramientas en función del valor de TI con las funcionalidades que incorporan y los aspectos técnicos.

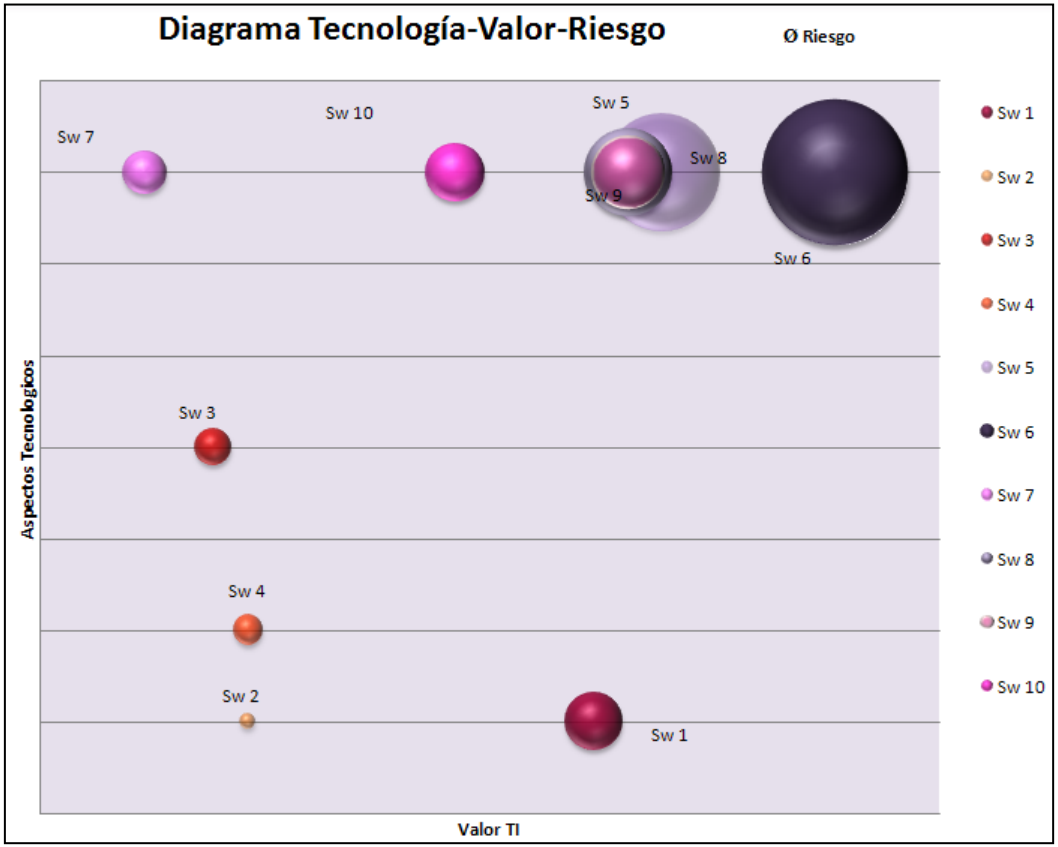


Figura 16. Diagrama Tecnología-Valor-Riesgo Herramientas

4 SOLUCIÓN TECNOLÓGICA PROPUESTA

El sistema a desarrollar consiste en una herramienta para el Gobierno de Seguridad de la Información. Se pretende que sea una herramienta sencilla pero útil, que permita crear, clasificar y mantener las entidades del sistema. Además, debe incorporar los tratamientos de las relaciones entre los riesgos, activos y controles, trabajar con el glosario de términos y ayudas, y obtener informes del sistema, entre otras funcionalidades.

El desarrollo de esta herramienta mejora, facilita o amplia las funcionalidades que ofrecen otras herramientas del mismo tipo.

La herramienta está destinada a todas aquellas personas o empresas que quieran disponer de un modo eficaz de una herramienta capaz de administrar su seguridad. Se pretende que la herramienta sea sencilla para el usuario, pero, obviamente, el usuario ha de tener unos conocimientos básicos acerca de la seguridad de la información, así como de la gestión de la misma.

De la parte del Servidor se dispondría de lo siguiente:

- **Apache:** es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.11 y la noción de sitio virtual.
- **Ruby on Rails**, también conocido como **RoR** o **Rails:** es un marco o "framework" de aplicaciones web de código abierto escrito en el lenguaje de programación Ruby, siguiendo el paradigma de la arquitectura Modelo Vista Controlador (MVC). Las piezas de la arquitectura Modelo Vista Controlador en Ruby on Rails son las siguientes:
  - **Modelo.** En las aplicaciones web orientadas a objetos sobre bases de datos, el Modelo consiste en las clases que representan a las tablas de la base de datos.
  - **Vista.** En MVC, Vista es la lógica de visualización, o cómo se muestran los datos de las clases del Controlador. Con frecuencia en las aplicaciones web la vista consiste en una cantidad mínima de código incluido en HTML. El método que se emplea en Rails por defecto es usar Ruby

Embebido (archivos.rhtml, desde la versión 2.x en adelante de RoR archivos.html.erb), que son básicamente fragmentos de código HTML con algo de código en Ruby, siguiendo una sintaxis similar a JSP. También pueden construirse vistas en HTML y XML con Builder o usando el sistema de plantillas Liquid.

- **Controlador.** En MVC, las clases del Controlador responden a la interacción del usuario e invocan a la lógica de la aplicación, que a su vez manipula los datos de las clases del Modelo y muestra los resultados usando las Vistas. En las aplicaciones web basadas en MVC, los métodos del controlador son invocados por el usuario usando el navegador web.

→ **MySQL.** Es un sistema de gestión de base de datos relacional, multi-hilo y multiusuario con más de seis millones de instalaciones.

Para acceder a la herramienta la parte del Cliente es la siguiente:

→ **Firefox Mozilla**: Es un navegador de internet libre. Mediante él se ofrece los servicios a los usuarios del sistema.

5 DISEÑO CONCEPTUAL

5.1 Descripción General

Para mostrar el modelo de Gobierno de la Seguridad TI propuesto, se muestra en este apartado el diseño conceptual para completarlo en el punto 6 con el diseño funcional. En el primer sub-apartado se describe a modo de enunciado de los requisitos del Sistema de Gobierno de la Seguridad de la Información y en el siguiente sub-apartado se describen estos con algo más de detalle (modelo conceptual).

5.2 Requisitos del Sistema de Gobierno de la Seguridad de la Información

El sistema consiste en una aplicación capaz de gestionar a nivel de Gobierno los riesgos en una organización que emplee en diferentes grados las TI, siendo válido en principio para cualquier tipo de empresa. Las funcionalidades principales de las que dispone nuestra herramienta son:

- → **Gestión de Usuarios:** La aplicación permitirá dar de alta, modificar, borrar y listar los datos de los Usuarios dentro de la aplicación, asignando los roles y permisos para acceder a la aplicación.
- → **Gestión de Riesgos:** La aplicación permitirá la gestión de múltiples Riesgos. En la aplicación se podrá añadir, modificar, borrar y listar los diversos Riesgos. Incluyendo funcionalidad de Evaluación del Riesgo, Aceptación del Riesgo y Priorización del Riesgo.
- → **Gestión de Áreas de Activos:** La aplicación permitirá la gestión de áreas de activos que conllevan un Riesgo. En la aplicación se podrá añadir, modificar, borrar y listar las diversas áreas de activos. Incluyendo funcionalidad para calcular el Impacto del Activo.
- → **Gestión de Acuerdos de Negocio:** La aplicación permitirá la gestión de múltiples Acuerdos de Negocio, en lo relativo a aspectos de seguridad, asociados a áreas de activos. En la aplicación se podrá añadir, modificar, borrar y listar los diversos Acuerdos de Negocio.

- → **Gestión de Incidencias:** La aplicación permitirá la gestión de Incidencias que conllevan un Riesgo. En la aplicación se podrán dar de alta, modificar, borrar y listar las diversas Incidencias. Incluyendo funcionalidad para calcular la Urgencia de resolución.
- → **Gestión de Clases de Amenazas:** La aplicación permitirá la gestión de Amenazas dentro de las Incidencias y Vulnerabilidades de los Activos y el entorno. En la aplicación se podrán dar de alta, modificar, borrar y listar las diversas Amenazas.
- → **Gestión de Clases de Vulnerabilidades de Activos:** La aplicación permitirá la gestión de Vulnerabilidades de los Activos y el entorno. En la aplicación se podrán dar de alta, modificar, borrar y listar las diversas Vulnerabilidades.
- → **Gestión de Requisitos ante un Riesgo:** La aplicación permitirá la gestión de Requisitos de los Riesgos localizados. En la aplicación se podrán dar de alta, modificar, borrar y listar los diversos Requisitos. Incluyendo funcionalidad de priorización de Requisitos para gestionar los controles necesarios.
- → **Gestión de Grupos de Controles:** La aplicación permitirá la gestión de los Controles establecidos en base a los riesgos del sistema. En la aplicación se podrá añadir, modificar, borrar y listar los diversos Controles. Incluyendo funcionalidad de costes y priorización de implantación de controles necesarios para cubrir los requisitos.
- → **Gestión de Planes de Seguimiento y Continuidad:** La aplicación permitirá la gestión de los Planes de Seguimiento y Continuidad establecidos en base a los riesgos del sistema. En la aplicación se podrá añadir, modificar, borrar y listar los diversos Planes de Seguimiento y Continuidad.
- → **Gestión de Políticas de Seguridad de TI:** La aplicación permitirá la gestión de las Políticas de Seguridad de TI establecidos en base a los riesgos del sistema. En la aplicación se podrá añadir, modificar, borrar y listar las diversas Políticas de Seguridad de TI.
- → **Gestión de Normativa Externas:** La aplicación permitirá la gestión de las Normativas Externas establecidos en base a los riesgos del sistema. En la aplicación se podrá añadir, modificar, borrar y listar las diversas Normativas Externas.
- → **Gestión de Líneas Estratégicas de Seguridad:** La aplicación permitirá la gestión de los Objetivos de Seguridad establecidos en base a los riesgos del sistema. En

la aplicación se podrá añadir, modificar, borrar y listar las diversas Líneas Estratégicas de Seguridad.

→ **Gestión de Evaluación del SGSI y Auditoria:** La aplicación permitirá la gestión de informes de cada requisito vinculados. En la aplicación se podrá consultar todos los requisitos y relaciones, y añadir y modificar informes de Evaluación del SGSI y Auditoria.

5.3 Modelo conceptual

Como se ha analizado en el estado del arte existen múltiples normas, estándares y mejores prácticas con propuestas relativas a la ejecución, Gestión y Gobierno de la Seguridad de las TI. Dentro de estas normas y estándares podemos encontrar: definición de políticas, definición de procesos, definición de controles y acciones, etc. El problema es que tanta disparidad de información con un elevado número de amenazas crecientes hace complicado tener una imagen simple de las fortalezas y debilidades de las organizaciones así como de los planes de acción a ejecutar. Por ello, se presenta el siguiente modelo conceptual de Gobierno de la Seguridad, en el que se quiere que en un plazo corto de tiempo determinar el nivel de madurez de la seguridad y las medidas ejecutivas a desplegar. También, el presente modelo conceptual permite poder realizar un Gobierno continuo de los aspectos de seguridad en las organizaciones sin que el exceso de información haga que las decisiones que se tomen no sean las correctas de acuerdo a criterios de prioridad y de aportación de valor.

En el presente diseño conceptual se tiene en cuenta que para mejorar la madurez en la seguridad TIC muchas veces es necesario cambios culturales y ejecutivos a establecerse, con más prioridad que la implantación de complejas herramientas o cambios en los procesos.

Todos los estándares, normas y mejores prácticas existentes pueden ser útiles, y se seleccionan y se priorizan a partir de las conclusiones que marca el proceso del Gobierno de la Seguridad TIC. El modelo de datos simplificado es el mostrado a continuación en la figura 17. El detalle de este modelo de datos con sus atributos y métodos se ve en los diagramas de clases del apartado de diseño funcional.

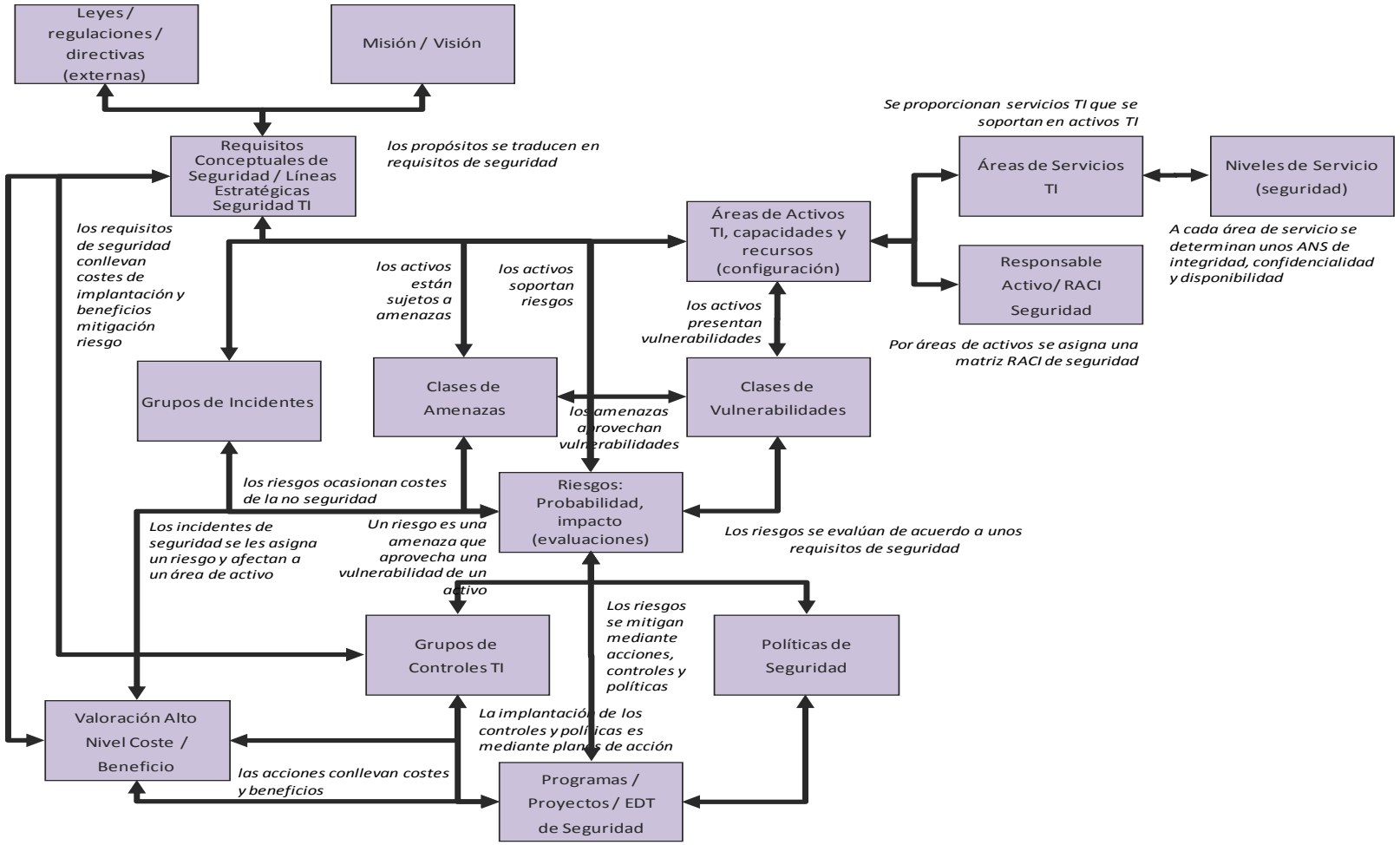


Figura 17. Principales entidades del modelo

A continuación, se muestra un resumen de las principales áreas del Gobierno de la Seguridad TI. En el apartado del diseño funcional se abre para cada una de ellas un diagrama de secuencia, y para las áreas que así lo requieran se definirán también diagramas de estado.

5.3.1 Visionado, marco general y estrategias básicas de la Seguridad:

Se informará de la misión, visión y líneas estratégicas de seguridad TI que se pretende dotar en la organización. Se informará de las herramientas de valoración de la estrategia TI seguidas (tanto internas como externas, como las cadenas de valor, DAFO o cinco fuerzas) y de los factores críticos de cambio (FCC) de la seguridad acordados y detectados. Se entiende como FCC de la seguridad aquel aspecto de seguridad, interno o externo al departamento TI, que tenga importancia estratégica, que sea susceptible de aportación de valor o de cumplimiento de normas políticas y regulaciones y que deberemos considerar como partida a la hora de definir las metas u objetivos estratégicos de seguridad. Se valoraran, sin entrar en gran detalle, cada una de las líneas estratégicas propuestas informando del coste de la no seguridad, coste de los controles, beneficio de la seguridad. Para determinar las líneas estratégicas se tendrá en cuenta el entorno (leyes, regulaciones y directivas) y por lo tanto información de las amenazas, de las vulnerabilidades y de los activos sobre los que afecta. También se informará de la entidad requisitos de seguridad a implantar para estar alineados con las líneas estratégicas y con la misión. Se llevará una relación de líneas estratégicas de seguridad TI con las líneas estratégicas de negocio de la que son parte.

5.3.2 Gobierno de las Áreas de Activos de Información

El modelo de Gobierno de la Seguridad, al ser un modelo de gobierno no baja a un detalle de información a nivel de activos, ni de elementos de configuración. La información está por área de activo pudiendo ser de dos tipos capacidades y recursos (el sistema mantiene el tipo de área de activo y el ciclo de vida donde interactúa el área de activos propuesta):

Recursos

- → Capital financiero
- → Infraestructura
  - Redes
  - Mainframe y servidores producción
  - Mainframe y servidores desarrollo, prueba y preproducción
  - Bases de datos producción
  - Bases de datos desarrollo, prueba y preproducción
  - Servidores web
  - Microinformática
- → Aplicaciones
  - Aplicaciones web
  - Sistemas operativos
  - Aplicaciones de negocio: RRHH
  - Aplicaciones de negocio: Financieras
  - Aplicaciones de negocio: Operación y logística
  - Aplicaciones de negocio: Clientes
  - Aplicaciones de soporte y gestión del soporte
  - Aplicaciones de gobierno negocio y TI
- → Información
  - Datos web
  - Datos de negocio: RRHH
  - Datos de negocio: Financieras
  - Datos de negocio: Operación y logística
  - Datos de negocio: Clientes
  - Datos de soporte y gestión del soporte
  - Datos de gobierno negocio y TI
- → Recursos humanos

Capacidades

- → Gestión
- → Organización
- → Procesos
- → Conocimiento
- → Recursos humanos

Para el caso de las aplicaciones se abrirá un activo desglosado por el momento del ciclo de vida en que se encuentre:

Tabla 4. Áreas de activo según el ciclo de vida

	Inicio y planificación	**Ejecución**	**Operación**	**Retiro**
Aplicaciones web	Área de Activo	Área de Activo	Área de Activo	Área de Activo

Sistemas operativos	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de negocio: RRHH	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de negocio: Financieras	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de negocio: Operación y logística	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de negocio: Clientes	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de soporte y gestión del soporte	Área de Activo	Área de Activo	Área de Activo	Área de Activo
Aplicaciones de gobierno negocio y TI	Área de Activo	Área de Activo	Área de Activo	Área de Activo

El motivo de este desglose es que, por ejemplo, se ha de controlar los riesgos de ejecución o los riesgos de confidencialidad de las aplicaciones retiradas. Con este desglose de áreas de activos se pueden gobernar los riesgos que acontecen en todas las fases del desarrollo de sistemas de información de manera diferenciada.

Las áreas de activos son clave pues para la fórmula de cálculo del modelo de Gobierno de la Seguridad TI, ya que asigna controles a nivel de área de activo (relación control y área de activo). También las amenazas son por área activo a las que van dirigidas y las vulnerabilidades son por las debilidades de cada área de activo (relación amenaza agrupada área de activo y relación vulnerabilidad agrupada área de activo). De esta forma se dispone de un riesgo, y después de aplicar los controles un riesgo residual por área de activo. Por lo tanto, el riesgo se asigna a cada área de activo.

Pero en un modelo de gobierno del riesgo que se propone también interesa tener como activo los sistemas de información en desarrollo que como amenaza conlleva, por poner un ejemplo, que el desconocimiento y la falta de experiencia del equipo conlleve variación en su coste y en su plazo de entrega. Las principales amenazas van a ser desconocimiento de los paradigmas, y tecnologías de diseño y desarrollo. Esta amenaza si nuestro equipo de desarrollo por falta de experiencia es vulnerable va a

provocar un riesgo, el cual va a tener consecuencias en menores y mas variables productividades de planificación y diseño por PF (punto función), en las productividades de desarrollo por puntos función, en las productividades del call center, las productividades de gestión de problemas y en las productividades de gestión de pruebas. Aparte del impacto en las productividades, también tendrá impacto en la variabilidad de estas productividades.

El sistema mantiene: Alcance indicando las áreas de activo con un campo indicativo de si están afectadas y las no afectadas por el Gobierno de la Seguridad, y mapa de sistemas (donde se muestra gráficamente las áreas de activos de aplicaciones de negocio y aplicaciones soporte).

Se informará tanto de activos internos como de activos externos (de terceras compañías que pueden trabajar para nosotros como proveedores) pero que puedan afectar a la misión y a las líneas estratégicas. Si es interno o externo lo indica un campo de nuestro aplicativo.

Por cada una de las líneas de activos se ha de mantener: Número de usuarios (críticos, neutros, no críticos), propietario del activo, principales requisitos del sistema, coste del activo (para valorar la pérdida), relación de otras áreas de activos afectadas (si se cae nuestra área que áreas que también se encuentran afectadas y en qué porcentaje) y grado de afectación.

En el caso de estructuras descentralizadas se permitirá el seguimiento de diferentes áreas de activo por unidad de negocio.

Por área de activo se informará de grandes cambios en la configuración con fecha o rango de validez del cambio y una pequeña descripción de a que afecta.

Para cada área de activo se enumeraran en una tabla las interconexiones que tiene, pues las interconexiones entre sistemas e infraestructuras son fuentes de riesgos de seguridad. Las interconexiones se les asignaran al sistema o infraestructura que envía mas información. Por poner un criterio.

5.3.3 Gobierno de las clases de amenazas

El sistema mantendrá un inventario de las amenazas agrupadas en clases de amenazas. Llevará un histórico de las clases de amenazas que han sucedido en la propia organización. Se podrá cargar por un proceso de carga información de amenazas de agencias y organismos externos por área de activo. Se informará de la agencia que lo propone. Se podrá informar de la probabilidad de la amenaza y el

componente aleatorio que conlleva. Se informará de las áreas de activos a los que afecta dicha clase de amenaza. La relación tiene una fecha de comienzo de vigencia y de fin de vigencia, pues a partir de ciertas fechas la amenaza no puede surtir efecto. La lista de clases de amenazas propuesta es la siguiente:

- → **Daños físicos:** Incendio, inundación, vandalismo, pérdida de potencia y los desastres naturales.
- → **La interacción humana:** Acción intencional o accidental u omisión que pueden interrumpir la productividad y/ o disponibilidad.
- → **Mal funcionamiento de equipos:** El fallo de sistemas y dispositivos periféricos.
- → **Ataques internos o externos:** Hacking, cracking, and attacking.
- → **El uso incorrecto de datos:** Compartiendo secretos comerciales; espionaje, fraude, y el robo.
- → **La pérdida de datos:** La pérdida intencional o no intencional de la información a través de medios destructivos.
- → **Error de aplicación:** Errores de cómputo, errores de entrada, y desbordamientos de búfer.

Se informará mediante un “check box” si la clase de amenaza es sobre la integridad o la confidencialidad o la disponibilidad. Puede afectar a una a dos o tres de dichos factores.

5.3.4 Gobierno de las clases de vulnerabilidades

Se dispondrá de un inventario de vulnerabilidades que estará relacionado con la amenaza, la cual puede aprovechar dicha debilidad o vulnerabilidad. También las vulnerabilidades irán asociadas a un área de activo con una fecha de alta y una fecha de baja.

Se informará mediante un “check box” si la vulnerabilidad es sobre la integridad o la confidencialidad o la disponibilidad. Puede afectar a una a dos o tres de dichos factores.

5.3.5 Gobierno de las políticas

Políticas externas: Se mantendrán un inventario de las políticas externas informando de si son: leyes internacionales, leyes nacionales, regulaciones, directivas, mejores prácticas de la industria, políticas de la organización, requisitos del sector. Se informará del tipo de obligación que conlleva indicando un valor de 0 a 10 en cuanto a

la obligatoriedad (recomendación, obligación, mejor práctica, etc). Se soportará el rango de validez de las políticas externas, y la política anterior y posterior con la que se relaciona.

Políticas internas: Dentro de esta área se soportará el documento que describe las políticas de seguridad interna párrafo a párrafo. El responsable de la aplicación de la política interna. El rango de fechas de vigencia de la política interna. También se soportará información de las normas, estándares y mejores prácticas externas en los que se basa o apoya la política. Asimismo, se informara de las métricas de seguimiento y control de la política, así como de los procedimientos de trabajo y los controles de seguridad que hay que llevar a cabo para el cumplimiento de la política.

Se definirán en esta fase tres políticas marco que se detallaran a lo largo de la implantación del Gobierno de la Seguridad TI. Estas cuatro políticas son de obligada incorporación en el modelo de Gobierno de los SI:

- → Política de Gobierno de la Seguridad de la Configuración
- → Política de Gobierno de la Continuidad de la Seguridad
- → Política de Gobierno de los Incidentes de Seguridad.
- → Procedimiento de Contingencia.

Aparte de estas políticas de obligada carga en el modelo se darán de alta las que se consideren necesarias.

En el caso de que las políticas se encuentren diferenciadas por unidades de negocio se informarán por unidad de negocio.

Se llevará un ciclo de revisión de políticas internas en que para cada política interna se informa de cuando es revisada, por quien es revisada y resultados de la revisión. También existirá un indicador de obsolescencia (de 0 a 5) de la política interna. Además se informará en el calendario de cambios las tecnologías o arquitecturas vigentes, y a que políticas afectan. Esto es soportado por un registro dentro de las áreas de activos que se llama gestión de la configuración, que informa solo de los grandes cambios que hay por área de activo. Automáticamente se informará de cambios en las políticas externas según se vayan produciendo, ligando las políticas que correspondan a diferentes versiones mediante una relación.

5.3.6 Gobierno de la estructura y roles de seguridad TI

Para cada área de Gobierno de la Seguridad se informará de las personas (nombre y apellidos, número de empleado, dirección, puesto) que tienen asignado cada una de las partes de la matriz RACI: la responsabilidad, al que reportan, informado o consultado. Puede haber más de una persona por cada rol. Por defecto es un único perfil por área de gobierno pero se permitirá diferentes perfiles por la combinación de área de gobierno y área de activo. Por ejemplo, un responsable de los incidentes de seguridad por los aplicativos de negocio, diferente al responsable de los incidentes de seguridad de la infraestructura tecnológica. En el caso de estructura de Gobierno de la Seguridad descentralizada (en el sistema se informará si es centralizada o descentralizada o hibrida cuando es una combinación de centralizada y descentralizada) será necesario abrir por área de activo o agrupación de áreas de activo y por unidad de negocio diferentes responsables de seguridad.

En el fichero de unidades de negocio se informará del número de usuarios totales (suma de los que se abran por áreas de activo) y de la ubicación u ubicaciones físicas. También se informará del presupuesto de seguridad por naturaleza de gasto y por factor de ingreso.

Por cada uno de los roles o roles ubicación se informará del nivel de madurez alcanzado y del numero de capacidades tanto técnicas como funcionales que debe tener dicho rol. Se llevará un inventario de capacidades de seguridad general indicando si son técnicas o funcionales.

5.3.7 Gobierno de las categorías de incidentes de seguridad

Definición de una política de gestión de incidentes, mostrando: forma de inventariarlos, soluciones temporales, forma de priorizarlos, análisis de costes y seguimiento posterior. Se realiza en el área de políticas.

Mantener un histórico catalogado de categorías de incidentes de seguridad (agrupación de incidentes de seguridad) por área de activo. También se informará si afecta a la disponibilidad, a la confidencialidad o a la integridad. Se graba la prioridad del incidente. Si se asigna controles, políticas o nuevos requisitos de seguridad se relacionará el incidente con la solución planteada. En el sistema se agrupan por tipo de

incidente y no se lleva un detalle incidente a incidente al tratarse un diseño de Gobierno de la Seguridad. Se informa del número de incidentes por mes y se lleva un gráfico de información estadística de tendencias. Se relaciona el incidente con el riesgo, la vulnerabilidad y la amenaza que lo provoca.

5.3.8 Gobierno de los niveles de servicio de seguridad

Se lleva para cada área de activo una relación y un registro de las áreas de servicio que lo emplean (en el modelo de gobierno la relación es cercana a 1:1 pero no tiene porque). Por cada área de servicio se informa de los niveles de acuerdo de servicio de seguridad a cubrir tanto de integridad como de disponibilidad y confidencialidad. Esta información es una descripción. Se soporta una descripción, unas bonificaciones y penalizaciones así como las métricas de medición y el plan de mejora continua con sus fechas y responsables. Todo ello agrupada por área de servicio.

5.3.9 Gobierno de los riesgos y riesgos residuales

Se entiende por riesgo como una función de la probabilidad de una fuente de amenaza que puede aprovechar una potencial vulnerabilidad y del resultante impacto del acontecimiento negativo en la organización. El modelo de gobierno propuesto sigue el diseño propuesta en esta definición que parte de las amenazas de las vulnerabilidades y del impacto.

Riesgo= Impacto del Área de Activo x Amenaza Agrupada x Vulnerabilidad Agrupada

Si se tiene un impacto por área de activo (que depende del número de usuarios y el valor del activo), amenazas por área de activo y vulnerabilidades por área de activo se puede calcular el nivel de riesgo por área de activo como se muestra en la tabla continua. Antes de aplicar controles, se tiene un nivel de vulnerabilidad con el que se calcula un riesgo, y después de aplicar controles se tiene una vulnerabilidad con controles y se puede calcular un riesgo residual. El riesgo por activo que aparece en la tabla continua va de 1 a 8.

La lista de riesgos es la misma que la misma lista de amenazas, por ejemplo, un listado de riesgos muy vinculado a amenazas son:

- → **Riesgo por daños físicos:** Incendio, inundación, vandalismo, pérdida de potencia y los desastres naturales.
- → **Riesgo por la interacción humana:** Acción intencional o accidental u omisión que pueden interrumpir la productividad y/ o disponibilidad.
- → **Riesgo por mal funcionamiento de equipos:** El fallo de sistemas y dispositivos periféricos.
- → **Riesgo por ataques internos o externos:** Hacking, cracking, and attacking.
- → **Riesgo por el uso incorrecto de datos:** Compartiendo secretos comerciales; espionaje, fraude, y el robo.
- → **Riesgo por la pérdida de datos:** La pérdida intencional o no intencional de la información a través de medios destructivos.
- → **Riesgo por error de aplicación:** Errores de cómputo, errores de entrada, y desbordamientos de búfer.

Tabla 5. Cálculo del nivel de riesgo a partir del nivel de amenaza, el nivel de vulnerabilidad y el impacto en áreas de activo

NIVEL DE AMENAZA									
IMPACTO	**BAJO**			**MEDIO**			**ALTO**		
	NIVEL DE VULNERABILIDAD								
ÁREA ACTIVO	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

El modelo calcula el impacto tanto del riesgo, como del riesgo residual de la siguiente forma:

Impacto área de activo: Impacto confidencialidad x Impacto integridad x impacto disponibilidad. El impacto en área de activos de nuestro modelo de gobierno TI viene dado por el número de usuarios afectados, la criticidad de estos y el valor del área de activo (si este se encuentra afectado por la amenaza). En principio creo que es bueno tener tres riesgos por área de activo: el riesgo de confidencialidad, el riesgo de integridad y el riesgo de disponibilidad.

EL sistema podrá mantener evaluaciones, o “assessment”, de riesgo. Para cada vez que se haga el assessment se informara en el sistema. Los resultados del assessment también se informarán en el sistema de Gobierno de la Seguridad TI.

Se informará de la opción de mitigación de riesgo: asume, evita, limita, planifica, investiga o transfiere. Según la técnica de mitigación los controles y acciones han de estar acordes.

5.3.10 Gobierno de los Planes y los Controles

Ahora se realiza una lista de controles. Aparte del nombre del sistema, se mantiene la descripción. También el responsable de la correcta ejecución del control y del rango de fechas de vigencia. La clasificación en base a la ISO 27001 es la siguiente:

→ Controles en Política de Seguridad
→ Controles en Organización de Seguridad de la Información
→ Controles en Gestión de Activos
→ Controles en Seguridad de Recursos Humanos
→ Controles en Seguridad Física y Medioambiental
→ Controles en Gestión de comunicaciones y operaciones
→ Controles en Acceso
→ Controles en Sistemas de Información en producción, desarrollo y mantenimiento
→ Controles en Gestión de Incidentes de Seguridad de la Información
→ Controles en Gestión de Continuidad del negocio
→ Controles en Cumplimiento

El sistema mantiene una relación de estos controles con los de: Control Objectives for Information and related Technology (COBIT), ISO 17799, FIPS Publication 200 y NIST 800-53 in the US. El control informa del coste y de cómo disminuye la vulnerabilidad (menor número de usuarios afectados, menor probabilidad o menor valor de la pérdida del activo).

Cuando se quiere mitigar un riesgo en el sistema se proponen una serie de controles. Para llevar a cabo ese control se puede requerir desarrollar una política o llevar a cabo iniciativas (comprar una infraestructura, hacer un programa o cambiar un responsable). Las iniciativas de seguridad se mantienen en el sistema relacionándolas con los controles que las han desencadenado. Las iniciativas se pueden agrupar en programas y proyectos de seguridad. No puede haber acciones que no tengan un control padre que las haya desencadenado. El control no tiene que ser nuevo, pues un control definido hace dos años puede requerir el desarrollo de una mejora en un software que incremente la eficacia del control en la fecha actual. Toda iniciativa o

acción que se quiera desarrollar y que requiera de unos recursos también tiene que estar asociada a un programa.

Ejemplo de tabla de Amenazas y mejores prácticas: En nuestro modelo las mejores prácticas son los controles agrupados de seguridad y que desencadenaran: acciones, definición de políticas, cambios de responsables o de la propia matriz RACI, etc.

Habrá una clase de controles o agrupación de controles que en principio serán: gestión, técnicos y operativos.

Los controles han de estar sometidos a un plan de revisión de mejora continúa. El sistema informara de fechas, responsables, resultados, etc.

5.3.11 Gobierno de las métricas y de la madurez

Existirá un inventario de métricas de seguridad y con la posibilidad de relacionarlas cuando una de las métricas dependa del resultado de otra u estén relacionadas de alguna forma. Las métricas tienen que estar asignada a una línea estratégica y a los requisitos de seguridad. De forma opcional puede estar asignada a un control (para el seguimiento del control) y/o a una acción (para el seguimiento de la ejecución de una acción). Por eso hay métricas de implantación y métricas de consecución de la misión de seguridad.

A partir de la información de las áreas de gobierno mencionadas, el modelo calculará una madurez de la seguridad de la organización que toma estos valores:

MODELO DE MADUREZ: DS5 Garantizar la Seguridad de los Sistemas

0 No Existente cuando: La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

1 Inicial / Ad Hoc cuando: La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

2 Repetible pero Intuitivo cuando Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con

los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

3 Definido cuando Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad TI y existen soluciones de seguridad motivadas por una análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe habilitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

4 Administrado y Medible cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad.

5 Optimizado cuando La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño.

La fórmula de cálculo de la madurez es la siguiente:

Nivel de madurez gobierno TIC= media ponderada por impacto de todos los riesgos residuales por área de activo.

Como los riesgos residuales pueden tomar los valores de cero a ocho y los niveles de seguridad son de 0 a 5, el sistema lo tiene que traducir.

En el modelo de Gobierno de la Seguridad TI que se presenta, se quiere contar con unos niveles de madurez integrados en un modelo de gobierno corporativo (completo) de las TI. Asimismo se considera indispensable que cualquier modelo de madurez se encuentre balanceado siguiendo las perspectivas propuestas por el cuadro de mando integral. Ambas dos visiones son mostradas en la figura continua, en donde en el eje de las X se muestra los dominios de gobierno del modelo (uno de ellos es el Gobierno de la Seguridad TI) y en el eje de las y las perspectivas del cuadro de mando integral. Aparte se ha de considerar la madurez de los procesos (políticas, estándares y procedimientos) y la madurez de las herramientas (aplicaciones y automatización en general).

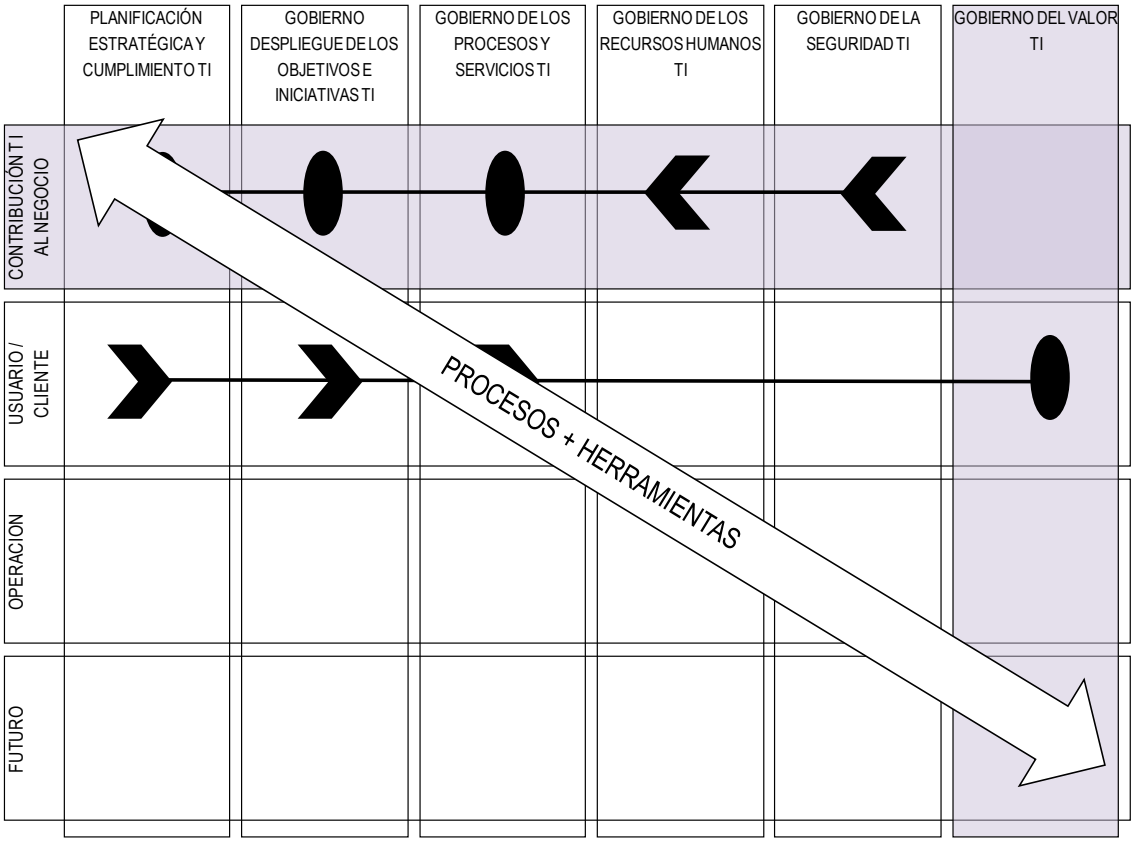


Figura 18. La madurez del gobierno corporativo de las TI como compendio de la madurez de los dominios en los que se divide.

Los dominios de gobierno TI son:

- → **Valoración y formulación del Gobierno TI:** contempla todo el análisis de las necesidades TI hasta llegar a los objetivos estratégicos.
- → **La elaboración, despliegue y control del gobierno TI:** Contempla la comunicación de la estrategia así como el despliegue balanceado de los objetivos estratégicos hasta llegar a acciones agrupadas en proyectos.
- → **El gobierno de los procesos y servicios TI:** Contempla el gobierno de todos los procesos TI (visión interna) así como el gobierno de todos los servicios TI (visión externa).
- → **El gobierno de los RRHH TI:** Los recursos humanos tanto por su criticidad como por afectar a todas las áreas y niveles de los modelos de gobierno TI son incluidos en este dominio.
- → **El Gobierno de la Seguridad TI:** La seguridad tanto por su criticidad como por afectar a todas las áreas y niveles de los modelos de gobierno TI son incluidos en este dominio.

→ **El gobierno del valor TI:** El modelo que se propone cuantifica el valor de todos los objetivos e iniciativas TI de acuerdo al valor, al coste a la flexibilidad y al riesgo. De acuerdo al análisis de riesgos propone una variabilidad para su consecución.

A nivel del Gobierno de la Seguridad se contemplan dos ejes de análisis uno que responde a las categorías de seguridad y otro a las partes de las que se descompone el gobierno de las TI. Dentro del primero de las categorías de la seguridad: gestión de activos, seguridad de los RRHH, seguridad física y del entorno, seguridad del equipamiento, seguridad de la adquisición y del desarrollo, seguridad de la operación (control de acceso y gestión de incidentes en la seguridad de la información) y gestión de la continuidad. En cuanto a las categorías de gobierno se definen estas cuatro:

→ Procesos, criterios y guías de gobierno
→ Estructuras y responsabilidades
→ Relaciones
→ Objetivos, niveles de servicio y métricas
→ Cumplimiento de normas y estándares

Se propone que la combinación de las categorías de seguridad con las categorías de gobierno de una buena visión del Gobierno de la Seguridad TI en la organización.

	PROCESOS, CRITERIOS Y GUÍAS DE GOBIERNO	**ESTRUCTURAS Y RESPONSABILIDADES**	**RELACIONES**	**OBJETIVOS, NIVELES DE SERVICIO Y MÉTRICAS**	**CUMPLIMIENTO DE NORMAS Y ESTÁNDARES**	**TOTAL**
GESTIÓNDE ACTIVOS	1->5	1->5	1->5	1->5	1->5	1->5
SEGURIDAD DE LOS RRHH	1->5	1->5	1->5	1->5	1->5	1->5
SEGURIDAD FÍSICA Y DEL ENTORNO	1->5	1->5	1->5	1->5	1->5	1->5
SEGURIDAD DEL EQUIPAMIENTO	1->5	1->5	1->5	1->5	1->5	1->5
SEGURIDAD DE LA ADQUISICIÓN Y DEL	1->5	1->5	1->5	1->5	1->5	1->5

DESARROLLO						
SEGURIDAD DE LA OPERACIÓN	1->5	1->5	1->5	1->5	1->5	1->5
GESTIÓNDE LA CONTINUIDAD	1->5	1->5	1->5	1->5	1->5	1->5
TOTAL	1->5	1->5	1->5	1->5	1->5	1->5

Figura 19. La madurez del Gobierno de la Seguridad TI como compendio de las áreas de activos de las que se compone

5.3.12 Gobierno de la Mejora Continua Seguridad TI

Este área es el compendio de las diferentes áreas donde impacta la mejora continua: como se encuentra la mejora continua de los controles, la mejora continúa de las políticas de seguridad y un análisis de tendencias de cómo evolucionan los riesgos residuales por áreas de activos y cómo evolucionan los incidentes por seguridad (tendencias). El nivel de incidentes es una medida de la efectividad de las políticas y controles de seguridad.

5.3.13 Gobierno Económico de la seguridad TI

En el modelo de Gobierno de la Seguridad TI las variables de salida son el aumento o disminución del coste de la no seguridad, el coste de los controles, el plazo de aplicar los controles, el valor por la seguridad y el nivel de riesgo. El coste tiene dos partidas, el coste de los controles a implantar y el coste de la no seguridad. Dentro de estos últimos están las desviaciones provocadas por desconocimientos que requerirá de mayores plazos y mayores costes. El plazo que afecta a la hora de calcular los ingresos pues los sistemas estarán operativos mas tarde y por lo tanto los ingresos dependen de cuando los sistemas de negocio entran en operación. El valor vendrá dado por los marcadores de valor de cada punto función de controles que entra en operación. Cada control afectara a unos marcadores de valor y cada marcador de valor mediante una fórmula matemática calculará el valor en euros.

5.3.14 Calendario de implantación

Como se adelantaba en la introducción el modelo de Gobierno de la Seguridad TI, tiene un enfoque estratégico y de cambio. Por todo ello, encaja proponer un calendario para su implantación basado en una filosofía de reingeniería de procesos que es muy aplicable a los procesos de seguridad. Hammer y Champy definen a la reingeniería de procesos como "la reconcepción fundamental y el rediseño radical de los procesos de negocios para lograr mejoras dramáticas en medidas de desempeño tales como en costos, calidad, servicio y rapidez". Un posible cronograma para la primera implantación sería:

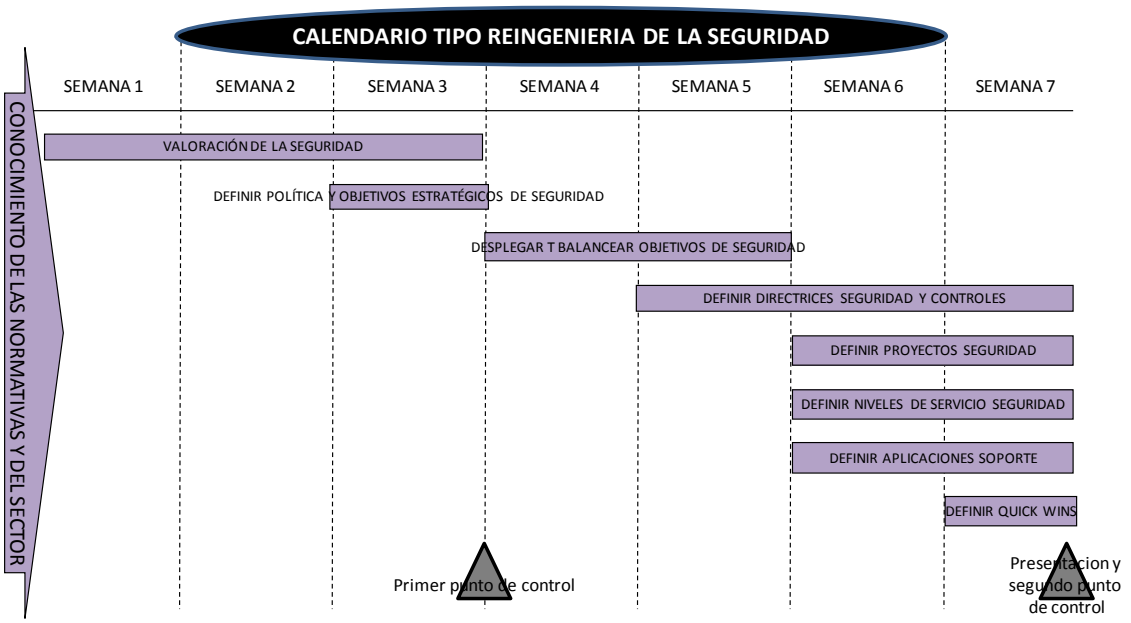


Figura 20. Calendario tipo de implantación Gobierno Seguridad TI

5.4 Roles de un Sistema de Gobierno de Seguridad de la información

Los principales Roles que accederán y gestionaran la aplicación de un SGSI son:

- → CEO (Chief Executive Officer o Director Gerente)
- → CFO
- → Ejecutivo del negocio
- → CIO (Chief Information Officer o Gerente de Sistemas)
- → Dueño Proceso negocio

- → Dueño Proceso TI.
  - Jefe Operaciones
  - Arquitecto Jefe.
  - Jefe Desarrollo
  - Jefe Administration TI
  - PMO (Project Management Office)
- → Cumplimiento, Auditoria, Riesgo y Seguridad
- → CSO (Chief Security Officer)

Estos roles desempeñan funciones y tienen diferentes permisos dentro de la aplicación:

- → CEO (Chief Executive Officer o Director Gerente): es la persona que tiene a su cargo la máxima autoridad de la gestión y dirección administrativa en una empresa, organismo, asociación o institución.
- → CFO (Chief Financial Officer o Director de Finanzas): es el ejecutivo a cargo del manejo de las finanzas de la organización. Es responsable de la planeación, el registro y los informes financieros
- → Ejecutivo del negocio.
- → CIO /CTO (Chief Information Officer/ Chief Information Technology o Director de Sistemas Informáticos/Director de la Tecnología de la Información): es la persona responsable de la tecnología de la información y sus sistemas informáticos.
- → Dueño Proceso negocio.
- → Dueño Proceso TI.
  - Jefe Operaciones
  - Arquitecto Jefe.
  - Jefe Desarrollo
  - Jefe Administracion TI
  - PMO (Project Management Office o Gestor de Proyectos): es la persona que define y mantiene los estándares de procesos, generalmente relacionados con la gestión de proyectos.
- → Cumplimiento, Auditoria, Riesgo y Seguridad.
- → CSO (Chief Security Officer o Director de la Seguridad): es la persona responsable del desarrollo, implementación y gestión de toda la seguridad de la organización, tanto física como digital.

5.5 Matriz RACI

En la siguiente matriz se muestran las responsabilidades de los roles de cada entidad del sistema.

Las responsabilidades principales son las siguientes:

- → R (Responsable)
- → A (Aprobador)
- → C (Consultado)
- → I (Informado)

Tabla 6. Matriz RACI

	CEO	Ejecutivo del Negocio	CIO	Dueño Procesos Negocio	Dueño Procesos TI	Cumplimiento, Auditoria, Riesgo y	CSO
Gestionar la operación del SGGS			A			R	
Consultar Usuarios (R. usuario y Auditoria)	C		C	C		C	
Gestionar Riegos	A		A	R	R		
Consultar Riesgos	C	C	C	C	C	C	C
Gestionar Activos			A	R	R		
Consultar Activos	C		C	C	C	C	C
Gestionar Acuerdos de Negocio			A	R	R		R
Consultar Acuerdos Negocio	C	C	C	C	C	C	
Gestionar Incidentes			A		R	R	
Consultar Incidencias	C	C	C	C	C	C	
Gestionar Amenazas			A			R	
Consultar Amenazas	C		C	C	C	C	

Gestionar Vulnerabilidades			A			R	
Consultar Vulnerabilidades	C		C	C	C	C	
Gestionar Requisitos		A	A	R	R		
Consultar Requisitos	C	C	C	C	C	C	C
Gestionar Controles		A	A	R	R		
Consultar Controles	C	C	C	C	C	C	
Gestionar Planes de Seguridad y Continuidad		A	A	R	R		
Consultar Planes continuidad	C	C	C	C	C	C	
Gestionar Politica de Seguridad de la Informacion			A			R	
Consultar Politica de Seguridad de la Informacion	C	C	C	C	C	C	
Gestionar Normativa Externa			A			R	
Consultar Normativa Externa	C	C	C	C	C	C	
Gestionar Líneas Estratégicas de Seguridad de la Información	A		R	R			
Consultar Líneas Estratégicas de Seguridad de la Información	C	C	C	C	C	C	
Gestionar Auditoria	A		R	R		R	

5.6 Casos de uso

5.6.1 CEO

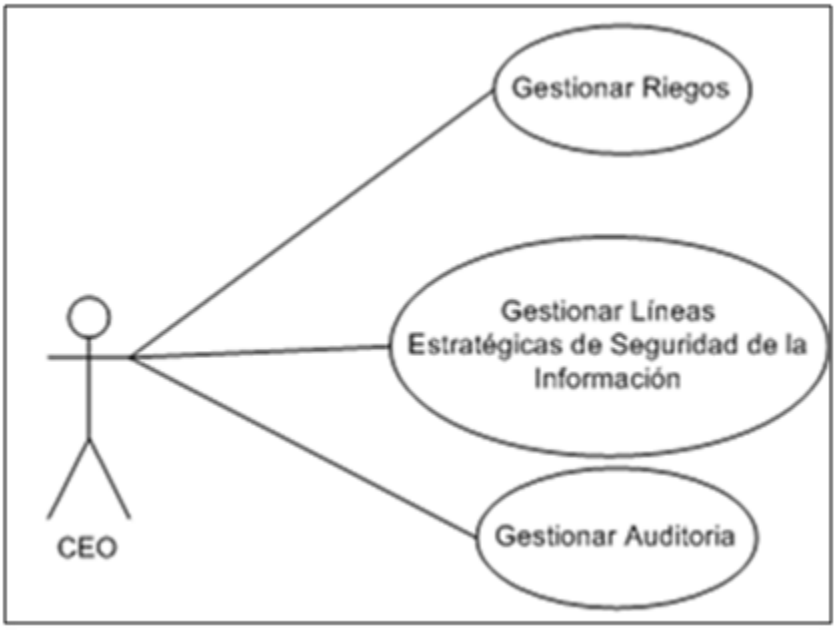


Figura 21. Casos de Uso CEO

Tabla 7. Casos de Uso. CEO Gestionar Riesgos

Nombre:	**Gestionar Riesgos**
Actores:	CEO
Objetivo:	Gestionar Riesgos. Se crean, modifican y eliminan los Riesgos.
Escenario básico:	1. Pulsar link “Gestión de Riesgos”

Tabla 8. Casos de Uso. CEO Gestionar Líneas Estratégicas de Seguridad de la Información

Nombre:	**Gestionar Líneas Estratégicas de Seguridad de la Información**

Actores:	CEO
Objetivo:	Gestionar Líneas Estratégicas. Se crean, modifican y eliminan las Líneas Estratégicas.
Escenario básico:	1. Pulsar link “Gestión de Líneas Estratégicas de Seguridad”

Tabla 9. Casos de Uso. CEO Gestionar Auditoria

Nombre:	**Gestionar Auditoria**
Actores:	CEO
Objetivo:	Gestionar Auditorias. Se crean, modifican y Eliminan las diversas Auditorias.
Escenario básico:	1. Pulsar link “Gestión de Auditorias”

5.6.2 Ejecutivo del negocio

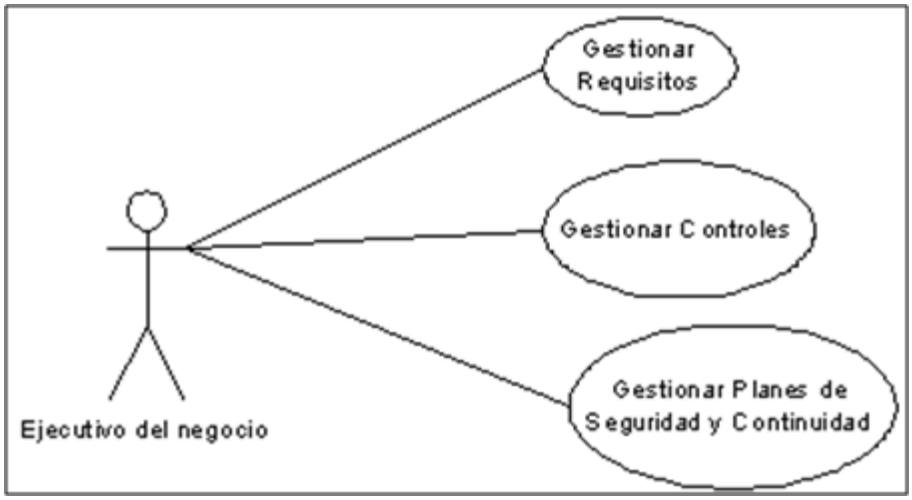


Figura 22. Casos de Uso Ejecutivo del negocio

Tabla 10. Casos de Uso. Ejecutivo del negocio Gestionar Requisitos

Nombre:	**Gestionar Requisitos**
Actores:	Ejecutivo del negocio
Objetivo:	Gestionar Requisitos. Se crean, modifican y eliminan los Requisitos.
Escenario básico:	1. Pulsar link “Gestión de Requisitos”

Tabla 11. Casos de Uso. Ejecutivo del negocio Gestionar Controles

Nombre:	**Gestionar Controles**
Actores:	Ejecutivo del negocio
Objetivo:	Gestionar Controles. Se crean, modifican y eliminan los Controles.
Escenario básico:	1. Pulsar link “Gestión de Controles”

Tabla 12. Casos de Uso. Ejecutivo del negocio Gestionar Planes de Seguridad y Continuidad

Nombre:	**Gestionar Planes de Seguridad y Continuidad**
Actores:	Ejecutivo del negocio
Objetivo:	Gestionar Planes. Se crean, modifican y eliminan los Planes de Continuidad y Seguridad.
Escenario básico:	1. Pulsar link “Gestión de Plan de Continuidad”

5.6.3 CIO

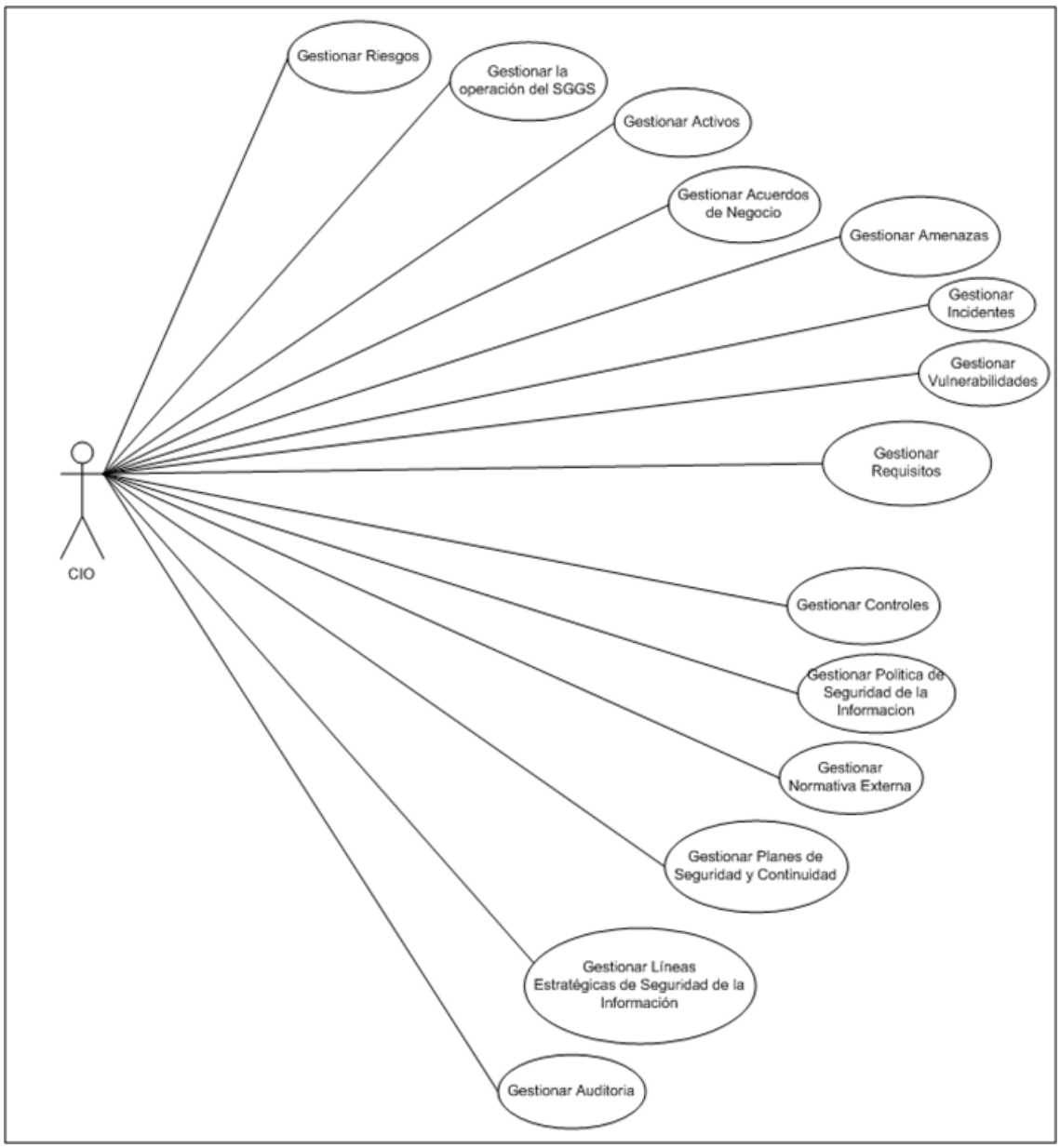


Figura 23. Casos de Uso CIO

Tabla 13. Casos de Uso. CIO Gestionar la operación del SGGS

Nombre:	**Gestionar la operación del SGGS**
Actores:	CIO
Objetivo:	Gestionar la operación del SGGS. Se crean,

	modifican y eliminan las operaciones del SGGS.
Escenario básico:	1. Pulsar link “Gestión de la operación del SGGS”

Tabla 14. Casos de Uso. CIO Gestionar Riesgos

Nombre:	**Gestionar Riesgos**
Actores:	CIO
Objetivo:	Gestionar Riesgos. Se crean, modifican y eliminan los Riesgos.
Escenario básico:	1. Pulsar link “Gestión de Riesgos”

Tabla 15. Casos de Uso. CIO Gestionar Activos

Nombre:	**Gestionar Activos**
Actores:	CIO
Objetivo:	Gestionar Activos. Se crean, modifican y eliminan los Activos.
Escenario básico:	1. Pulsar link “Gestión de Activos”

Tabla 16. Casos de Uso. CIO Gestionar Acuerdos de Negocio

Nombre:	**Gestionar Acuerdos de Negocio**
Actores:	CIO
Objetivo:	Gestionar Acuerdos de Negocio. Se crean, modifican y eliminan los Acuerdos de Negocio.
Escenario básico:	1. Pulsar link “Gestión de Acuerdos de Negocio”

Tabla 17. Casos de Uso. CIO Gestionar Incidentes

Nombre:	**Gestionar Incidentes**
Actores:	CIO
Objetivo:	Gestionar Incidentes. Se modifican y eliminan los Incidentes.
Escenario básico:	1. Pulsar link “Gestión de Incidentes”

Tabla 18. Casos de Uso. CIO Gestionar Amenazas

Nombre:	**Gestionar Amenazas**
Actores:	CIO
Objetivo:	Gestionar Amenazas. Se crean, modifican y eliminan las Amenazas.
Escenario básico:	1. Pulsar link “Gestión de Amenazas”

Tabla 19. Casos de Uso. CIO Gestionar Vulnerabilidades

Nombre:	**Gestionar Vulnerabilidades**
Actores:	CIO
Objetivo:	Gestionar Vulnerabilidades. Se crean, modifican y eliminan las Vulnerabilidades.
Escenario básico:	1. Pulsar link “Gestión de Vulnerabilidades”

Tabla 20. Casos de Uso. CIO Gestionar Requisitos

Nombre:	**Gestionar Requisitos**
Actores:	CIO

Objetivo:	Gestionar Requisitos. Se crean, modifican y eliminan los Requisitos.
Escenario básico:	1. Pulsar link “Gestión de Requisitos”

Tabla 21. Casos de Uso. CIO Gestionar Controles

Nombre:	**Gestionar Controles**
Actores:	CIO
Objetivo:	Gestionar Controles. Se crean, modifican y eliminan los Controles.
Escenario básico:	1. Pulsar link “Gestión de Controles”

Tabla 22. Casos de Uso. CIO Gestionar Planes de Seguridad y Continuidad

Nombre:	**Gestionar Planes de Seguridad y Continuidad**
Actores:	CIO
Objetivo:	Gestionar Planes. Se crean, modifican y eliminan los Planes de Continuidad y Seguridad.
Escenario básico:	1. Pulsar link “Gestión de Plan de Continuidad”

Tabla 23. Casos de Uso. CIO Gestionar Política de Seguridad de la Información

Nombre:	**Gestionar Política de Seguridad de la Información**
Actores:	CIO
Objetivo:	Gestionar Políticas. Se crean, modifican y eliminan las Políticas.

Escenario básico:	1. Pulsar link “Gestión de Políticas”

Tabla 24. Casos de Uso. CIO Gestionar la Normativa Externa

Nombre:	**Gestionar la Normativa Externa**
Actores:	CIO
Objetivo:	Gestionar la Normativa Externa. Se crean, modifican y eliminan la Normativa Externa.
Escenario básico:	1. Pulsar link “Gestión de Normativa Externa”

Tabla 25. Casos de Uso. CIO Gestionar Líneas Estratégicas de Seguridad de la Información

Nombre:	**Gestionar Líneas Estratégicas de Seguridad de la Información**
Actores:	CIO
Objetivo:	Gestionar Líneas Estratégicas. Se crean, modifican y eliminan las Líneas Estratégicas.
Escenario básico:	1. Pulsar link “Gestión de Líneas Estratégicas de Seguridad”

Tabla 26. Casos de Uso. CIO Gestionar Auditoria

Nombre:	**Gestionar Auditoria**
Actores:	CIO
Objetivo:	Gestionar Auditorias. Se crean, modifican y Eliminan las diversas Auditorias.

Escenario básico:	1. Pulsar link “Gestión de Auditorias”

5.6.4 Dueño del Proceso de Negocio

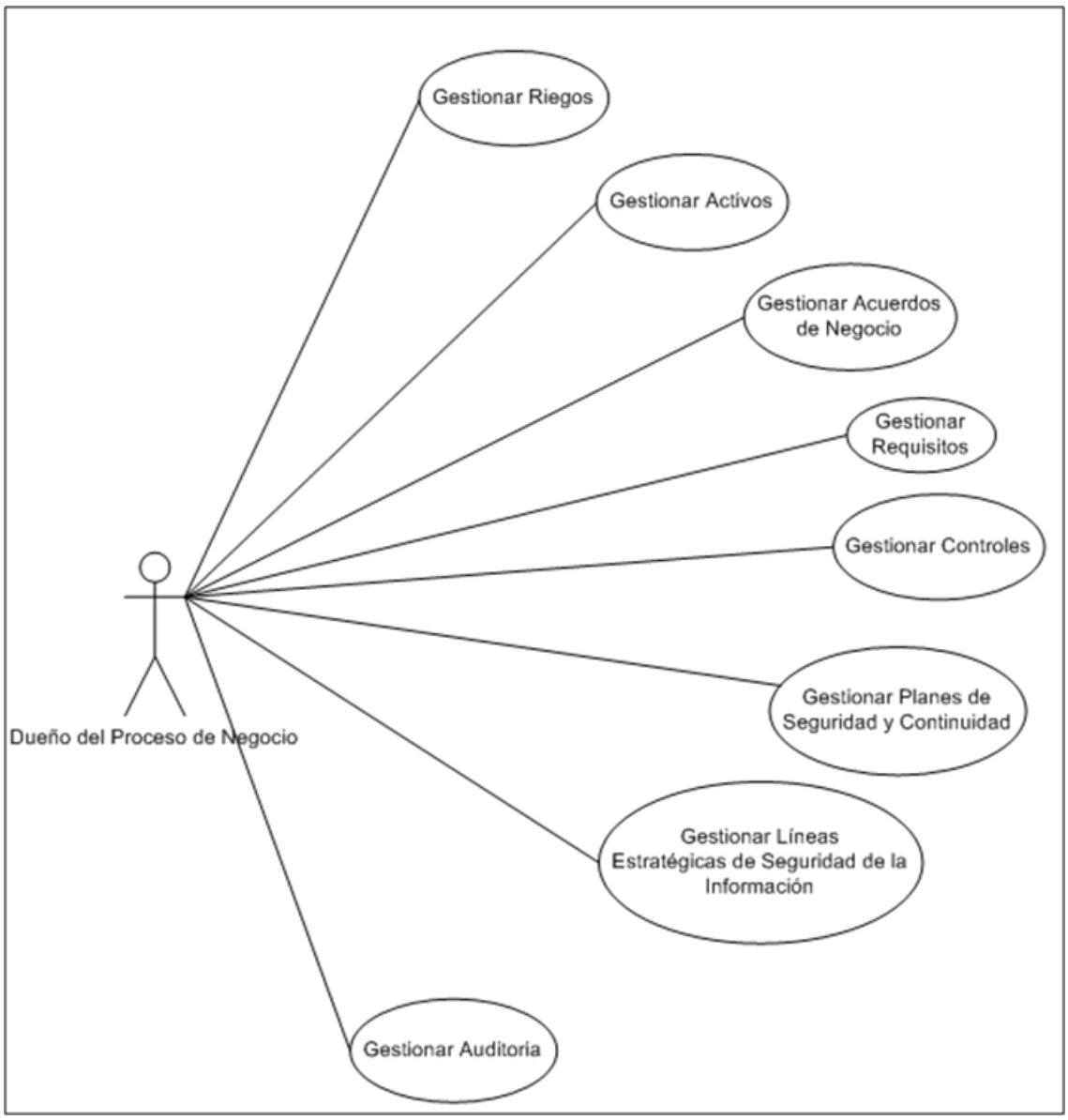


Figura 24. Casos de Uso Dueño del Proceso de Negocio

Tabla 27. Casos de Uso. Dueño del Proceso de Negocio Gestionar Riesgos

Nombre:	**Gestionar Riesgos**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Riesgos. Se crean, modifican y eliminan los Riesgos.

Escenario básico:	1. Pulsar link “Gestión de Riesgos”

Tabla 28. Casos de Uso. Dueño del Proceso de Negocio Gestionar Activos

Nombre:	**Gestionar Activos**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Activos. Se crean, modifican y eliminan los Activos.
Escenario básico:	1. Pulsar link “Gestión de Activos”

Tabla 29. Casos de Uso. Dueño del Proceso de Negocio Gestionar Acuerdos de Negocio

Nombre:	**Gestionar Acuerdos de Negocio**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Acuerdos de Negocio. Se crean, modifican y eliminan los Acuerdos de Negocio.
Escenario básico:	1. Pulsar link “Gestión de Acuerdos de Negocio”

Tabla 30. Casos de Uso. Dueño del Proceso de Negocio Gestionar Requisitos

Nombre:	**Gestionar Requisitos**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Requisitos. Se crean, modifican y eliminan los Requisitos.
Escenario básico:	1. Pulsar link “Gestión de Requisitos”

Tabla 31. Casos de Uso. Dueño del Proceso de Negocio Gestionar Controles

Nombre:	**Gestionar Controles**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Controles. Se crean, modifican y eliminan los Controles.
Escenario básico:	1. Pulsar link "Gestión de Controles"

Tabla 32. Casos de Uso. Dueño del Proceso de Negocio Gestionar Planes de Seguridad y Continuidad

Nombre:	**Gestionar Planes de Seguridad y Continuidad**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Planes. Se crean, modifican y eliminan los Planes de Continuidad y Seguridad.
Escenario básico:	1. Pulsar link "Gestión de Plan de Continuidad"

Tabla 33. Casos de Uso. Dueño del Proceso de Negocio Gestionar Líneas Estratégicas de Seguridad de la Información

Nombre:	**Gestionar Líneas Estratégicas de Seguridad de la Información**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Líneas Estratégicas. Se crean, modifican y eliminan las Líneas Estratégicas.
Escenario básico:	1. Pulsar link "Gestión de Líneas Estratégicas de Seguridad"

Tabla 34. Casos de Uso. Dueño del Proceso de Negocio Gestionar Auditoria

Nombre:	**Gestionar Auditoria**
Actores:	Dueño del Proceso de Negocio
Objetivo:	Gestionar Auditorias. Se crean, modifican y Eliminan las diversas Auditorias.
Escenario básico:	1. Pulsar link “Gestión de Auditorias”

5.6.5 Dueño de Proceso TI

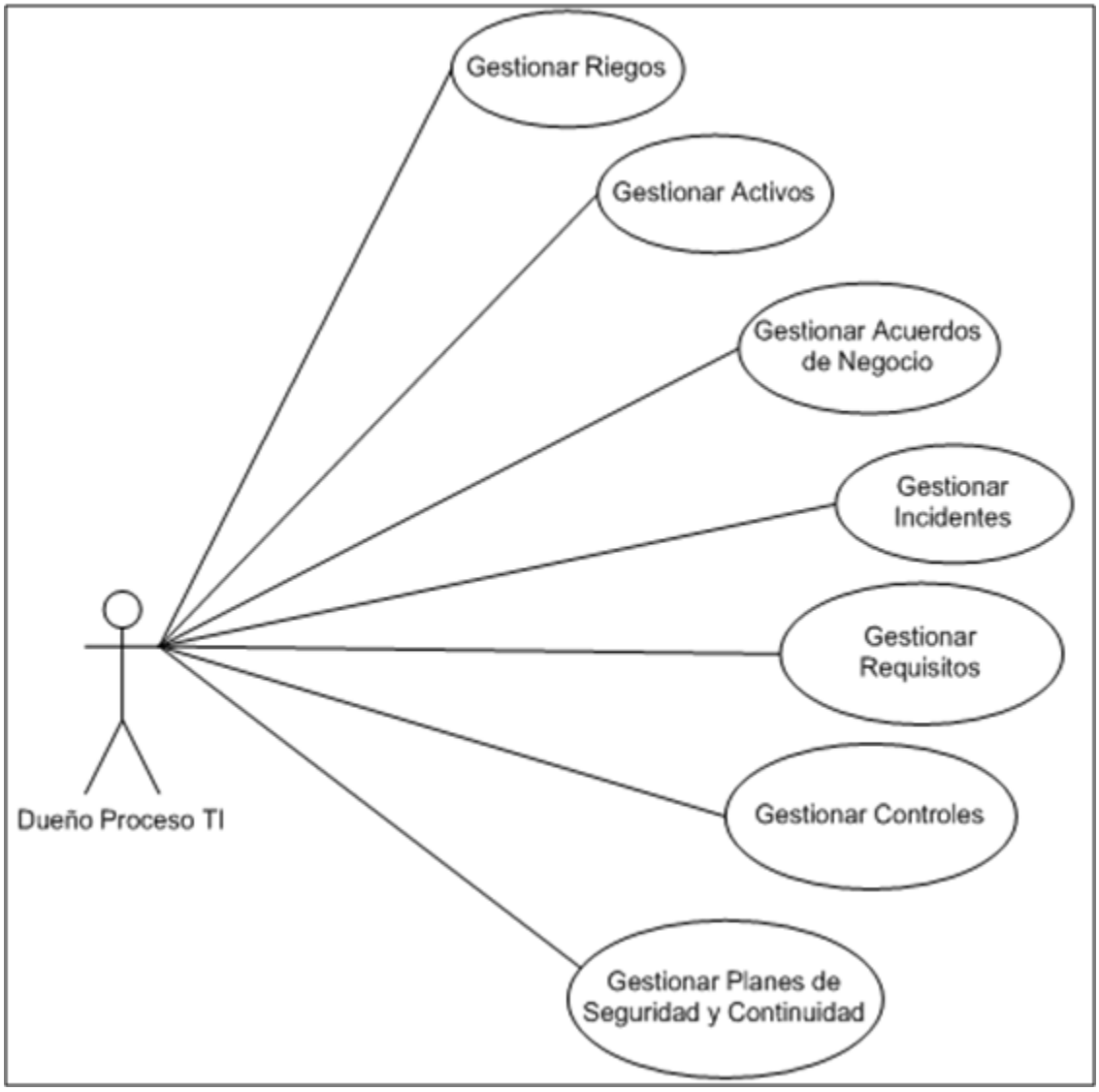


Figura 25. Casos de Uso Dueño Proceso TI

Tabla 35. Casos de Uso. Dueño del Proceso TI Gestionar Riesgos

Nombre:	**Gestionar Riesgos**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Riesgos. Se crean, modifican y eliminan los Riesgos.

Escenario básico:	1. Pulsar link “Gestión de Riesgos”

Tabla 36. Casos de Uso. Dueño del Proceso TI Gestionar Activos

Nombre:	**Gestionar Activos**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Activos. Se crean, modifican y eliminan los Activos.
Escenario básico:	1. Pulsar link “Gestión de Activos”

Tabla 37. Casos de Uso. Dueño del Proceso TI Gestionar Acuerdos de Negocio

Nombre:	**Gestionar Acuerdos de Negocio**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Acuerdos de Negocio. Se crean, modifican y eliminan los Acuerdos de Negocio.
Escenario básico:	1. Pulsar link “Gestión de Acuerdos de Negocio”

Tabla 38. Casos de Uso. Dueño del Proceso TI Gestionar Incidencias

Nombre:	**Gestionar Incidentes**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Incidentes. Se modifican y eliminan los Incidentes.
Escenario básico:	1. Pulsar link “Gestión de Incidentes”

Tabla 39. Casos de Uso. Dueño del Proceso TI Gestionar Requisitos

Nombre:	**Gestionar Requisitos**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Requisitos. Se crean, modifican y eliminan los Requisitos.
Escenario básico:	1. Pulsar link “Gestión de Requisitos”

Tabla 40. Casos de Uso. Dueño del Proceso TI Gestionar Controles

Nombre:	**Gestionar Controles**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Controles. Se crean, modifican y eliminan los Controles.
Escenario básico:	1. Pulsar link “Gestión de Controles”

Tabla 41. Casos de Uso. Dueño del Proceso TI Gestionar Planes de Seguridad y Continuidad

Nombre:	**Gestionar Planes de Seguridad y Continuidad**
Actores:	Dueño del Proceso TI
Objetivo:	Gestionar Planes. Se crean, modifican y eliminan los Planes de Continuidad y Seguridad.
Escenario básico:	1. Pulsar link “Gestión de Plan de Continuidad”

5.6.6 Cumplimiento, Auditoria, Riesgo y Seguridad

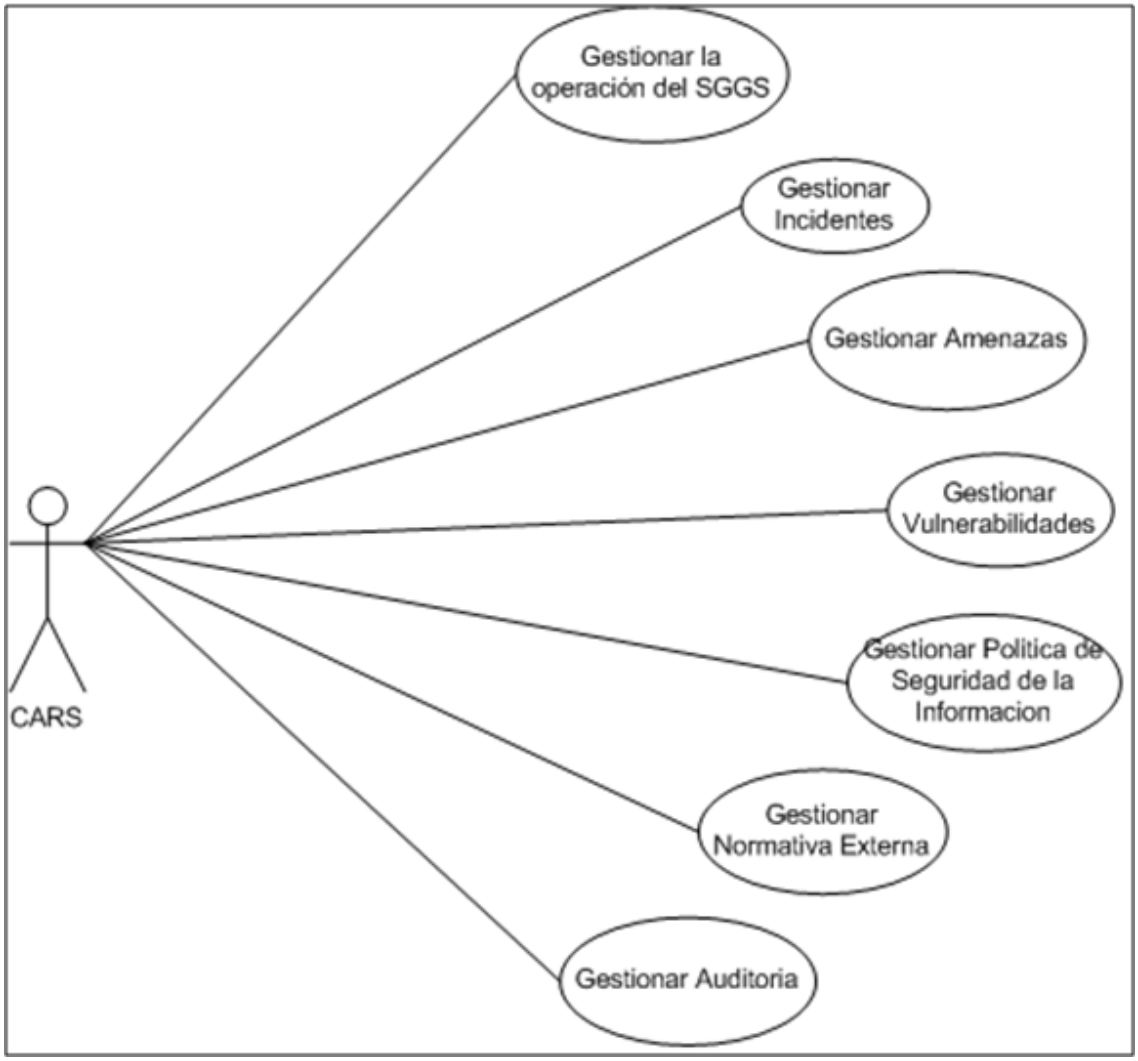


Figura 26. Casos de Uso Cumplimiento, Auditoria, Riesgo y Seguridad

Tabla 42. Casos de Uso. CARS Gestionar la operación del SGGS

Nombre:	**Gestionar la operación del SGGS**
Actores:	CARS
Objetivo:	Gestionar la operación del SGGS. Se crean, modifican y eliminan las operaciones del SGGS.

Escenario básico:	1. Pulsar link “Gestión de la operación del SGGS”

Tabla 43. Casos de Uso. CARS Gestionar Incidentes

Nombre:	**Gestionar Incidentes**
Actores:	CARS
Objetivo:	Gestionar Incidentes. Se modifican y eliminan los Incidentes.
Escenario básico:	1. Pulsar link “Gestión de Incidentes”

Tabla 44. Casos de Uso. CARS Gestionar Amenazas

Nombre:	**Gestionar Amenazas**
Actores:	CARS
Objetivo:	Gestionar Amenazas. Se crean, modifican y eliminan las Amenazas.
Escenario básico:	1. Pulsar link “Gestión de Amenazas”

Tabla 45. Casos de Uso. CARS Gestionar Vulnerabilidades

Nombre:	**Gestionar Vulnerabilidades**
Actores:	CARS
Objetivo:	Gestionar Vulnerabilidades. Se crean, modifican y eliminan las Vulnerabilidades.
Escenario básico:	1. Pulsar link “Gestión de Vulnerabilidades”

Tabla 46. Casos de Uso. CARS Gestionar Política de Seguridad de la Información

Nombre:	**Gestionar Política de Seguridad de la Información**
Actores:	CARS
Objetivo:	Gestionar Políticas. Se crean, modifican y eliminan las Políticas.
Escenario básico:	1. Pulsar link “Gestión de Políticas”

Tabla 47. Casos de Uso. CARS Gestionar la Normativa Externa

Nombre:	**Gestionar la Normativa Externa**
Actores:	CARS
Objetivo:	Gestionar la Normativa Externa. Se crean, modifican y eliminan la Normativa Externa.
Escenario básico:	1. Pulsar link “Gestión de Normativa Externa”

Tabla 48. Casos de Uso. CARS Gestionar Auditoria

Nombre:	**Gestionar Auditoria**
Actores:	CARS
Objetivo:	Gestionar Auditorias. Se crean, modifican y Eliminan las diversas Auditorias.
Escenario básico:	1. Pulsar link “Gestión de Auditorias”

5.6.7 CSO

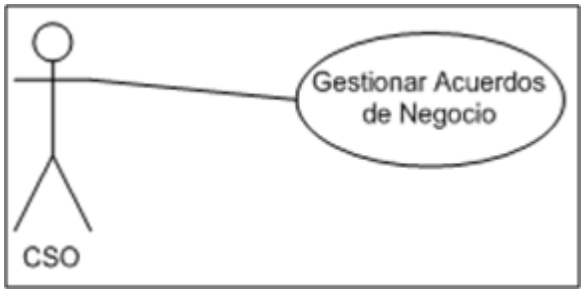


Figura 27. Casos de Uso CSO

Tabla 49. Casos de Uso. CSO Gestionar Acuerdos de Negocio

Nombre:	**Gestionar Acuerdos de Negocio**
Actores:	CSO
Objetivo:	Gestionar Acuerdos de Negocio. Se crean, modifican y eliminan los Acuerdos de Negocio.
Escenario básico:	1. Pulsar link “Gestión de Acuerdos de Negocio”

5.6.8 Gestión de Usuarios

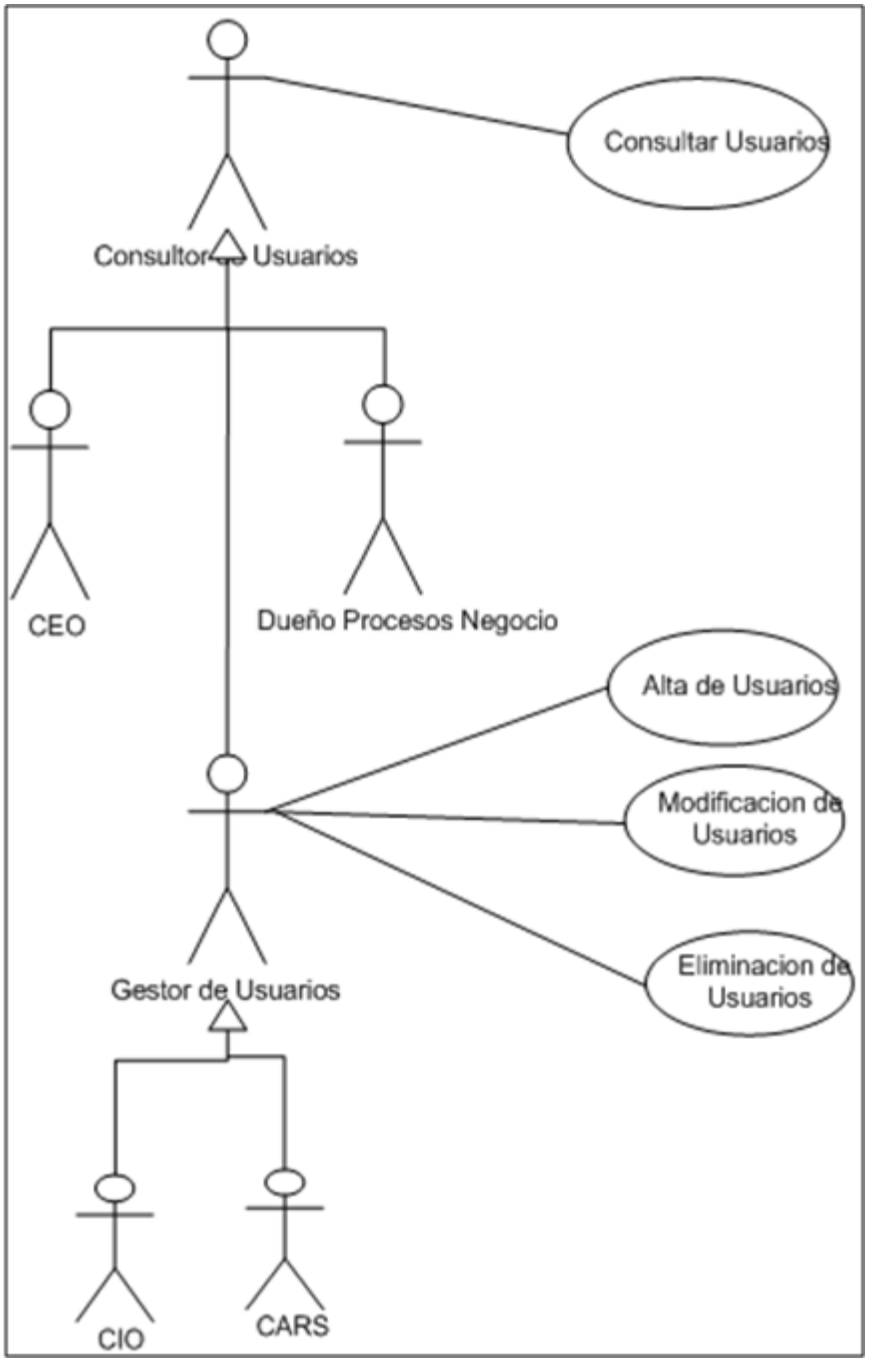


Figura 28. Casos de Uso de Gestión de Usuarios

Tabla 50. Casos de Uso. Alta de Usuario

Nombre:	**Alta de Usuario**

Actores:	CIO y CARS
Objetivo:	Dar de alta a un Usuario de la aplicación
Escenario básico:	1. Pulsar el botón “Usuarios”. 2. Pulsar el botón “Crear Nuevo Usuario”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Usuario. 4. La operación finalizará con el mensaje de éxito o error del alta del Usuario.

Tabla 51. Casos de Uso. Modificar Usuario

Nombre:	**Modificar Usuario**
Actores:	CIO y CARS
Objetivo:	Modificar los datos de un Usuario de la aplicación
Escenario básico:	1. Pulsar el botón “Usuarios”. 2. Escribir el nombre del Usuario que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Usuarios en el botón “Listar Usuarios”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Usuario. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Usuario modificado.

	4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Usuario.

Tabla 52. Casos de Uso. Eliminar Usuario

Nombre:	**Eliminar Usuario**
Actores:	CIO y CARS
Objetivo:	Eliminar uno de los Usuarios de la aplicación
Escenario básico:	1. Pulsar el botón “Usuarios”. 2. Escribir el nombre del Usuario que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Usuarios en el botón “Listar Usuarios”. 3. Pulsar el botón “Eliminar” del Usuario que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Usuario. 4.1 Pulsar “Aceptar”, se eliminará el usuario seleccionado. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 53. Casos de Uso. Consultar Usuario

Nombre:	**Consultar Usuario**
Actores:	CIO, CARS, CEO y Dueño Procesos Negocio
Objetivo:	Consultar detalle de uno de los Usuarios de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Usuarios”.

	3. Escribir el nombre del Usuario que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Usuarios en el botón “Listar Usuarios”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.9 Gestión de Riesgos

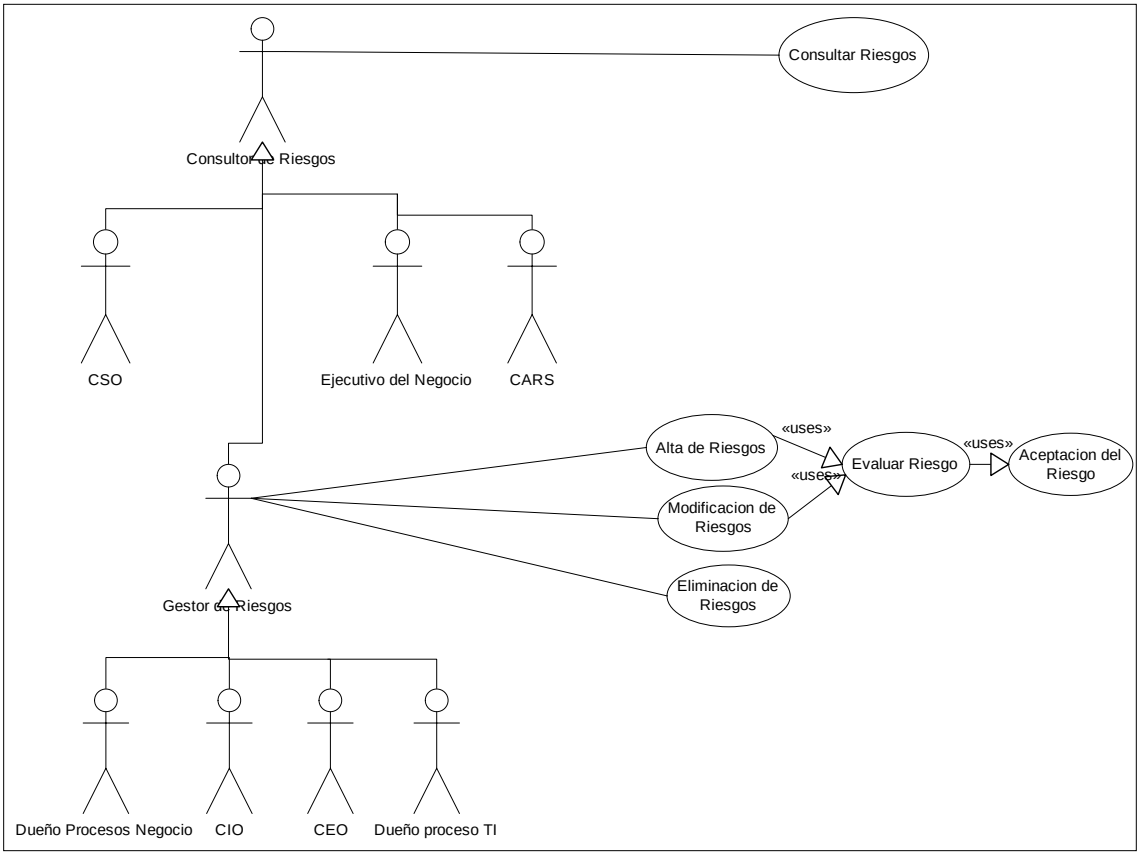


Figura 29. Casos de Uso de Gestión de Riesgos

Tabla 54. Casos de Uso. Alta de Riesgo

Nombre:	**Alta de Riesgo**
Actores:	Dueño Procesos Negocio, CIO, CEO y Dueño Procesos TI
Objetivo:	Dar de alta un Riesgo en la aplicación
Escenario básico:	1. Pulsar el botón “Riesgos”. 2. Pulsar el botón “Crear Nuevo Riesgo”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y

	volver al punto 2. 3.2 Pulsar "Guardar", se guardarán todos los datos del Riesgo. 4. La operación finalizará con el mensaje de éxito o error del alta del Riesgo.

Tabla 55. Casos de Uso. Modificar Riesgo

Nombre:	**Modificar Riesgo**
Actores:	Dueño Procesos Negocio, CIO, CEO y Dueño Procesos TI
Objetivo:	Modificar los datos de un Riesgo de la aplicación
Escenario básico:	1. Pulsar el botón "Riesgos". 2. Escribir el nombre del Riesgo que se desea modificar en el recuadro "Buscar por:" o bien hacer un listado de todos los Riesgos en el botón "Listar Riesgos". 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar "Cancelar" para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Riesgo. 3.2 Pulsar "Guardar", se guardarán todos los datos del Riesgo modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Riesgo.

Tabla 56. Casos de Uso. Eliminar Riesgo

Nombre:	**Eliminar Riesgo**
Actores:	Dueño Procesos Negocio, CIO, CEO y Dueño

	Procesos TI
Objetivo:	Eliminar uno de los Riesgos de la aplicación
Escenario básico:	1. Pulsar el botón “Riesgos”. 2. Escribir el nombre del Riesgo que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Riesgos en el botón “Listar Riesgos”. 3. Pulsar el botón “Eliminar” del Riesgo que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Riesgo. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 57. Casos de Uso. Evaluar Riesgo

Nombre:	**Evaluar Riesgo**
Actores:	Dueño Procesos Negocio, CIO, CEO y Dueño Procesos TI
Objetivo:	Evaluar uno de los Riesgos de la aplicación
Escenario básico:	1. Pulsar el botón “Evaluar Riesgo”. 2 Asignara un indicador en función de la probabilidad e impacto que supone dicho Riesgo.

Tabla 58. Casos de Uso. Aceptación del Riesgo

Nombre:	**Aceptación del Riesgo**
Actores:	Dueño Procesos Negocio, CIO, CEO y Dueño

	Procesos TI
Objetivo:	Realizar la Aceptación de uno de los Riesgos de la aplicación
Escenario básico:	1. Pulsar el botón “Aceptación del Riesgo”. 2. Rellenar del formulario los datos que se solicitar y pulsar los siguientes botones: 2.1 Pulsar “Cancelar” para abandonar el detalle de la Aceptación del Riesgo y volver al punto 1 sin que se guarden los cambios hechos. 2.2 Pulsar “Guardar”, se guardarán todos los datos.

Tabla 59. Casos de Uso. Consultar Riesgo

Nombre:	**Consultar Riesgos**
Actores:	Dueño Procesos Negocio, CIO, CEO, Dueño Procesos TI, CSO, Ejecutivo del Negocio y CARS
Objetivo:	Consultar detalle de uno de los Riesgos de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Riesgos”. 3. Escribir el Riesgo que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Riesgos en el botón “Listar Riesgos”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.10 Gestión de Activos

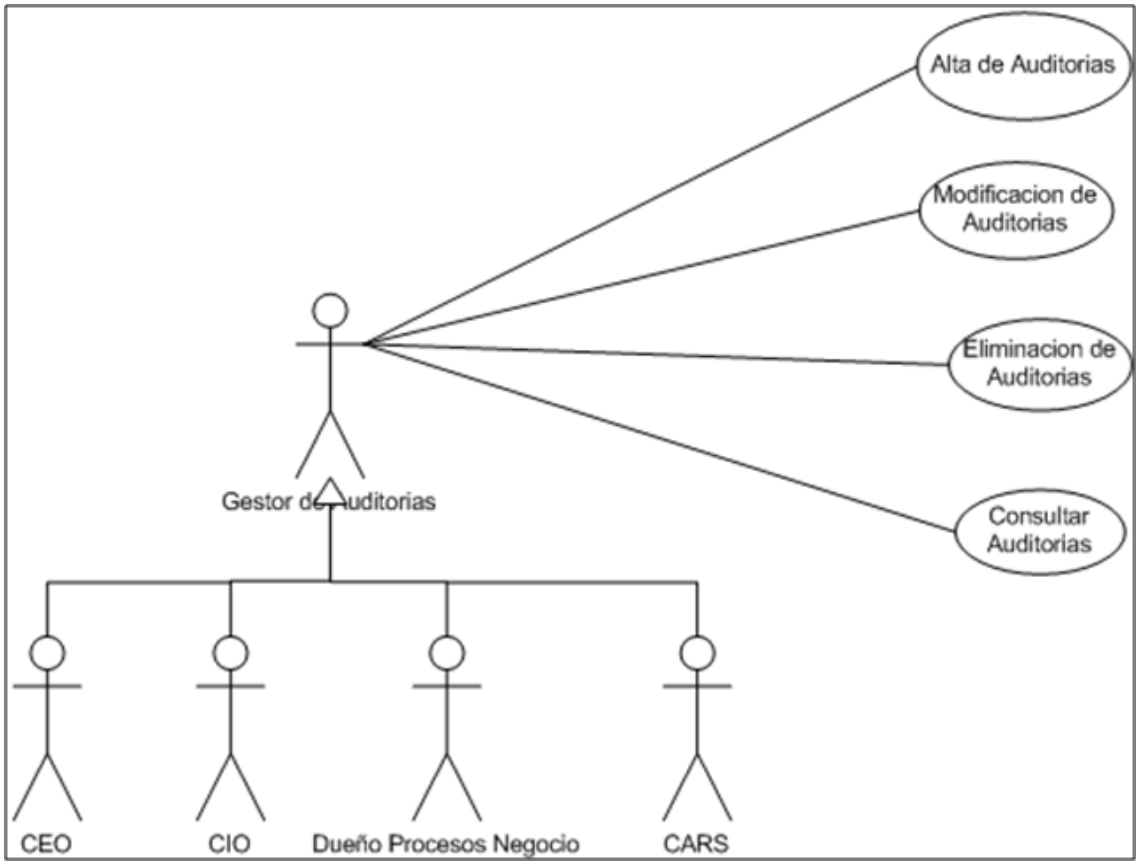


Figura 30. Casos de Uso de Gestión de Activos

Tabla 60. Casos de Uso. Alta de Activo

Nombre:	**Alta de Activo**
Actores:	CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Dar de alta un Activo en la aplicación
Escenario básico:	1. Pulsar el botón “Activos”. 2. Pulsar el botón “Crear Nuevo Activo”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y

	volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Activo. 4. La operación finalizará con el mensaje de éxito o error del alta del Activo.

Tabla 61. Casos de Uso. Modificar Activo

Nombre:	**Modificar Activo**
Actores:	CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Modificar los datos de un Activo de la aplicación
Escenario básico:	1. Pulsar el botón “Activos”. 2. Escribir el nombre del Activo que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Activos en el botón “Listar Activos”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Activo. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Activo modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Activo.

Tabla 62. Casos de Uso. Eliminar Activo

Nombre:	**Eliminar Activo**
Actores:	CIO, Dueño Procesos Negocio y Dueño Procesos

	TI
Objetivo:	Eliminar uno de los Activos de la aplicación
Escenario básico:	1. Pulsar el botón “Activos”. 2. Escribir el nombre del Activo que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Activos en el botón “Listar Activos”. 3. Pulsar el botón “Eliminar” del Activo que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Activo. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 63. Casos de Uso. Evaluar impacto del Negocio del Activo

Nombre:	**Evaluar impacto del Negocio del Activo**
Actores:	CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Evaluar el impacto del Negocio de uno de los Activos de la aplicación
Escenario básico:	1. Pulsar el botón “Evaluar Activo”. 2 Asignara un indicador en función de los Acuerdos de Negocio sobre el activo y la disponibilidad y Alcance del Activo.

Tabla 64. Casos de Uso. Consultar Activo

Nombre:	**Consultar Activo**

Actores:	CIO, Dueño Procesos Negocio, Dueño Procesos TI, CEO, CARS y CSO
Objetivo:	Consultar detalle de uno de los Activos de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Activos”. 3. Escribir el nombre del Activo que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Activos en el botón “Listar Activos”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.11 Gestión de Acuerdos de Negocio

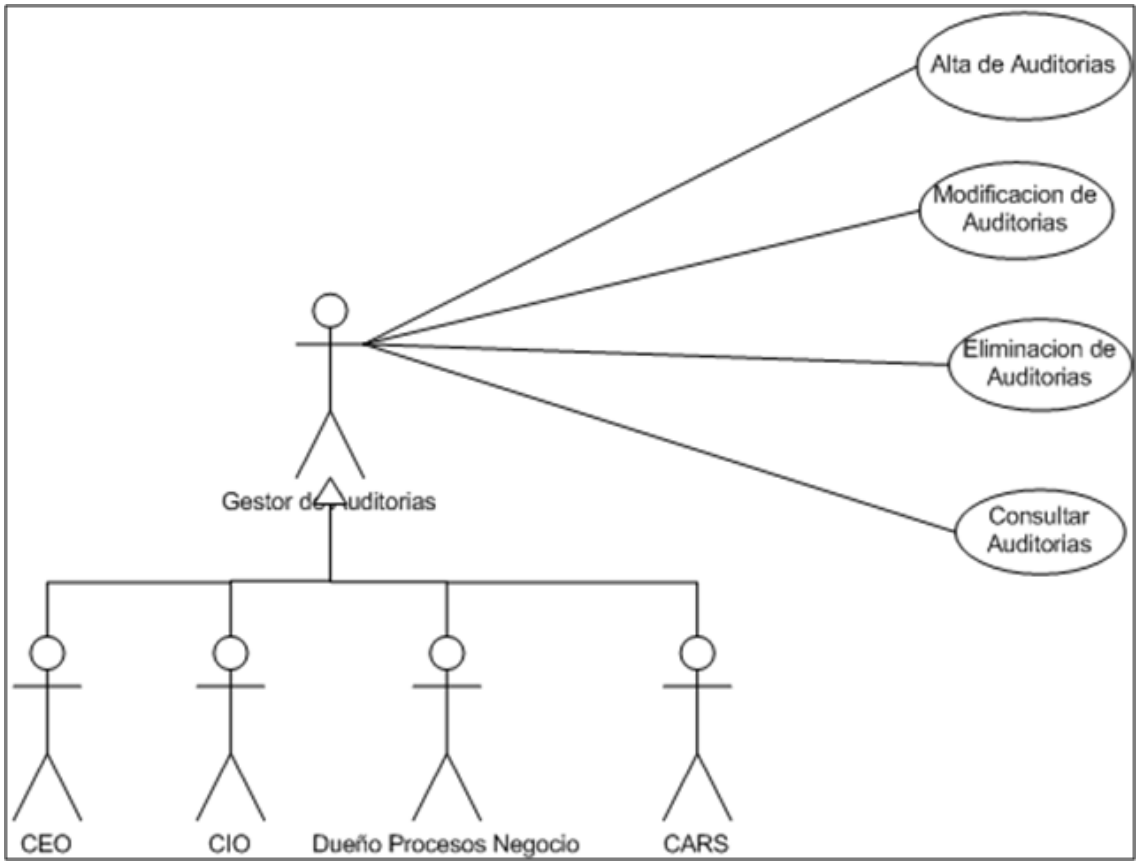


Figura 31. Casos de Uso de Gestión de Acuerdos de Negocio

Tabla 65. Casos de Uso. Alta de Acuerdo de Negocio

Nombre:	**Alta de Acuerdo de Negocio**
Actores:	CIO, Dueño Procesos Negocio, Dueño Procesos TI y CSO
Objetivo:	Dar de alta un Acuerdo de Negocio en la aplicación
Escenario básico:	1. Pulsar el botón “Acuerdos de Negocio”. 2. Pulsar el botón “Crear Nuevo Acuerdo de Negocio”. 3. Rellenar el formulario y pulsar los siguientes

	botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Acuerdo de Negocio. 4. La operación finalizará con el mensaje de éxito o error del alta del Acuerdo de Negocio.

Tabla 66. Casos de Uso. Modificar de Acuerdo de Negocio

Nombre:	**Modificar Acuerdo de Negocio**
Actores:	CIO, Dueño Procesos Negocio, Dueño Procesos TI y CSO
Objetivo:	Modificar los datos de un Acuerdo de Negocio de la aplicación
Escenario básico:	1. Pulsar el botón “Acuerdos de Negocio”. 2. Escribir el nombre del Acuerdo de Negocio que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Acuerdos de Negocio en el botón “Listar Acuerdos de Negocio”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Acuerdo de Negocio. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Acuerdo de Negocio modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Acuerdo de Negocio.

Tabla 67. Casos de Uso. Eliminar de Acuerdo de Negocio

Nombre:	**Eliminar Acuerdo de Negocio**
Actores:	CIO, Dueño Procesos Negocio, Dueño Procesos TI y CSO
Objetivo:	Eliminar uno de los Acuerdo de Negocios de la aplicación
Escenario básico:	1. Pulsar el botón “Acuerdos de Negocio”. 2. Escribir el nombre del Acuerdo de Negocio que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Acuerdos de Negocio en el botón “Listar Acuerdos de Negocio”. 3. Pulsar el botón “Eliminar” del Acuerdo de Negocio que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Acuerdo de Negocio. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 68. Casos de Uso. Consultar de Acuerdo de Negocio

Nombre:	**Consultar Acuerdo de Negocio**
Actores:	CIO, Dueño Procesos Negocio, Dueño Procesos TI , CSO, CEO, Ejecutivo del Negocio y CARS
Objetivo:	Consultar detalle de uno de los Acuerdos de Negocio de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Acuerdos de Negocio”. 3. Escribir el nombre del Acuerdo de Negocio que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Acuerdos de

	Negocio en el botón “Listar Acuerdos de Negocio”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.12 Gestión de Incidentes

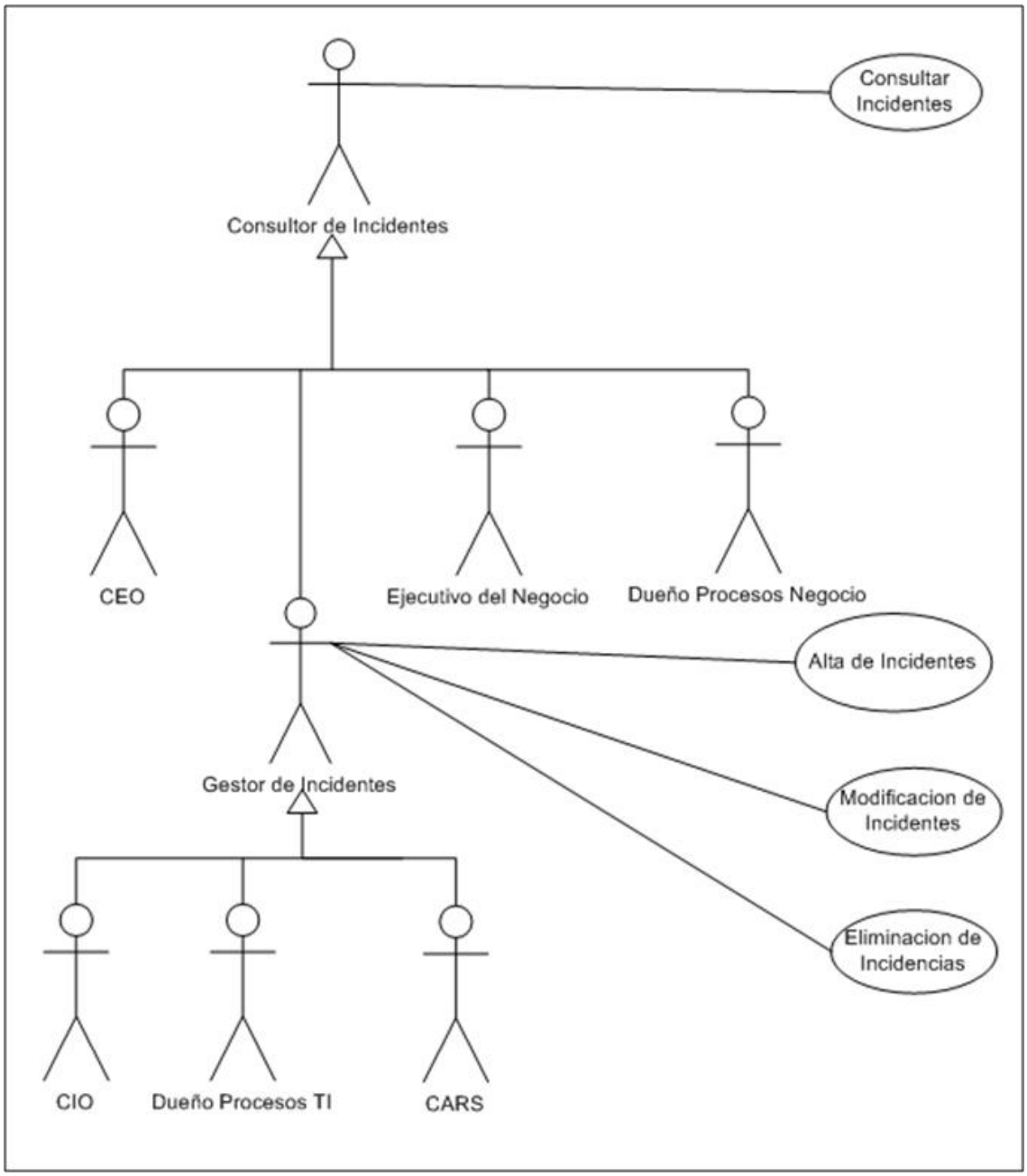


Figura 32. Casos de Uso de Gestión de Incidentes

Tabla 69. Casos de Uso. Alta de Incidente

Nombre:	**Alta de Incidente**

Actores:	CIO, Dueño Procesos TI y CARS
Objetivo:	Dar de alta un Incidente en la aplicación
Escenario básico:	1. Pulsar el botón “Incidentes”. 2. Pulsar el botón “Crear Nuevo Incidente”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Incidente. 4. La operación finalizará con el mensaje de éxito o error del alta del Incidente.

Tabla 70. Casos de Uso. Modificar Incidente

Nombre:	**Modificar Incidente**
Actores:	CIO, Dueño Procesos TI y CARS
Objetivo:	Modificar los datos de un Incidente de la aplicación
Escenario básico:	1. Pulsar el botón “Incidentes”. 2. Escribir el nombre de la Incidencia que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Incidentes en el botón “Listar Incidentes”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Incidente. 3.2 Pulsar “Guardar”, se guardarán todos los

	datos del Incidente modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Incidente

Tabla 71. Casos de Uso. Eliminar Incidente

Nombre:	**Eliminar Incidente**
Actores:	CIO, Dueño Procesos TI y CARS
Objetivo:	Eliminar una de los Incidentes de la aplicación
Escenario básico:	1. Pulsar el botón “Incidentes”. 2. Escribir el nombre del Incidente que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Incidentes en el botón “Listar Incidentes”. 3. Pulsar el botón “Eliminar” del Incidente que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Incidente. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 72. Casos de Uso. Consultar Incidente

Nombre:	**Consultar Incidente**
Actores:	CIO, Dueño Procesos TI, CARS, CEO, Ejecutivo del Negocio y Dueño Procesos Negocio
Objetivo:	Consultar detalle de uno de los Incidentes de la aplicación

Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Incidentes”. 3. Escribir el nombre del Incidente que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Incidentes en el botón “Listar Incidentes”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.13 Gestión de Amenazas

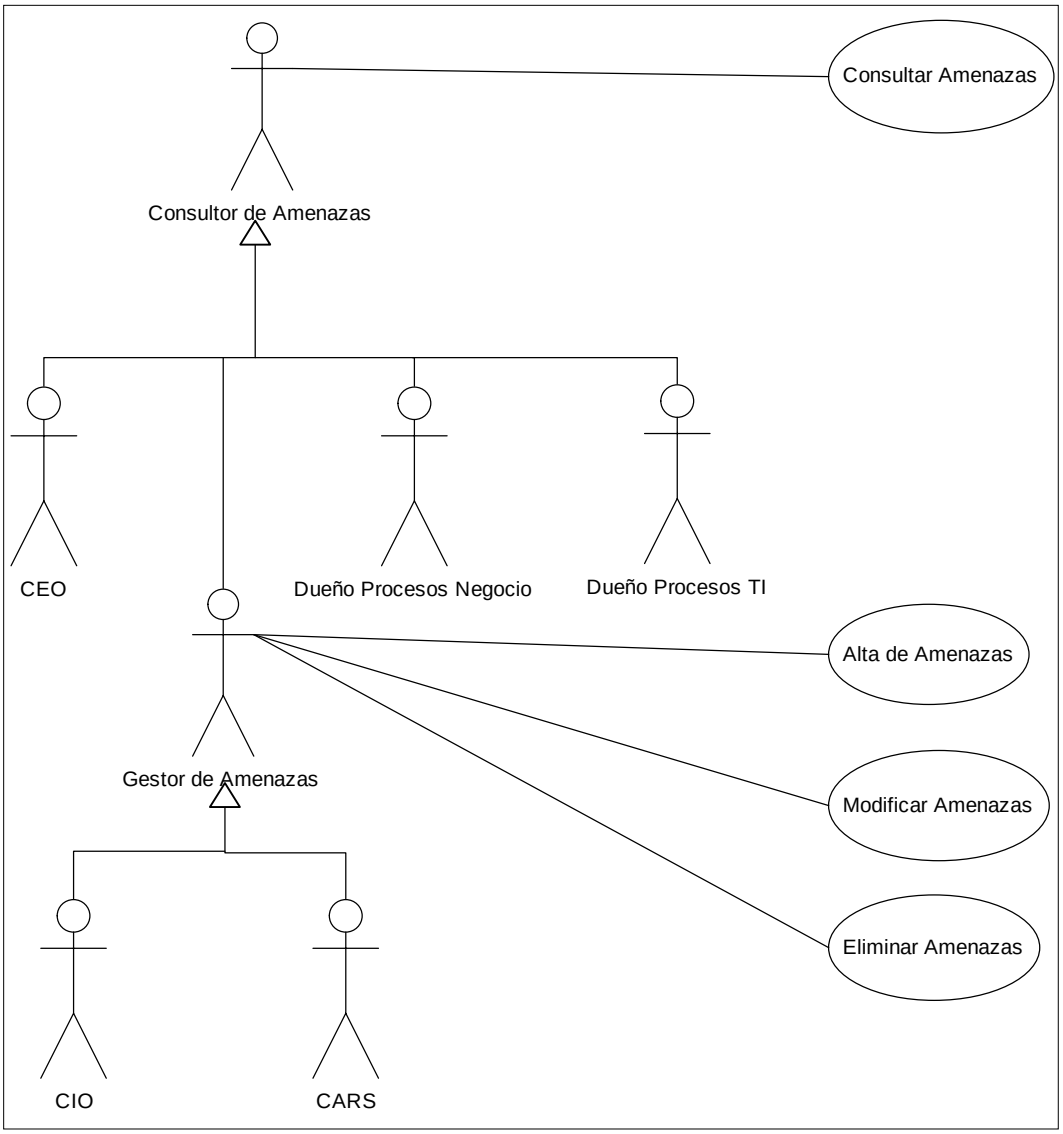


Figura 33. Casos de Uso de Gestión de Amenazas

Tabla 73. Casos de Uso. Alta de Amenaza

Nombre:	**Alta de Amenaza**
Actores:	CIO y CARS
Objetivo:	Dar de alta una Amenaza en la aplicación

Escenario básico:	1. Pulsar el botón “Amenazas”. 2. Pulsar el botón “Crear Nueva Amenaza”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Amenaza. 4. La operación finalizará con el mensaje de éxito o error del alta de la Amenaza.

Tabla 74. Casos de Uso. Modificar Amenaza

Nombre:	**Modificar Amenaza**
Actores:	CIO y CARS
Objetivo:	Modificar los datos de una Amenaza de la aplicación
Escenario básico:	1. Pulsar el botón “Amenazas”. 2. Escribir el nombre de la Amenaza que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todas las Amenazas en el botón “Listar Amenazas”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Amenaza. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Amenaza modificada. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Amenaza.

Tabla 75. Casos de Uso. Eliminar Amenaza

Nombre:	**Eliminar Amenaza**
Actores:	CIO y CARS
Objetivo:	Eliminar una de las Amenazas de la aplicación
Escenario básico:	1. Pulsar el botón “Amenazas”. 2. Escribir el nombre de la Amenaza que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todas las Amenazas en el botón “Listar Amenazas”. 3. Pulsar el botón “Eliminar” de la Amenaza que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Amenaza. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 76. Casos de Uso. Consultar Amenaza

Nombre:	**Consultar Amenaza**
Actores:	CIO, CARS, CEO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Consultar detalle de una de las Amenazas de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Amenazas”. 3. Escribir el nombre de la Amenaza que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos las Amenazas en el botón “Listar

	Amenazas". 4. Pulsar el botón "Consultar" para más detalle. 4.1 Pulsar "Salir" para abandonar la consulta y volver al punto 3.

5.6.14 Gestión de Vulnerabilidades

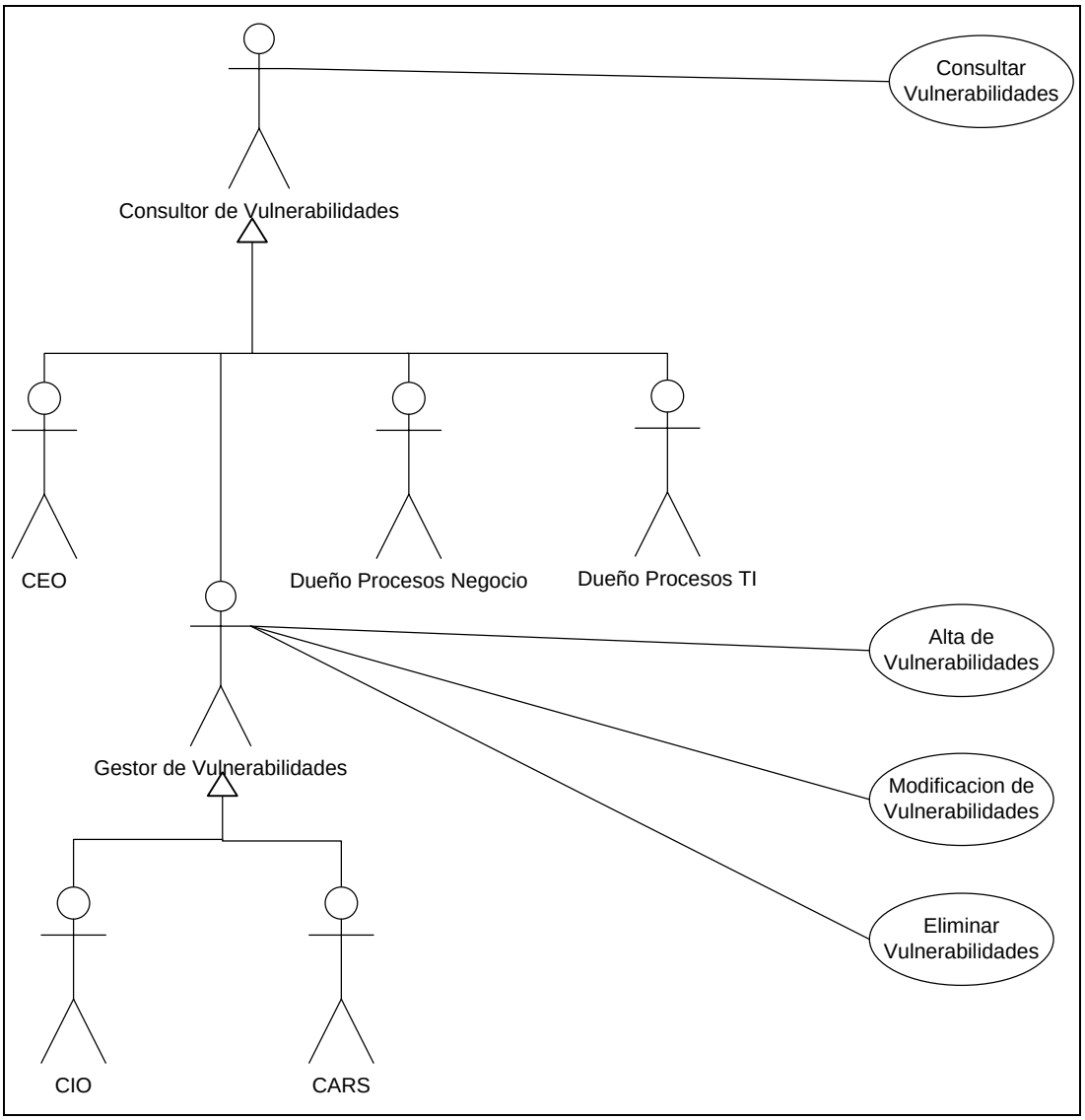


Figura 34. Casos de Uso de Gestión de Vulnerabilidades

Tabla 77. Casos de Uso. Alta de Vulnerabilidad

Nombre:	**Alta de Vulnerabilidad**
Actores:	CIO y CARS
Objetivo:	Dar de alta una Vulnerabilidad en la aplicación
Escenario básico:	1. Pulsar el botón “Vulnerabilidades”.

	2. Pulsar el botón “Crear Nuevo Vulnerabilidad”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Vulnerabilidad. 4. La operación finalizará con el mensaje de éxito o error del alta de la Vulnerabilidad.

Tabla 78. Casos de Uso. Modificar Vulnerabilidad

Nombre:	**Modificar Vulnerabilidad**
Actores:	CIO y CARS
Objetivo:	Modificar los datos de una Vulnerabilidad de la aplicación
Escenario básico:	1. Pulsar el botón “Vulnerabilidades”. 2. Escribir el nombre de la Vulnerabilidad que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todas las Vulnerabilidades en el botón “Listar Vulnerabilidades”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Vulnerabilidad. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Vulnerabilidad modificada. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Vulnerabilidad.

Tabla 79. Casos de Uso. Eliminar Vulnerabilidad

Nombre:	**Eliminar Vulnerabilidad**
Actores:	CIO y CARS
Objetivo:	Eliminar una de las Vulnerabilidades de la aplicación
Escenario básico:	1. Pulsar el botón “Vulnerabilidades”. 2. Escribir el nombre de la Vulnerabilidad que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todas las Vulnerabilidades en el botón “Listar Vulnerabilidades”. 3. Pulsar el botón “Eliminar” de la Vulnerabilidad que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Vulnerabilidad. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 80. Casos de Uso. Consultar Vulnerabilidad

Nombre:	**Consultar Vulnerabilidad**
Actores:	CIO, CARS, CEO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Consultar detalle de una de las Vulnerabilidades de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Vulnerabilidades”. 3. Escribir el nombre de la Vulnerabilidad que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos las Vulnerabilidades en el

	botón “Listar Vulnerabilidades”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.15 Gestión de Requisitos

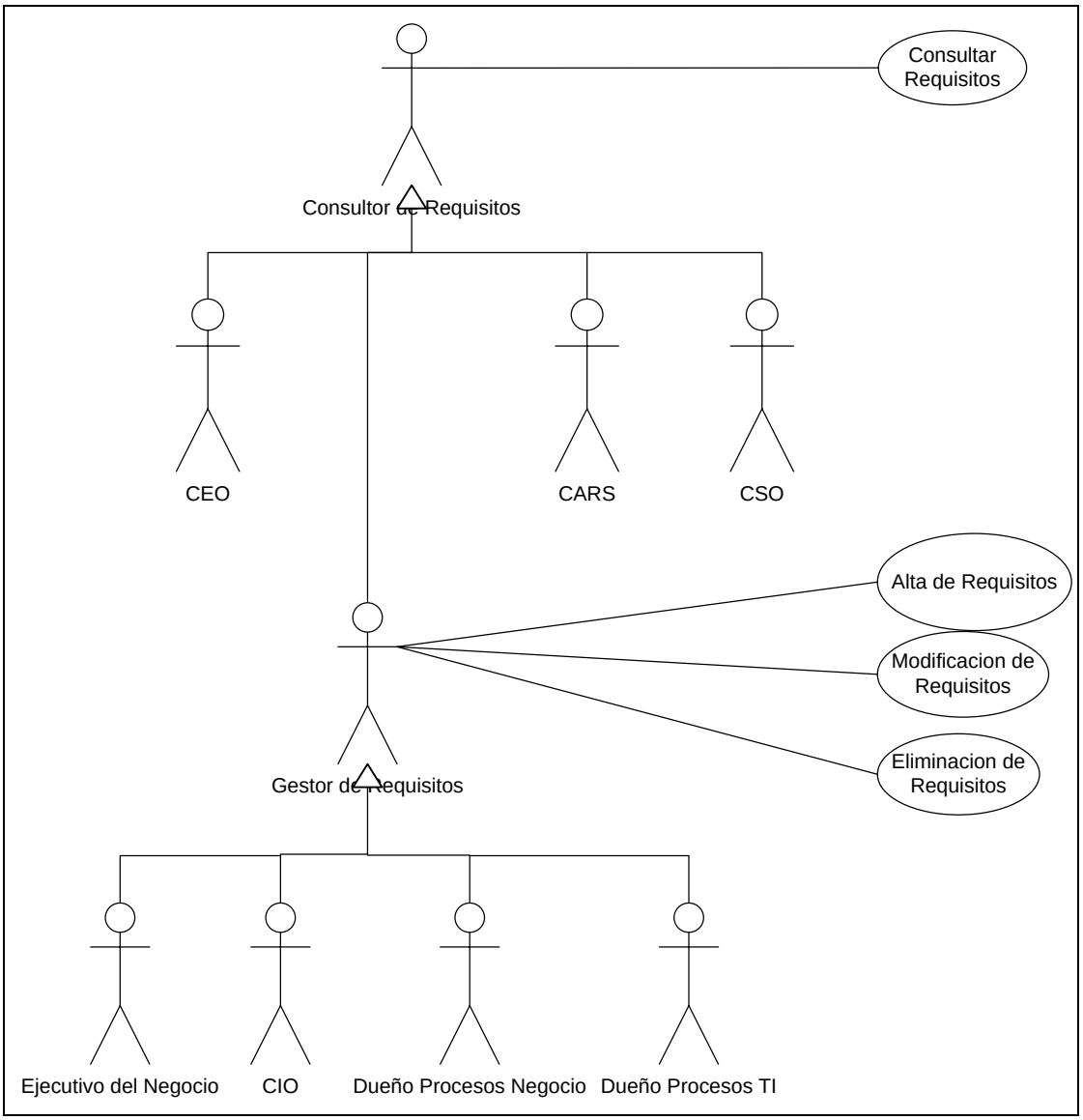


Figura 35. Casos de Uso de Gestión de Requisitos

Tabla 81. Casos de Uso. Alta de Requisito

Nombre:	**Alta de Requisito**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI

Objetivo:	Dar de alta un Requisito de la aplicación
Escenario básico:	1. Pulsar el botón “Requisitos”. 2. Pulsar el botón “Crear Nuevo Requisito”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Requisito. 4. La operación finalizará con el mensaje de éxito o error del alta del Requisito.

Tabla 82. Casos de Uso. Modificar Requisito

Nombre:	**Modificar Requisito**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Modificar los datos de un Requisito de la aplicación
Escenario básico:	1. Pulsar el botón “Requisitos”. 2. Escribir el nombre del Requisito que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Requisitos en el botón “Listar Requisitos”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Requisito. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Requisito modificado.

	4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Requisito.

Tabla 83. Casos de Uso. Eliminar Requisito

Nombre:	**Eliminar Requisito**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Eliminar uno de los Requisito de la aplicación
Escenario básico:	1. Pulsar el botón “Requisitos”. 2. Escribir el nombre del Requisito que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Requisitos en el botón “Listar Requisitos”. 3. Pulsar el botón “Eliminar” del Requisito que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Requisito. 4.1 Pulsar “Aceptar”, se eliminará el Requisito seleccionado. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 84. Casos de Uso. Consultar Requisito

Nombre:	**Consultar Requisito**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio, Dueño Procesos TI, CEO, CARS y CSO
Objetivo:	Consultar detalle de uno de los Requisitos de la aplicación

Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Requisitos”. 3. Escribir el nombre del Requisito que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Requisitos en el botón “Listar Requisitos”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.16 Gestión de Controles

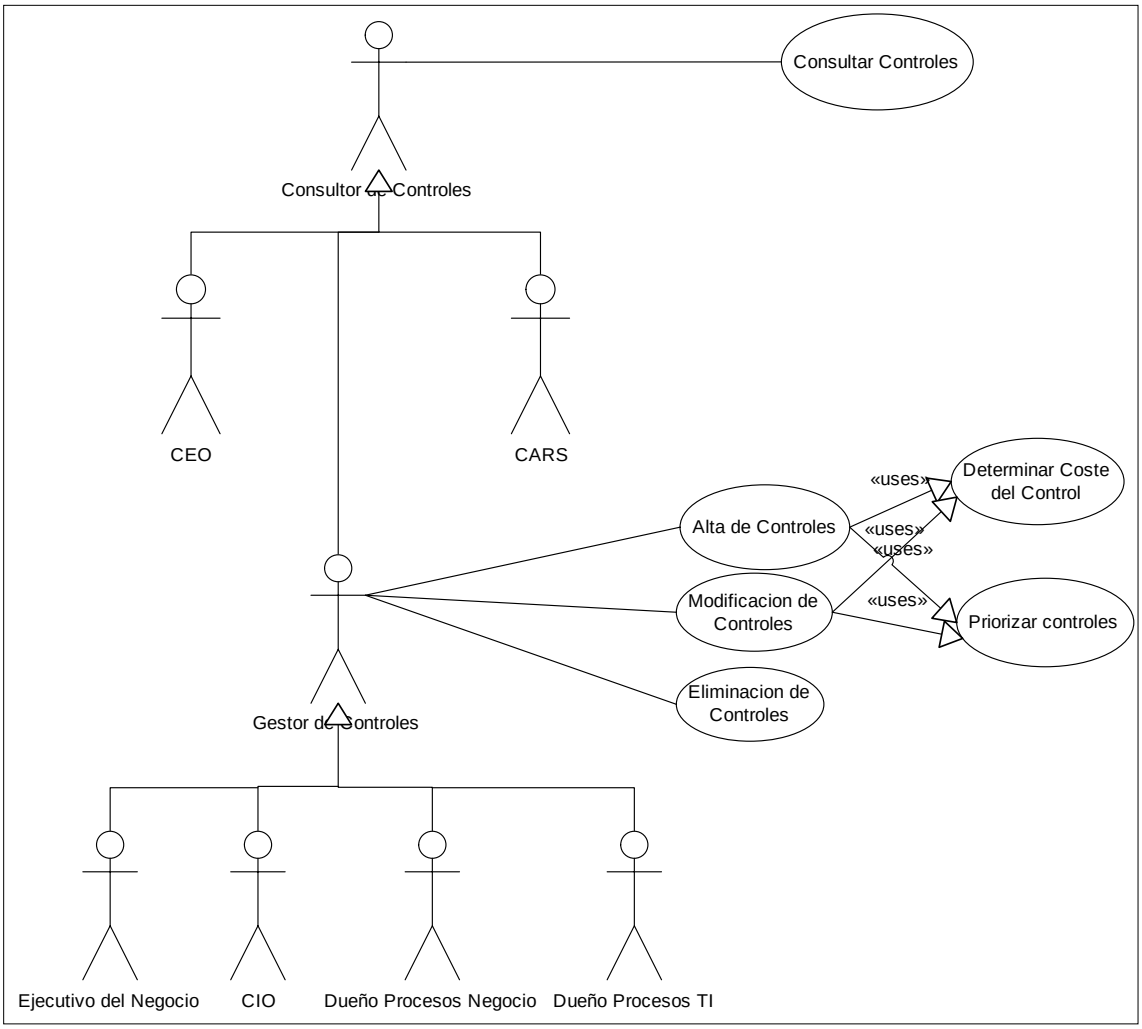


Figura 36. Casos de Uso de Gestión de Controles

Tabla 85. Casos de Uso. Alta de Control

Nombre:	**Alta de Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Dar de alta un Control de la aplicación
Escenario básico:	1. Pulsar el botón “Controles”.

	2. Pulsar el botón “Crear Nuevo Control”. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Control. 4. La operación finalizará con el mensaje de éxito o error del alta del Control.

Tabla 86. Casos de Uso. Modificar Control

Nombre:	**Modificar Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Modificar los datos de un Control de la aplicación
Escenario básico:	1. Pulsar el botón “Control”. 2. Escribir el nombre del Control que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todos los Controles en el botón “Listar Controles”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Control. 3.2 Pulsar “Guardar”, se guardarán todos los datos del Control modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Control.

Tabla 87. Casos de Uso. Eliminar Control

Nombre:	**Eliminar Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Eliminar uno de los Controles de la aplicación
Escenario básico:	1. Pulsar el botón “Controles”. 2. Escribir el nombre del Control que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todos los Controles en el botón “Listar Controles”. 3. Pulsar el botón “Eliminar” del Control que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Control. 4.1 Pulsar “Aceptar”, se eliminará el usuario seleccionado. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 88. Casos de Uso. Determinar Coste del Control

Nombre:	**Determinar Coste del Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Determinar el Coste de uno de los Controles de la aplicación
Escenario básico:	1. Pulsar el botón “Coste del Control”. 2 Asignara un valor financiero que supone la instalación de dicho control.

Tabla 89. Casos de Uso. Priorizar Control

Nombre:	**Priorizar Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Establecer un indicador de Priorización de uno de los Controles de la aplicación
Escenario básico:	1. Pulsar el botón “Priorización de Control”. 2 Asignara un indicador en función de la necesidad de dicho control.

Tabla 90. Casos de Uso. Consultar Control

Nombre:	**Consultar Control**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio, Dueño Procesos TI, CEO y CARS
Objetivo:	Consultar detalle de uno de los Controles de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Controles”. 3. Escribir el nombre del Control que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Controles en el botón “Listar Controles”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.17 Gestión de Planes de Seguimiento y Continuidad

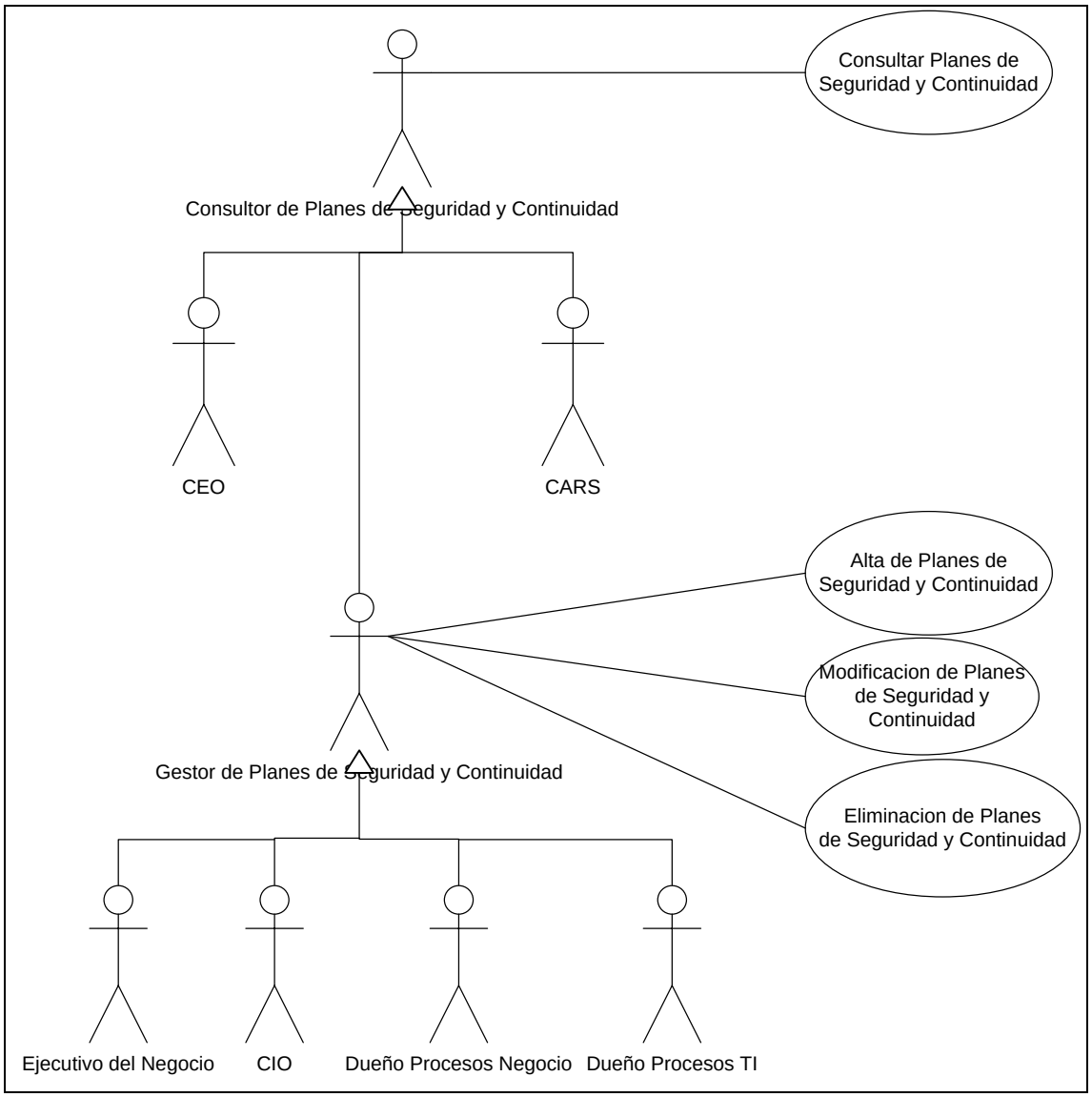


Figura 37. Casos de Uso de Gestión de Planes de Seguimiento y Continuidad

Tabla 91. Casos de Uso. Alta de Plan de Seguimiento y Continuidad

Nombre:	**Alta de Plan de Seguimiento y Continuidad**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos

	Negocio y Dueño Procesos TI
Objetivo:	Dar de alta un Plan de Seguimiento y Continuidad de la aplicación
Escenario básico:	1. Pulsar el botón "Planes de Seguimiento y Continuidad". 2. Pulsar el botón "Crear Nuevo Plan de Seguimiento y Continuidad". 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar "Cancelar" para abandonar el alta y volver al punto 2. 3.2 Pulsar "Guardar", se guardarán todos los datos del Plan de Seguimiento y Continuidad. 4. La operación finalizará con el mensaje de éxito o error del alta del Plan de Seguimiento y Continuidad.

Tabla 92. Casos de Uso. Modificar Plan de Seguimiento y Continuidad

Nombre:	**Modificar Plan de Seguimiento y Continuidad**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Modificar los datos de un Plan de Seguimiento y Continuidad de la aplicación
Escenario básico:	1. Pulsar el botón "Planes de Seguimiento y Continuidad". 2. Escribir el nombre del Plan de Seguimiento y Continuidad que se desea modificar en el recuadro "Buscar por:" o bien hacer un listado de todos los Planes de Seguimiento y Continuidad en el botón "Listar Planes de Seguimiento y Continuidad". 3. Rellenar del formulario los datos que se desean

	modificar y pulsar los siguientes botones: 3.1 Pulsar "Cancelar" para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en el Plan de Seguimiento y Continuidad. 3.2 Pulsar "Guardar", se guardarán todos los datos del Plan de Seguimiento y Continuidad modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos del Plan de Seguimiento y Continuidad

Tabla 93. Casos de Uso. Eliminar Plan de Seguimiento y Continuidad

Nombre:	**Eliminar Plan de Seguimiento y Continuidad**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Eliminar uno de los Planes de Seguimiento y Continuidad de la aplicación
Escenario básico:	1. Pulsar el botón "Planes de Seguimiento y Continuidad". 2. Escribir el nombre del Plan de Seguimiento y Continuidad que se desea borrar en el recuadro "Buscar por:" o bien hacer un listado de todos los Planes de Seguimiento y Continuidad en el botón "Listar Planes de Seguimiento y Continuidad". 3. Pulsar el botón "Eliminar" del Plan de Seguimiento y Continuidad que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar el Plan de Seguimiento y Continuidad. 4.1 Pulsar "Aceptar", se eliminará el usuario seleccionado.

	4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 94. Casos de Uso. Consultar Plan de Seguimiento y Continuidad

Nombre:	**Consultar Plan de Seguimiento y Continuidad**
Actores:	Ejecutivo del Negocio, CIO, Dueño Procesos Negocio, Dueño Procesos TI, CEO y CARS
Objetivo:	Consultar detalle de uno de los Planes de Seguimiento y Continuidad de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Planes de Seguimiento y Continuidad”. 3. Escribir el nombre del Plan de Seguimiento y Continuidad que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todos los Planes de Seguimiento y Continuidad en el botón “Listar Planes de Seguimiento y Continuidad”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.18 Gestión de Políticas de Seguridad de TI

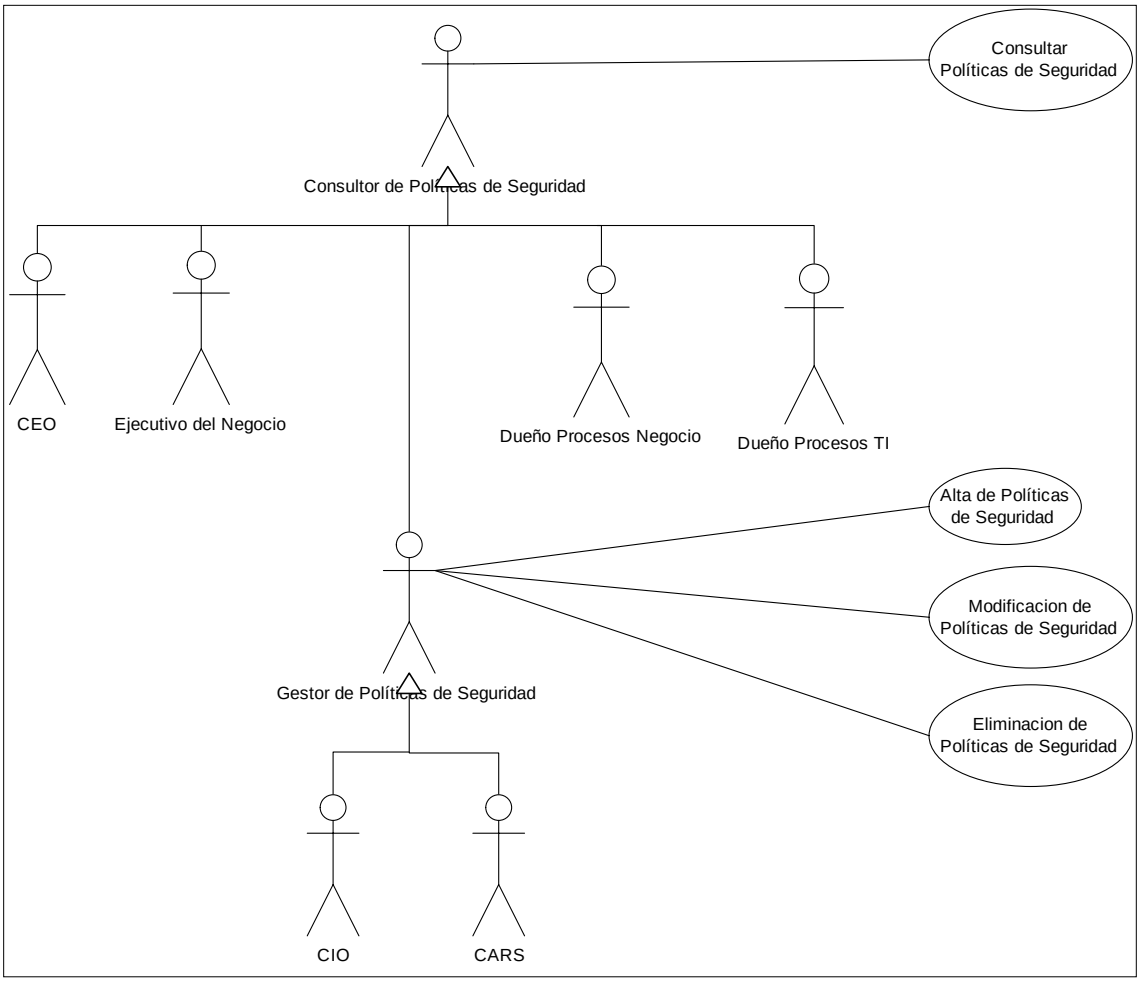


Figura 38. Casos de Uso de Gestión de Políticas

Tabla 95. Casos de Uso. Alta de Política

Nombre:	**Alta de Política**
Actores:	CIO y CARS
Objetivo:	Dar de alta una Política en la aplicación
Escenario básico:	1. Pulsar el botón “Políticas”. 2. Pulsar el botón “Crear Nueva Política”. 3. Rellenar el formulario y pulsar los siguientes

	botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Política. 4. La operación finalizará con el mensaje de éxito o error del alta de la Política.

Tabla 96. Casos de Uso. Modificar Política

Nombre:	**Modificar Política**
Actores:	CIO y CARS
Objetivo:	Modificar los datos de una Política de la aplicación
Escenario básico:	1. Pulsar el botón “Políticas”. 2. Escribir el nombre de la Política que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todas las Políticas en el botón “Listar Políticas”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Política. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Política modificada. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Política.

Tabla 97. Casos de Uso. Eliminar Política

Nombre:	**Eliminar Política**

Actores:	CIO y CARS
Objetivo:	Eliminar una de las Políticas de la aplicación
Escenario básico:	1. Pulsar el botón “Políticas”. 2. Escribir el nombre de la Política que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todas las Políticas en el botón “Listar Políticas”. 3. Pulsar el botón “Eliminar” de la Política que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Política. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 98. Casos de Uso. Consultar Política

Nombre:	**Consultar Política**
Actores:	CIO, CARS, CEO, Ejecutivo del Negocio, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Consultar detalle de una de las Políticas de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Políticas”. 3. Escribir el nombre de la Política que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todas las Políticas en el botón “Listar Políticas”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y

	volver al punto 3.

5.6.19 Gestión de Normativa Externa

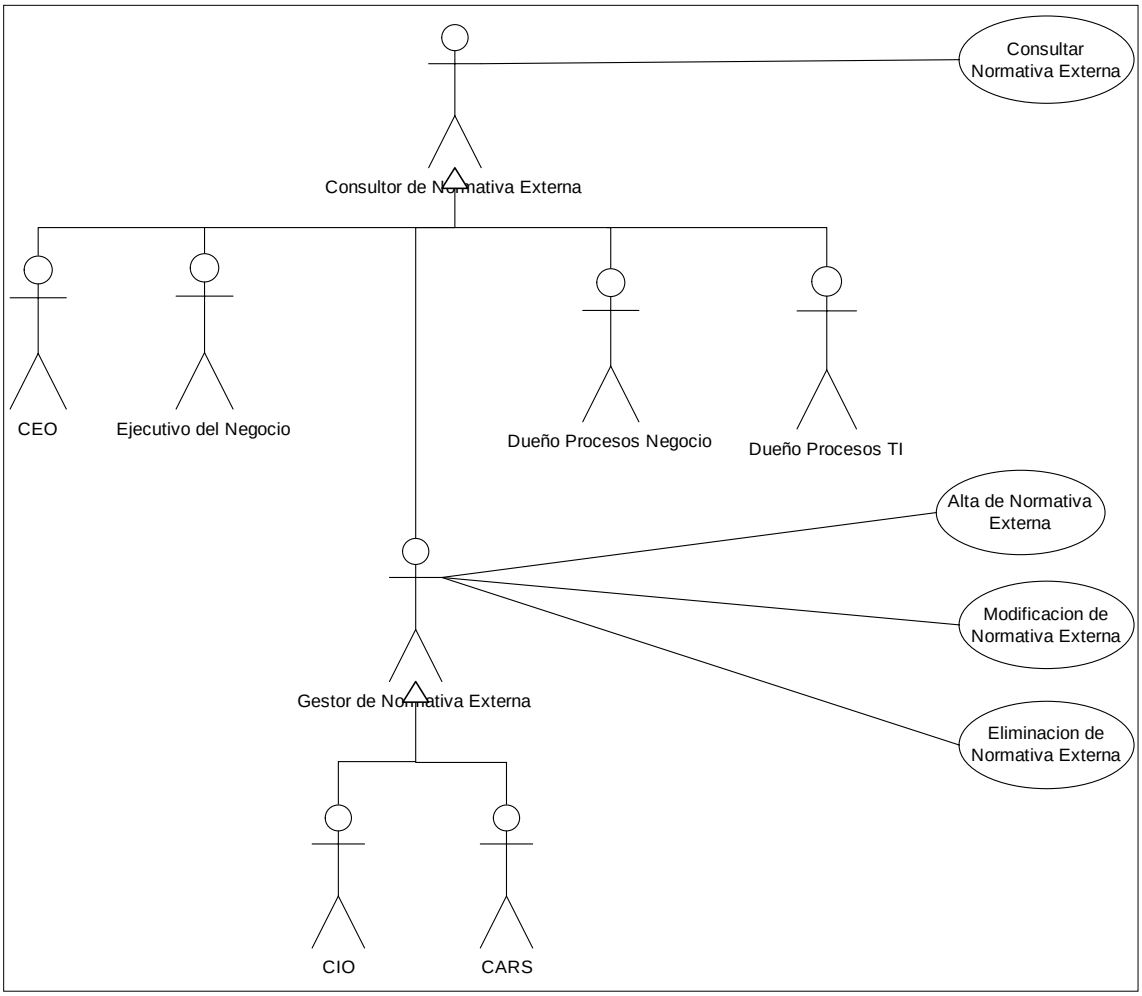


Figura 39. Casos de Uso de Gestión de Normativa Externa

Tabla 99. Casos de Uso. Alta de Normativa

Nombre:	**Alta de Normativa**
Actores:	CIO y CARS
Objetivo:	Dar de alta una Normativa en la aplicación
Escenario básico:	1. Pulsar el botón “Normativas”. 2. Pulsar el botón “Crear Nueva Normativa”. 3. Rellenar el formulario y pulsar los siguientes

	botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Normativa. 4. La operación finalizará con el mensaje de éxito o error del alta de la Normativa.

Tabla 100. Casos de Uso. Modificar Normativa

Nombre:	**Modificar Normativa**
Actores:	CIO y CARS
Objetivo:	Modificar los datos de una Normativa de la aplicación
Escenario básico:	1. Pulsar el botón “Normativas”. 2. Escribir el nombre de la Normativa que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todas las Normativas en el botón “Listar Normativas”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Normativa. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Normativa modificada. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Normativa.

Tabla 101. Casos de Uso. Eliminar Normativa

Nombre:	**Eliminar Normativa**
Actores:	CIO y CARS
Objetivo:	Eliminar una de las Normativas de la aplicación
Escenario básico:	1. Pulsar el botón “Normativas”. 2. Escribir el nombre de la Normativa que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todas las Normativas en el botón “Listar Normativas”. 3. Pulsar el botón “Eliminar” de la Normativa que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Normativa. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 102. Casos de Uso. Consultar Normativa

Nombre:	**Consultar Normativa**
Actores:	CIO, CARS, CEO, Ejecutivo del Negocio, Dueño Procesos Negocio y Dueño Procesos TI
Objetivo:	Consultar detalle de una de las Normativas de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Normativas”. 3. Escribir el nombre de la Normativa que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todas las Normativas en el botón “Listar Normativas”.

	4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.20 Gestión de Líneas Estratégicas de Seguridad de la Información

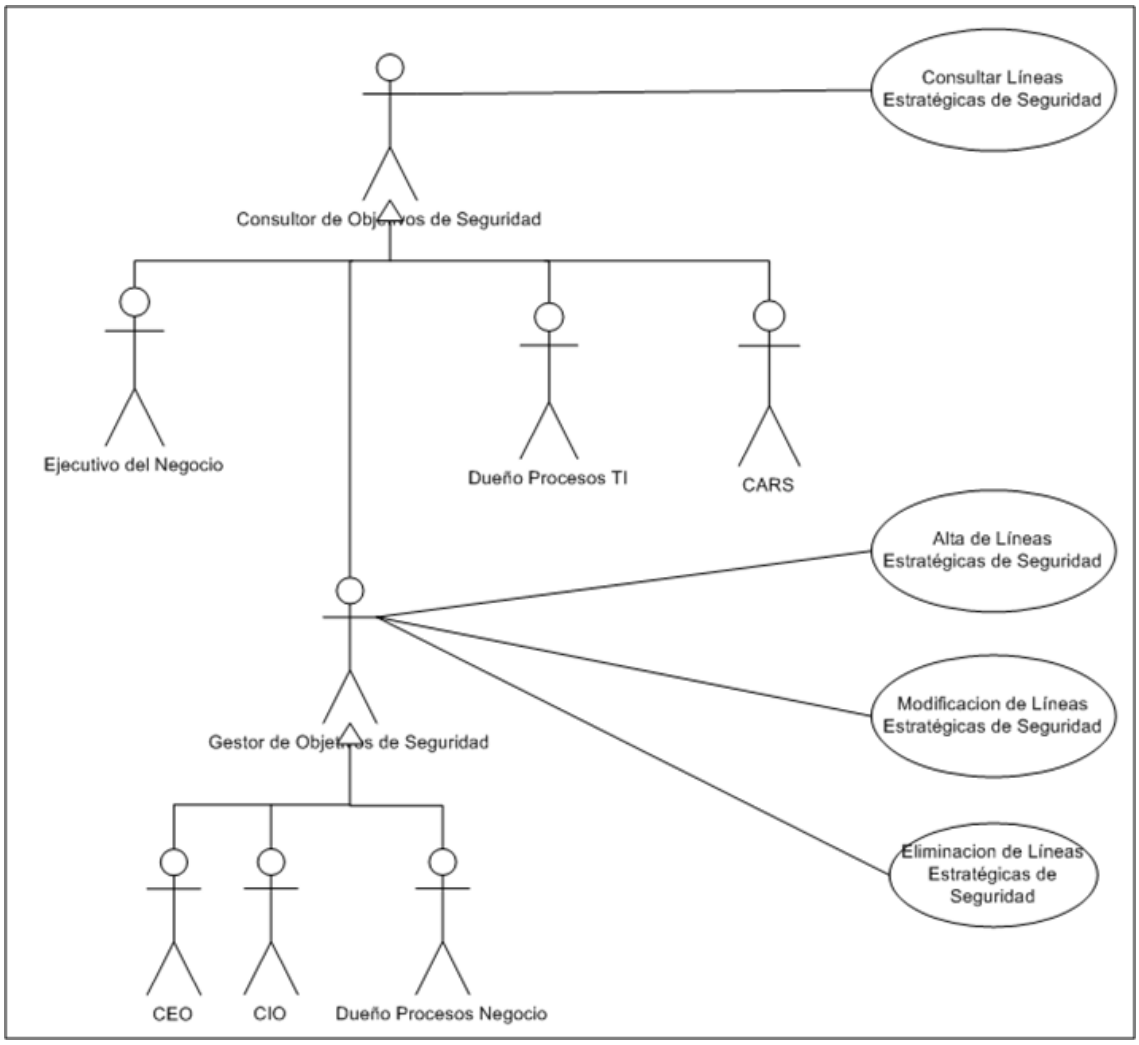


Figura 40. Casos de Uso de Gestión de Líneas Estratégicas de Seguridad

Tabla 103. Casos de Uso. Alta de Líneas Estratégicas de Seguridad

Nombre:	**Alta de Líneas Estratégicas de Seguridad**
Actores:	CEO, CIO y Dueño Procesos Negocio
Objetivo:	Dar de alta una Línea Estratégica en la aplicación
Escenario básico:	1. Pulsar el botón "Líneas Estratégicas de

	Seguridad". 2. Pulsar el botón "Crear Nueva Línea Estratégica de Seguridad". 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar "Cancelar" para abandonar el alta y volver al punto 2. 3.2 Pulsar "Guardar", se guardarán todos los datos de la Línea Estratégica de Seguridad. 4. La operación finalizará con el mensaje de éxito o error del alta de la Línea Estratégica de Seguridad.

Tabla 104. Casos de Uso. Modificar Líneas Estratégicas de Seguridad

Nombre:	**Modificar Líneas Estratégicas de Seguridad**
Actores:	CEO, CIO y Dueño Procesos Negocio
Objetivo:	Modificar los datos de una Línea Estratégica de Seguridad de la aplicación
Escenario básico:	1. Pulsar el botón "Línea Estratégica de Seguridad". 2. Escribir el nombre de la Línea Estratégica de Seguridad que se desea modificar en el recuadro "Buscar por:" o bien hacer un listado de todas las Líneas Estratégicas de Seguridad en el botón "Listar Líneas Estratégicas de Seguridad". 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar "Cancelar" para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Línea Estratégica de Seguridad. 3.2 Pulsar "Guardar", se guardarán todos los datos de la Línea Estratégica de Seguridad

	modificado. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Línea Estratégica de Seguridad.

Tabla 105. Casos de Uso. Eliminar Líneas Estratégicas de Seguridad

Nombre:	**Eliminar Líneas Estratégicas de Seguridad**
Actores:	CEO, CIO y Dueño Procesos Negocio
Objetivo:	Eliminar una de las Líneas Estratégicas de Seguridad de la aplicación
Escenario básico:	1. Pulsar el botón "Líneas Estratégicas de Seguridad". 2. Escribir el nombre de la Línea Estratégica de Seguridad que se desea borrar en el recuadro "Buscar por:" o bien hacer un listado de todas las Líneas Estratégicas de Seguridad en el botón "Listar Líneas Estratégicas de Seguridad". 3. Pulsar el botón "Eliminar" de la Línea Estratégica de Seguridad que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Línea Estratégica de Seguridad. 4.1 Pulsar "Aceptar" para continuar y volver al punto 2. 4.2 Pulsar "Cancelar" para anular la operación y volver al punto 2.

Tabla 106. Casos de Uso. Consultar Línea Estratégica de Seguridad

Nombre:	**Consultar Línea Estratégica de Seguridad**
Actores:	CEO, CIO, Dueño Procesos Negocio, Ejecutivo del

	Negocio, Dueño Procesos TI y CARS
Objetivo:	Consultar detalle de una de las Líneas Estratégicas de Seguridad de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Líneas Estratégicas de Seguridad”. 3. Escribir el nombre de la Línea Estratégica de Seguridad que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todas las Líneas Estratégicas de Seguridad en el botón “Listar Líneas Estratégicas de Seguridad”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

5.6.21 Gestión de Auditoria

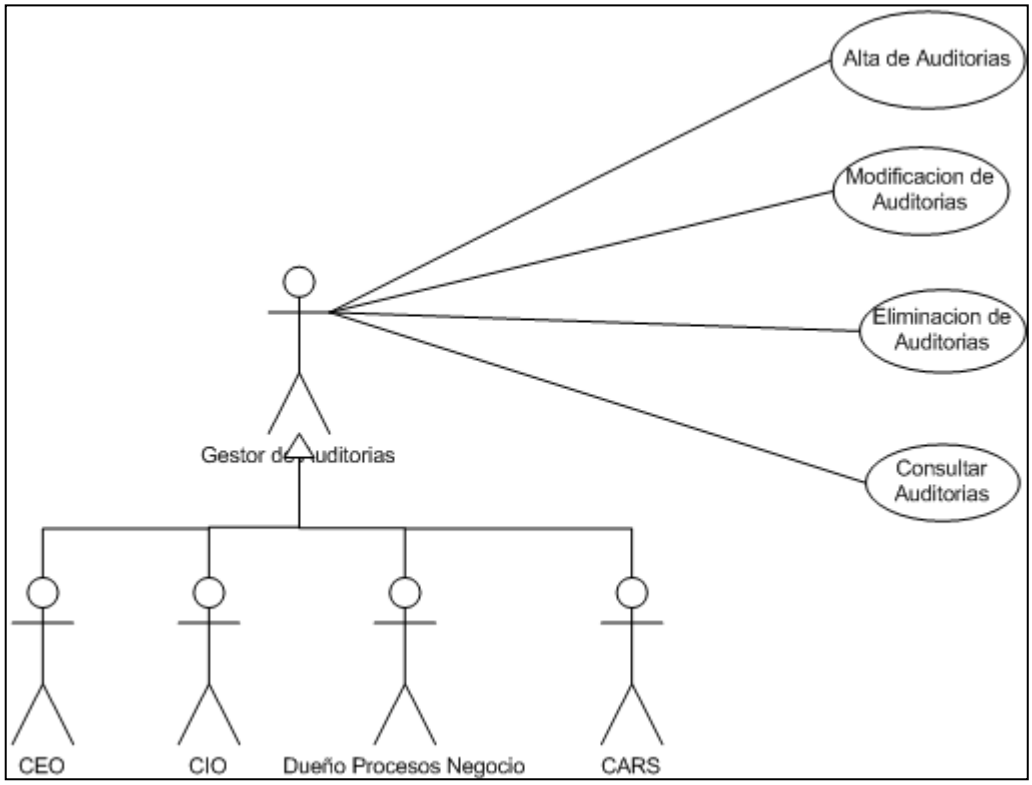


Figura 41. Casos de Uso de Gestión de Evaluación y Auditoría

Tabla 107. Casos de Uso. Alta de Auditoria

Nombre:	**Alta de Auditoria**
Actores:	CEO, CIO, Dueño Procesos Negocio y CARS
Objetivo:	Dar de alta una Auditoria en la aplicación
Escenario básico:	1. Pulsar el botón “Auditorias”. 2. Pulsar el botón “Crear Nueva Auditoria”. 3. Selección la categoría de la entidad del sistema que se desea Auditar. 3. Rellenar el formulario y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar el alta y volver al punto 2.

	3.2 Pulsar “Guardar”, se guardarán todos los datos de la Auditoria. 4. La operación finalizará con el mensaje de éxito o error del alta de la Auditoria.

Tabla 108. Casos de Uso. Modificar Auditoria

Nombre:	**Modificar Auditoria**
Actores:	CEO, CIO, Dueño Procesos Negocio y CARS
Objetivo:	Modificar los datos de una Auditoria de la aplicación
Escenario básico:	1. Pulsar el botón “Auditorias”. 2. Escribir el nombre de la Auditoria que se desea modificar en el recuadro “Buscar por:” o bien hacer un listado de todas las Auditorias en el botón “Listar Auditorias”. 3. Rellenar del formulario los datos que se desean modificar y pulsar los siguientes botones: 3.1 Pulsar “Cancelar” para abandonar la modificación y volver al punto 2 sin que se guarden los cambios hechos en la Auditoria. 3.2 Pulsar “Guardar”, se guardarán todos los datos de la Auditoria modificada. 4. La operación finalizará con el mensaje de éxito o error de la modificación de los datos de la Auditoria.

Tabla 109. Casos de Uso. Eliminar Auditoria

Nombre:	**Eliminar Auditoria**
Actores:	CEO, CIO, Dueño Procesos Negocio y CARS

Objetivo:	Eliminar una de las Auditorias de la aplicación
Escenario básico:	1. Pulsar el botón “Auditorias”. 2. Escribir el nombre de la Auditoria que se desea borrar en el recuadro “Buscar por:” o bien hacer un listado de todas las Auditorias en el botón “Listar Auditorias”. 3. Pulsar el botón “Eliminar” de la Auditoria que se desea eliminar. 4. Se muestra un Pop-Up en el que se informa de que se va a eliminar la Auditoria. 4.1 Pulsar “Aceptar” para continuar y volver al punto 2. 4.2 Pulsar “Cancelar” para anular la operación y volver al punto 2.

Tabla 110. Casos de Uso. Consultar Auditoria

Nombre:	**Consultar Auditoria**
Actores:	CEO, CIO, Dueño Procesos Negocio y CARS
Objetivo:	Consultar detalle de una de las Auditorias de la aplicación
Escenario básico:	1. Pulsar el botón “Consultas”. 2. Elegir del desplegable “Auditorias”. 3. Escribir el nombre de la Auditoria que se desea consultar en el recuadro “Buscar por:” o bien hacer un listado de todas las Auditorias en el botón “Listar Auditorias”. 4. Pulsar el botón “Consultar” para más detalle. 4.1 Pulsar “Salir” para abandonar la consulta y volver al punto 3.

6 DISEÑO FUNCIONAL

6.1 Diagrama de clases

El diagrama de clases es un tipo de diagrama estático que describe la estructura de un sistema mostrando sus clases, atributos, métodos y las relaciones entre ellos. A continuación, se presenta el diagrama de clases dividido en varios diagramas, con el fin de mejorar su legibilidad.

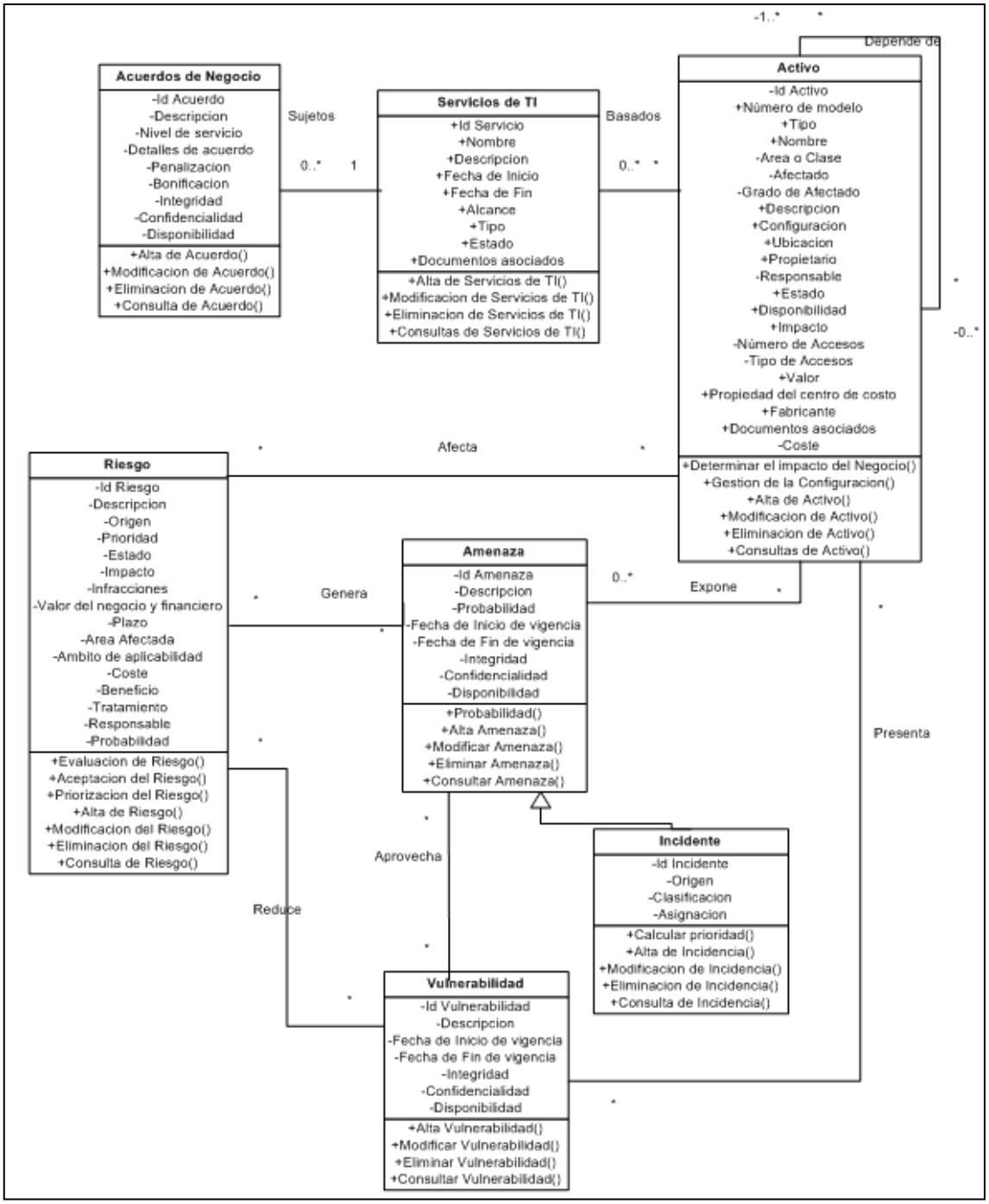


Figura 42. Diagrama de Clases origen del Riesgo

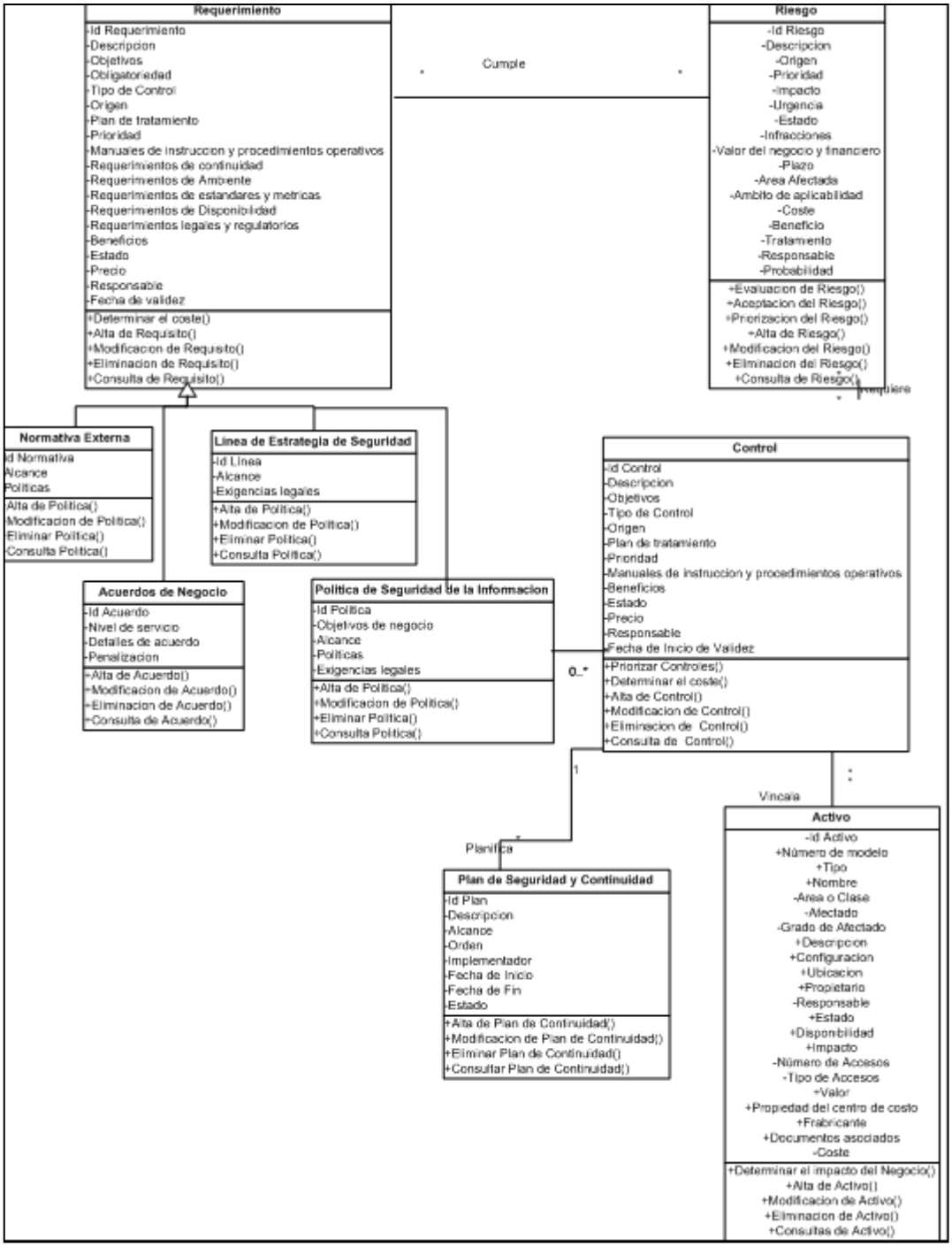


Figura 43. Diagrama de Clases. Diagnóstico del Riesgo

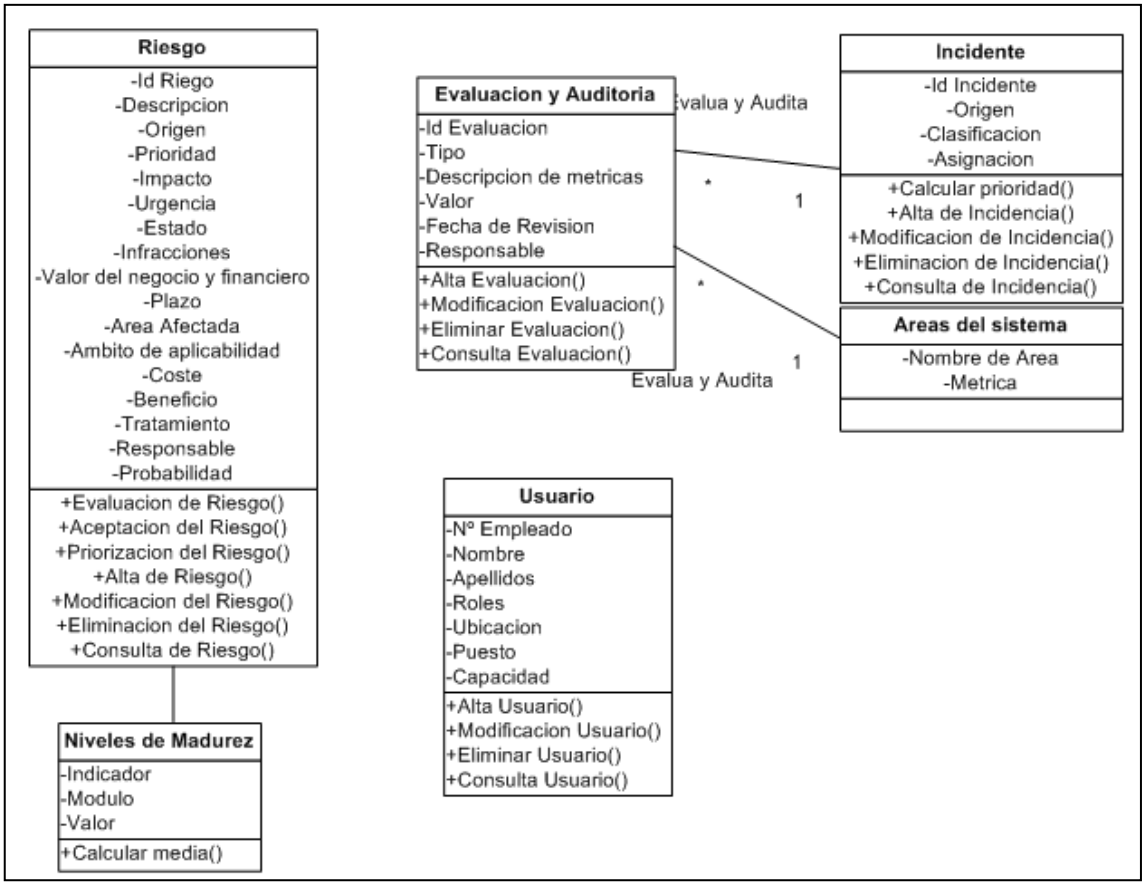


Figura 44. Diagrama de Clases. Evaluación del Sistema

6.2 Diagrama de secuencia

Los diagramas de secuencia son un tipo de diagrama usado para modelar la interacción entre objetos en un sistema según UML. Estos diagramas muestran la interacción de un conjunto de objetos en una aplicación a través del tiempo y se modela para cada método de la clase.

En este diagrama aparece un CIO a la hora de registrar una Amenaza, y relacionarla con los activos y vulnerabilidades afectados para posteriormente generar un Riesgo.

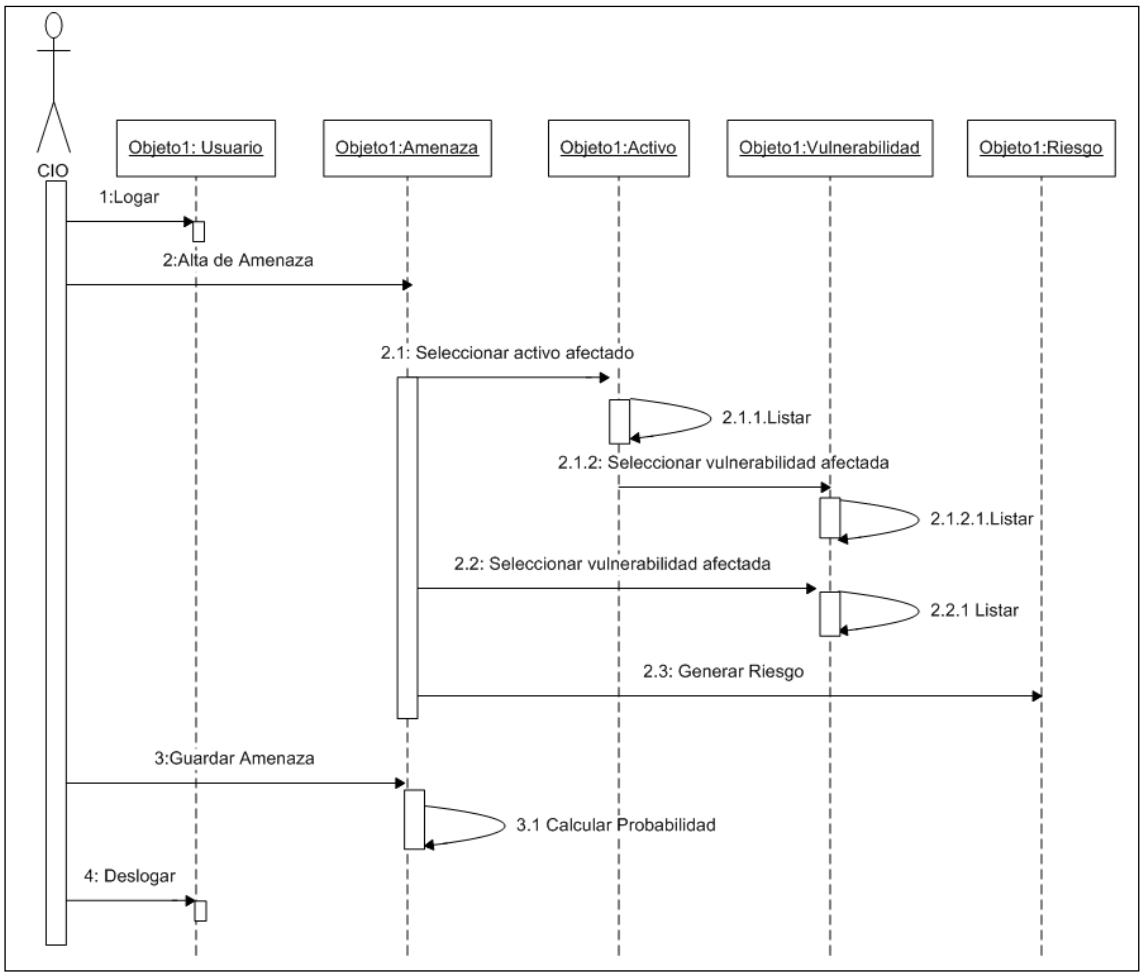


Figura 45. Diagrama de Secuencia. Alta de Amenaza

En este diagrama aparece un CIO a la hora de registrar un Activo, y relacionarla con las amenazas, vulnerabilidades, riesgos y niveles de servicio implicados para posteriormente generar un Activo.

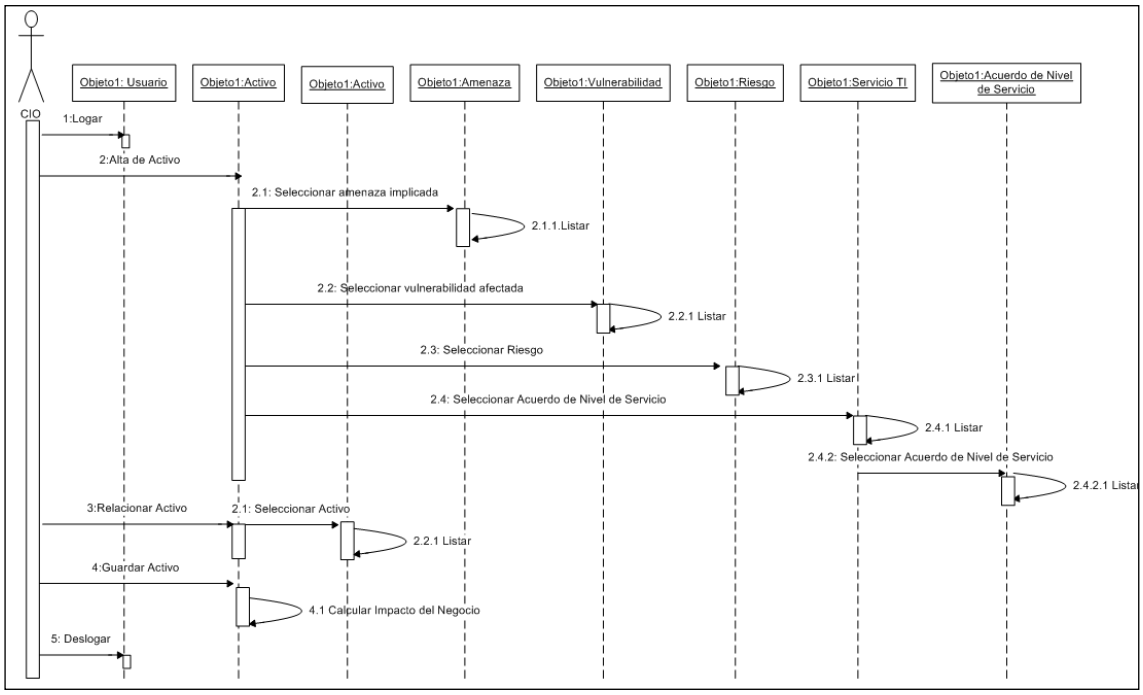


Figura 46. Diagrama de secuencia. Alta de Activo

En este diagrama aparece un CIO a la hora de registrar una Vulnerabilidad, y relacionarla con las amenazas y activos implicados para posteriormente generar la vulnerabilidad.

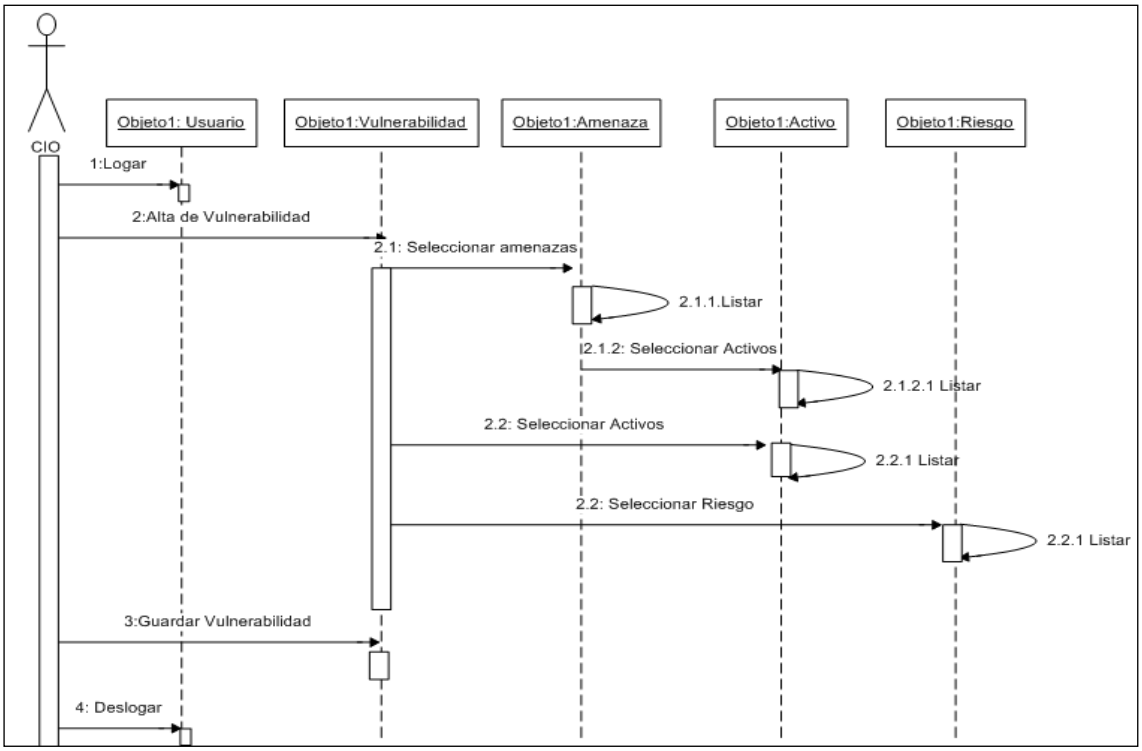


Figura 47. Diagrama de secuencia. Alta de vulnerabilidad

En este diagrama aparece un CIO a la hora de registrar un Riesgo, y relacionarlo con los requerimientos que cumple, y la política y controles que solventan el riesgo en un plan de seguimiento y control. Una vez se guarda el Riesgo se establece automáticamente la Evaluación del Riesgo, la Aceptación del Riesgo y la Priorización de éste.

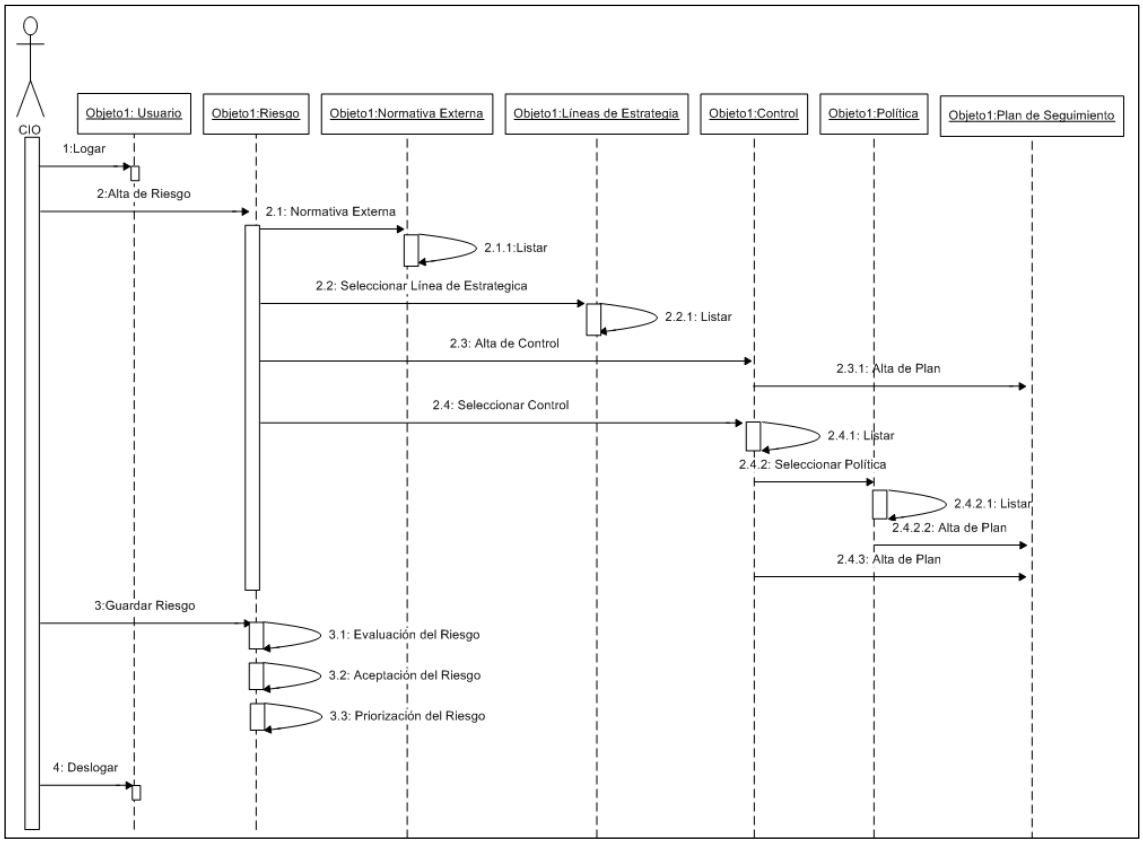


Figura 48. Diagrama de secuencia. Alta de Riesgo

En este diagrama aparece un CIO a la hora de registrar un Control, y relacionarlo con los riesgos y políticas que intervienen en el control, y establecer un plan de seguimiento. Una vez se guarda el Control se establece automáticamente la Priorización del Control y el coste de éste.

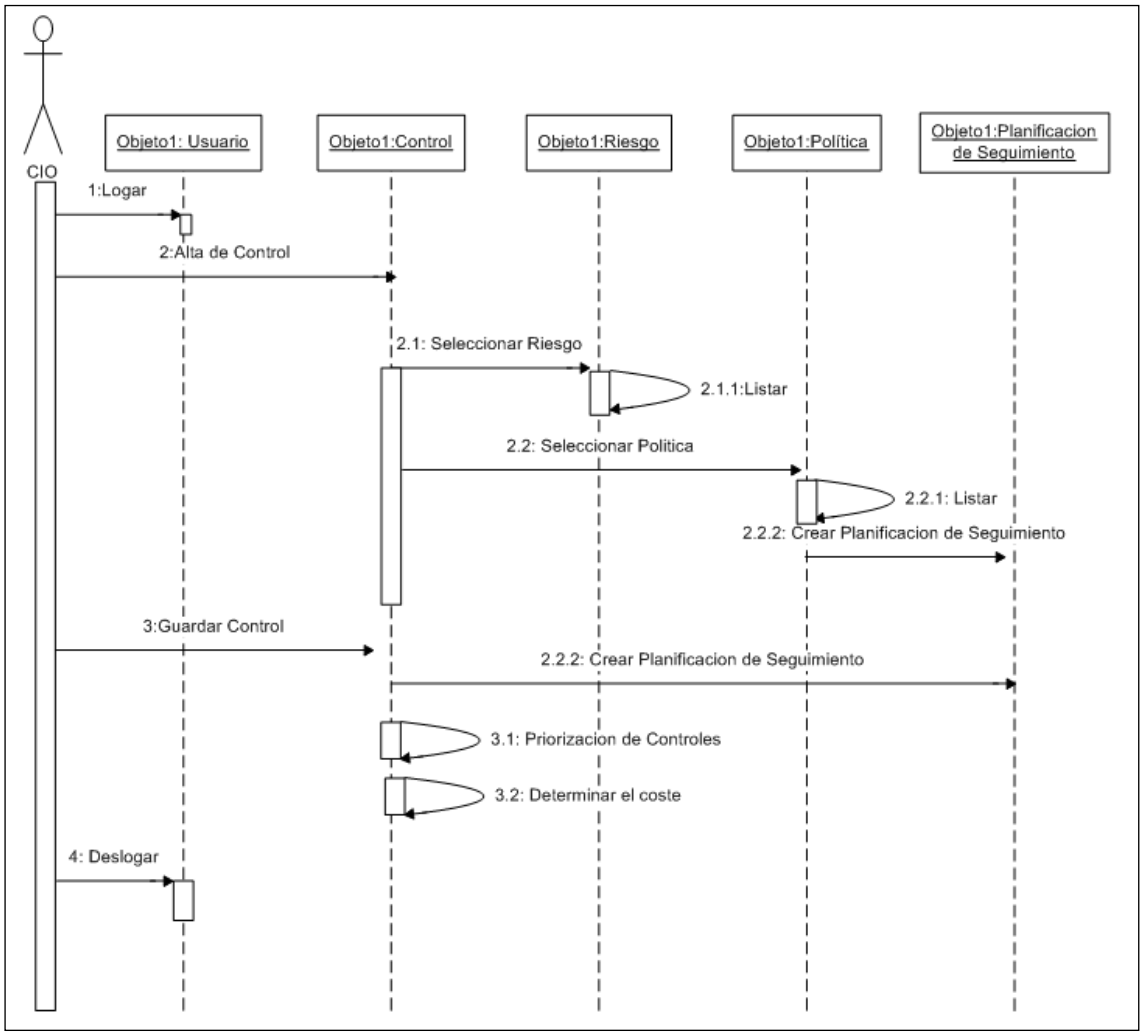


Figura 49. Diagrama de Secuencia. Alta de Control

En este diagrama aparece un CIO a la hora de registrar un Requerimiento de tipo Norma Externa, Objetivo de Negocio y Política, y relacionarlo con los riesgos que sustentan bajo dichos requerimientos. Una vez se guarda el Requerimiento se establece automáticamente el coste de éste.

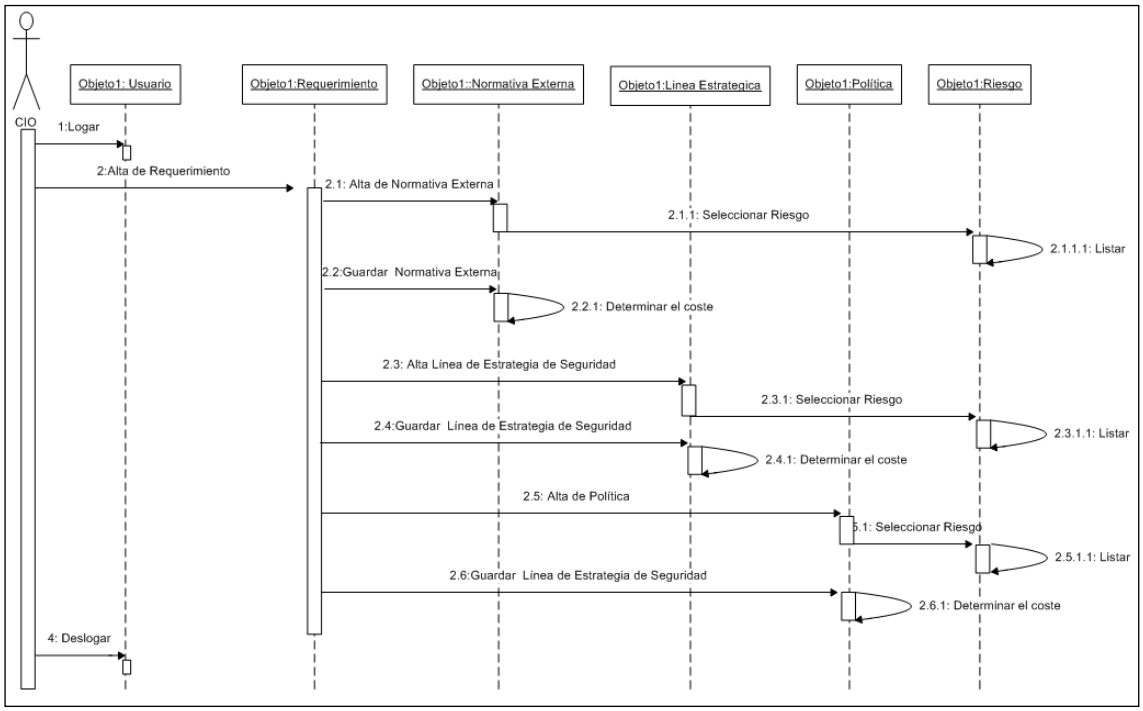


Figura 50. Diagrama de Secuencia. Alta de Requerimiento

En este diagrama aparece un CIO a la hora de registrar un Plan de Seguimiento de dos controles que están pendientes de establecer el plan de acción.

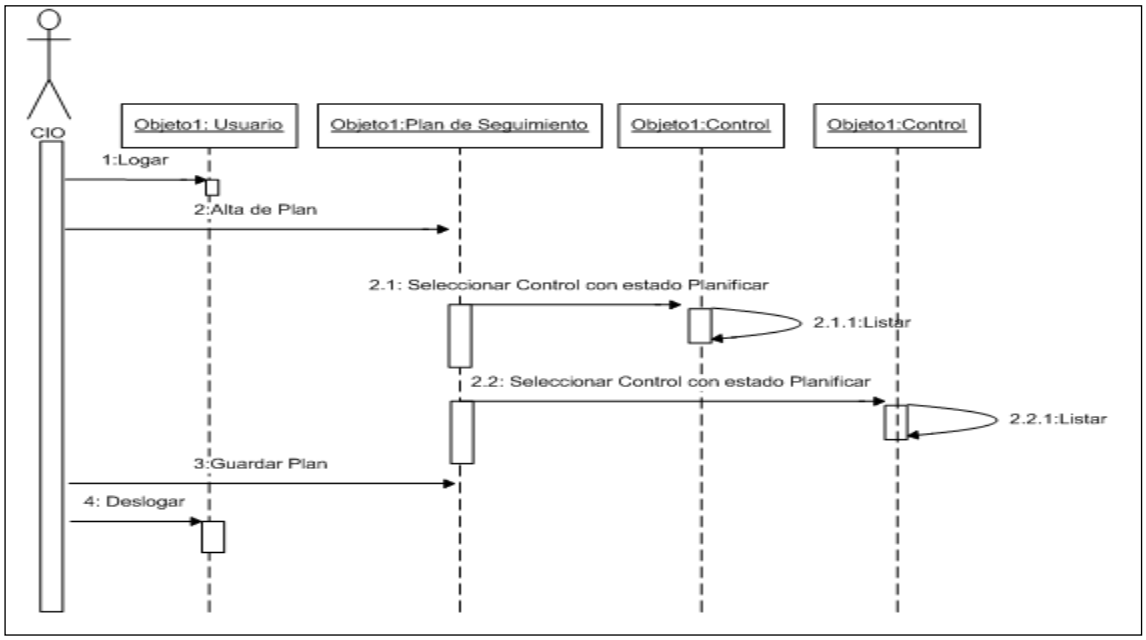


Figura 51. Diagrama de Secuencia. Alta de Plan de Seguimiento y Continuidad

En este diagrama aparece un CIO a la hora de registrar una Evaluación del sistema a través de las métricas establecidas de todas las áreas del sistema.

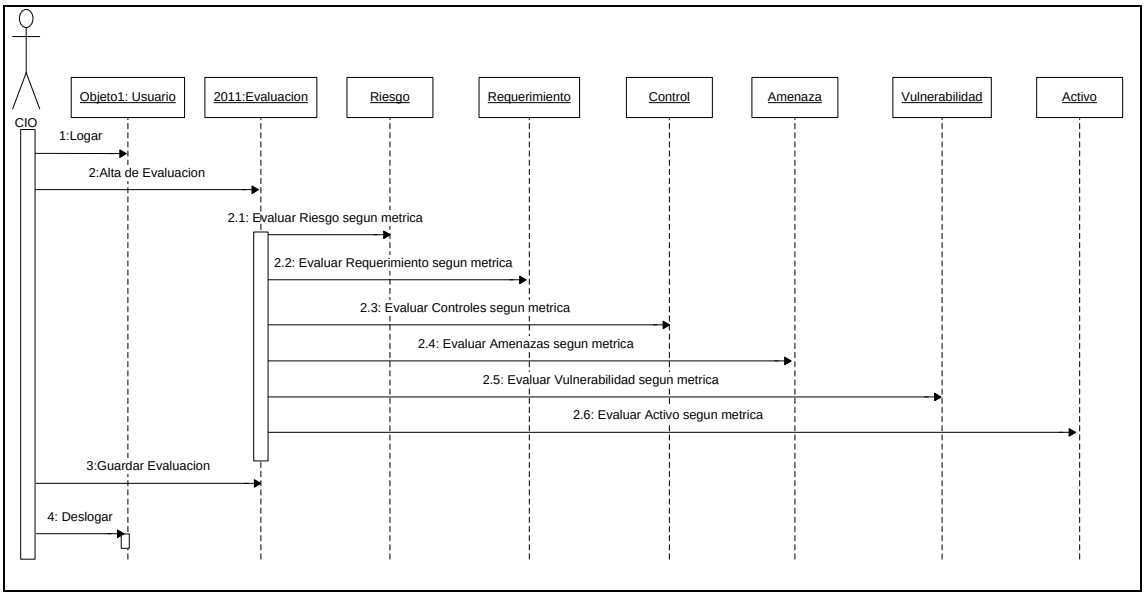


Figura 52. Diagrama de Secuencia. Alta de Evaluación

6.3 Diagrama de estados

Para mostrar de una manera más clara las rutas o caminos que puede tomar el usuario dentro de una clase se han hecho los siguientes diagramas de estados:

- El siguiente diagrama de estados corresponde a la activación de un riesgo. Representa el ciclo de vida de un riesgo desde su registro mediante un activo o amenaza o vulnerabilidad, relacionándolo con los requerimientos que asume, los controles y políticas que se establecen, y quizás crear políticas para controles o crear controles para políticas, junto con el plan de seguimiento y mejora continua. También se muestra su ciclo de Aceptación, Evaluación y Priorización.

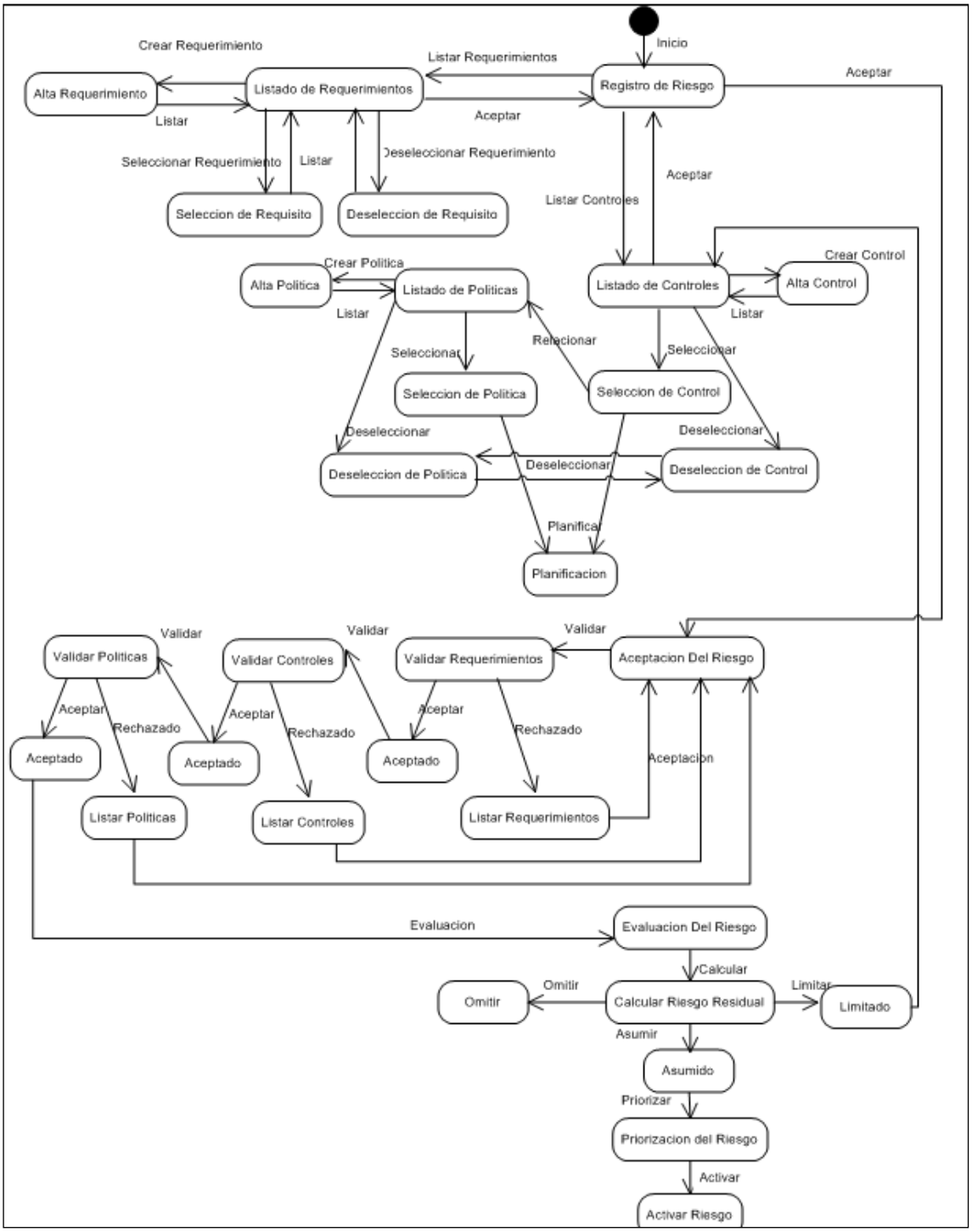


Figura 53. Diagrama de Estados. Alta de Riesgo

- El siguiente diagrama de estados corresponde a la creación de un Activo. Representa el ciclo de vida de un activo desde su registro, con los servicios y acuerdos de nivel de servicio que asume, hasta la asociación con los riesgos, vulnerabilidades y amenazas con los que se relaciona.

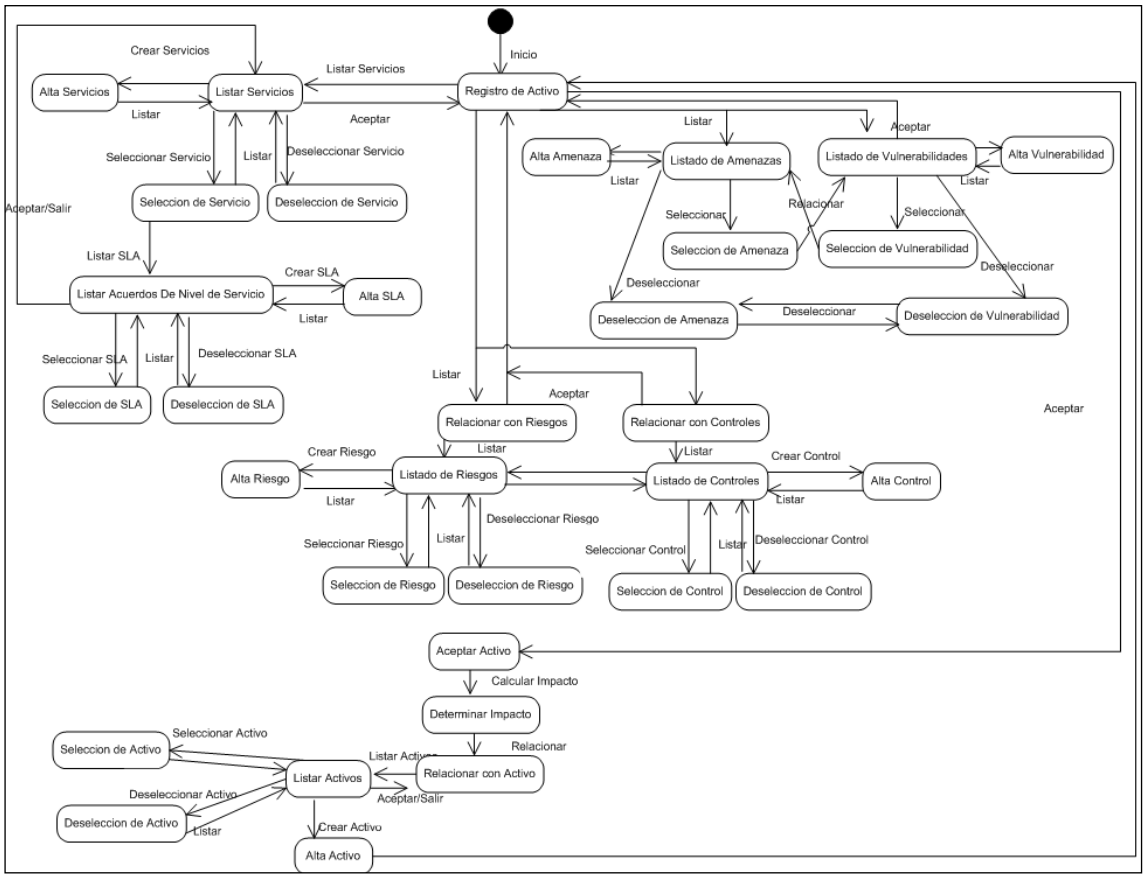


Figura 54. Diagrama de Estados. Alta de Activo

- El siguiente diagrama de estados corresponde a un caso de alta de control sin estar relacionado inicialmente con ningún riesgo. Se muestra las relaciones del control con los riesgos y políticas asociadas, junto con la planificación y las operaciones propias del control como son la valoración económica y priorización hasta el estado pendiente de implementar.

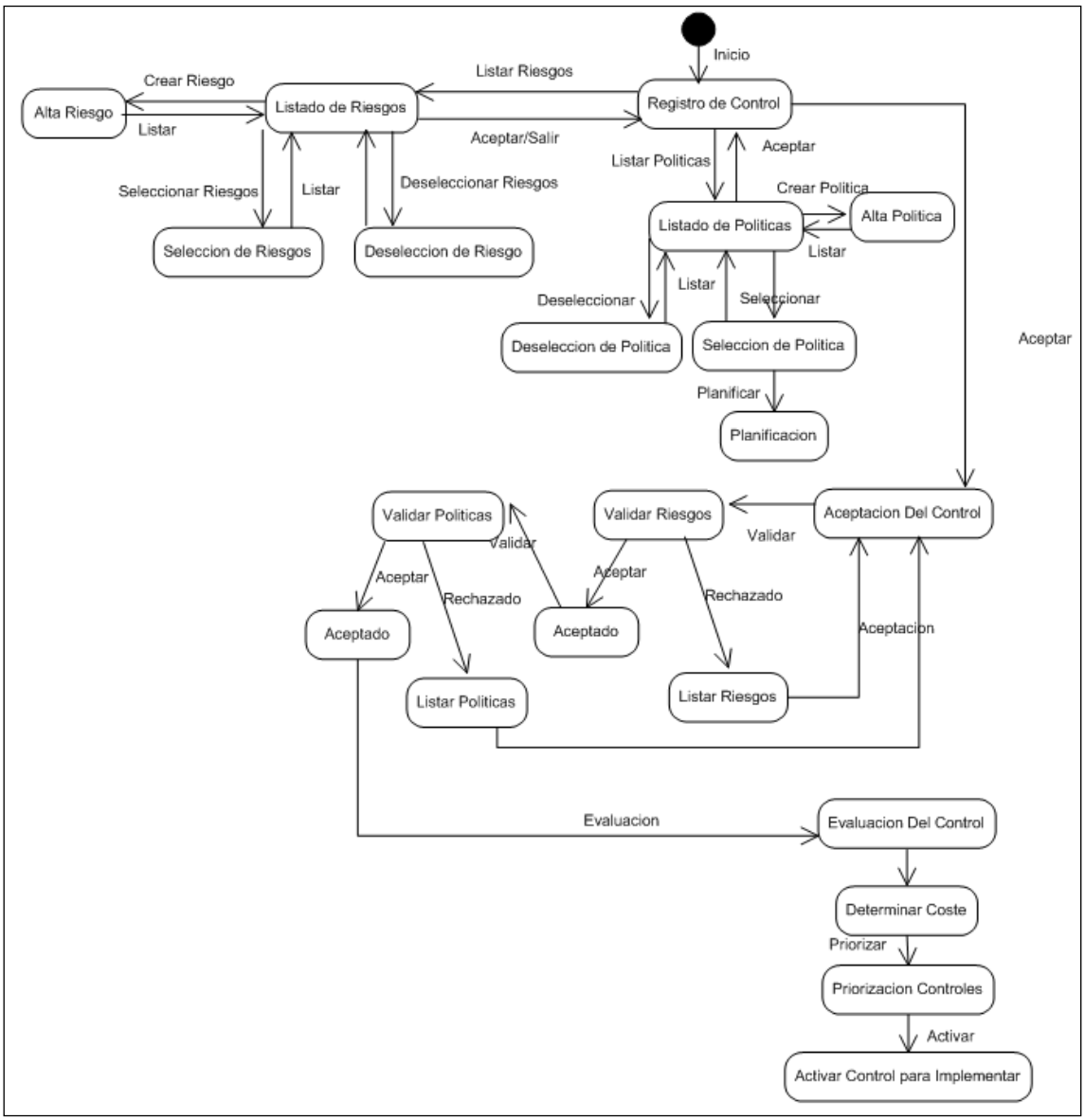


Figura 55. Diagrama de Estados. Alta de control

- El siguiente diagrama de estados corresponde a la casuística de activación de los controles una vez implementados y las actualizaciones de seguridad que se realizan con las áreas relacionadas.

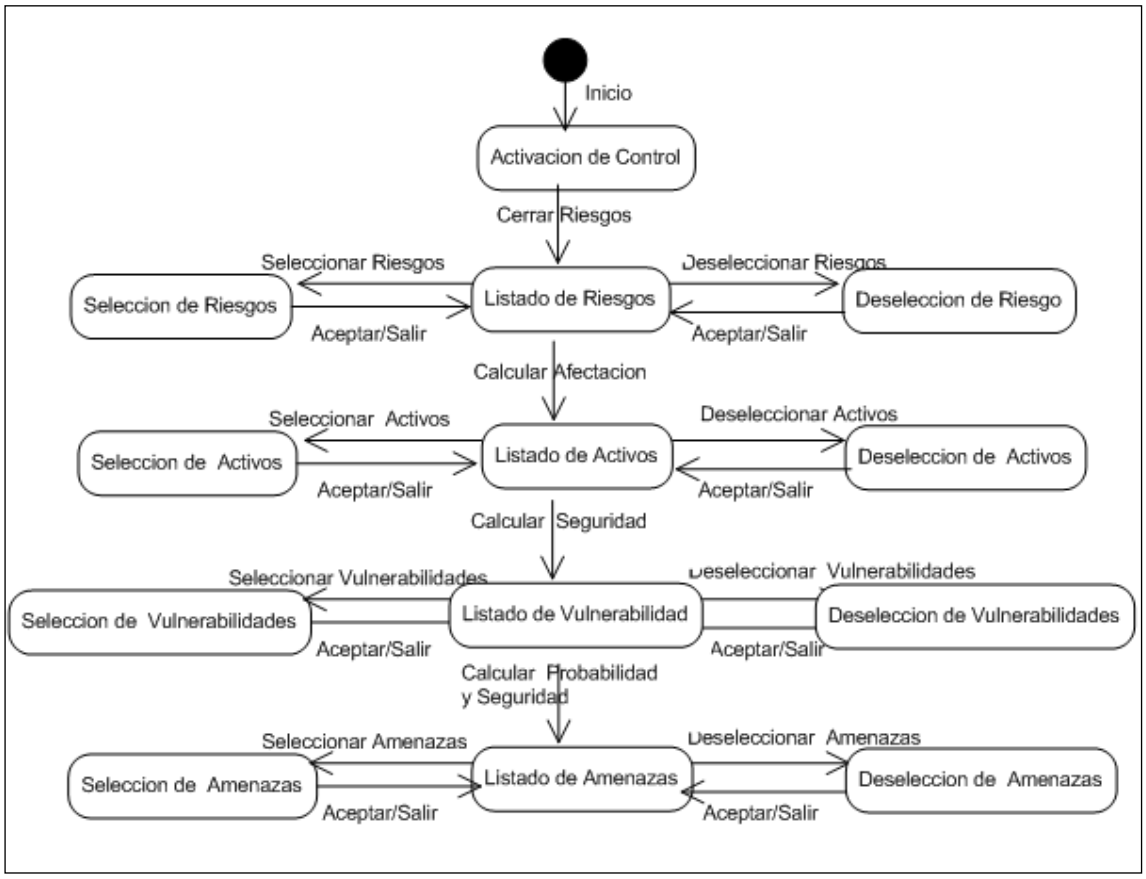


Figura 56. Diagrama de Estados. Activación de Control

-El siguiente diagrama de estados corresponde a la resolución de una incidencia. Representa el ciclo de vida de una incidencia desde su registro, con los activos y vulnerabilidades afectadas, y con los riesgos y controles que ocasiona. Hasta la resolución de la incidencia mediante la asociación de todos los controles asociados a los riesgos que implica.

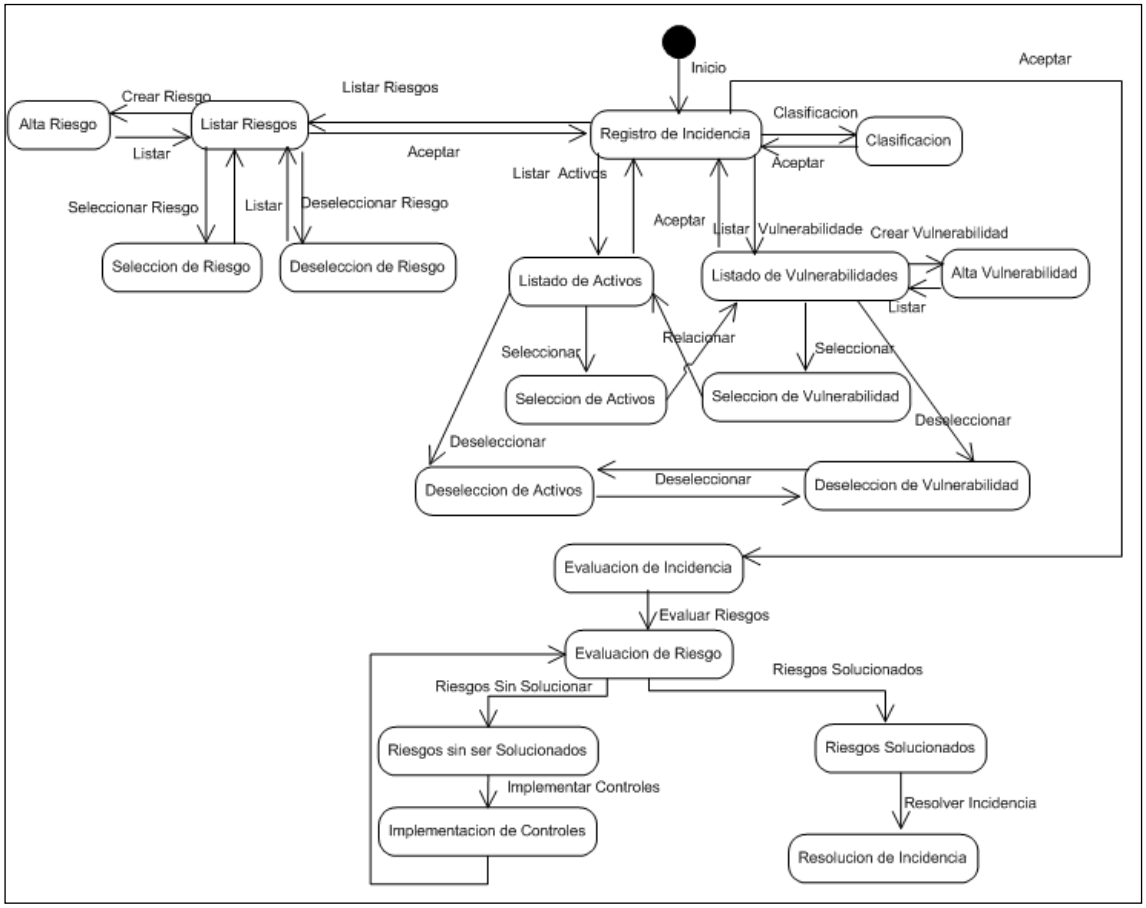


Figura 57. Diagrama de Estados. Ciclo de Vida de una Incidencia

-El siguiente diagrama de estados corresponde a la realización de una evaluación. Representa el ciclo de vida de una evaluación para una fecha programada, en la cual se establece la aplicación de métricas para todas las áreas del sistema y sus relaciones, y como se trataría la evaluación de estas métricas.

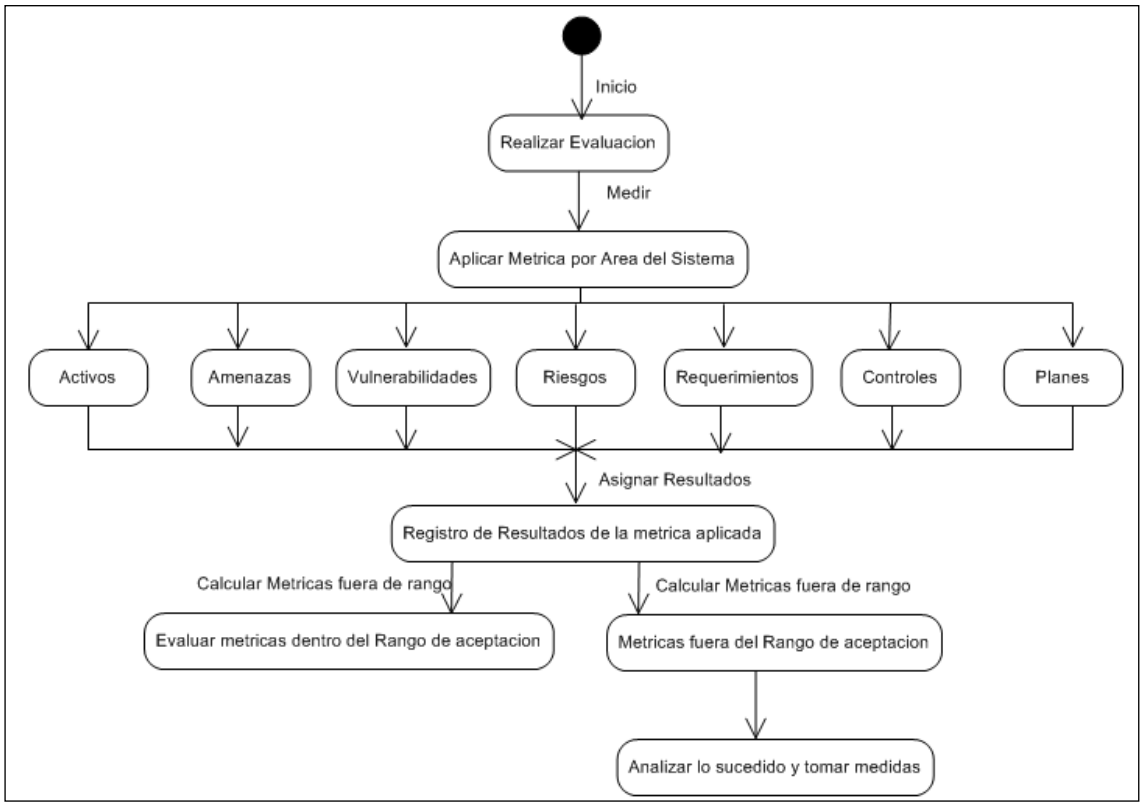


Figura 58. Diagrama de Estados. Ciclo de Vida de una Evaluación

6.4 Diagrama de base de datos

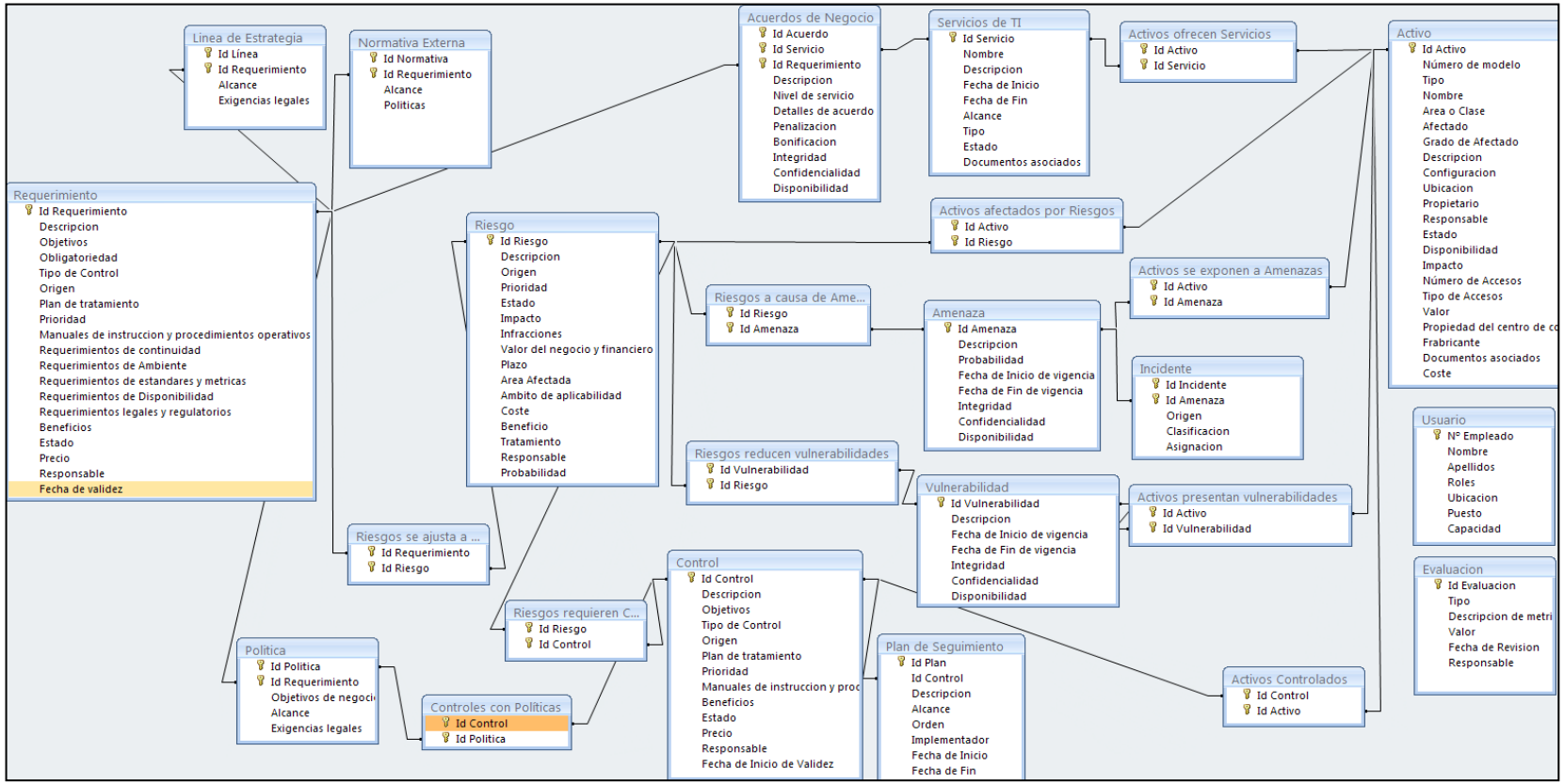


Figura 59. Diagrama de base de datos

7 MODELO DE SIMULACIÓN GOBIERNO DE LA SEGURIDAD TI

En los modelos de gobierno es positivo el empleo de herramientas de simulación que permitan prever el funcionamiento de las propuestas antes de incurrir en costes. La simulación es una técnica imprescindible en el área del Gobierno de la Seguridad TI puesto que se deben tener en cuenta múltiples variables internas y del entorno que, si se consideran erróneamente, pueden provocar importantes pérdidas para la organización en entornos sujetos a vertiginosos cambios donde las organizaciones TI han de llevar a cabo cambios importantes. La forma de ejecutar el modelo de simulación es mediante la creación de escenarios que permitan determinar el correcto reglaje de los controles que dan respuesta a las amenazas y a las vulnerabilidades de las áreas de activos de nuestra organización.

Los modelos de simulación son esenciales en cualquier proceso de planificación estratégica de la seguridad TI dado que se trabaja con incertidumbres en la predicción del futuro y en entornos afectados por muchas variables, generalmente con una evolución desconocida. Dentro de estas variables que afectan a las decisiones de cualquier departamento de TI se encuentran: variables externas que afectan a la seguridad (regulaciones, amenazas, conocimiento en nuevas tecnologías, experiencia fuerza laboral tecnológica, etc), variables de decisión interna de las áreas funcionales de la empresa (políticas adoptadas, requisitos de seguridad, etc) y variables de decisión internas al departamento de TI (procesos de negocio a cubrir, grado de subcontratación TI, seguridad del software adquirido, etc).

Un modelo es una representación simplificada de un sistema en un momento determinado de tiempo con el que se pretende facilitar el entendimiento del sistema real. Los modelos son requeridos cuando tratamos con múltiples variables, que se relacionan con otras variables, con posibilidades de retardos y formulas y, además, presentan retroalimentación. Las retroalimentaciones y retardos impiden solucionar este tipo de problemas con ecuaciones matemáticas. Con el modelo se permite simular diferentes escenarios de una forma rápida y ágil, sin incurrir en costes y prediciendo situaciones adversas que se puedan producir en un futuro. Asimismo, la utilización de modelos para el Gobierno de la Seguridad TI permite abrir un fructífero debate entre todos los numerosos participantes, que sin la existencia del modelo no se produciría.

7.1 Metodología seguida en el modelo de simulación.

En general, los modelos de simulación dinámica se componen de cinco pasos (parecido al ciclo de mejora continua de Deming), tal y como se muestra en la figura adjunta:

1. **Definición del problema:** Cuál es el problema que refleja la situación que se quiere modelar para predecir el futuro. En esta etapa se limita el alcance y se deciden las variables más importantes a medir. Para ello se toma como información de partida los factores críticos de cambio (FCC) de la etapa de valoración de opciones estratégicas.

2. **Establecer diferentes escenarios dinámicos:** En esta etapa, y de acuerdo a las tendencias tecnológicas, la información histórica, las debilidades de la organización y el conocimiento del sector de las personas que están modelando (recogidas en los FCC), se procederá a definir diferentes grupos de variables de entrada cuyas salidas a través de la ejecución del modelo se deben conocer. Se define un escenario como una imagen creíble de un posible futuro entorno en el que nuestra organización TI tiene que operar.

3. **Formulación y generación del modelo:** Para la selección de variables del modelo de simulación se ha partido del diseño conceptual y funcional mostrado en los apartados anteriores. También se requiere realizar un análisis de las principales variables de la organización y del entorno a modelar. Tras la definición de la lista completa de variables se procede a la hora de cargar datos de entrada para simular, seleccionar las más importantes según los FCC de la etapa de valoración de opciones estratégicas de seguridad TI y a clasificarlas como variables de nivel y variables auxiliares de acuerdo a la metodología de modelado dinámico.

4. **Confirmación con evidencias:** La calidad de los modelos de simulación viene dada por la capacidad de reproducir la realidad lo mejor posible, y para ello es necesario ajustar las primeras versiones del modelo para la correcta predicción de las tendencias. Tras la última confirmación de la simulación se pueden traducir los resultados de la simulación en objetivos estratégicos de seguridad TI y en la fijación de las estrategias básicas para la consecución de los objetivos estratégicos.

5. **Propuesta de nuevas mejoras:** Incorporar las propuestas en el modelo y proceder a realizar de nuevo el proceso hasta la consecución del ajuste esperado.

7.2 Funcionamiento del Modelo Propuesto

El modelo propuesto es una versión simplificada del diseño propuesto. Los modelos de simulación por propia definición han de ser versiones simplificadas de los artefactos.

Tal y como se observa en la figura adjunta el modelo tiene dos vistas diferenciadas

- **Vista del cálculo del riesgo residual:** Al igual que propone el diseño propuesto, por área de activo y a partir de las amenazas y vulnerabilidades y del impacto (por afectar a usuarios o por el valor de los activos) el modelo calcula un nivel de riesgos. Tras aplicar los controles el modelo dispone de un nivel de riesgo residual. De manera simplificada el modelo dispone de áreas de activos en desarrollo y de áreas de activos en operación El motivo es que los tipos de activos afectados son muy diferentes e interactúan de manera muy diferenciada. Los activos en desarrollo incorporan riesgos en ejecución que afectan a la productividad del diseño y a la productividad del desarrollo (programación y configuración) y a la aleatoriedad de esta productividad. Por contra los activos en operación su impacto se restringe a impactos en la disponibilidad y a la continuidad, y por ende al porcentaje de puntos función que están en incidentes y problemas o a los puntos función que están en operación.
- **Vista del impacto en el funcionamiento de los sistemas de información:** Un modelo dinámico que trate el avance de los puntos función de los sistemas de información entre las diferentes fases (planificación, diseño, desarrollo, prueba y operación) es esencial para determinar el impacto en plazos y en coste de un nivel de Gobierno de la Seguridad.

Carga de clases de amenazas en el modelo de simulación

CLASE DE AMENAZA / ÁREA DE ACTIVO	EXTENDED ERP& WEB APPLICATIONS IN DEVELOPMENT	MAINFRAME AND SERVERS	NETWORK	EXTENDED ERP	WEB APPLICATIONS
Daños físicos: Incendio, inundación, vandalismo, pérdida de potencia y los desastres naturales.	2				
La interacción humana: Acción intencional o accidental u omisión que pueden interrumpir la productividad y/ o disponibilidad.	3				
Mal funcionamiento de equipos: El fallo de sistemas y dispositivos periféricos.	4				
Ataques internos o externos: Hacking, cracking, and attacking.	5				
El uso incorrecto de datos: Compartiendo secretos comerciales; espionaje, fraude, y el robo.	3				
La pérdida de datos: La pérdida intencional o no intencional de la información a través de medios destructivos.	3				
Error de aplicación: Errores de cómputo, errores de entrada, y	4				

desbordamientos de búfer.					

0 – Nulo, 1 bajo 2- medio 3- Medio alto 4 Alto 5 Muy Alto

1. Controles en Política de Seguridad
2. Controles en Organización de Seguridad de la Información
3. Controles en Gestión de Activos
4. Controles en Seguridad de Recursos Humanos
5. Controles en Seguridad Física y Medioambiental
6. Controles en Gestión de comunicaciones y operaciones
7. Controles en Acceso
8. Controles en Sistemas de Información en producción, desarrollo y mantenimiento
9. Controles en Gestión de Incidentes de Seguridad de la Información
10. Controles en Gestión de Continuidad del negocio
11. Controles en Cumplimiento

0 – Nulo, 1 bajo 2- medio 3- Medio alto 4 Alto 5 Muy Alto

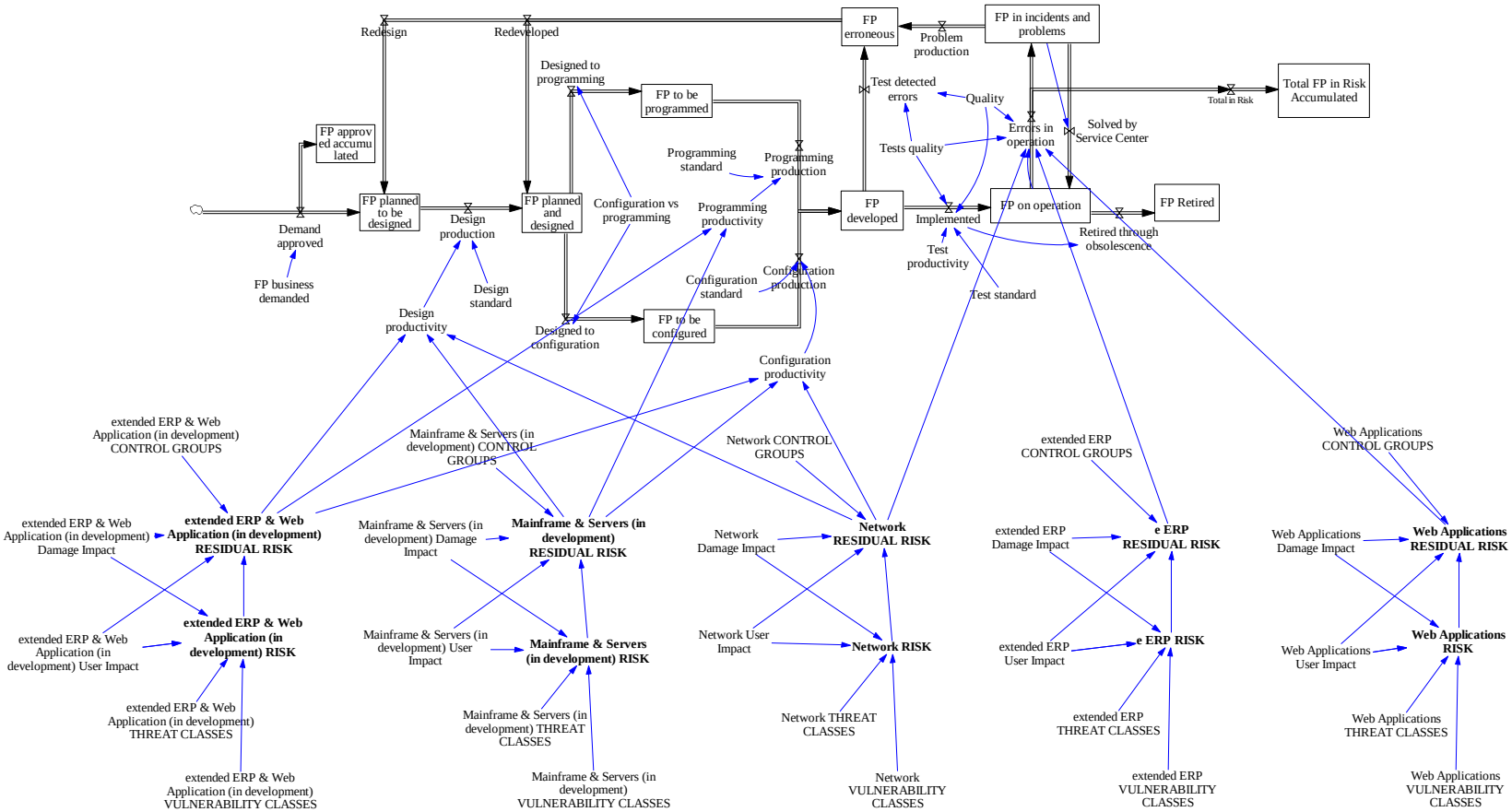


Figura 60. Modelo de Simulación empleado para el Gobierno de la Seguridad TI

8 ANÁLISIS ECONÓMICO

8.1 Plan de Trabajo

A continuación, se muestran las actividades realizadas durante el desarrollo de este proyecto, así como los recursos que han intervenido en ellas y la duración de cada una.

Para comprenderlas mejor este punto se desglosará en:

- → El WBS (Work Breakdown Structure), que ayuda a controlar que no se olvide ninguna actividad.
- → El PBS (Product Breakdown Structure), que representa los productos a obtener a lo largo del desarrollo del proyecto, asociándolos a la actividad correspondiente.
- → RBS (Resource Breakdown Structure), que muestra los recursos que intervienen en el proyecto.
- → Cronograma, en él se muestra el diagrama de Gantt asociado al proyecto. Se muestra tanto el planificado como el real.

8.1.1 WBS

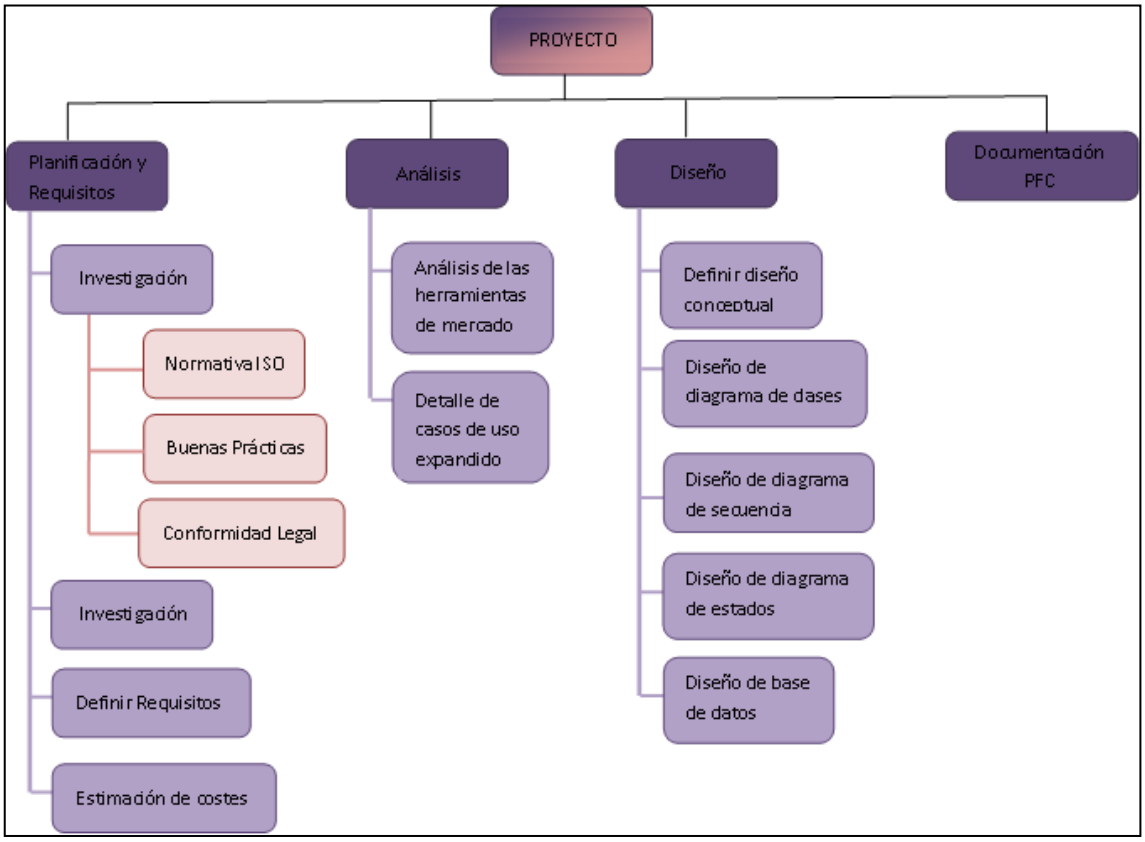


Figura 61. WBS (Work Breakdown Structure)

8.1.2 PBS

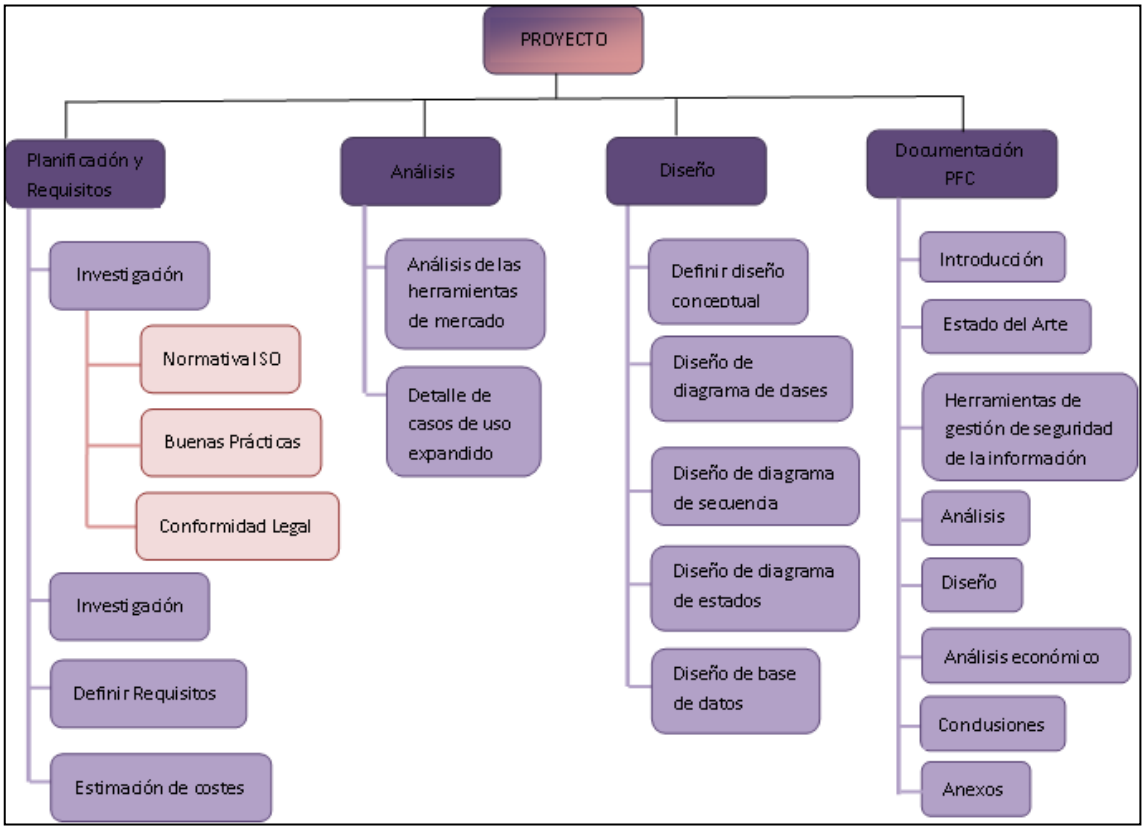


Figura 62. PBS (Product Breakdown Structure)

8.1.3 RBS

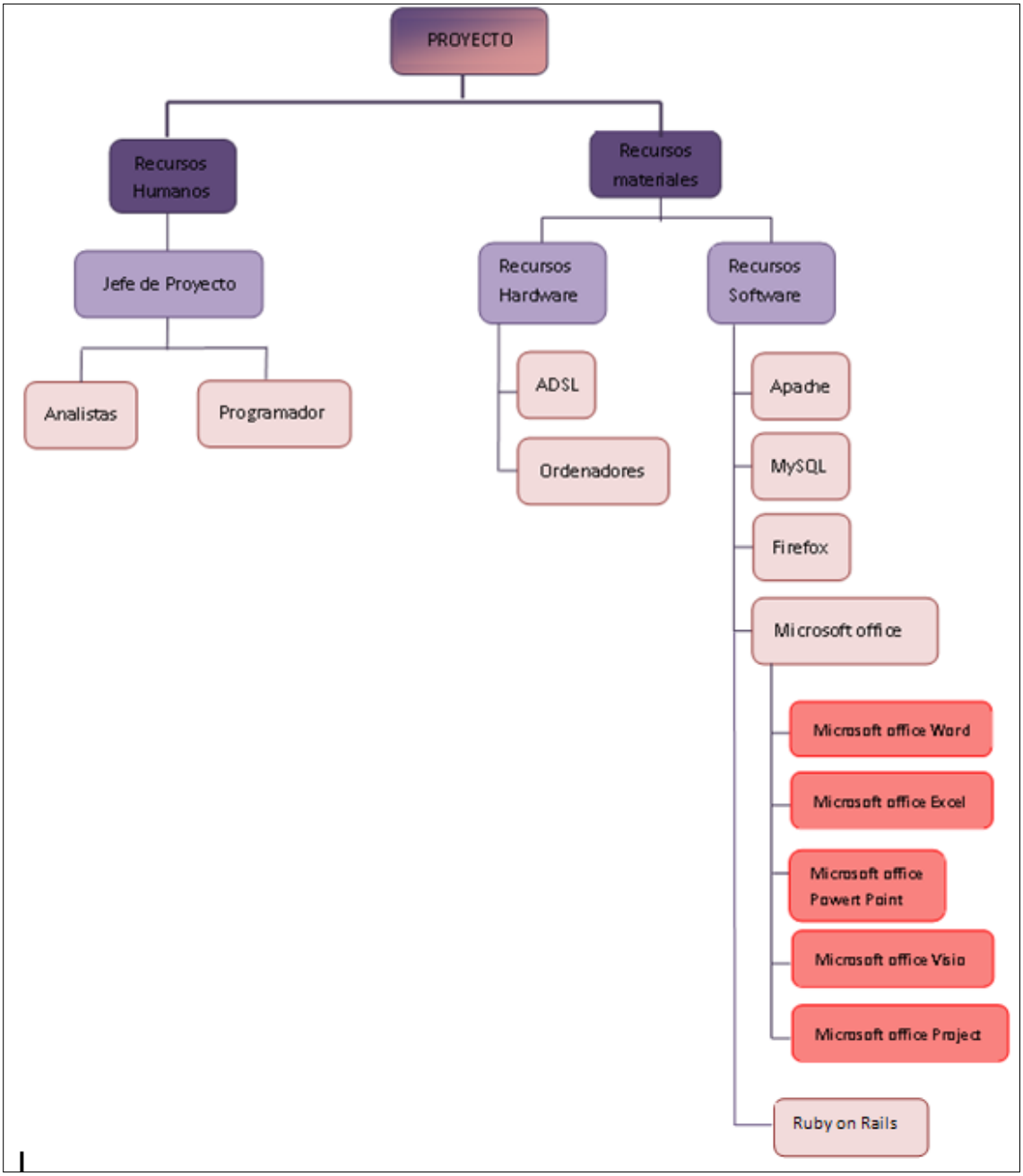


Figura 63. RBS (Resource Breakdown Structure)

8.1.4 Planificación del proyecto. Cronograma Planificado

A continuación se muestra el gráfico del resultado del diagrama Gantt planificado:

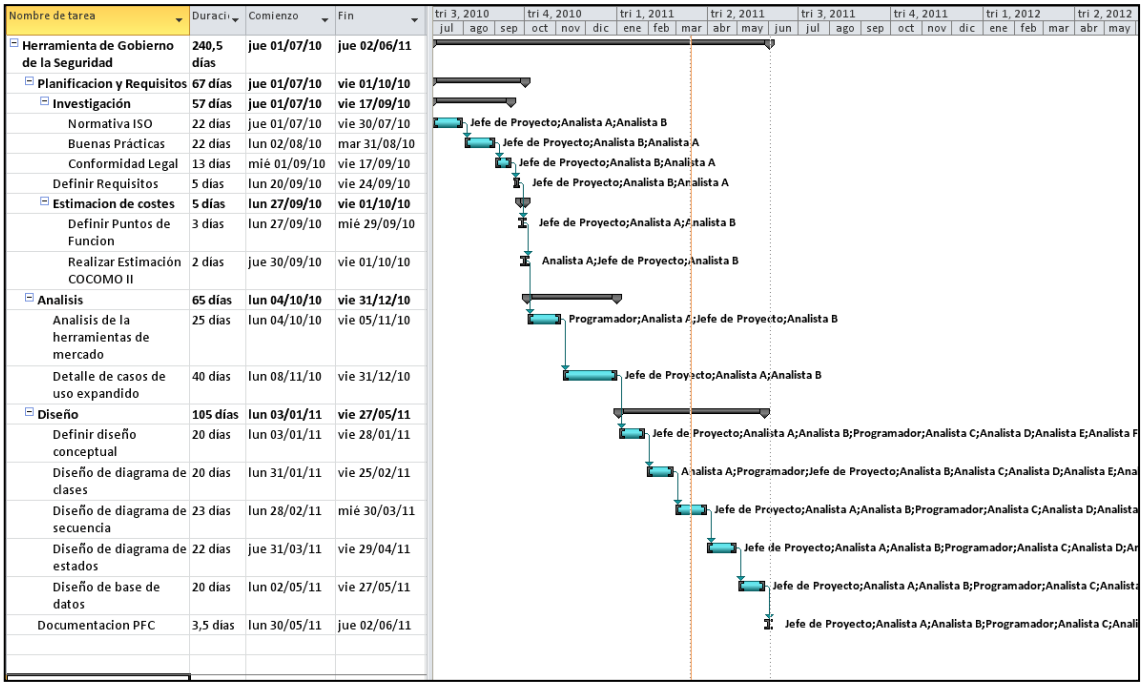


Figura 64. Cronograma Planificado

8.1.5 Planificación del proyecto real. Cronograma Real

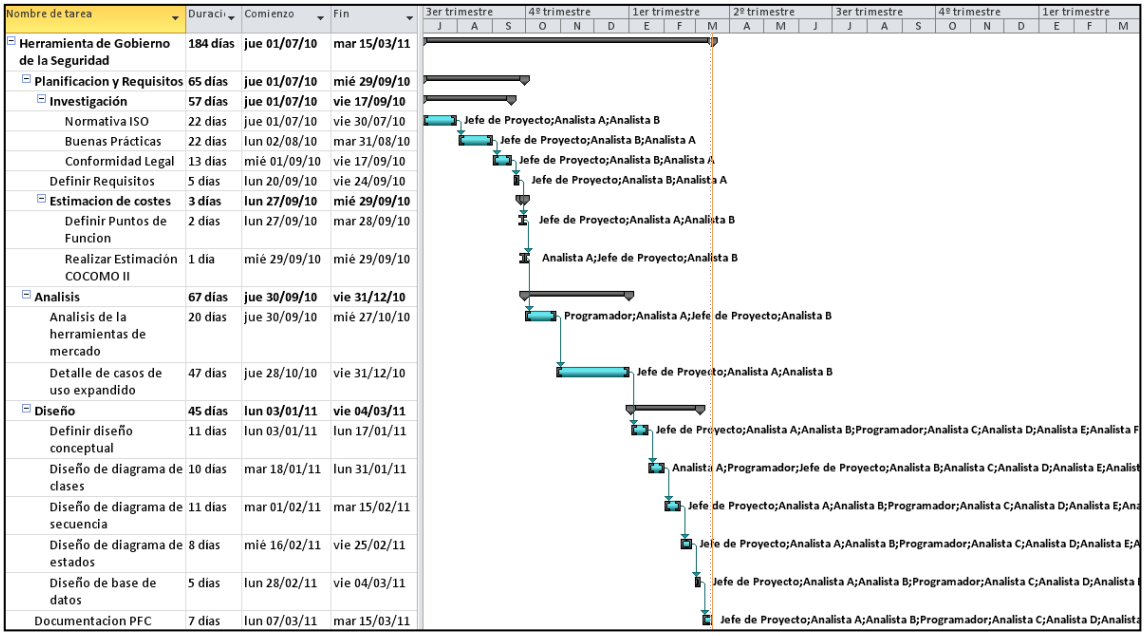


Figura 65. Cronograma real

8.2 Calculo de puntos de función de Albretch

La métrica del punto función es un método utilizado en ingeniería del software para medir el tamaño del software. Fue definida por Allan Albrecht y pretende medir la funcionalidad entregada al usuario independientemente de la tecnología utilizada para la construcción y puesta en marcha del software. Este método es útil en cualquiera de las fases del ciclo de vida del software, desde el diseño hasta el mantenimiento. (www.wikipedia.org).

Primero se van a clasificar todos los almacenes y procesos del sistema según los criterios que define este método y se va a calcular la complejidad de cada almacén y proceso.

8.2.1 Almacenes

Hay dos tipos de almacenes:

Ficheros lógicos Internos (ILF Internal Logic File).

Ficheros lógicos Externos (EIF External Logic File).

Para el cálculo de la complejidad de los almacenes hay que tener en cuenta dos cosas:

DET (tipo de elemento dato): Se identifican porque cada campo es único, no recursivo y reconocible por el usuario, se cuenta un DET por cada dato que exista en un almacén.

RET (tipo de elemento registro): Se cuenta un RET por cada grupo de DET además de contar uno por defecto siempre.

Ficheros lógicos Internos (ILF Internal Logic File): Es un grupo de datos relacionados, identificables por los usuarios o información de control mantenidos y utilizados dentro de los límites de la aplicación.

A continuación se enumeran los DET, RET y la complejidad de cada almacén:

Activo			
DET	RET	Tipo	Complejidad
Id de Activos	IdentificadorAct		
Número de modelo	RetDefectoAct		
Nombre			
Afectado			
Grado de Afectado			
Descripción			
Configuración			
Ubicación			
Propietario			
Responsable		ILF	Baja
Estado			
Propiedad del centro de costo			
Fabricante			
Documentos asociados			
Disponibilidad	RetSeguridadAct		

Impacto			
Número de Accesos			
Tipo de Accesos			
Valor			
Coste			
Área o Clase	RetClasificacion		
Tipo			
TOTAL DET: 22	TOTAL RET: 4		

Activos se exponen a Amenazas			
DET	RET	Tipo	Complejidad
Id Activo	Identificador	ILF	Baja
Id Amenaza	ActAme		
TOTAL DET: 2	TOTAL RET: 1		

Activos afectados por Riesgos			
DET	RET	Tipo	Complejidad
Id Activo	Identificador	ILF	Baja
Id Riesgo	ActRie		
TOTAL DET: 2	TOTAL RET: 1		

Activos Controlados

DET	RET	Tipo	Complejidad
Id Control	Identificador	ILF	Baja
Id Activo	ActCont		
TOTAL DET: 2	TOTAL RET: 1		

Activos ofrecen Servicios			
DET	RET	Tipo	Complejidad
Id Activo	Identificador	ILF	Baja
Id Servicio	ActSer		
TOTAL DET: 2	TOTAL RET: 1		

Activos presentan vulnerabilidades			
DET	RET	Tipo	Complejidad
Id Activo	Identificador	ILF	Baja
Id Vulnerabilidad	ActVul		
TOTAL DET: 2	TOTAL RET: 1		

Acuerdos de Negocio			
DET	RET	Tipo	Complejidad
Id Acuerdo	Identificador	ILF	Baja
Id Servicio	AcuSerReq		
Id Requerimiento			
Descripción	RetDefectoAcu		
Nivel de servicio			
Detalles de acuerdo			
Penalización			
Bonificación			
Integridad	RetSeguridad		
Confidencialidad	Acu		
Disponibilidad			
TOTAL DET: 11	TOTAL RET: 3		

Amenaza			
DET	RET	Tipo	Complejidad
Id Amenaza	Identificador Ame	ILF	Baja
Descripción	RetDefectoAcu		
Probabilidad			
Fecha de Inicio de vigencia			
Fecha de Fin de			

vigencia			
Integridad	RetSeguridad		
Confidencialidad	Ame		
Disponibilidad			
TOTAL DET: 8	TOTAL RET: 3		

Control			
DET	RET	Tipo	Complejidad
Id Control	Identificador Con	ILF	Baja
Descripción	RetDefectoCon		
Objetivos			
Tipo de Control			
Origen			
Plan de tratamiento			
Prioridad			
Manuales de instrucción y procedimientos operativos			
Beneficios			
Estado			
Precio			
Responsable			
Fecha de Inicio de	RetFechActivaci		

Validez	onCon		
TOTAL DET: 13	TOTAL RET: 3		

Controles con Políticas			
DET	RET	Tipo	Complejidad
Id Control	Identificador	ILF	Baja
Id Política	ConPol		
TOTAL DET: 2	TOTAL RET: 1		

Evaluación			
DET	RET	Tipo	Complejidad
Id Evaluación	Identificador Eva	ILF	Baja
Tipo	RetDefectoEva		
Descripción de métricas			
Valor			
Responsable			
Fecha de Revisión	RetFechActivacionEva		
TOTAL DET: 6	TOTAL RET: 3		

Línea de Estrategia			
DET	RET	Tipo	Complejidad
Id Línea	Identificador		

Id Requerimiento	LinReq	ILF	Baja
Alcance	RetDefectoLin		
Exigencias legales			
TOTAL DET: 4	TOTAL RET: 2		

Normativa Externa			
DET	RET	Tipo	Complejidad
Id Normativa	Identificador	ILF	Baja
Id Requerimiento	NorReq		
Alcance	RetDefectoPol		
Políticas			
TOTAL DET: 4	TOTAL RET: 2		

Plan de Seguimiento			
DET	RET	Tipo	Complejidad
Id Plan	Identificador	ILF	Baja
Id Control	PlaCon		
Descripción	RetDefectoPla		
Alcance			
Orden			
Implementador			
Fecha de Inicio	RetFechasPla		
Fecha de Fin			

Estado			
TOTAL DET: 9	TOTAL RET: 3		

Política			
DET	RET	Tipo	Complejidad
Id Política	Identificador		
Id Requerimiento	PolReq		
Objetivos de negocio	RetDefectoPol	ILF	Baja
Alcance			
Exigencias legales			
TOTAL DET: 5	TOTAL RET: 2		

Requerimiento			
DET	RET	Tipo	Complejidad
Id Requerimiento	Identificador Req		
Descripción	RetDefectoReq		
Objetivos			
Obligatoriedad			
Tipo de Control			
Origen			
Plan de tratamiento			
Prioridad			

Manuales de instrucción y procedimientos operativos		ILF	Baja
Requerimientos de continuidad			
Requerimientos de Ambiente			
Requerimientos de estándares y métricas			
Requerimientos de Disponibilidad			
Requerimientos legales y regulatorios			
Beneficios			
Precio			
Responsable			
Fecha de validez	RetFechaReq		
Estado			
TOTAL DET: 19	TOTAL RET: 3		

Riesgo			
DET	RET	Tipo	Complejidad
Id Riesgo	Identificador Rie		
Descripción			
Origen			
Prioridad			

Estado	RetDefectoRie	ILF	Baja
Impacto			
Infracciones			
Valor del negocio y financiero			
Plazo			
Área Afectada			
Ámbito de aplicabilidad			
Coste			
Beneficio			
Tratamiento			
Responsable			
Probabilidad			
TOTAL DET: 16	TOTAL RET: 2		

Riesgos a causa de Amenazas			
DET	RET	Tipo	Complejidad
Id Riesgo	Identificador	ILF	Baja
Id Amenaza	RieAme		
TOTAL DET: 2	TOTAL RET: 1		

Riesgos reducen vulnerabilidades			
DET	RET	Tipo	Complejidad

Id Vulnerabilidad	Identificador	ILF	Baja
Id Riesgo	RieVul		
TOTAL DET: 2	TOTAL RET: 1		

Riesgos requieren Controles			
DET	RET	Tipo	Complejidad
Id Riesgo	Identificador	ILF	Baja
Id Control	RieCon		
TOTAL DET: 2	TOTAL RET: 1		

Riesgos se ajusta a Requerimiento			
DET	RET	Tipo	Complejidad
Id Requerimiento	Identificador	ILF	Baja
Id Riesgo	RieReq		
TOTAL DET: 2	TOTAL RET: 1		

Servicio de TI			
DET	RET	Tipo	Complejidad
Id Servicio	Identificador Ser	ILF	Baja
Nombre	RetDefectoSer		
Descripción			
Alcance			
Tipo			

Documentos asociados			
Fecha de Inicio	RetFechaSer		
Fecha de Fin			
Estado			
TOTAL DET: 9	TOTAL RET: 3		

Usuario			
DET	RET	Tipo	Complejidad
Nº Empleado	Identificador Emp	ILF	Baja
Nombre	RetDefectoEmp		
Apellidos			
Roles			
Ubicación			
Puesto			
Capacidad			
TOTAL DET: 7	TOTAL RET: 2		

Vulnerabilidad			
DET	RET	Tipo	Complejidad
Id Vulnerabilidad	Identificador Vul	ILF	Baja
Descripción	RetDefectoEmp		
Integridad	RetSeguridad		

Confidencialidad	Vul		
Disponibilidad			
Fecha de Inicio de vigencia	RetFechaVul		
Fecha de Fin de vigencia			
TOTAL DET: 7	TOTAL RET: 4		

Ficheros de Interfaz Externos (EIF External Logic File): Es un grupo de datos relacionados, identificables por el usuario o información de control utilizada por la aplicación, pero mantenida por otro sistema.

A continuación se detalla el único almacén que cumplen con estas características:

Incidente			
DET	RET	Tipo	Complejidad
Id Incidente	Identificador	ILF	Baja
Id Amenaza	IncAme		
Origen	RetDefectoInc		
Clasificación			
Asignación			
TOTAL DET: 5	TOTAL RET: 2		

8.2.2 Procesos

Hay tres tipos de procesos:

Entrada externa (EI External Input).

Salida Externa (EO External Output).

Consulta (EQ External Query).

Para el cálculo de las complejidades de los procesos hay que tener en cuenta dos cosas:

DET (tipo de elemento dato): Se cuenta un DET por cada dato que exista en un EI.

FTR (tipo de fichero referenciado): Número de accesos a los almacenes cuando se procesa una transacción.

Entrada externa (EI External Input): Datos o información de control que se introduce en la aplicación desde fuera de sus límites.

Salida Externa (EO External Output): Datos o información de control que sale de los límites de la aplicación.

A continuación, se detallan todas las entradas y salidas externas:

	Alta de Activo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Número de modelo	Id Activo		
	Nombre	OK/Error		
	Afectado			
	Grado de Afectado			
	Descripción			
	Configuración			
	Ubicación			
	Propietario			
	Responsable		EI/EO	BAJA
	Estado			
	Propiedad del centro de costo			
	Fabricante			
	Documentos asociados			
	Disponibilidad			
	Impacto			
	Número de Accesos			
	Tipo de Accesos			
	Valor			
	Coste			

	Área o Clase			
	Tipo			
	TOTAL: 21	TOTAL: 2		
FTR	Activo	Activo		
	TOTAL:1	TOTAL:1		

	Modificar Activo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Número de modelo	OK/Error		
	Nombre			
	Afectado			
	Grado de Afectado			
	Descripción			
	Configuración			
	Ubicación			
	Propietario			
	Responsable		EI/EO	Baja
	Estado			
	Propiedad del centro de costo			
	Fabricante			
	Documentos asociados			

	Disponibilidad			
	Impacto			
	Número de Accesos			
	Tipo de Accesos			
	Valor			
	Coste			
	Área o Clase			
	Tipo			
	TOTAL: 21	TOTAL: 1		
FTR	Activo			
	TOTAL:1	TOTAL: 0		

	Eliminar Activo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Activo			
	TOTAL:1	TOTAL: 0		

	Alta de Activos se exponen a Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Amenaza	Id Amenaza	EI/EO	BAJA
	Id Activo	Id Activo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Activos	Activos se exponen a Amenazas		
	Amenaza			
	TOTAL:2	TOTAL: 1		

	Eliminar Activos se exponen a Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Amenaza		EI	BAJA
	Id Activo			
	TOTAL: 2	TOTAL: 0		
FTR	Activos se exponen a Amenazas			
	TOTAL:1	TOTAL: 0		

	Alta de Activos afectados por Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EI/EO	BAJA
	Id Activo	Id Activo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Activo	Activos afectados por Riesgos		
	Riesgo			
	TOTAL:2	TOTAL: 1		

	Eliminar Activos afectados por Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo		EI	BAJA
	Id Activo			
	TOTAL: 2	TOTAL: 0		
FTR	Activos afectados por Riesgos			
	TOTAL:1	TOTAL: 0		

	Alta de Activos Controlados		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control	Id Control	EI/EO	BAJA
	Id Activo	Id Activo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Activo	Activos Controlados		
	Control			
	TOTAL:2	TOTAL: 1		

	Eliminar Activos Controlados		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control		EI	BAJA
	Id Activo			
	TOTAL: 2	TOTAL: 0		
FTR	Activos Controlados			
	TOTAL:1	TOTAL: 0		

	Alta de Activos ofrecen Servicios		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Servicio	Id Servicio	EI/EO	BAJA
	Id Activo	Id Activo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Activo	Activos ofrecen Servicios		
	Servicio			
	TOTAL:2	TOTAL: 1		

	Eliminar Activos ofrecen Servicios		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Servicio		EI	BAJA
	Id Activo			
	TOTAL: 2	TOTAL: 0		
FTR	Activos ofrecen Servicios			
	TOTAL:1	TOTAL: 0		

	Alta de Activos presentan vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Vulnerabilidad	Id Vulnerabilidad	EI/EO	BAJA
	Id Activo	Id Activo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Activo	Activos ofrecen Servicios		
	Vulnerabilidad			
	TOTAL:2	TOTAL: 1		

	Eliminar Activos presentan vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Vulnerabilidad		EI	BAJA
	Id Activo			
	TOTAL: 2	TOTAL: 0		
FTR	Activos presentan vulnerabilidades			
	TOTAL:1	TOTAL: 0		

	Alta de Acuerdo de Negocio		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Acuerdo	EI/EO	Baja
	Nivel de servicio	OK/Error		
	Detalles de acuerdo			
	Penalización			
	Bonificación			
	Integridad			
	Confidencialidad			
	Disponibilidad			
	TOTAL: 8	TOTAL: 2		
FTR	Acuerdo de Negocio	Acuerdo de Negocio		
	TOTAL:1	TOTAL:1		

	Modificar Acuerdo de Negocio		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error	EI/EO	Baja
	Nivel de servicio			
	Detalles de acuerdo			
	Penalización			
	Bonificación			
	Integridad			

	Confidencialidad			
	Disponibilidad			
	TOTAL: 8	TOTAL: 1		
FTR	Acuerdo de Negocio			
	TOTAL:1	TOTAL: 0		

	Eliminar Acuerdo de Negocio		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Acuerdo		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Acuerdo de Negocio			
	TOTAL:1	TOTAL: 0		

	Alta de Amenaza		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Amenaza	EI/EO	Baja
	Probabilidad	OK/Error		
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	Integridad			
	Confidencialidad			

	Disponibilidad			
	TOTAL: 7	TOTAL: 2		
FTR	Amenaza	Amenaza		
	TOTAL:1	TOTAL:1		

	Modificar Amenaza		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error	EI/EO	Baja
	Probabilidad			
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	Integridad			
	Confidencialidad			
	Disponibilidad			
	TOTAL: 7	TOTAL: 1		
FTR	Amenaza			
	TOTAL:1	TOTAL: 0		

	Eliminar Amenaza		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Amenaza		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Amenaza			
	TOTAL:1	TOTAL: 0		

	Alta de Control		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Control	EI/EO	Baja
	Objetivos	OK/Error		
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Beneficios			
	Estado			
	Precio			
	Responsable			
	Fecha de Inicio de Validez			

	TOTAL: 12	TOTAL: 2
FTR	Control	Control
	TOTAL:1	TOTAL:1

	Modificar Control		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error	EI/EO	Baja
	Objetivos			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Beneficios			
	Estado			
	Precio			
	Responsable			
	Fecha de Inicio de Validez			
	TOTAL: 12	TOTAL: 1		
FTR	Control			
	TOTAL:1	TOTAL: 0		

	Eliminar Control		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Control			
	TOTAL:1	TOTAL: 0		

	Alta de Controles con Políticas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control	Id Control	EI/EO	BAJA
	Id Política	Id Política		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Control	Controles con Políticas		
	Política			
	TOTAL:2	TOTAL: 1		

	Eliminar Controles con Políticas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control		EI	BAJA
	Id Política			
	TOTAL: 2	TOTAL: 0		
FTR	Controles con Políticas			
	TOTAL:1	TOTAL: 0		

	Alta de Evaluación		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Tipo	Id Evaluación	EI/EO	BAJA
	Descripción de métricas	OK/Error		
	Valor			
	Responsable			
	Fecha de Revisión			
	TOTAL: 5	TOTAL: 2		
FTR	Evaluación	Evaluación		
	TOTAL:1	TOTAL:1		

	Modificar Evaluación		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Tipo	OK/Error	EI/EO	Baja
	Descripción de métricas			
	Valor			
	Responsable			
	Fecha de Revisión			
	TOTAL: 5	TOTAL: 1		
FTR	Evaluación			
	TOTAL:1	TOTAL: 0		

	Eliminar Evaluación		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Evaluación		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Evaluación			
	TOTAL:1	TOTAL: 0		

	Alta de Línea de Estrategia		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Alcance	Id Línea	EI/EO	Baja
	Exigencias legales	Id Requerimiento		
	Descripción	OK/Error		
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos legales y regulatorios			
	Beneficios			
	Precio			

	Responsable			
	Fecha de validez			
	Estado			
	TOTAL: 20	TOTAL: 3		
FTR	Línea de Estrategia	Línea de Estrategia		
	Requerimiento	Requerimiento		
	TOTAL: 2	TOTAL:2		

	Modificar Línea de Estrategia		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Alcance	OK/Error	EI/EO	Baja
	Exigencias legales			
	Descripción			
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			

	Requerimientos de Ambiente	
	Requerimientos de estándares y métricas	
	Requerimientos de Disponibilidad	
	Requerimientos legales y regulatorios	
	Beneficios	
	Precio	
	Responsable	
	Fecha de validez	
	Estado	
	TOTAL: 20	TOTAL: 1
FTR	Línea de Estrategia	
	Requerimiento	
	TOTAL:2	TOTAL: 0

	Eliminar Línea de Estrategia		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Línea		EI	Baja
	Id Requerimiento			
	TOTAL: 2	TOTAL: 0		
FTR	Línea de Estrategia			
	Requerimiento			

	TOTAL:2	TOTAL: 0

	Alta de Normativa Externa		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Alcance	Id Normativa	EI/EO	Baja
	Políticas	Id Requerimiento		
	Descripción	OK/Error		
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos			

	legales y regulatorios			
	Beneficios			
	Precio			
	Responsable			
	Fecha de validez			
	Estado			
	TOTAL: 20	TOTAL: 3		
FTR	Normativa Externa	Normativa Externa		
	Requerimiento	Requerimiento		
	TOTAL: 2	TOTAL: 3		

	Modificar Normativa Externa		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Alcance	OK/Error	EI/EO	Baja
	Políticas			
	Descripción			
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de			

	instrucción y procedimientos operativos	
	Requerimientos de continuidad	
	Requerimientos de Ambiente	
	Requerimientos de estándares y métricas	
	Requerimientos de Disponibilidad	
	Requerimientos legales y regulatorios	
	Beneficios	
	Precio	
	Responsable	
	Fecha de validez	
	Estado	
	TOTAL: 20	TOTAL: 1
FTR	Normativa Externa	
	Requerimiento	
	TOTAL:2	TOTAL: 0

	Eliminar Normativa Externa		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Normativa		EI	Baja

	Id Requerimiento	
	TOTAL: 2	TOTAL: 0
FTR	Normativa Externa	
	Requerimiento	
	TOTAL:2	TOTAL: 0

	Alta de Plan de Seguimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Plan	EI/EO	Baja
	Alcance	OK/Error		
	Orden			
	Implementador			
	Fecha de Inicio			
	Fecha de Fin			
	Estado			
	TOTAL: 7	TOTAL: 2		
FTR	Plan de Seguimiento	Plan de Seguimiento		
	TOTAL: 1	TOTAL:1		

	Modificar Plan de Seguimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error		

	Alcance			
	Orden			
	Implementador		EI/EO	Baja
	Fecha de Inicio			
	Fecha de Fin			
	Estado			
	TOTAL: 7	TOTAL: 1		
FTR	Plan de Seguimiento			
	TOTAL:1	TOTAL: 0		

	Eliminar Plan de Seguimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Plan de Seguimiento		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Plan de Seguimiento			
	TOTAL:1	TOTAL: 0		

	Alta de Política		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Objetivos de negocio	Id Política	EI/EO	Baja
	Alcance	Id Requerimiento		
	Exigencias legales	OK/Error		
	Descripción			
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			

	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos legales y regulatorios			
	Beneficios			
	Precio			
	Responsable			
	Fecha de validez			
	Estado			
	TOTAL: 21	TOTAL: 3		
FTR	Política	Política		
	Requerimiento	Requerimiento		
	TOTAL: 2	TOTAL: 2		

	Modificar Política		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Objetivos de negocio	OK/Error		
	Alcance			
	Exigencias legales			

	Descripción		EI/EO	Baja
	Objetivos			
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos legales y regulatorios			
	Beneficios			
	Precio			
	Responsable			
	Fecha de validez			
	Estado			

	TOTAL: 21	TOTAL: 1
FTR	Política	
	Requerimiento	
	TOTAL:2	TOTAL: 0

	Eliminar Política		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Política		EI	Baja
	Id Requerimiento			
	TOTAL: 2	TOTAL: 0		
FTR	Política			
	Requerimiento			
	TOTAL:2	TOTAL: 0		

	Alta de Requerimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Requerimiento	EI/EO	Baja
	Objetivos	OK/Error		
	Obligatoriedad			
	Tipo de Control			
	Origen			
	Plan de tratamiento			
	Prioridad			

	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos legales y regulatorios			
	Beneficios			
	Precio			
	Responsable			
	Fecha de validez			
	Estado			
	TOTAL: 18	TOTAL: 2		
FTR	Requerimiento	Requerimiento		
	TOTAL: 1	TOTAL:1		

	Modificar Requerimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error		
	Objetivos			

	Obligatoriedad			
	Tipo de Control		EI/EO	Baja
	Origen			
	Plan de tratamiento			
	Prioridad			
	Manuales de instrucción y procedimientos operativos			
	Requerimientos de continuidad			
	Requerimientos de Ambiente			
	Requerimientos de estándares y métricas			
	Requerimientos de Disponibilidad			
	Requerimientos legales y regulatorios			
	Beneficios			
	Precio			
	Responsable			
	Fecha de validez			
	Estado			
	TOTAL: 21	TOTAL: 1		
FTR	Requerimiento			

	TOTAL:1	TOTAL: 0

	Eliminar Requerimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Requerimiento		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Requerimiento			
	TOTAL:1	TOTAL: 0		

	Alta de Riesgo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	Id Riesgo	EI/EO	Baja
	Origen	OK/Error		
	Prioridad			
	Estado			
	Impacto			
	Infracciones			
	Valor del negocio y financiero			
	Plazo			
	Área Afectada			
	Ámbito de aplicabilidad			
	Coste			

	Beneficio			
	Tratamiento			
	Responsable			
	Probabilidad			
	TOTAL: 15	TOTAL: 2		
FTR	Riesgo	Riesgo		
	TOTAL: 1	TOTAL:1		

	Modificar Riesgo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Descripción	OK/Error		
	Origen			
	Prioridad		EI/EO	Baja
	Estado			
	Impacto			
	Infracciones			
	Valor del negocio y financiero			
	Plazo			
	Área Afectada			
	Ámbito de aplicabilidad			
	Coste			
	Beneficio			

	Tratamiento			
	Responsable			
	Probabilidad			
	TOTAL: 15	TOTAL: 1		
FTR	Riesgo			
	TOTAL:1	TOTAL: 0		

	Eliminar Riesgo		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Riesgo			
	TOTAL:1	TOTAL: 0		

	Alta de Riesgos a causa de Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EI/EO	BAJA
	Id Amenaza	Id Amenaza		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Riesgo	Riesgos a causa de Amenazas		
	Amenaza			
	TOTAL:2	TOTAL: 1		

	Eliminar Riesgos a causa de Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo		EI	BAJA
	Id Amenaza			
	TOTAL: 2	TOTAL: 0		
FTR	Riesgos a causa de Amenazas			
	TOTAL:1	TOTAL: 0		

	Alta de Riesgos reducen vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EI/EO	BAJA
	Id Vulnerabilidad	Id Vulnerabilidad		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Riesgo	Riesgos reducen vulnerabilidades		
	Vulnerabilidad			
	TOTAL:2	TOTAL: 1		

	Eliminar Riesgos reducen vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad

DET	Id Riesgo		EI	BAJA
	Id Vulnerabilidad			
	TOTAL: 2	TOTAL: 0		
FTR	Riesgos reducen vulnerabilidades			
	TOTAL:1	TOTAL: 0		

	Alta de Riesgos requieren Controles		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EI/EO	BAJA
	Id Control	Id Control		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Riesgo	Riesgos requieren Controles		
	Control			
	TOTAL:2	TOTAL: 1		

	Eliminar Riesgos requieren Controles		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo		EI	BAJA
	Id Control			
	TOTAL: 2	TOTAL: 0		
FTR	Riesgos requieren			

	Controles	
	TOTAL:1	TOTAL: 0

	Alta Riesgos se ajustan a Requerimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Requerimiento	Id Requerimiento	EI/EO	BAJA
	Id Riesgo	Id Riesgo		
		OK/Error		
	TOTAL: 2	TOTAL: 3		
FTR	Riesgo	Riesgos se ajusta a Requerimiento		
	Requerimiento			
	TOTAL:2	TOTAL: 1		

	Eliminar Riesgos se ajustan a Requerimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Requerimiento		EI	BAJA
	Id Riesgo			
	TOTAL: 2	TOTAL: 0		
FTR	Riesgos se ajusta a Requerimiento			
	TOTAL:1	TOTAL: 0		

	Alta de Servicio de TI		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nombre	Id Servicio	EI/EO	Baja
	Descripción	OK/Error		
	Alcance			
	Tipo			
	Documentos asociados			
	Fecha de Inicio			
	Fecha de Fin			
	Estado			
	TOTAL: 8	TOTAL: 2		
FTR	Servicio	Servicio		
	TOTAL: 1	TOTAL:1		

	Modificar Servicio de TI		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nombre	OK/Error	EI/EO	Baja
	Descripción			
	Alcance			
	Tipo			
	Documentos asociados			
	Fecha de Inicio			

	Fecha de Fin			
	Estado			
	TOTAL: 8	TOTAL: 1		
FTR	Servicio			
	TOTAL:1	TOTAL: 0		

	Eliminar Servicio de TI		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Servicio		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Servicio			
	TOTAL:1	TOTAL: 0		

	Alta de Usuario		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nombre	Nº Empleado	EI/EO	Baja
	Apellidos	OK/Error		
	Roles			
	Ubicación			
	Puesto			
	Capacidad			
	TOTAL: 6	TOTAL: 2		
FTR	Usuario	Usuario		

	TOTAL:1	TOTAL:1

	Modificar Usuario		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nombre	OK/Error	EI/EO	Baja
	Apellidos			
	Roles			
	Ubicación			
	Puesto			
	Capacidad			
	TOTAL: 6	TOTAL: 1		
FTR	Usuario			
	TOTAL:1	TOTAL: 0		

	Eliminar Usuario		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nº Empleado		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Usuario			
	TOTAL:1	TOTAL: 0		

	Alta de Vulnerabilidad		Online	
	Entrada	Salida	Tipo	Complejidad

DET	Nombre	Id Vulnerabilidad	EI/EO	Baja
	Descripción	OK/Error		
	Integridad			
	Confidencialidad			
	Disponibilidad			
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	TOTAL: 7	TOTAL: 2		
FTR	Vulnerabilidad	Vulnerabilidad		
	TOTAL: 1	TOTAL:1		

	Modificar Vulnerabilidad		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Nombre	OK/Error	EI/EO	Baja
	Descripción			
	Integridad			
	Confidencialidad			
	Disponibilidad			
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	TOTAL: 7	TOTAL: 1		

FTR	Vulnerabilidad	
	TOTAL:1	TOTAL: 0

	Eliminar Vulnerabilidad		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Vulnerabilidad		EI	Baja
	TOTAL: 1	TOTAL: 0		
FTR	Vulnerabilidad			
	TOTAL:1	TOTAL: 0		

	Alta de Incidente		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Origen	Id Incidente	EI/EO	Baja
	Clasificacion	Id Amenaza		
	Asignación	OK/Error		
	Descripción			
	Probabilidad			
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	Integridad			
	Confidencialidad			
	Disponibilidad			

	TOTAL: 10	TOTAL: 3
FTR	Incidente	Incidente
	Amenaza	Amenaza
	TOTAL:2	TOTAL:2

	Modificar Incidente		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Origen	OK/Error	EI/EO	Baja
	Clasificacion			
	Asignación			
	Descripción			
	Probabilidad			
	Fecha de Inicio de vigencia			
	Fecha de Fin de vigencia			
	Integridad			
	Confidencialidad			
	Disponibilidad			
	TOTAL: 10	TOTAL: 1		
FTR	Incidente			
	Amenaza			
	TOTAL:2	TOTAL: 0		

	Eliminar Incidente		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Incidente		EI	Baja
	Id Amenaza			
	TOTAL: 2	TOTAL: 0		

FTR	Incidente	
	Amenaza	
	TOTAL:2	TOTAL: 0

Consulta (EQ External Query): Datos no calculados que se obtienen por la combinación de una EI y de una EO, ningún ILF se modifica en un proceso de consulta.

A continuación se detallan todas las consultas externas:

	Consultar Activo		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Activo		
		Número de modelo		
		Nombre	EQ (Entrada)	Baja
		Afectado		
		Grado de Afectado		
		Descripción		
		Configuración		
		Ubicación	EQ (Salida)	Baja
		Propietario		
		Responsable		
		Estado		
		Propiedad del		

		centro de costo		
		Fabricante		
		Documentos asociados		
		Disponibilidad		
		Impacto		
		Número de Accesos		
		Tipo de Accesos		
		Coste		
		Área o Clase		
		Tipo		
	TOTAL: 0	TOTAL: 22		
FTR		Activo		
	TOTAL: 0	TOTAL:1		

	Consultar Activos se exponen a Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo	Id Amenaza	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos se exponen a Amenazas	Activos se exponen a Amenazas		

	TOTAL:1	TOTAL:1

	Consultar Amenazas que actúan sobre Activos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Amenaza	Id Amenaza	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos se exponen a Amenazas	Activos se exponen a Amenazas		
	TOTAL:1	TOTAL:1		

	Consultar Activos afectados por Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo	Id Riesgo	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos afectados por Riesgos	Activos afectados por Riesgos		
	TOTAL:1	TOTAL:1		

Consultar Riesgos que actúan sobre Activos	Online

	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos afectados por Riesgos	Activos afectados por Riesgos		
	TOTAL:1	TOTAL:1		

	Consultar Activos Controlados		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo	Id Control	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos Controlados	Activos Controlados		
	TOTAL:1	TOTAL:1		

	Consultar Controles que actúan sobre Activos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control	Id Control	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos Controlados	Activos Controlados		
	TOTAL:1	TOTAL:1		

	Consultar Activos ofrecen Servicios		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo	Id Servicio	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos ofrecen Servicios	Activos ofrecen Servicios		
	TOTAL:1	TOTAL:1		

	Consultar Servicios que actúan sobre Activos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Servicio	Id Servicio	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos ofrecen Servicios	Activos ofrecen Servicios		
	TOTAL:1	TOTAL:1		

	Consultar Activos presentan vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Activo	Id Vulnerabilidad	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos presentan vulnerabilidades	Activos presentan vulnerabilidades		
	TOTAL:1	TOTAL:1		

	Consultar Vulnerabilidades que actúan sobre Activos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Vulnerabilidad	Id Vulnerabilidad	EQ (Entrada)	Baja
		Id Activo	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Activos presentan vulnerabilidades	Activos presentan vulnerabilidades		
	TOTAL:1	TOTAL:1		

	Consultar Acuerdo de Negocio		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Acuerdo		
		Descripción		
		Nivel de servicio	EQ (Entrada)	Baja
		Detalles de acuerdo	EQ (Salida)	Baja
		Penalización		
		Bonificación		
		Integridad		
		Confidencialidad		
		Disponibilidad		
	TOTAL: 0	TOTAL: 9		

FTR		Acuerdo de Negocio
	TOTAL: 0	TOTAL:1

	Consultar Amenaza		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Amenaza		
		Descripción		
		Probabilidad		
		Fecha de Inicio de vigencia	EQ (Entrada)	Baja
		Fecha de Fin de vigencia	EQ (Salida)	Baja
		Integridad		
		Confidencialidad		
		Disponibilidad		
	TOTAL: 0	TOTAL: 22		
FTR		Amenaza		
	TOTAL: 0	TOTAL: 1		

	Consultar Control		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Control		
		Descripción		
		Objetivos		
		Tipo de Control	EQ (Entrada)	Baja
		Origen	EQ (Salida)	Baja
		Plan de tratamiento		
		Prioridad		
		Manuales de instrucción y procedimientos operativos		
		Beneficios		
		Estado		
		Precio		
		Responsable		
		Fecha de Inicio de Validez		
	TOTAL: 0	TOTAL: 13		
FTR		Control		
	TOTAL: 0	TOTAL: 1		

Consultar Controles con Políticas	Online

	Entrada	Salida	Tipo	Complejidad
DET	Id Política	Id Control	EQ (Entrada)	Baja
		Id Política	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Controles con Políticas	Controles con Políticas		
	TOTAL:1	TOTAL:1		

	Consultar Políticas que actúan sobre Controles		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control	Id Control	EQ (Entrada)	Baja
		Id Política	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Controles con Políticas	Controles con Políticas		
	TOTAL:1	TOTAL:1		

	Consultar Evaluación		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Evaluación		
		Tipo	EQ (Entrada)	Baja
		Descripción de	EQ (Salida)	Baja

		métricas		
		Valor		
		Responsable		
		Fecha de Revisión		
	TOTAL: 0	TOTAL: 6		
FTR		Evaluación		
	TOTAL:1	TOTAL:1		

	Consultar Incidente		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Incidente		
		Id Amenaza		
		Origen		
		Clasificacion		
		Asignación	EQ (Entrada)	Baja
		Descripción	EQ (Salida)	Baja
		Probabilidad		
		Fecha de Inicio de vigencia		
		Fecha de Fin de vigencia		
		Integridad		
		Confidencialidad		
		Disponibilidad		

	TOTAL: 0	TOTAL: 11
FTR		Incidente
		Amenaza
	TOTAL: 0	TOTAL: 2

	Consultar Línea de Estrategia		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Línea		
		Id Requerimiento		
		Alcance		
		Exigencias legales		
		Descripción	EQ (Entrada)	Baja
		Objetivos	EQ (Salida)	Baja
		Obligatoriedad		
		Tipo de Control		
		Origen		
		Plan de tratamiento		
		Prioridad		
		Manuales de instrucción y procedimientos operativos		
		Requerimientos de continuidad		

		Requerimientos de Ambiente		
		Requerimientos de estándares y métricas		
		Requerimientos de Disponibilidad		
		Requerimientos legales y regulatorios		
		Beneficios		
		Precio		
		Responsable		
		Fecha de validez		
		Estado		
	TOTAL: 0	TOTAL: 22		
FTR		Línea de Estrategia		
		Requerimiento		
	TOTAL: 0	TOTAL: 2		

	Consultar Normativa Externa		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Normativa		
		Id Requerimiento		
		Alcance		
		Exigencias legales		
		Descripción	EQ (Entrada)	Baja
		Objetivos	EQ (Salida)	Baja
		Obligatoriedad		
		Tipo de Control		
		Origen		
		Plan de tratamiento		
		Prioridad		
		Manuales de instrucción y procedimientos operativos		
		Requerimientos de continuidad		
		Requerimientos de Ambiente		
		Requerimientos de estándares y métricas		
		Requerimientos de Disponibilidad		
		Requerimientos		

		legales y regulatorios		
		Beneficios		
		Precio		
		Responsable		
		Fecha de validez		
		Estado		
	TOTAL: 0	TOTAL: 22		
FTR		Normativa Externa		
		Requerimiento		
	TOTAL: 0	TOTAL: 2		

	Consultar Política		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Política		
		Id Requerimiento		
		Objetivos de negocio		
		Alcance		
		Exigencias legales	EQ (Entrada)	Baja
		Descripción	EQ (Salida)	Baja
		Objetivos		
		Obligatoriedad		
		Tipo de Control		
		Origen		

		Plan de tratamiento		
		Prioridad		
		Manuales de instrucción y procedimientos operativos		
		Requerimientos de continuidad		
		Requerimientos de Ambiente		
		Requerimientos de estándares y métricas		
		Requerimientos de Disponibilidad		
		Requerimientos legales y regulatorios		
		Beneficios		
		Precio		
		Responsable		
		Fecha de validez		
		Estado		
	TOTAL: 0	TOTAL: 23		
FTR		Política		
		Requerimiento		
	TOTAL: 0	TOTAL: 2		

Consultar Requerimiento	Online

	Entrada	Salida	Tipo	Complejidad
DET		Id Requerimiento		
		Descripción		
		Objetivos		
		Obligatoriedad		
		Tipo de Control		
		Origen	EQ (Entrada)	Baja
		Plan de tratamiento	EQ (Salida)	Baja
		Prioridad		
		Manuales de instrucción y procedimientos operativos		
		Requerimientos de continuidad		
		Requerimientos de Ambiente		
		Requerimientos de estándares y métricas		
		Requerimientos de Disponibilidad		
		Requerimientos legales y regulatorios		
		Beneficios		

		Precio		
		Responsable		
		Fecha de validez		
		Estado		
	TOTAL: 0	TOTAL: 23		
FTR		Requerimiento		
	TOTAL: 0	TOTAL: 1		

	Consultar Plan de Seguimiento		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Plan de Seguimiento		
		Descripción		
		Alcance	EQ (Entrada)	Baja
		Orden	EQ (Salida)	Baja
		Implementador		
		Fecha de Inicio		
		Fecha de Fin		
		Estado		
	TOTAL: 0	TOTAL: 8		
FTR		Plan de Seguimiento		
	TOTAL: 0	TOTAL: 1		

	Consultar Riesgo		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Riesgo		
		Descripción		
		Origen		
		Prioridad		
		Estado		
		Impacto	EQ (Entrada)	Baja
		Infracciones	EQ (Salida)	Baja
		Valor del negocio y financiero		
		Plazo		
		Área Afectada		
		Ámbito de aplicabilidad		
		Coste		
		Beneficio		
		Tratamiento		
		Responsable		
		Probabilidad		
	TOTAL: 0	TOTAL: 16		
FTR		Riesgo		
	TOTAL: 0	TOTAL: 1		

	Consultar Riesgos a causa de Amenazas		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Amenaza	Id Riesgo	EQ (Entrada)	Baja
		Id Amenaza	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos a causa de Amenazas	Riesgos a causa de Amenazas		
	TOTAL:1	TOTAL:1		

	Consultar Amenazas que actúan sobre Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EQ (Entrada)	Baja
		Id Amenaza	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos a causa de Amenazas	Riesgos a causa de Amenazas		
	TOTAL:1	TOTAL:1		

	Consultar Riesgos reducen vulnerabilidades		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Vulnerabilidad	Id Riesgo	EQ (Entrada)	Baja

		Id Vulnerabilidad	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos reducen vulnerabilidades	Riesgos reducen vulnerabilidades		
	TOTAL:1	TOTAL:1		

	Consultar Vulnerabilidades que actúan sobre Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EQ (Entrada)	Baja
		Id Vulnerabilidad	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos reducen vulnerabilidades	Riesgos reducen vulnerabilidades		
	TOTAL:1	TOTAL:1		

	Consultar Riesgos requieren Controles		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Control	Id Riesgo	EQ (Entrada)	Baja
		Id Control	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos requieren Controles	Riesgos requieren Controles		
	TOTAL:1	TOTAL:1		

	Consultar Controles que actúan sobre Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EQ (Entrada)	Baja
		Id Control	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos requieren Controles	Riesgos requieren Controles		
	TOTAL:1	TOTAL:1		

	Consultar Riesgos se ajusta a Requerimientos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Requerimiento	Id Riesgo	EQ (Entrada)	Baja

		Id Requerimiento	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos se ajusta a Requerimiento	Riesgos se ajusta a Requerimiento		
	TOTAL:1	TOTAL:1		

	Consultar Requerimientos que actúan sobre Riesgos		Online	
	Entrada	Salida	Tipo	Complejidad
DET	Id Riesgo	Id Riesgo	EQ (Entrada)	Baja
		Id Requerimiento	EQ (Salida)	Baja
	TOTAL: 1	TOTAL: 2		
FTR	Riesgos se ajusta a Requerimiento	Riesgos se ajusta a Requerimiento		
	TOTAL:1	TOTAL:1		

	Consultar Servicio de TI		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Servicio		
		Nombre	EQ (Entrada)	Baja
		Descripción	EQ (Salida)	Baja

		Alcance		
		Tipo		
		Documentos asociados		
		Fecha de Inicio		
		Fecha de Fin		
		Estado		
	TOTAL: 0	TOTAL: 9		
FTR		Servicio		
	TOTAL: 0	TOTAL: 1		

	Consultar Usuario		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Nº Empleado		
		Nombre		
		Apellidos	EQ (Entrada)	Baja
		Roles	EQ (Salida)	Baja
		Ubicación		
		Puesto		
		Capacidad		
	TOTAL: 0	TOTAL: 7		
FTR		Usuario		
	TOTAL: 0	TOTAL: 1		

	Consultar Vulnerabilidad		Online	
	Entrada	Salida	Tipo	Complejidad
DET		Id Vulnerabilidad		
		Nombre		
		Descripción		
		Integridad	EQ (Entrada)	Baja
		Confidencialidad	EQ (Salida)	Baja
		Disponibilidad		
		Fecha de Inicio de vigencia		
		Fecha de Fin de vigencia		
	TOTAL: 0	TOTAL: 8		
FTR		Vulnerabilidad		
	TOTAL: 0	TOTAL: 1		

8.2.3 Resultados Obtenidos

A partir de las complejidades se pueden calcular los puntos de función sin ajustar (PFSA). Para ello se tienen que aplicar los siguientes multiplicadores:

Tabla 111Multiplicadores PFSA método de Albrecht

	Baja	**Media**	**Alta**
EI	x3	x4	x 6
EO	x4	x5	x 7
EQ	x3	x4	x 6
EIF	x5	x7	x 10
ILF	x7	x10	x 15

En las siguientes tablas se puede ver un resumen de las complejidades de los distintos almacenes y procesos:

Tabla 112. Albrecht. Resumen complejidades almacenes

Almacén	ILF			EIF		
	B	M	A	B	M	A
Activo	X					
Activos se exponen a Amenazas	X					
Activos afectados por Riesgos	X					
Activos Controlados	X					
Activos ofrecen Servicios	X					
Activos presentan vulnerabilidades	X					
Acuerdos de Negocio	X					
Amenaza	X					
Control	X					
Controles con Políticas	X					
Evaluación	X					
Línea de Estrategia	X					
Normativa Externa	X					
Plan de Seguimiento	X					
Política	X					

Requerimiento	X					
Riesgo	X					
Riesgos a causa de Amenazas	X					
Riesgos reducen vulnerabilidades	X					
Riesgos requieren Controles	X					
Riesgos se ajusta a Requerimiento	X					
Servicio de TI	X					
Usuario	X					
Vulnerabilidad	X					
Incidente				X		
TOTAL FUNCIONES	**24**	**0**	**0**	**1**	**0**	**0**
TOTAL	**24**			**1**		
PFSA(Almacenes)	(X7)	(X10)	(X15)	(X5)	(X7)	(X10)
	168	**0**	**0**	**5**	**0**	**0**
	168			**5**		
	173					

Proceso	EI			EO			EQ		
	B	M	A	B	M	A	B	M	A
Alta de Activo	X			X					
Modificar Activo	X			X					
Eliminar Activo	X								
Alta de Activos se exponen a Amenazas	X			X					
Eliminar Activos se exponen a Amenazas	X								
Alta de Activos afectados por Riesgos	X			X					
Eliminar Activos afectados por Riesgos	X								
Alta de Activos Controlados	X			X					
Eliminar Activos Controlados	X								
Alta de Activos ofrecen Servicios	X			X					
Eliminar Activos ofrecen Servicios	X								
Alta de Activos presentan vulnerabilidades	X			X					
Eliminar Activos presentan vulnerabilidades	X								
Alta de Acuerdo de Negocio	X			X					
Modificar Acuerdo de Negocio	X			X					
Eliminar Acuerdo de Negocio	X								

Alta de Amenaza	X			X					
Modificar Amenaza	X			X					
Eliminar Amenaza	X								
Alta de Control	X			X					
Modificar Control	X			X					
Eliminar Control	X								
Alta de Controles con Políticas	X			X					
Eliminar Controles con Políticas	X								
Alta de Evaluación	X			X					
Modificar Evaluación	X			X					
Eliminar Evaluación	X								
Alta de Línea de Estrategia	X			X					
Modificar Línea de Estrategia	X			X					
Eliminar Línea de Estrategia	X								
Alta de Normativa Externa	X			X					
Modificar Normativa Externa	X			X					
Eliminar Normativa Externa	X								
Alta de Plan de Seguimiento	X			X					
Modificar Plan de Seguimiento	X			X					
Eliminar Plan de Seguimiento	X								
Alta de Política	X			X					
Modificar Política	X			X					
Eliminar Política	X								

Alta de Requerimiento	X			X					
Modificar Requerimiento	X			X					
Eliminar Requerimiento	X								
Alta de Riesgo	X			X					
Modificar Riesgo	X			X					
Eliminar Riesgo	X								
Alta de Riesgos a causa de Amenazas	X			X					
Eliminar Riesgos a causa de Amenazas	X								
Alta de Riesgos reducen vulnerabilidades	X			X					
Eliminar Riesgos reducen vulnerabilidades	X								
Alta de Riesgos requieren Controles	X			X					
Eliminar Riesgos requieren Controles	X								
Alta Riesgos se ajustan a Requerimiento	X			X					
Eliminar Riesgos se ajustan a Requerimiento	X								
Alta de Servicio de TI	X			X					
Modificar Servicio de TI	X			X					
Eliminar Servicio de TI	X								
Alta de Usuario	X			X					

Modificar Usuario	X			X					
Eliminar Usuario	X								
Alta de Vulnerabilidad	X			X					
Modificar Vulnerabilidad	X			X					
Eliminar Vulnerabilidad	X								
Alta de Incidente	X			X					
Modificar Incidente	X			X					
Eliminar Incidente	X						X		
Consultar Activo							X		
Consultar Activos se exponen a Amenazas							X		
Consultar Amenazas que actúan sobre Activos							X		
Consultar Activos afectados por Riesgos							X		
Consultar Riesgos que actúan sobre Activos							X		
Consultar Activos Controlados							X		
Consultar Controles que actúan sobre Activos							X		
Consultar Activos ofrecen Servicios							X		
Consultar Servicios que actúan sobre Activos							X		
Consultar Activos presentan vulnerabilidades							X		

Consultar Vulnerabilidades que actúan sobre Activos							X		
Consultar Acuerdo de Negocio							X		
Consultar Amenaza							X		
Consultar Control							X		
Consultar Controles con Políticas							X		
Consultar Políticas que actúan sobre Controles							X		
Consultar Evaluación							X		
Consultar Incidente							X		
Consultar Línea de Estrategia							X		
Consultar Normativa Externa							X		
Consultar Política							X		
Consultar Requerimiento							X		
Consultar Plan de Seguimiento							X		
Consultar Riesgo							X		
Consultar Riesgos a causa de Amenazas							X		
Consultar Amenazas que actúan sobre Riesgos							X		
Consultar Riesgos reducen vulnerabilidades							X		
Consultar Vulnerabilidades que actúan sobre Riesgos							X		
Consultar Riesgos requieren							X		

Controles									
Consultar Controles que actúan sobre Riesgos							X		
Consultar Riesgos se ajusta a Requerimientos							X		
Consultar Requerimientos que actúan sobre Riesgos							X		
Consultar Servicio de TI							X		
Consultar Usuario							X		
Consultar Vulnerabilidad							X		
TOTAL FUNCIONES	**65**	**0**	**0**	**40**	**0**	**0**	**36**	**0**	**0**
TOTAL	**65**				**40**		**3 6**		

Tabla 113. Albrecht. Resumen complejidades Procesos

Proceso	**EI**			**EO**			**EQ**		
	B	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
TOTAL FUNCIONES	**65**	**0**	**0**	**40**	**0**	**0**	**36**	**0**	**0**
TOTAL	**65**				**40**		**36**		
PFSA(Almacenes)	(X3)	(X4)	(X6)	X4)	(X5)	(X7)	(X3)	(X4)	(X6)
	195	**0**	**0**	**160**	**0**	**0**	**108**	**0**	**0**
		195			**160**			**108**	
	463								

PFSA= PFSADatos + PFSAProcesos = 173 + 463 =636

Para el cálculo de los puntos de función ajustados (PF) se necesita calcular los Grados de Influencia (GDI) de Albretch.

Tabla 114. Albretch. GDI

Grado	Nombre	Justificación	Valor
C1	Comunicación de datos	Se debe disponer de un terminal conectado a Internet ya que todas las gestiones se basaran en protocolos de Internet. Tras una validación el usuario podrá intercambiar datos con el sistema y realizar sus gestiones de forma normal.	5
C2	Funciones distribuidas	El proceso distribuido y la transferencia de datos son On-line en ambas direcciones, es decir, habrá una interacción entre servidor y usuarios los cuales intercambian información.	4
C3	Rendimiento	Los requisitos y el rendimiento del sistema son diseñados y revisados antes de poner en práctica la aplicación.	1
C4	Configuraciones fuertemente utilizadas	En los procesos On-line existirán algunas restricciones referentes a la seguridad puesto que la base de datos contendrá información importante que no se podría perder. Se trabaja sobre una aplicación segura, el acceso será validado.	2
C5	Frecuencia de transacciones	Existe una frecuencia de transacciones alta diariamente, y ésta influirá sobre el soporte de la aplicación.	4
C6	Entrada de datos On-line	Al disponer de acciones del tipo alta, consulta, validación, etc., el nivel de transacciones relacionadas entre sí es alto, es decir, la acción de realizar una consulta implica que previamente se haya realizado un alta. En casi todos los procesos, el usuario introducirá de forma directa todos los datos.	5

C7	Eficiencia del usuario	La formación informática de los empleados es básica, por lo que se facilitará el uso al máximo, incluyendo menús, pantallas de ayuda, etc. Se necesitan conocimientos específicos de la Gestión de Seguridad y de Cobit e ITIL u otros marcos de trabajo para comprender la aplicación.	3
C8	Actualización On-line	En la interacción con el sistema se actualizan la mayoría de los ficheros lógicos internos, y es esencial la protección contra la perdida de datos.	4
C9	Procesos complejos	Básicamente los procesos consisten en altas, bajas, modificaciones, consultas y obtención de listados. También, presenta procesos matemáticos complejos y sobre seguridad del sistema.	2
C10	Reutilización	La aplicación se diseñaría para que al menos el 10% de la aplicación tenga en cuenta las necesidades de más de un usuario.	3
C11	Facilidad de instalación	Por parte del usuario no existen requisitos especiales en cuanto a la instalación, pero si en el servidor web en el que se instale.	1
C12	Facilidad de operación	La aplicación debe diseñarse sin intervención de operadores, es decir el ordenador no debe intervenir más que para arrancar y parar la aplicación.	5
C13	Instalación en distintos lugares	El sistema ha de ser lo más independiente posible tanto del hardware como del software del que disponga el usuario final. Por otra parte, se facilita la documentación de la aplicación.	3
C14	Facilidad de cambio	Se realizan consultas de complejidad media y se mantienen datos de control mediante procesos on-line de forma inmediata. La mayoría de las operaciones son alta, baja, modificación y consultas sin grandes problemas para ser cambiadas.	2
		GDI TOTAL	44

Con estos datos, ya se pueden calcular los puntos de función ajustados:

PF = FA (Factor de ajuste) x PFSA

FA = 0.65 + (0.01 x GDI)

FA = 0.65 + (0.01 x 44) = 1.09

PF = 1.09 * 636 = 693.24

Debido a la antigüedad de la herramienta COCOMO II no se encuentra disponible la tecnología .HTML y Ruby entre sus opciones, por lo que la que mejor se adapta es la del lenguaje de cuarta generación que cumple las siguientes características:

- Lenguaje orientado a objetos.
- Gestor de base de datos MySQL.
- Generación de formularios automáticamente.
- Generación de informes a través de una plantilla de informe.

Por lo que el número de líneas equivalentes será de 20 para un lenguaje de cuarta generación según el manual de COCOMO II.

LOC = PF * 20 = **693.24 * 20** = 13864,8LOC = 13,8648 KLOC

COCOMO II es un modelo de tres niveles que permite estimaciones cada vez más detalladas y que pueden realizarse a la vez que progresa el desarrollo del proyecto.

El Modelo post-arquitectura es el modelo más detallado. Se utiliza una vez que se ha desarrollado por completo la arquitectura del proyecto.

8.3 Estimación COCOMO II

COCOMO 2 es un modelo de tres niveles que permite estimaciones cada vez más detalladas y que pueden realizarse a la vez que progresa el desarrollo del proyecto.

Mediante un modelo Post-Arquitectura se van a establecer los factores de escala y los drivers de coste, con sus respectivas justificaciones, para realizar la estimación mediante COCOMO II.

8.3.1 Factores de Escala

Tabla 115. COCOMO II. Factores de escala

Factor	Nombre	Justificación	Valor
PREC	Precedencia.	Éste es un proyecto sin precedentes, no existe experiencia del equipo en software de este tipo.	Muy Bajo 6.20
FLEX	Flexibilidad de desarrollo.	Es un proyecto al que no se le ha puesto una fecha fin inamovible y en el que los requisitos no son primordiales.	Nominal 3.04
RESL	Arquitectura/ Resolución de riesgos.	Es un proyecto donde se identifican todos los riesgos críticos y establece hitos para resolverlos, calendario y presupuesto toma en cuenta riesgos, la herramienta resuelve/mitiga los riesgos y verificar especificaciones de la arquitectura, muy poca incertidumbre	Extra Alto 0.0
TEAM	Cohesión del Equipo.	Grupo joven con ganas de trabajar y personalidades afines, por el contrario es un grupo con poca experiencia en este tipo de aplicaciones.	Nominal 3.29
PMAT	Madurez del proceso.	Como no se tienen todos los datos necesarios para realizar en análisis y los que se conocen llevan al valor nominal.	Nominal 4,68

8.3.2 Drivers de coste

Los drivers de coste se usan para capturar características del desarrollo del software que afectan al esfuerzo para completar el proyecto. Tienen un nivel de medida que expresa el impacto del driver en el esfuerzo de desarrollo. Estos valores pueden ir desde Extra Bajo hasta Extra Alto. Para el propósito del análisis cuantitativo, cada nivel de medida de cada driver de coste tiene un peso asociado. El peso se llama multiplicador de esfuerzo (EM). En este caso como se trata de un modelo de post-arquitectura son 17 multiplicadores.

Tabla 116. COCOMO II. Drivers de Coste

Driver	Nombre	Justificación	Valor
RELY	Fiabilidad Requerida de Software.	El sistema se encuentra instalado en un servidor y una cualidad básica que se le exigirá es que sea consistente y se produzcan las mínimas	Alto 1.10

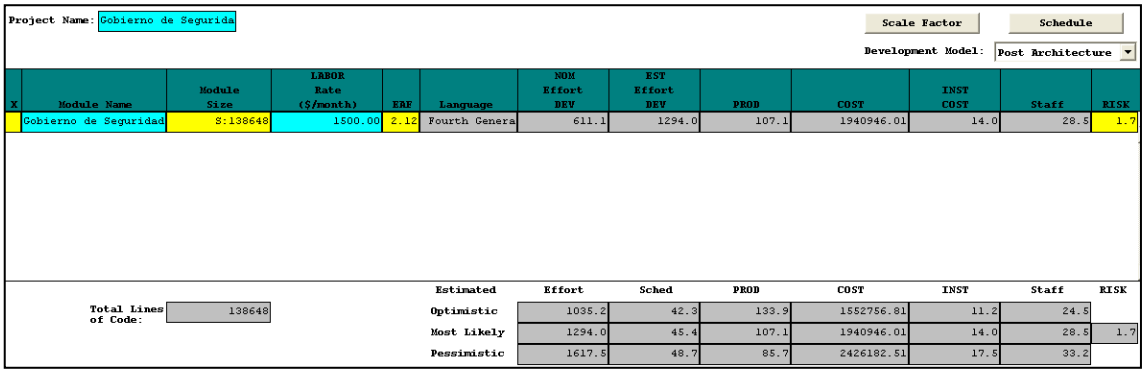
		excepciones posibles. La información es suficientemente importante y las perdidas a veces no serán recuperables.	
DATA	Medida del Volumen de Datos.	Se considera que el número de registros en la base de datos y el volumen de datos de dichos registros serán usuales.	Nominal 1.00
CPLX	Complejidad del Producto.	-Funcionamiento de control: Nominal, se realizan en su mayoría funciones sencillas. -Funcionamiento computacional: Bajo, no se realizan operaciones complejas. -Operaciones dependientes del dispositivo: Nominal, ya que, el procesamiento de I/O incluye selección de dispositivo, estado de validación (validar usuario) y procesamiento de errores. -Funcionamiento del sector de datos: Nominal, ya que pueden producirse modificaciones en los ficheros o borrado de algunos datos. -Funcionamiento del Gestor de Interfaz de Usuario: Nominal, lo suficientemente simple para que un usuario inexperto no tenga problemas en el manejo.	Nominal 1.00
RUSE	Reutilización Requerida.	A lo largo de todo el proyecto se genera una serie de documentación que puede ser utilizada como referencia en otras aplicaciones, existe la posibilidad de reutilizar parte del código.	Alto 1.07
RELY	Fiabilidad Requerida de Software.	El sistema se encuentra instalado en un servidor y una cualidad básica que se le exigirá es que sea consistente y se produzcan las mínimas excepciones posibles. La información es suficientemente importante y las perdidas a veces no serán recuperables.	Alto 1.10
DOCU	Documentación asociada a las fases del ciclo de vida.	Se ha usado un ciclo de vida en cascada, cada una de sus fases lleva su documentación que es usada como base para la toma de decisiones.	Alto 1.11
TIME	Restricción del Tiempo de Ejecución.	Ninguna de las aplicaciones consume un tiempo de ejecución excesivo puesto que los procesos no son especialmente complicados.	Nominal 1.00
STOR	Restricción de Almacenamiento Principal.	A priori, no se conoce el volumen de datos que se va a manejar, ya que esto depende de las necesidades de cada organización.	Nominal 1.00
PVOL	Volatilidad de la Plataforma.	El sistema principalmente no precisa de requerimientos hardware y software muy elevados.	Bajo 0.87
ACAP	Habilidad del Analista.	Bajo debido a la falta de experiencia.	Bajo 1.19
PCAP	Habilidad del Programador.	Bajo debido a la falta de experiencia.	Bajo 1.15

AEXP	Experiencia en las Aplicaciones.	Bajo debido a la falta de experiencia.	Bajo 1.10
PEXP	Experiencia en la Plataforma.	Bajo debido a la falta de experiencia.	Bajo 1.09
LTEX	Experiencia en la herramienta y en el Lenguaje.	Bajo debido a la falta de experiencia.	Bajo 1.09
PCON	Continuidad del Personal.	Bajo, por tratarse de un proyecto de final de carrera.	Bajo 1.12
TOOL	Uso de Herramientas Software.	La utilización de herramientas será la normal, las que se consideren para cada fase del ciclo de vida.	Nominal 1.00
SITE	Desarrollo multilugar.	Se trabajara en la misma ciudad o área metropolitana.	Alto 0.93
SCED	Calendario de Desarrollo Requerido.	Como no hay una fecha establecida de entrega y el personal es inexperto se considera que el valor es alto.	Alto 1.00

8.3.3 Resultados finales

A continuación, se adjuntan los datos obtenidos de la herramienta COCOMO

II al aplicar los factores de escala y los drivers de coste estimados anteriormente:


Project Name: Gobierno de Segurida

Scale Factor | Schedule

Development Model: Post Architecture

X	Module Name	Module Size	LABOR Rate ($/month)	EAF	Language	NOM Effort DEV	EST Effort DEV	PROD	COST	INST COST	Staff	RISK
	Gobierno de Seguridad	S:138648	1500.00	2.12	Fourth Genera	611.1	1294.0	107.1	1940946.01	14.0	28.5	1.7

Total Lines of Code: 138648

Estimated	Effort	Sched	PROD	COST	INST	Staff	RISK
Optimistic	1035.2	42.3	133.9	1552756.81	11.2	24.5	
Most Likely	1294.0	45.4	107.1	1940946.01	14.0	28.5	1.7
Pessimistic	1617.5	48.7	85.7	2426182.51	17.5	33.2	

Figura 66. COCOMO II. Resultado general

En los resultados obtenidos se puede observar información de interés sobre el proyecto, como son el riesgo, estimación optimista, moderada y pesimista, y la productividad.

La duración total del proyecto es de **45,4** meses.

Según esta estimación, el coste final del proyecto sería de **1.940.946** euros.

Para completar el estudio de la planificación, vamos a incluir los datos obtenidos de la herramienta COCOMO II, distribuidos en cada una de las fases:

Proyecto total:

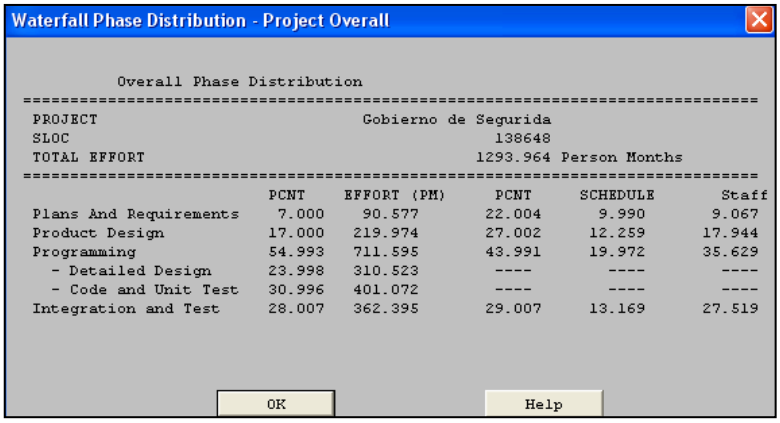


Figura 67. COCOMO II. Datos de estimación

Planificación y Requisitos:

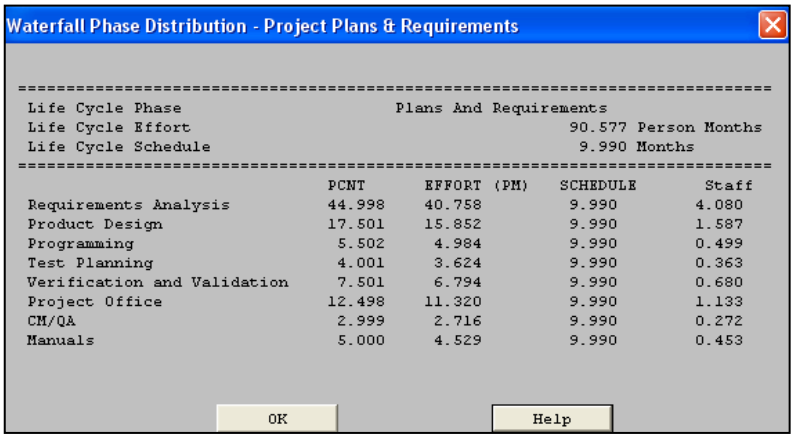


Figura 68. COCOMO II. Fase Planificación y Requisitos

Diseño:

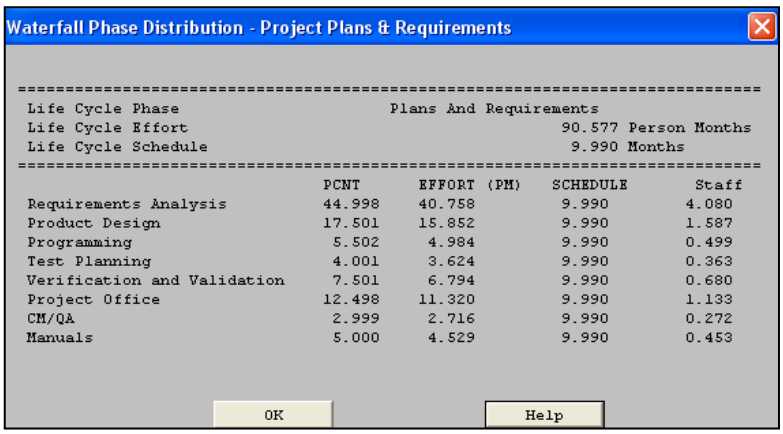


Figura 69. COCOMO II. Diseño

Desarrollo:

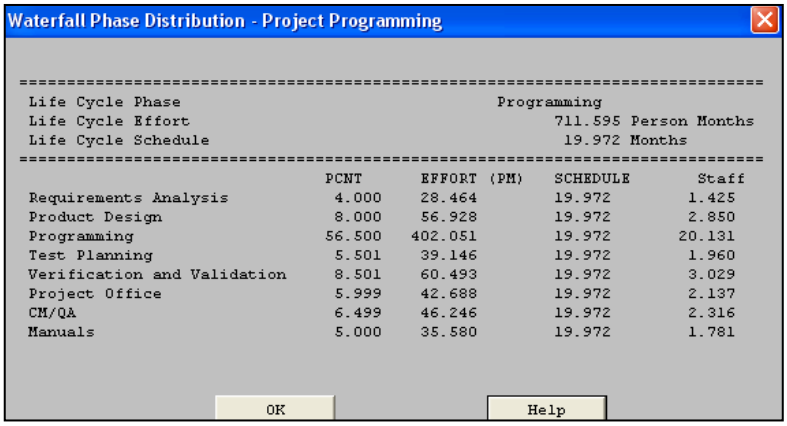


Figura 70. COCOMO II. Desarrollo

Integración y Pruebas:

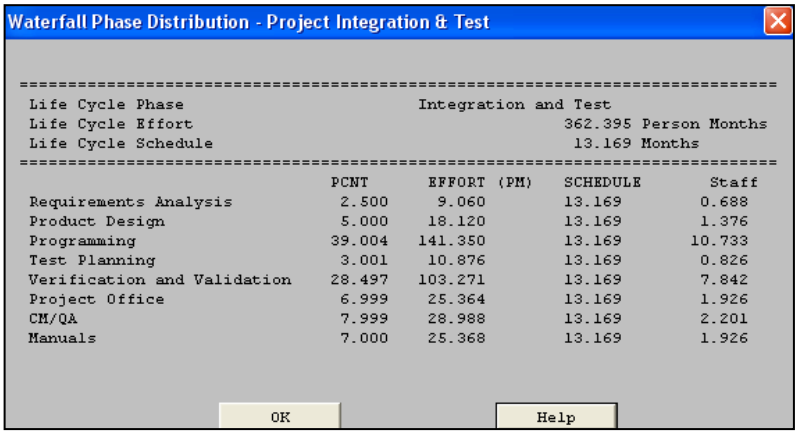


Figura 71. COCOMO II. Integración y Pruebas

8.4 Control del Proyecto: Técnica Valor Ganado

La Gestión del Valor Ganado es una técnica de gestión de proyectos que permite controlar la ejecución de un proyecto a través de su presupuesto y de su calendario.

Compara la cantidad de trabajo ya completada en un momento dado con la estimación realizada antes del comienzo del proyecto. De este modo, se tiene una medida de cuánto trabajo se ha realizado, cuanto queda para finalizar el proyecto y extrapolando a partir del esfuerzo invertido en el proyecto, el jefe de proyecto puede estimar los recursos que se emplearán para finalizar el proyecto.

Con esta metodología se puede estimar en cuanto tiempo se completaría el proyecto si se mantienen las condiciones con las que se elaboró el cronograma.

La técnica del valor ganado se puede expresar en función del coste o el tiempo. Para crear el grafico que muestran la curva real, la planificada y el valor conseguido, los cálculos realizados se muestran a lo largo de este punto en las correspondientes tablas.

Para los cálculos económicos se han tenido en cuenta las siguientes consideraciones:

Nombre del recurso	Tipo	Tasa estándar	Tasa horas extras	Acumular
PC1	Material	500 €		Comienzo
PC2	Material	500 €		Comienzo
PC3	Material	500 €		Comienzo
PC4	Material	500 €		Comienzo
PC5	Material	500 €		Comienzo
PC6	Material	500 €		Comienzo
PC7	Material	500 €		Comienzo
PC8	Material	500 €		Comienzo
Servidor	Material	500 €		Comienzo
Despacho	Material	1.000 €		Prorrateo
ADSL	Material	36 €		Prorrateo

Jefe de Proyecto	Trabajo	50 € / hora	60 € / hora	Prorrateo
Analista	Trabajo	36 € / hora	45 € / hora	Prorrateo
Programador	Trabajo	20 € / hora	28 € / hora	Prorrateo

Figura 72. Recursos Planificados

Nombre del recurso	Tipo	Tasa estándar	Tasa horas extras	Acumular
PC1	Material	1.000 €		Comienzo
PC2	Material	1.000 €		Comienzo
PC3	Material	1.000 €		Comienzo
PC4	Material	1.000 €		Comienzo
PC5	Material	1.000 €		Comienzo
PC6	Material	1.000 €		Comienzo
PC7	Material	1.000 €		Comienzo
PC8	Material	1.000 €		Comienzo
Servidor	Material	1.000 €		Comienzo
Despacho	Material	1.000 €		Prorrateo
ADSL	Material	36 €		Prorrateo
Jefe de Proyecto	Trabajo	50 € / hora	60 € / hora	Prorrateo
Analista	Trabajo	36 € / hora	45 € / hora	Prorrateo
Programador	Trabajo	20 € / hora	28 € / hora	Prorrateo

Figura 73. Recursos Reales

En esta tabla aparecen los costes mensuales y acumulados en el caso real y el planificado.

Tabla 117. Costes Planificados y Reales

Fecha		Planificado		Real	
Año	**Meses**	**coste/mes**	**coste acumulado**	**coste/mes**	**coste acumulado**
	Julio	21.472,00 €	5.536,00 €	21.472,00 €	10.036,00 €
	Agosto	21.471,92 €	49.515,92 €	21.471,92 €	54.015,92 €
2010	Septiembre	21.472,00 €	70.987,92 €	21.632,00 €	76.683,92 €
	Octubre	23.696,00 €	94.683,92 €	23.536,00 €	100.219,92 €
	Noviembre	22.272,00 €	116.955,92 €	21.472,00 €	121.691,92 €
	Diciembre	22.448,00 €	139.403,92 €	22.448,00 €	144.139,92 €
	Enero	48.048,00 €	187.451,92 €	45.248,00 €	189.387,92 €
	Febrero	37.360,00 €	224.811,92 €	45.760,00 €	235.147,92 €
	Marzo	52.624,00 €	277.435,92 €	25.168,00 €	260.315,92 €
2011	Abril	48.048,00 €	325.483,92 €		
	Mayo	50.336,00 €	375.819,92 €		
	Junio	3.432,00 €	379.251,92 €		

Para la realización del valor ganado es necesario obtener el control de avance y el coste total por tarea planificada.

El control de avance se calcula obteniendo el porcentaje real completado de cada una de las actividades en un mes. Aquí los tantos porciento se muestran en forma decimal.

Tabla 118. Control de avance

	2010						2011		
TAREA	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Enero**	**Febrero**	**Marzo**
1. Planificación y Requisitos									
1.1 Investigación									
1.1.1 Normativa ISO	**1**								
1.1.2 Buenas Prácticas		**1**							
1.1.3 Conformidad Legal			**1**						
1.2 Definir Requisitos			**1**						
1.3 Estimación de costes									
1.3.1 Definir Puntos de Función			**1**						
1.3.2 Realizar Estimación COCOMO II			**1**						
2. Análisis									
2.1 Análisis de la herramientas de mercado			**0,05**	**0,95**					
2.2 Detalle de casos de uso expandido				**0,04**	**0,47**	**0,49**			
3. Diseño									
3.1 Definir diseño conceptual							**1**		
3.2 Diseño de diagrama de clases							**1**		
3.3 Diseño de diagrama de secuencia								**1**	
3.4 Diseño de diagrama de estados								**1**	
3.5 Diseño de base de datos								**0,2**	**0,8**
4 Documentación PFC									**1**

El valor ganado se obtiene de la multiplicación de los porcentajes del control de avance con el coste total por actividad planificada, de este modo se ha calculado la siguiente tabla.

Tabla 119. Valor Ganado

	2010						2011		
TAREA	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Enero**	**Febrero**	**Marzo**
1. Planificación y Requisitos									
1.1 Investigación									
1.1.1 Normativa ISO	**21.472,00 €**								
1.1.2 Buenas Prácticas		**21.471,92 €**							
1.1.3 Conformidad Legal			**12.688,00 €**						
1.2 Definir Requisitos			**4.880,00 €**						
1.3 Estimación de costes									
1.3.1 Definir Puntos de Función			**2.928,00 €**						
1.3.2 Realizar Estimación COCOMO II			**976,00 €**						
2. Análisis									
2.1 Análisis de la herramientas de mercado				**21.584,00 €**					
2.2 Detalle de casos de uso expandido					**7.798,24 €**	**10.999,52 €**			
3. Diseño									
3.1 Definir diseño conceptual							**45.760,00 €**		
3.2 Diseño de diagrama de clases							**2.288,00 €**		
3.3 Diseño de diagrama de secuencia								**2.288,00 €**	
3.4 Diseño de diagrama de estados									
3.5 Diseño de base de datos									
4 Documentación PFC									
Total de coste	21.472,00 €	21.471,92 €	21.472,00 €	21.584,00 €	7.798,24 €	10.999,52 €	48.048,00 €	2.288,00 €	- €
Total acumulado	21.472,00 €	42.943,92 €	64.415,92 €	85.999,92 €	93.798,16 €	104.797,68 €	152.845,68 €	155.133,68 €	155.133,68 €

A continuación, se puede ver la estimación de costes para este proyecto aplicando la técnica del valor conseguido con los datos de las estimaciones hechas en los puntos anteriores de este apartado.

En rojo se ve el coste de la planificación estimada del proyecto, en morado el coste de la planificación real y en azul el valor ganado.

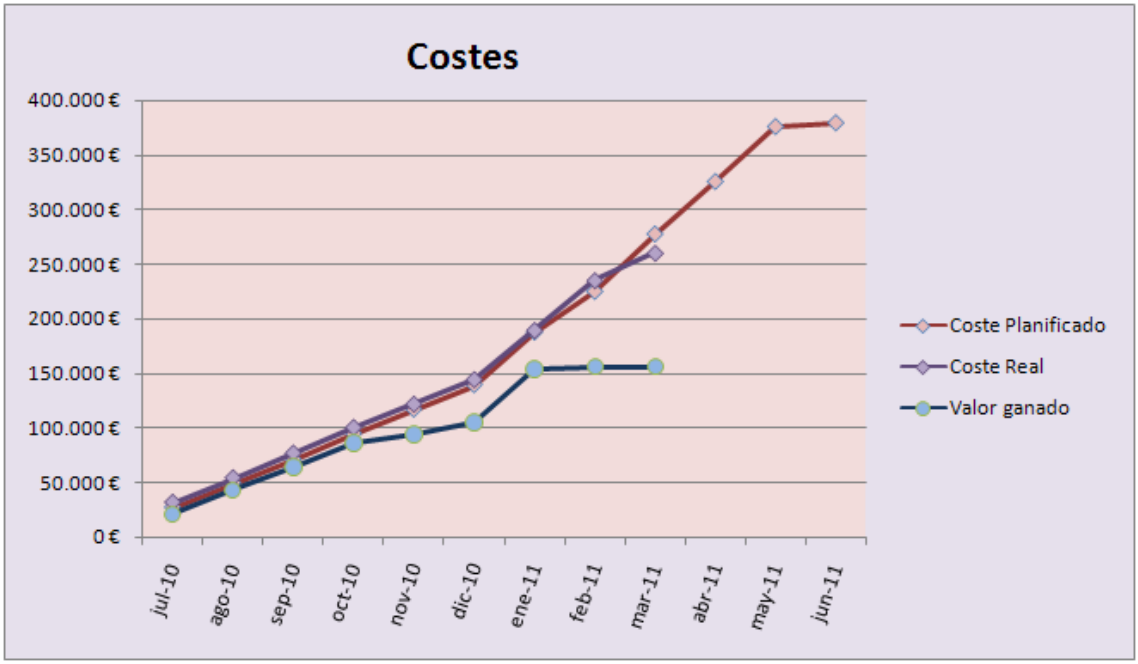


Figura 74. Diagrama Tecnología Valor Ganado

9 APORTACIONES DE UN GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

9.1 Aportaciones del Gobierno de la Seguridad TI

Los principales beneficios que aporta un Gobierno de Seguridad de la Información TI son:

- → Establecer una metodología estructurada para realizar el Gobierno de la Seguridad evitando desconocimiento e indecisiones.
- → Determinar las acciones ejecutivas de seguridad que ayuden a no emprender acciones de detalle costosas no requeridas.
- → Ayudar a la planificación estratégica de la seguridad (proponer requisitos de seguridad estratégicos) y coordinar la estrategia con una revisión continuada.
- → Integrar la información de incidentes de seguridad para definir un gobierno que ayude a optimizar su resolución definitiva.
- → Incorporar en el modelo de gobierno el cumplimiento de las normas y estándares relacionados con las mejores recomendaciones en seguridad.
- → Ayudar a determinar las responsabilidades adecuadas para cubrir los diferentes puestos que el Gobierno de la Seguridad TI requiere.
- → Mejorar la confianza de clientes y socios estratégicos por la existencia de un modelo de Gobierno de la Seguridad que ayude a comunicar que todo se encuentra bajo control.
- → Proponer un modelo de seguridad que se integra con el gobierno corporativo de las TI y a su vez con el gobierno corporativo de la organización.
- → Integrar dentro del modelo de Gobierno de la Seguridad los aspectos de continuidad de negocio.
- → Integrar el modelo de gobierno propuesto en la organización bajo dos aspectos: integración con los modelos de gestión y operación de la seguridad y resto de modelos de gobierno de mayor alcance..

Para obtener los citados beneficios al tratarse de un modelo de gobierno que incorpora cambios y resistencia a los cambios, los siguientes cuatro aspectos son clave:

- → Compromiso y apoyo de la Dirección de la Organización, tanto funcional como técnica.
- → Concienciación y formación del personal en la importancia de la seguridad y del gobierno de esta.
- → Compromiso de mejora continua, pensando que la solución a los riesgos nunca es una foto fija y requiere de una evaluación continuada con toma de decisiones continuada.
- → Al afectar la seguridad a toda la organización es clave mantener la sencillez de las soluciones y propuestas, pues por contra podemos proponer soluciones demasiado complejas para llevarlas a la práctica de manera eficiente y eficaz.

9.2 Conclusiones personales del proyecto

Al ser mi primer diseño amplio he podido sacar bastantes experiencias que emplearé en el futuro. Las principales conclusiones que he sacado del proyecto han sido las siguientes:

- → Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados. Es la mejor manera de evitar desviaciones.
- → No reinventar la rueda antes de emprender cualquier actividad en el área TI: apoyarse lo más posible en estándares, métodos y guías ya establecidos, así como en la experiencia de otras organizaciones.
- → Reservar la dedicación necesaria diaria o semanal ya que se ha de trabajar con continuidad en el proyecto y con plazos razonables.
- → Definición poco clara del alcance y de lo que es gobierno. Los temas estratégicos son complejos de definir y requieren ideas claras si queremos evitar desviaciones.
- → La importancia de la mejora continua y que los proyectos de seguridad al igual que del resto de áreas de SI no terminan cuando el proyecto termina y requieren de procesos de mejora continua.

10 REFERENCIAS

[1] Aceituno, Vicente. (2007). ISM3 Information Security Management Maturity Model. ISM3 Consortium

[2] Agencia Estatal Boletín Oficial del Estado. Consultado del 1 al 17 de Septiembre 2010. http://www.boe.es/

[3] Baggett, W. O. (2003). Creating a culture of security. The Internal Auditor, 60 (3), 37–41.

[4] Brabeion Polaris IT GRC Management Suite. Consultado el 4 de Octubre 2010. http://www.networkproductsguide.com/best/2008/Brabeion_Software.html

[5] Bresz, F.P. (2004). People—Often the weakest link in security, but one of the best places to start. Journal of Health Care Compliance, 6 (4), 57–60.

[6] Build Security In. Setting a higher standard for software ussurance. Homeland Security. (2006). Consultado en 28 de Octubre de 2010. https://buildsecurityin.us-cert.gov/

[7] Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. Work Study. 44 (8), 11–18.

[8] Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, William R. Wilson. (1999) Operationally Critical Threat, Asset, and Vulnerability Evaluacion (OCTAVE) Framework. Carnegie Mellon. Software Engineering Institute

[9] COBIT security baseline—An information security survival kit. (2004). Rolling Meadows, USA: IT Governance Institute.

[10] Computer Security Division. Computer Security Resource Center. National Institute of Standards and Technology. (2007). Consultado en Agosto y Octubre 2010. http://csrc.nist.gov/

[11] Da Veiga, A., Martins, N., & Eloff J. H. P. (2007). Information security culture—validation of an assessment instrument. Southern African Business Review, 11 (1): 147–166.

[12] Donaldson, W. H. (2005). U.S. capital markets in the post-Sarbanes- Oxley world: Why our markets should matter to foreign issuers. U.S. Securities and Exchange Commission. London School of Economics and Political Science.

[13] EAR/Pilar. Consultado el 1 de Octubre 2010. http://www.ar-tools.com/

[14] Electronic Communications and Transactions Act. (2002). Consultado el 30 de Octubre 2010: http://www.acts.co.za/ect_act/

[15] Eloff, J. H. P. & Eloff, M. (2005). Integrated Information Security Architecture, Computer Fraud and Security, 2005 (11), 10–16.

[16] Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. In Security and Privacy in Dynamic Environments. IFIP/ SEC2005; Boston: Kluwer Academic Publishers, 87–97.

[17] Gary Stoneburner, Alice Goguen, and Alexis Feringa. (2001). Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce

[18] Hellriegel, D., Slocum, J. W. (Jr), & Woodman, R. W. (1998). Organizational Behavior. (8th ed.). Cincinnati, OH: South-Western College Publishing. Holborn Books. Information Security architecture: An integrated approach to security in the organization (2005). Consultado el 31 de Octubre 2010: http://www.holbornbooks.co.uk/details. aspx?sn=1244811

[19] Infogov. The leader in Web-based IT Governance, Risk, Compliance and Fraud Management. (2009). Consultado en Agosto y Octubre 2010. http://www.infogov.co.uk/

[20] Information Security Forum (ISF). (2011). Consultado en Agosto y Octubre 2010. https://www.securityforum.org/

[21] Information Security Governance: Guidance for Boards of Directors and Executive Management. 2nd Edition.

[22] Information Systems Audit and Control Association. (2011). Consultado en 10 de Agosto de 2010. http://www.isaca.org/

[23] International Software, Benchmarking Standards Group. (2002). The Software Metrics Compendium

[24] Inventory of Risk Management / Risk Assessment methods and tools. Enisa (European Network and Information Security Agency). Consultado en Octubre 2010. http://rm-inv.enisa.europa.eu

[25] ISACA. (2009). An Introduction to the Business Model for Information Security.

[26] ISO 27000.ES el portal de ISO 27001 en Español. (2005). Consultado el 5 de Julio de 2010. http://www.iso27000.es/

[27] ISO 27001. Security home. (2011). Consultado el 1 de Julio de 2010. http://www.iso27001security.com

[28] ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

[29] ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements, Britain.

[30] ISO/IEC 27005. (2008). Information technology-Security techniques-Information security risk management, Britain.

[31] IT Governance Institute. (2007). Cobit 4.1

[32] IT Governance Institute. (2011). Consultado en 15 de Noviembre 2010. http://www.itgi.org/

[33] ITIL- Gestión de Servicios TI. Osiatis. Consultado en 2 Agosto 2010. http://itil.osiatis.es

[34] ITSMF. (2007). An Introductory Overview of ITIL v3. Best Management Practice

[35] Jaquith, Andrew. (2007). Security Metrics. Replacing Fear, Uncertainty, and Doubt. Addison-Wesley

[36] King Report. (2001). The King Report of corporate governance for South Africa. Consultado el 31 de Octubre 2010: http://www.iodsa.co.za/ downloads/King%20II%20Report%20CDRom%20Brochure.pdf

[37] Knapp, J. K., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). Top ranked information security issues: The 2004 International Information Systems Security Certification Consortium (SIC) survey results. Auburn, Alabama: College of Business Auburn University.

[38] Lockheed Martin. (2003). Systems Security Engineering Capability Maturity Model (SSE-CMM). Model Description Document Version 3.0

[39] Martins, A. & Eloff, J. H. P. (2002). Information Security Culture. In Security in the information society. IFIP/SEC2002. (pp. 203–214). Boston: Kluwer Academic Publishers.

[40] Martins, N. (2002). A model for managing trust. International Journal of Manpower. 23 (8), 754–769. The Concise Oxford Dictionary. (1983). Sykes, J.B. (Ed.) Oxford: Clarendon Press.

[41] McCarthy, M. P. & Campbell, S. (2001). Security Transformation. McGraw-Hill: New York. Martins, A. (2002). Information Security Culture. Master's dissertation, Rand Afrikaans University, Johannesburg, South Africa.

[42] Modulo Risk Manager (Modulo). Consultado el 5 de Octubre 2010. http://www.modulo.com/risk-manager

[43] Official ITIL Website. OGC. (2007). Consultado el 4 Agosto 2010. http://www.itil-officialsite.com/

[44] Posthumus, S. & Von Solms, R. (2005). IT Governance. Computer Fraud and Security. 2005 (6), 11–17.

[45] PriceWaterhouseCoopers. Information Security Breaches Survey. (2004). Consultado el 1 de Noviembre 2010: http://www.dti.gov.uk/industry_files/ pdf/isbs_2004v3.pdf

[46] PRiskVision OpenGRC (Agiliance). Consultado el 4 de Octubre 2010. http://www.agiliance.com/products/platform.html

[47] Promotion of Access to Information Act. (2000). Consultado el 2 de Noviembre 2010: http://www.acts.co.za/prom_of_access_to_info/index. htm

[48] Proteus (InfoGov). Consultado el 1 de Octubre 2010. http://www.infogov.co.uk/proteus_enterprise/step6.php

[49] Richards, N. (2002). The critical importance of information security to financial institutions. Business Credit, 104 (9), 35–36.

[50] Robbins, S. (2001). Organizational Behaviour. (9th ed.). New Jersey: Prentice Hall.

[51] Ross, B. (2000). New directives beef up trust in e-commerce. Computer Weekly News. Security. 2005. Security, innovation head CIO's 2005 agenda. Computer Fraud and Security, 2005 (1), 1–2.

[52] RSA Archer eGRC Solutions. Consultado el 4 de Octubre 2010. http://www.archer.com/solutions/index.html

[53] RSAM. Consultado el 5 de Octubre 2010. http://www.rsam.com/RsamPlatform.htm

[54] Security Art Work. S2 Grupo). Consultado en Agosto y Octubre 2010. http://www.securityartwork.es/

[55] Seguridad de la Información. Segu-Info. (2000). Consultado en Agosto y Octubre 2010. http://www.segu-info.com.ar/

[56] Sharon Taylor, David Cannon, David Wheeldon. (2007). ITIL V3. Service Transition. OGC (Office of Govemment Commerce)

[57] Sharon Taylor, Gary Case, George Spalding. (2007). ITIL V3. Continual Service Improvement. OGC (Office of Govemment Commerce)

[58] Sharon Taylor, Majid Iqbal, Michael Nieves. (2007). ITIL V3. Service Startegies. OGC (Office of Govemment Commerce)

[59] Sharon Taylor, Shirley Lacy, Ivor Macfarlane. (2007). ITIL V3. Service Operation. OGC (Office of Govemment Commerce)

[60] Sharon Taylor, Vernon Lloyd, Colin Rudd. (2007). ITIL V3. Service Design. OGC (Office of Govemment Commerce)

[61] Sistemas de Gestión Seguridad de la Información. Consultado el 2 de Julio de 2010. http://sgsi-iso27001.blogspot.com/

[62] STREAM Integrated Risk Manager (Acuity). Consultado el 30 de Septiembre 2010. http://www.acuityrm.com/

[63] Symantec. Consultado el 6 de Octubre 2010. http://www.symantec.com

[64] Teufel, S. (2003). Information Security Management—State of the art and future trends. In Proceedings of the Annual International Information Security South Africa (ISSA) conference. Johannesburg, SA, UNISA Press. Tretic, B. (2001 January). Can you keep a secret? Intelligent Enterprise. 4 (1).

[65] The Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC). (2003). IT Governance Institute, Board Briefing on IT Governance, 2nd Edition, USA.

[66] Trompeter, C. M. & Eloff, J. H. P. (2001). A framework for the implementation of Socio-ethical controls in Information Security. Computers and Security, 20 (5), 384–391.

[67] Tudor, J. K. (2000). Information Security Architecture—An integrated approach to security in an organization. Boca Raton, FL: Auerbach.

[68] Verton, D. (2000). Companies aim to build security awareness. Computerworld, 34 (48), 24.

[69] Virginia Information Technologies Agency (VITA). (w006). Information Technology Resouce Management (ITRM). Information Technology Risk Management Guidelin. Apeendix D- Risk Assessment Instructions

[70] Von Solms, R. (1997). Driving safely on the information superhighway. Information Management & Computer Security, 5 (1), 20–22. Von Solms, B. (2000). Information security—The third wave? Computers and Security, 19(7). November, 615-620.

[71] Von Solms, S. H. (2005). Information Security Governance—Compliance management vs. operational Management. Computers and Security, 24 (6), 443–447.

[72] Von Solms, S. H. (2006). Information Security Governance — Guidance for Boards of Directors and Executive Management

[73] Von Solms, S. H. (2006). Information Security—The fourth wave. Computers and Security. 25 (2006), 165–168.

[74] Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers and Security, 23 (33), 191–198.

[75] Witty, R. J. & Hallawell, A. (2003). Client issues for security policies and architecture. Gartner. ID number: K-20-7780.

11 ACRÓNIMOS

- Recurso (Asset): Cualquier cosa que tenga valor para la organización.
- Disponibilidad (Availability): Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.
- **Confidencialidad (Confidentiality):** Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
- **Eventos de seguridad de la información:** Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.
- **Incidente de seguridad:** uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.
- **Sistema de administración de la seguridad de la información (ISMS**): Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.
- **Integridad:** Propiedad de salvaguardar la precisión y completitud de los recursos.
- **Riesgo residual:** El riesgo remanente después de una amenaza a la seguridad.
- **Aceptación de riesgo:** Decisión de aceptar un riesgo.
- **Análisis de riego:** Uso sistemático de la información para identificar fuentes y estimar riesgos.
- **Valoración de riesgo:** Totalidad de los procesos de análisis y evaluación de riesgo.

- → **Evaluación de riesgo:** Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado significativo del riesgo.
- → **Administración del riesgo:** Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.
- → **Tratamiento del riesgo:** Proceso de selección e implementación de mediciones para modificar el riesgo.

Declaración de aplicabilidad: Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del ISMS.

12 ABREVIATURAS

- **ASL:** Application Services Library (Biblioteca de servicios de aplicativos)
- **CI:** Configuration Item.
- **CMDB:** Configuration Manager Database
- **CMM/CMMI:** Modelo de Capacidad y Madurez
- **COBIT:** Control Objectives for Information and related Technology
- **COCOMO:** Constructive Cost Model
- **DSDM:** Dynamic Systems Development Method (Método de desarrollo de sistemas dinámicos)
- **IEC:** Comisión Internacional de Electrotécnica
- **ISM:** Information Security Management
- **ISMS:** Information Security Management System
- **ISO:** Organización Internacional de Estándares
- **ISPL:** Services Procurement Library (Biblioteca de adquisición de servicios de información)
- **ISRM:** Gestión de riesgos de seguridad de la información
- **ITIL:** Information Technology Infrastructure Library
- **JTC 1:** Join Technical Committee Nº
- **MVC:** Modelo Vista Controlador.
- **OLA:** Operational Level Agreement
- **PDCA:** Plan-Do-Check-Act
- **RACI:** Las siglas de la matriz RACI de los tipos de responsabilidad, responsable, aprobador, consultado e informado.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información
- **SLA:** Service Level Agreement
- **SLR:** Service Level Reporting
- **TI:** Tecnología de la información