UNIVERSIDAD DE ALCALÁ

Escuela Téc. Sup. de Ingeniería Informática

MÁSTER EN DIRECCIÓN DE PROYECTOS INFORMÁTICOS

Trabajo Fin de Máster

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA COMPAÑÍA DE SOFTWARE QUE PROVEE SERVICIOS PAAS

Jonathan Ayala Santandreu

2021

Universidad de Alcalá

Escuela Politécnica Superior

Máster Universitario en Dirección de Proyectos de Informáticos

Trabajo Fin de Máster

"Diseño del Sistema de Gestión de Seguridad de la Información para una compañía de software que provee servicios PaaS"

Autor : **D. Jonathan Ayala Santandreu**

Director Máster : **Dr. D. Roberto Barchino Plata**

Tribunal evaluador :

Presidente del Tribunal :

Vocal 1º:

Vocal 2º :

Calificación : _____

Alcalá de Henares a, 16 de Julio del 2021

Índice

Contenido

Índice de figuras

Índice de tablas

RESUMEN

El objetivo principal de este proyecto es diseñar el Sistema de Gestión de Seguridad de la Información para una compañía de software que explota un gestor de contenidos a través de servicios cloud de tipo plataforma como servicio o PaaS.

Para desarrollar el SGSI, se utiliza la norma estándar para la seguridad de la información ISO 27001:2017, las prácticas para los controles de seguridad recogidos en la norma ISO 27002:2017 y los controles específicos para servicios en la nube recogidos en la norma ISO 27017:2021. Además, se lleva a cabo un completo análisis de riesgos siguiendo la Metodología de Análisis y Gestión de Riesgos de los sistemas de la Información MAGERIT.

El proyecto trata de relacionar los conocimientos académicos adquiridos en diferentes asignaturas del máster en materia de seguridad de la información y cumplimiento normativo con el mundo real de la empresa actual donde gran parte de los servicios TI son contratados a través de proveedores cloud.

Palabras clave: Seguridad de la información, Sistema de gestión de seguridad de la información, SGSI, ISO 27001, ISO 27002, ISO 27017, Cloud, PaaS, MAGERIT, análisis de riesgos.

ABSTRACT

The main goal of this project is designing the Information Security Management System for a service company that provides a CMS as a cloud solution based on a Platform as a Service model (PaaS).

To develop the ISMS, the international standard on information security management ISO 27001:2017 is used as well as the practices for information security controls of the standard ISO 27002:2017 and specific controls for cloud services from the standard ISO 27017:2021. Furthermore, a thorough risk analysis is performed following the Risks Analysis and Management for Information Systems Methodology MAGERIT.

The project aims to relate the academic knowledge acquired from this master studies in terms of information security and compliance to the real business world, in which currently IT services are widely hired to cloud service providers.

Keywords: Information security, Information Security Management System, ISMS, Risk Management, ISO 27001, ISO 27002. ISO 27017, Cloud computing, PaaS, MAGERIT.

1. Introducción

En la actualidad un gran número de empresas decide hacer uso de los servicios *cloud* proporcionados por proveedores especializados, ya que les permiten reducir la complejidad de sus procesos TI al externalizar la infraestructura tecnológica y su administración. A su vez, una gran mayoría de empresas proveedoras de software han adaptado su modelo de negocio a la oferta de servicios *cloud* que permiten hacer uso de sus aplicaciones liberando de la necesidad de mantener los elementos hardware y de comunicaciones necesarios para su despliegue a las empresas clientes que son usuarias de su software. Por tanto, las soluciones *cloud* nacen a partir de la necesidad de reducir la complejidad del área TI que muestran un gran número de empresas, pero, por otro lado, trae consigo la consecuente preocupación por la seguridad de la información, que abandona los límites de la empresa para ser alojada y/o procesada en sistemas gestionados por terceras partes. En ese sentido, la aparición de diversas normas, estándares y frameworks en materia de gestión de la seguridad de la información ha ayudado a las empresas a reforzar su estrategia de seguridad, haciéndola más eficaz y fácilmente gestionable, además de posicionarse ante los clientes como entidades preocupadas por garantizar la seguridad de la información que almacenan de sus usuarios.

Dentro de este escenario, el presente proyecto tiene como objetivo llevar a cabo el diseño del sistema de gestión de seguridad de la información para una compañía de software. Concretamente se centra en la parte de servicios en la nube que provee la compañía de tipo plataforma como servicio.

El trabajo se estructura en dos grandes secciones que corresponden a una parte teórica que pone de manifiesto los conceptos en los que se basa el proyecto como la seguridad de la información, normas, estándares y metodologías existentes o la seguridad aplicable en escenarios de servicios *cloud*. Una segunda parte que se centra en el trabajo personal desarrollado para diseñar el sistema de gestión de seguridad de la información del área de servicios *cloud* de la compañía propuesta. Finalmente se presentan los resultados y conclusiones tras el trabajo realizado y los posibles trabajos que pueden ser desarrollados en el futuro para ampliar o complementar a este.

Para llevar a cabo este trabajo fin de máster se han aplicado los conocimientos adquiridos en diferentes asignaturas que se han cursado en el Máster en Dirección de Proyectos Informáticos impartido por la Universidad de Alcalá de Henares. Además, se ha realizado un trabajo de investigación paralelo para profundizar en algunos de estos conocimientos adquiridos y también conocer nuevos conceptos, metodologías y herramientas necesarios para la consecución del proyecto.

2. Marco teórico y conceptual del proyecto

En este apartado se van a desarrollar los conceptos fundamentales y específicos sobre el que se sustentan los contenidos del trabajo realizado.

2.1. Computación en la nube

Se conoce como *cloud computing* al paradigma de tecnologías de la información que permite al usuario utilizar recursos hardware alojados remotamente y accesibles a través de Internet. Es decir, libera al cliente de tener que realizar inversiones en infraestructura tecnológica a través de la subcontratación de esta a un prestador de servicios en la nube.

2.1.1. Tipos de nubes

Privada

Los recursos hardware en una nube privada son de uso exclusivo para la empresa que la utiliza. Normalmente, es la propia empresa la que provee y gestiona la nube privada y los servicios que se ofrecen en ella. Grandes corporaciones o empresas gubernamentales suelen ser los principales usuarios de este tipo de nubes.

Pública

Los servicios *cloud* de una nube pública son ofertados a todos los clientes de forma que diferentes empresas comparten estos servicios. Ejemplos de estas nubes son Microsoft Azure, Google *cloud* o *Amazon Web Services*.

Híbrida

Existe un tipo de nube que es una combinación de las dos anteriores. Estas se caracterizan por combinar los servicios de la nube privada, por ejemplo, si manejan información crítica que no desean alojar en una nube pública, y el resto de los servicios, no críticos, pasan a alojarse en la nube pública. Este tipo de implementaciones viene dado por la idiosincrasia de la empresa que lo implanta.

2.1.2. Tipos de servicios de computación en la nube

Los servicios de computación en la nube se pueden clasificar de forma general en tres tipos: IaaS, PaaS y SaaS.

Infraestructura como servicio IaaS

Es el tipo más básico de computación en la nube. En él, no se ofrece ningún tipo de valor añadido, solo la infraestructura tecnológica para el alojamiento y el cómputo. Dos ejemplos de este tipo de servicio ofrecidos por Amazon Web Services (AWS) son EC2 y RDS, que se utilizarán en el desarrollo de este trabajo.

Software como servicio SaaS

En el nivel superior se encuentra este tipo de servicio cloud en el que se ofrecen las aplicaciones finales que son utilizadas por los clientes (empresas o particulares) para realizar el tratamiento de datos. Ejemplos de este tipo de servicio cloud pueden ser la suite de Google (Gmail, calendario, Dropbox…), Netflix o aplicaciones de streaming de música como Spotify.

Plataforma como servicio PaaS

En el nivel intermedio entre los dos mencionados anteriormente, se encuentra este tipo de servicio cloud que provee tanto de la infraestructura tecnológica que permite el alojamiento y

cómputo de información como las herramientas y funcionalidades necesarias para que los clientes puedan incluir sus propios desarrollos y configurar su propia solución software.

El siguiente diagrama muestra de forma esquemática el alcance de cada uno de los tipos de servicio de computación en la nube, así como los servicios que consume el cliente de servicios *cloud*.

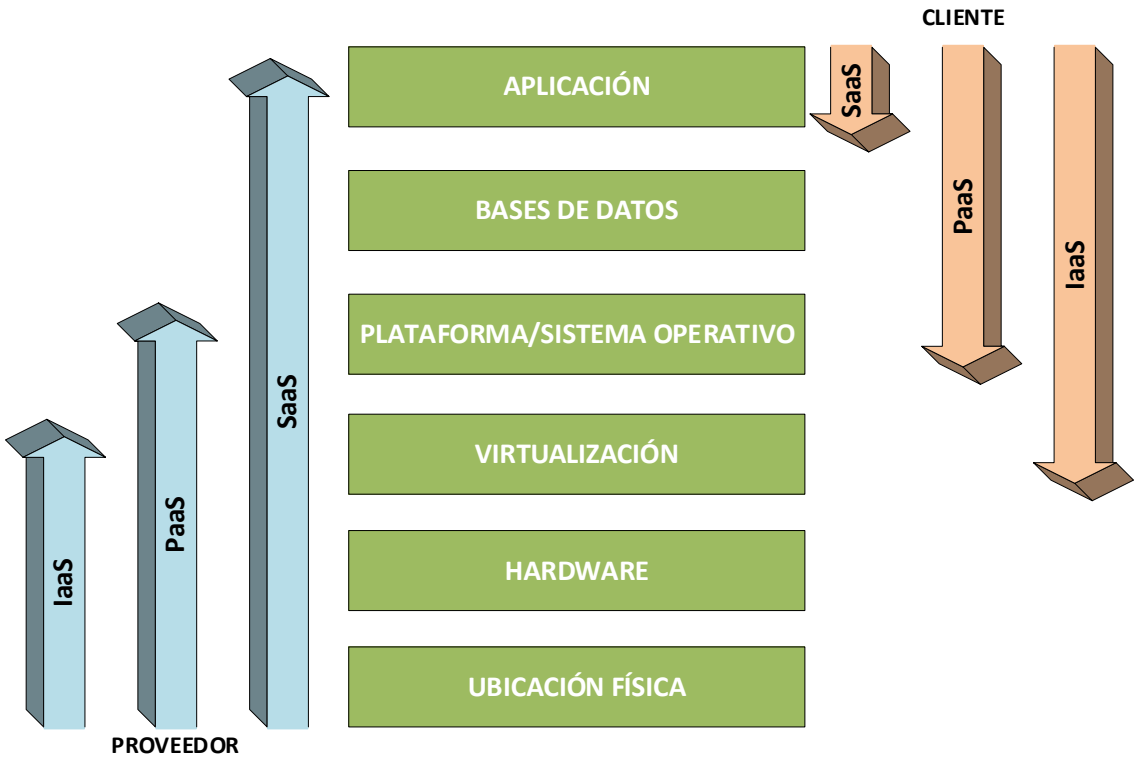

Figura 1. Alcance de los servicios de computación en la nube. Fuente: Elaboración propia

2.1.3. Aspectos de seguridad en los servicios de computación en la nube

Cuando se contratan los servicios de un proveedor *cloud* se deben tener en cuenta una serie de consideraciones específicas en cuando a la seguridad de la información. La Agencia Española de Protección de Datos nos ayuda en esta tarea con su *guía para clientes que contraten servicios de cloud computing* [1]. En ella se recogen los siguientes riesgos de seguridad:

- Posible falta de transparencia por parte de los proveedores de servicios *cloud* que impide conocer con exactitud los detalles del tratamiento de los datos que se alojan en la nube. Esto impide que se pueda llevar a cabo la evaluación de riesgos y la implementación de controles específicos para abordarlos.
- Posible falta de control a la hora de acceder a la información en todo momento o conocer su ubicación exacta. Esto puede propiciar una falta de control efectivo de la información.

Ante estos riesgos, la AEPD en su guía propone a los posibles clientes de servicios de cloud que antes de contratar el servicio evalúen los tratamientos de datos que realizan para estudiar los beneficios de trasladarlos a un servicio cloud, así como los riesgos potenciales que se pueden asumir. Para ello se propone la realización de un exhaustivo análisis de riesgos que indique qué información puede ser transferida a la nube. Además, este análisis de riesgos se debe contrastar

con la información que ofrece el proveedor acerca de las condiciones en las que se presta el servicio que siempre deberán cumplir los requisitos legalmente establecidos.

2.2. Seguridad de la información

Según las diversas definiciones que se pueden encontrar acerca de este término, se concluye que la seguridad de la información son las acciones que se llevan a cabo con el fin de preservar sus principios básicos o dimensiones: confidencialidad, integridad y disponibilidad. [2]

Por tanto, la seguridad de la información incluye todas las prácticas tanto proactivas como reactivas que se aplican a los sistemas de información para garantizar que se mantienen las dimensiones de la seguridad en el mayor grado posible.

Confidencialidad

Mantener la confidencialidad de la información implica restringir su acceso de forma que únicamente pueda ser accedida de forma autorizada. Es decir, sólo las personas y/o procesos autorizados podrán leer una pieza de información, de forma que terceras partes no puedan acceder.

Integridad

La integridad de la información se garantiza cuando únicamente puede ser modificada de forma autorizada. Únicamente los procesos y/o personas autorizadas podrán realizar modificaciones en una pieza de información. De esta forma se asegura que la información no ha sido alterada de ninguna forma.

Disponibilidad

Mantener la disponibilidad de la información es garantizar que esta será accesible siempre que se requiera. Es decir, implica que no se perderá o que no será inaccesible en aquellos momentos en que se requiera su consulta por parte de personas y/o procesos.

2.2.1. Gestión de la seguridad de la información

La gestión de la seguridad de la información, como cualquier otro proceso de gestión, se basa en el ciclo de Deming o mejora continua ya que se asume que nunca se va a alcanzar un estado final en el que la seguridad del sistema está 100% garantizada. Esto es debido a las variaciones que pueden ocurrir dentro de los procesos de la compañía, así como en su naturaleza o la de las propias amenazas que puedan ir surgiendo con el paso del tiempo. Es, por tanto, un ciclo que tendrá una duración igual a la del ciclo de vida de la compañía o los procesos para los que se haya implementado.

A continuación, se va a explicar en detalle cada una de las fases del ciclo de Deming y como se aplican en el contexto que nos ocupa de la gestión de la seguridad de la información.

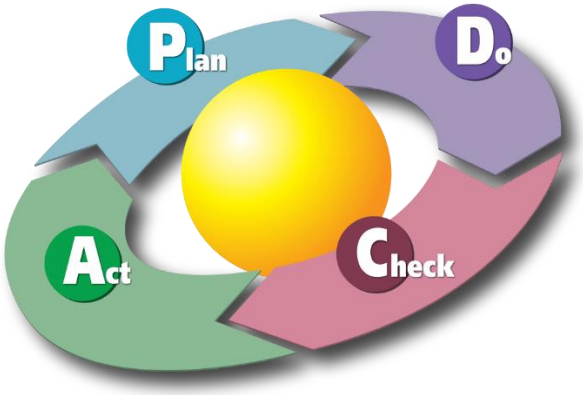

Figura 2. Ciclo de Deming. Fuente: https://commons.wikimedia.org/wiki/File:PDCA_Cycle.svg [3]

Planear (Plan)
Es la primera fase del ciclo, en ella se establecen los objetivos y se identifican las actividades o tareas necesarias para conseguirlos. También se pueden identificar cambios en tareas o actividades existentes con el fin de mejorarlas. Además, se planifica el tiempo de consecución de los objetivos en cada tarea.

Hacer (Do)
En esta etapa se ponen en práctica las actividades, tareas o mejoras resultado de la fase anterior.

Verificar (Check)
Se comprueba el grado de consecución de los objetivos una vez pasado el periodo de tiempo planificado.

Actuar (Act)
Tras la verificación de los resultados se toman decisiones en base a estos que pueden llevar a realizar ajustes en las tareas o actividades para conseguir un mayor grado de consecución de los objetivos. En ese caso se vuelve al inicio del ciclo.

2.2.2. Marcos de referencia para la gestión de seguridad de la información

Dada la importancia de la seguridad de la información para las compañías, existen diferentes marcos de referencia que abordan cuestiones relacionadas con esta [14]. Se van a describir brevemente los que tienen mayor presencia y son más utilizados por compañías de todo el mundo.

ISO 27000
La serie de normas de la familia 27000 desarrolladas por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commision), estableces los estándares y mejores prácticas relacionados con la seguridad de la información con el fin de establecer un marco común para el desarrollo, implementación y mantenimiento de Sistemas de Gestión de Seguridad de la Información (SGSI). Dentro de esta serie de normas, la principal es la ISO 27001 que desarrolla los requisitos para la implantación del sistema de gestión de seguridad de la información. El resto de las normas de esta familia son ampliaciones o especificaciones concretas como auditoría del SGSI, controles específicos para ciertos escenarios, uso de redes, entornos cloud, escenarios interorganizacionales etc.

Cobit

Objetivos de Control para las tecnologías de la información (Cobit) es un marco de trabajo que establece las mejores prácticas para el gobierno y gestión de la tecnología y la información de las empresas. En lo relacionado con la seguridad, Cobit propone integrar la seguridad de la información de forma transversal en cada aspecto de la gestión y operaciones de la compañía y establece procesos relacionados con la seguridad de la información [4].

ITIL

La librería de infraestructura de tecnología de la información (ITIL) es un marco de trabajo que describe una serie de buenas prácticas para la gestión de servicios de tecnologías de la información. En materia de seguridad, ITIL plantea el proceso de gestión de la seguridad de la información que se recoge en la fase de diseño del servicio por lo que se aplica de manera transversal a todos los servicios de la empresa

2.3. Normas y estándares de seguridad de la información utilizados en el proyecto

A continuación, se enumeran las normas y estándares de seguridad que se han seguido para la realización del proyecto.

2.3.1. ISO 27001: 2017

La norma internacional ISO 27001 establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de las organizaciones [5]. Además, incluye los requisitos para la evaluación y tratamiento de riesgos de seguridad de la información.

Es la norma que se va a seguir exhaustivamente para diseñar el sistema de gestión de seguridad de la información que recoge este proyecto.

2.3.2. ISO 27002: 2017

Otra norma de la familia ISO 27000 en la que describen prácticas para la selección, implantación y gestión de controles de seguridad para el sistema de gestión de seguridad de la información basado en la norma ISO 27001 de acuerdo con el entorno de riesgos de la compañía.

Esta norma viene a completar la información descrita en la ISO 27001, proporcionando un mayor nivel de detalle en cuanto a los controles que se debe implementar el SGSI.

2.3.3. ISO 27017:2021

La tercera norma de la familia ISO 27000 que se utiliza en este proyecto viene a completar las dos anteriores en cuanto a la especificidad del entorno de servicios *cloud* propuesto en este proyecto.

La norma ISO 27017 establece una serie de directrices para los controles de seguridad implementados por el sistema de gestión de seguridad de la información basado en la norma ISO 27001 que estén relacionados con servicios *cloud*. Su principal particularidad es la división de responsabilidades entre proveedores y clientes.

Gracias a esta norma, los clientes de servicios *cloud* pueden garantizar la seguridad de la información de sus sistemas a pesar de que esta se encuentre alojada en servicios en la nube de terceros.

2.4. Metodología utilizada

En este apartado se describe la metodología que se ha utilizado para realizar el análisis de riesgos del sistema de gestión de seguridad de la información.

2.4.1. MAGERIT

Es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica (Comisión de Estrategia TIC en la actualidad) para reducir el riesgo que presenta la implantación y utilización de las TI en las organizaciones, principalmente diseñada para su utilización dentro del ámbito de las Administraciones Públicas.

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información [6].

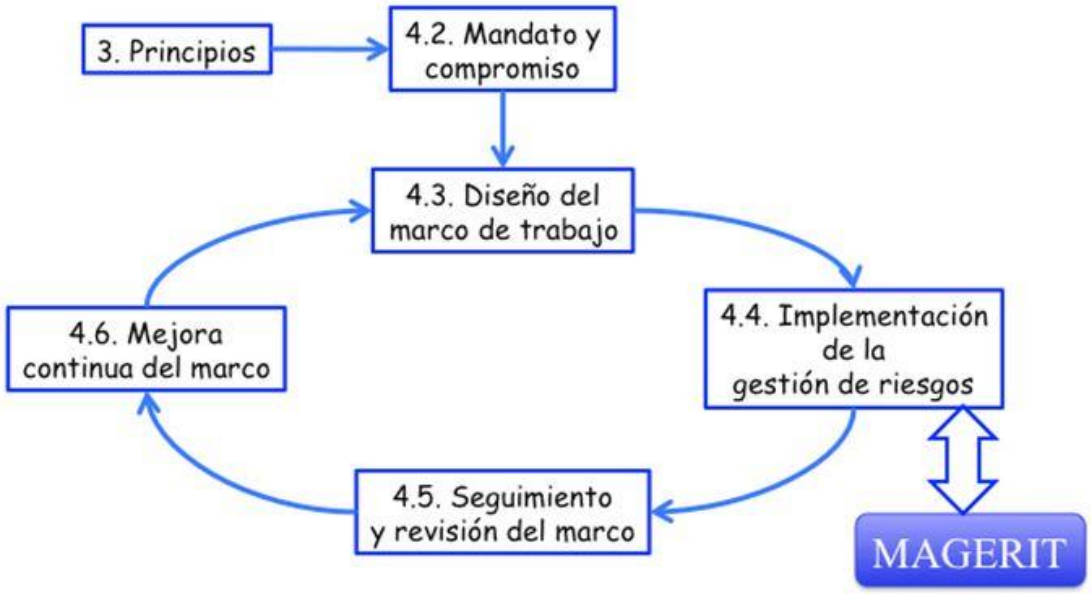

Figura 3. MAGERIT. Fuente: MINHAP

Una de las características de la metodología MAGERIT es que propone dos dimensiones de seguridad de la información adicionales a las tres mencionadas anteriormente:

- **Disponibilidad** de los servicios para poder ser usados cuando se necesite.
- **Integridad** o mantenimiento de las completitud y corrección de la información
- **Confidencialidad** para que la información llegue únicamente a las personas autorizadas
- **Autenticidad** que asegura que la entidad que maneja la información es quien dice ser o bien que garantiza la fuente de la que proceden los datos
- **Trazabilidad** para poder determinar quién hizo qué y cuando.

MAGERIT propone el análisis de riesgos mediante los siguientes pasos [6]:

1. Identificar los activos relevantes para la Organización, sus relaciones con otros activos y su valor, respecto al daño (coste) que supondría su degradación
2. Identificar las amenazas a las que se exponen los activos
3. Determinar las salvaguardas disponibles y su eficacia frente al riesgo

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto

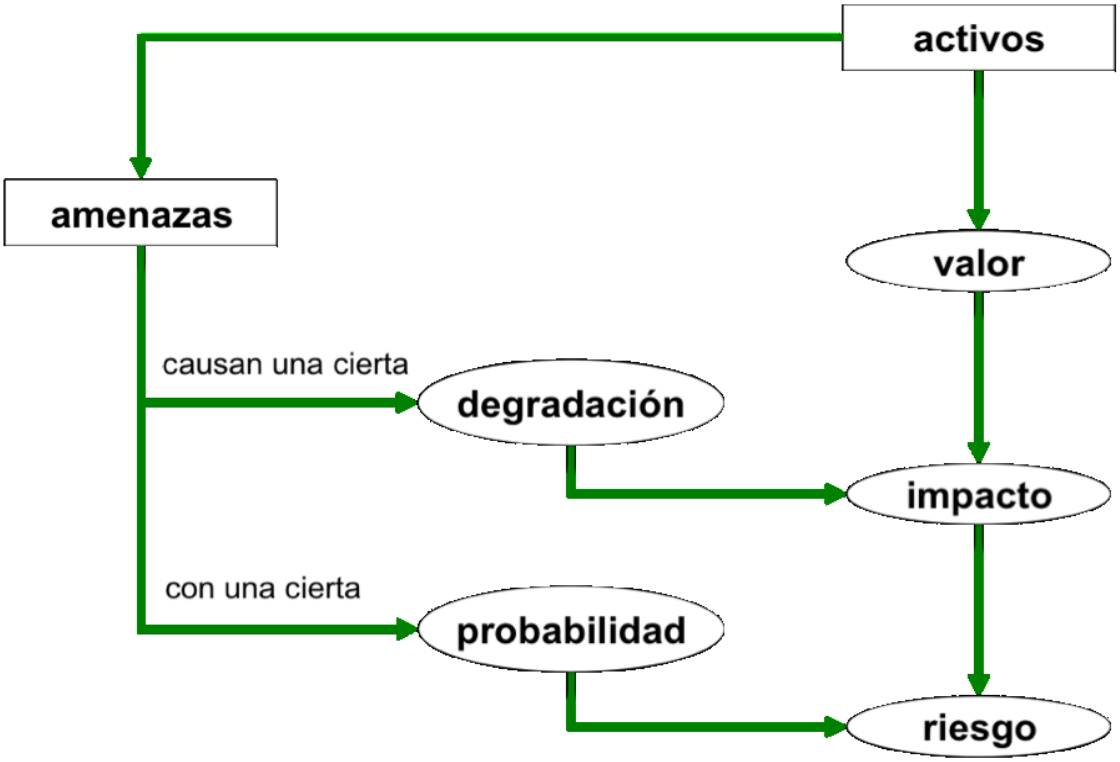

Figura 4. Elementos del análisis de riesgos. Fuente: MINHAP

3. Diseño del Sistema de Gestión de Seguridad de la Información

El presente capítulo desarrolla todo el trabajo realizado para la elaboración del diseño del SGSI para la compañía propuesta en este proyecto. Para ello, se irán describiendo todos los apartados declarados por la ISO 27001 que deben cumplirse en un SGSI.

3.1. Contexto de la organización

En este apartado se va a describir el contexto del entorno donde se va a realizar el diseño del sistema de gestión de la seguridad de la información.

3.1.1. Información de la compañía

La compañía en la que se va a desarrollar este proyecto se dedica a la explotación de un producto software que consiste en un gestor de contenidos o CMS. Este gestor de contenidos aparte de proveer las funciones de almacenamiento y clasificación de información también ofrece funcionalidades de creación de sitios web mediante un sistema de plantillas y configuraciones específicas que dota de una gran flexibilidad a las empresas a la hora de crear completos sitios web sin apenas esfuerzo.

El CMS se explota en dos versiones, una llamada *on-premises* que es aquella en la que el cliente recibe el software para explotarlo en su propia infraestructura y la versión *cloud* que se ofrece como una solución de tipo plataforma como servicio o PaaS, es decir, a través de una nube pública se proveen a los clientes las herramientas necesarias que les permiten construir sus propias soluciones tomando como base el CMS de la compañía.

3.1.1.1. Misión, visión y valores

Se podría definir la misión, visión y valores de la compañía como sigue.

Misión

Desarrollar el mejor CMS que ayude a todas las compañías que necesiten gestionar sus contenidos de forma sencilla, ágil, eficaz y con el menor impacto posible en su negocio en cuanto a costes y tiempos de implementación.

Visión

Convertirse en el CMS líder de ventas con el mayor número usuarios y con el que se sirvan las páginas web de todas las marcas líderes en su sector.

Valores

Éxito, aprendizaje, innovación, libertad y comunidad.

3.1.1.2. Estructura interna de la compañía

La compañía está dividida en las siguientes áreas que se muestran en el siguiente organigrama

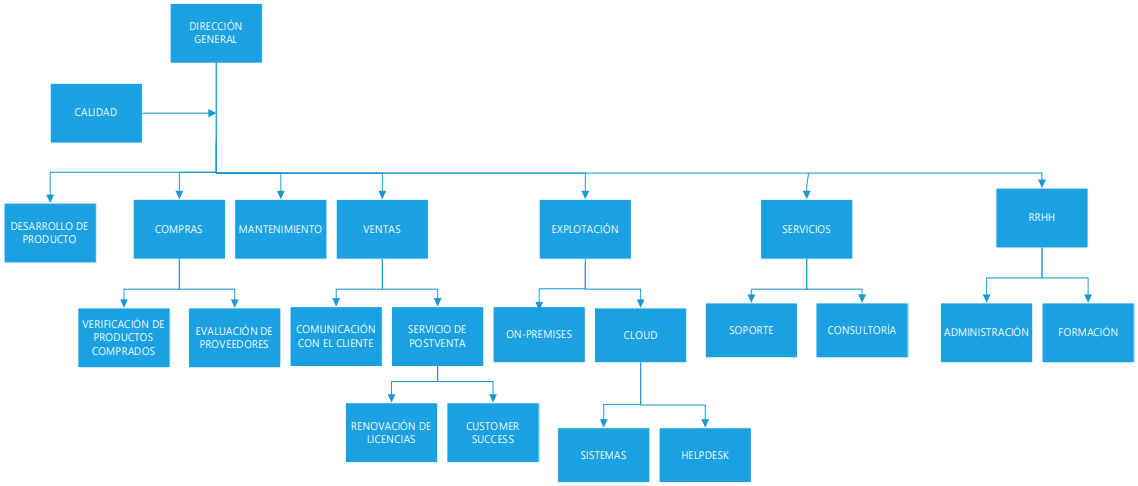

Figura 5. Organigrama de la compañía. Fuente: Elaboración propia

Dirección general

Este departamento está conformado por la alta dirección. Serán quienes elaborarán la política de seguridad y asignarán responsabilidades y autoridades a los roles relacionados con la seguridad que correspondan.

Desarrollo de producto

Esta área se encarga del desarrollo del software. Está principalmente compuesto por ingenieros, programadores, analistas, expertos en interfaz de usuario y *product owners*.

Compras

En esta área se gestionan las compras que se realizan en la empresa, desde los equipos informáticos para los trabajadores hasta los *caterings* y materiales para eventos comerciales.

Mantenimiento

Esta área también compuesta en su mayoría por programadores se encarga del mantenimiento de las versiones ya lanzadas del producto, solución de errores de código, creación de parches y pruebas del software

Ventas

Aquí se realiza la venta del producto a través de un sistema de licencias. Los integrantes de esta área son en su mayoría personal de desarrollo de negocio y éxito de clientes que se encargan tanto de la búsqueda e identificación de potenciales clientes como de mantener satisfechos a los clientes ya existentes y mediación en la renovación de licencias.

Explotación

La explotación del producto se realiza en dos formatos, uno de ellos es *on-premises*, en la que el cliente tiene que utilizar su propia infraestructura para desplegar la aplicación. La segunda es

en la nube o *cloud*. En esta última, el despliegue y alojamiento de datos se gestiona desde la propia compañía que a su vez utiliza un servicio en la nube de terceros llamado *Amazon Web Services* (AWS).

Por tanto, en esta área se lleva a cabo la explotación del producto en sus dos modalidades. La versión *on-premises* que se encargarán de tener los repositorios actualizados donde los clientes puedan obtener todos los componentes necesarios para montar su arquitectura. Aquí participan los programadores e ingenieros de las áreas de desarrollo de producto y mantenimiento.

Para la versión *cloud* se ofrecen todas las funcionalidades a través de servicios en la nube. Está conformado en su mayoría por los ingenieros de confiabilidad del servicio o SREs que son los que monitorizan, gestionan y mantienen los servicios funcionando con normalidad. Dentro de este grupo, existe un subconjunto que están más dedicados a temas de seguridad. Además, existe un área de *helpdesk* en la que los clientes reportan dudas o problemas encontrados que son resueltas por ingenieros de la compañía y otra de sistemas donde los SREs se encargan de monitorizar los recursos y asegurarse de que todas las instancias estén levantadas y funcionando correctamente.

Servicios

El área de servicios ofrece por una parte un excelente servicio de soporte compuesto por ingenieros que acompañan a los clientes durante su experiencia de uso del producto ayudándoles con cualquier problema que pueda surgir, así como con dudas de carácter técnico. También existe un área de servicios de consultoría dedicados a sus clientes que así lo requieren.

RRHH

Esta área se encarga de los recursos humanos de la empresa, tanto de la contratación, entrevistas, nóminas como de fomentar el bienestar de los empleados mediante actividades diversas.

3.1.1.3. Clientes

A continuación, se enumeran una serie de clientes tipo de la compañía para reflejar qué clase de información se puede manejar.

Agencia de viajes

La agencia de viajes ha decidido comprar una licencia para utilizar el CMS que provee nuestra empresa. Utilizará el gestor de contenidos para almacenar toda la información de sus activos que son hoteles, apartamentos, casas rurales, viajes organizados, vuelos programados y billetes de tren y autobús. Además, utiliza el sistema de plantillas para mostrar de una forma atractiva todos sus servicios en el sitio web que han creado con la funcionalidad correspondiente. Hacen gran uso de las capacidades de personalización para ofrecer ofertas personalizadas a los visitantes a la web.

Periódico estatal

Un prestigioso periódico estatal de un país europeo también se ha decidido por este CMS para poder gestionar sus contenidos. Con él, los editores pueden almacenar toda la información de las noticias además de los elementos gráficos como fotos o vídeos. Gracias a la potente

herramienta de búsqueda y la organización jerárquica de los contenidos, es tremendamente sencillo para ellos encontrar información relevante con la que poder ampliar o argumentar sus artículos. También hacen uso de las funciones para creación de sitios web para exponer sus noticias online a través de su página web.

Universidad

Una reputada universidad centrada a los estudios de negocios decidió hacer uso de los servicios *cloud* del CMS para gestionar la información relativa a su oferta académica, así como al portal del alumno. Por tanto, por una parte, se gestiona la información de los cursos que se ofertan, sus contenidos, profesorado, experiencias de alumnos anteriores y trámites administrativos, mientras que por otro lado se implementa la intranet donde los alumnos pueden acceder para conocer información de su matriculación, entrar a las asignaturas en curso y descargar los materiales correspondientes.

3.1.2. Descripción del entorno tecnológico

En este apartado se va a detallar el entorno tecnológico sobre el que se va a trabajar con el fin de dar a conocer la arquitectura del sistema y aquellos puntos que son de acceso, los actores involucrados y el almacenamiento de datos. En primer lugar, se va a profundizar en la arquitectura de la instalación típica de cada cliente para después pasar a ver la arquitectura general de todo el sistema *cloud* de la compañía.

3.1.2.1. Arquitectura específica por cliente

Cada cliente que contrate una licencia de uso de la solución *cloud* del CMS obtiene automáticamente los elementos que se muestran en la siguiente ilustración.

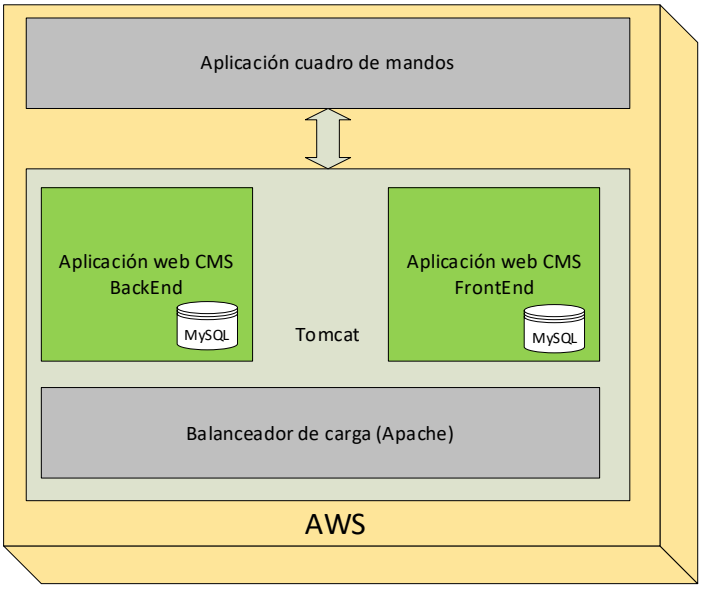

Figura 6. Arquitectura específica por cliente. Fuente: Elaboración propia

Aplicaciones web CMS

Se genera un alojamiento en la nube pública de servicios web de Amazon (AWS), concretamente EC2, para un alojar un servidor apache tomcat que despliega la aplicación web del CMS para la parte backend, es decir, aquella que será utilizada por los usuarios de la compañía para gestionar contenidos y la forma en que serán presentados. Por otro lado, en otra instancia EC2 de AWS

independiente se despliega la aplicación web del CMS para la parte *frontend*, que es la utilizada para exponer el contenido a los usuarios generales. Será la aplicación web que exponga los sitios y servicios web que muestran el contenido al público objetivo de la compañía. Esta aplicación puede duplicarse en aquellos casos en que sea necesario debido a una alta demanda para así garantizar la alta disponibilidad.

Bases de datos

Como puede verse en la ilustración, cada aplicación web está asociada a una base de datos MySQL que será la encargada de almacenar tanto las configuraciones y datos necesarios para el funcionamiento de la aplicación web CMS como el contenido propiamente dicho. Esta base de datos será desplegada a través de una instancia de Amazon RDS independiente para cara una de las aplicaciones de CMS.

Balanceador de carga

Frente a las aplicaciones web desplegadas, se ubica un balanceador de carga con el fin de garantizar los tiempos de respuesta y minimizar posibles retardos.

Aplicación cuadro de mandos

Por último, se ofrece una aplicación de autoservicio desde la cual se pueden controlar los servicios en la nube. Por ejemplo, reiniciar los servidores, actualizar alguna de las aplicaciones web, incluir algún nuevo módulo, comprobar el estado de la base de datos y realizar o restaurar *backups* en caso de fallos.

3.1.2.2. Arquitectura general del sistema

A continuación, se describe la arquitectura completa del sistema *cloud* de la aplicación CMS.

Como se puede observar en la siguiente ilustración, todas instalaciones de clientes son alojadas en la nube pública de AWS. Para cada uno de ellos se tendrá la arquitectura específica mencionada en el apartado anterior.

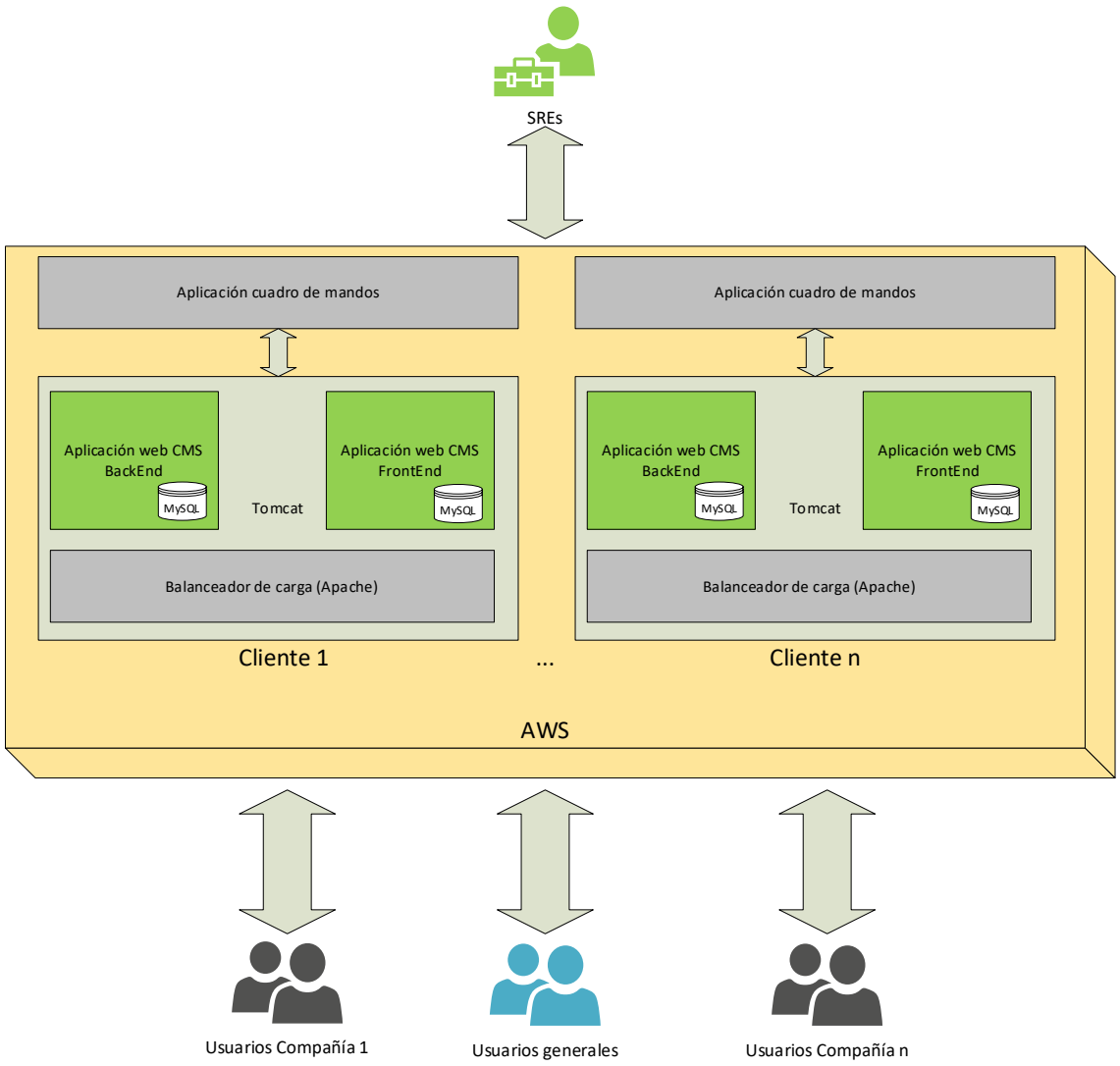

Figura 7. Arquitectura general del sistema. Fuente: Elaboración propia

A continuación, se describen los diferentes actores que forman parte del sistema.

SREs

Como se explicó en el apartado de información sobre la compañía y sus departamentos, los ingenieros de confiabilidad del sistema participan activamente en la administración y mantenimiento de los servicios *cloud* que se proveen a los clientes. Por tanto, ellos tienen acceso a todas las instalaciones para administrarlas a través de la aplicación de cuadro de mandos o accediendo directamente a los elementos software que componen la instalación como pueden ser el servidor Tomcat, apache o la base de datos MySQL de cada CMS desplegado.

Usuarios compañía X

Los usuarios de una compañía que han contratado el servicio *cloud* del CMS, pueden ser desde editores de contenido o maquetadores hasta programadores, técnicos y administradores. Se trata de todos aquellos pertenecientes a la compañía que van a hacer uso de la aplicación CMS desde el punto de vista de gestor de contenidos, ya sea para introducir una nueva funcionalidad

que han programado, añadir nuevo contenido relativo a su negocio o para administrar los permisos de qué contenido puede ver cada usuario.

Estos usuarios, en función del perfil que tengan, accederán tanto a la aplicación del cuadro de mandos para asegurarse que todo está funcionando correctamente y administrar el sistema como a la parte de *backend*. Según sea su perfil y permisos asociados, tendrán acceso total, parcial o restringido al contenido de la base de datos y funcionalidades de la aplicación CMS.

Usuarios generales

Estos son los usuarios que desde cualquier origen pueden hacer uso del sistema. Accederán a la aplicación CMS *frontend* y no tendrán, en ningún caso, acceso total a la base de datos, tan solo a aquellos contenidos que se hayan hecho públicos y sean accesibles de acuerdo con el perfil que tengan. Continuando con los ejemplos de clientes que se mencionaron en el apartado anterior, se trataría de los subscriptores al periódico estatal, los alumnos de la escuela que acceden a la intranet, una persona cualquiera que se interesa por uno de los estudios de la universidad y accede al sitio web para buscar más información o la persona que busca viajes programados en el sitio web de la agencia de viajes. Es decir, son usuarios que no pertenecen a la compañía que ha contratado la licencia de uso del CMS, sino, generalmente, sus clientes.

3.1.3. Necesidades

Como se explicó anteriormente, en el contexto propuesto, la misión de la empresa tiene como objetivo estratégico posicionarse como líderes dentro de su segmento y para ello tienen que crecer en lo que a número de clientes de la versión *cloud* se refiere y para ello es necesario asegurarles que sus contenidos van a disponer de todas las garantías en lo relacionado con la seguridad.

Por esta razón se ha identificado la necesidad de implantar un sistema de gestión de seguridad de la información en la compañía. Para acelerar este proceso de transformación, se ha decidido comenzar por el área de explotación de la solución *cloud*, que es la que inicialmente se quiere dotar de las máximas garantías de seguridad. Esto será un factor diferenciador que mejorará la imagen de marca y animará a los clientes a confiar en el servicio *cloud* del CMS. Es importante controlar todas las dimensiones de la seguridad pues es de vital importancia mantener la integridad de los datos manejados por los clientes, su confidencialidad para todos los casos y su disponibilidad en todo momento.

3.1.3.1. Partes interesadas

Según establece la ISO 27001, la organización debe determinar las partes interesadas que son relevantes para el SGSI y sus requisitos correspondientes [5]. Por tanto, se identifican como partes interesadas las siguientes:

Clientes

Serán los que contraten y hagan uso de los servicios *cloud* ofrecidos por la compañía. De cara a la ley de protección de datos, según establece por la Agencia Española de Protección de Datos en su guía para clientes que contraten servicios de *cloud computing*, seguirían siendo los responsables del tratamiento de los datos personales que puedan almacenar sus sistemas [1]

Compañía

Es la que ofrece la versión PaaS de su software CMS. Para proveer de este servicio, subcontratarán, a su vez, la infraestructura a proveedor externos de servicios de computación en la nube como es *Amazon Web Services*. De esta forma y según se indica en la norma ISO 27017, la compañía es a su vez proveedora de servicios *cloud* y cliente de un proveedor de servicios *cloud* [7]. Además, de cara a la ley de protección de datos, según establece por la Agencia Española de Protección de Datos en su guía para clientes que contraten servicios de *cloud computing*, les convierte en encargado de tratamiento de datos personales.

Proveedor de servicios *cloud* externos

Será la empresa a la que se contratan los servicios de computación en la nube como tal, es decir la infraestructura tecnológica para, en base a ella, desplegar la plataforma de servicios conformada por el CMS y sus diferentes funcionalidades, así como la aplicación de cuadro de mandos. Este proveedor va a ser

3.2. Alcance del Sistema de Gestión de Seguridad de la Información

De acuerdo con lo establecido por la norma ISO 27001 respecto al alcance del SGSI, este debe ser determinado por la organización en base a su contexto y necesidades [5]. Por tanto, en el caso propuesto para este trabajo tenemos que el SGSI abarcaría a los procesos dentro del área de explotación *cloud* del producto, las actividades que se llevan a cabo en el mismo y los actores involucrados.

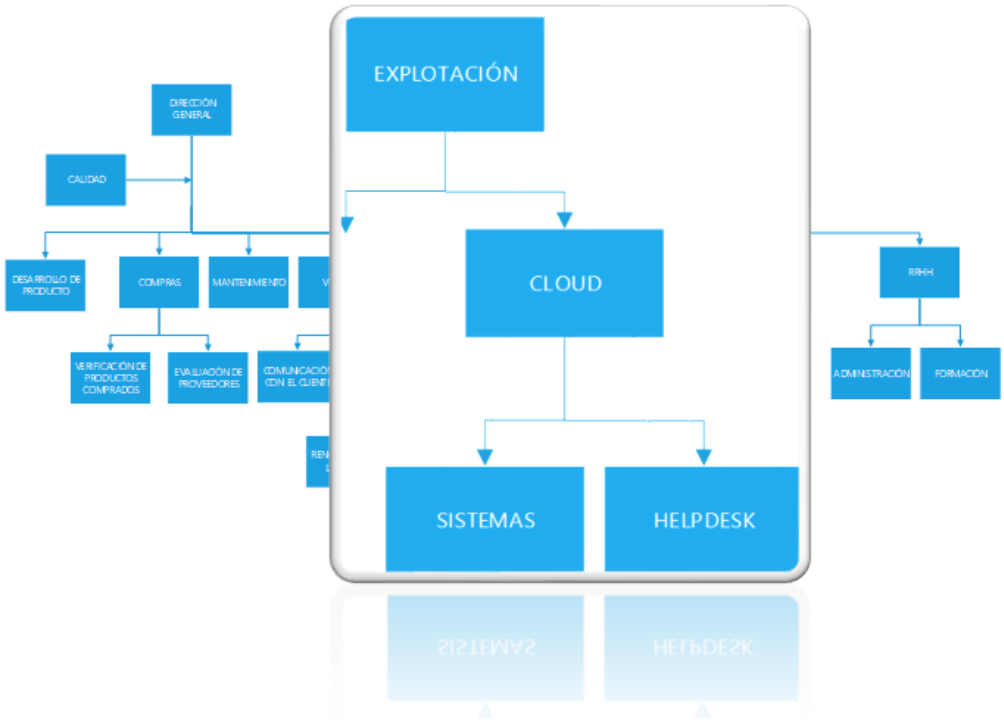

Figura 8. Áreas de lcance del Proyecto. Fuente: Elaboración propia

3.2.1. Procesos, activos, actores y ubicaciones incluidos en el SGSI

A continuación, se van a enumerar todos los procesos que van a ser incluidos en el SGSI, detallando las actividades que en ellos se realizan, los activos que comprende, así como los actores que intervienen y las ubicaciones donde se encuentran.

Explotación

El proceso de explotación estará parcialmente incluido en el SGSI, ya que únicamente se contemplarán aquellas actividades relacionadas con el área de explotación *cloud* del producto. Esto incluye los repositorios donde se almacena el código fuente que se va a explotar en producción y/o otros entornos de pruebas, los ingenieros encargados de administrar estas funciones y los entornos asociados.

Activos

- Repositorio donde se aloja el código fuente que va a ser desplegado.
- Equipos informáticos utilizado por los ingenieros con los que se administra el repositorio.

Actores

- Ingenieros que administran el repositorio

Ubicaciones

- CPD de la compañía donde se almacena el repositorio
- Área de infraestructura de la compañía donde se encuentran los ingenieros

Cloud

El proceso de explotación de la versión Cloud del CMS es el más complejo y será el núcleo del SGSI, en él se incluye el código fuente que proviene de los entornos anteriormente descritos, los recursos hardware necesarios para desplegar toda la infraestructura sobre la que se ejecuta el CMS, es decir, los servidores de aplicaciones, la aplicación de control “cuadro de mandos” desde la que se monitorizan todos los recursos y la actividad del CMS,

Activos

- Software desplegado: Aplicación CMS *frontend* y *backend*
- Servidores de aplicaciones que donde se despliega el software
- Servidores web que permiten regular la carga (balanceadores de carga)
- Servidores de Bases de datos
- Datos contenidos en la base de datos: es importante resaltar que el SGSI no incluirá el contenido en sí de los datos en cuestiones de cumplimiento legal, que corresponde al cliente, sino la disponibilidad e integridad y confidencialidad de la información almacenada. Este límite se explicará con mayor detalle en el siguiente apartado.
- Software desplegado: Aplicación cuadro de mandos para monitorización de aplicaciones CMS desplegadas

Actores

- Ingenieros de confiabilidad del sistema SRE
- Clientes (usuarios finales) de la aplicación CMS y cuadro de mandos
- Usuario general que será usuario de la aplicación CMS de los clientes

Ubicaciones

- Área de infraestructura de la compañía donde se encuentran los SREs

- Infraestructura *cloud* de la que se conoce únicamente la región geográfica en la que se encuentra. Es importante resaltar que, en este punto, el control viene dado por la empresa prestadora de servicios *cloud* (AWS) por lo que se podrá incluir en el SGSI hasta cierto punto. Este límite se explicará con mayor detalle en el siguiente apartado.

Sistemas

El proceso de administración de sistemas también estará incluido en el SGSI. Este incluye las actividades de administración de los recursos de infraestructura tecnológica descritos en el apartado anterior

Activos

- Equipos informáticos utilizados por los SREs para administrar los sistemas
- Instancias de AWS donde se alojan los servidores de aplicaciones
- Instancias de AWS donde se alojan los servidores web
- Instancias de AWS donde se alojan los servidores de bases de datos
- Aplicaciones de monitorización de recursos

Actores

- Ingenieros de confiabilidad del sistema SRE
- Proveedor de servicios *cloud* (AWS)

Ubicaciones

- Área de infraestructura de la compañía donde se encuentran los SREs
- CPD de la compañía donde ejecuta la aplicación de control

Helpdesk

El SGSI también abarcará el proceso de *helpdesk* en el que se recogen y se resuelven incidencias de clientes a través de un sistema de *ticketing* (JIRA).

Activos

- Software desplegado: Sistema de *ticketing* (JIRA)

Actores

- Ingenieros de la compañía encargados de las tareas de soporte
- Clientes (usuarios finales) de la aplicación CMS

Ubicaciones

- CPD de la compañía donde se almacena la información recogida por el sistema de *ticketing*.
- Área de infraestructura de la compañía donde se encuentran los ingenieros

3.2.2. Interfaces y dependencias con otras compañías

La norma ISO27001 propone que el alcance del SGSI debe determinar las interfaces y dependencias de las actividades llevadas a cabo por la propia compañía y por otras externas.

Así mismo, la norma ISO 27017, establece las relaciones que pueden existir en un escenario *cloud* como el del presente proyecto en el que una empresa (apartado 4.2) puede ser cliente de un proveedor de servicios *cloud* al que contrata la infraestructura tecnológica necesaria para montar los servicios que provee a sus clientes, siendo a su vez, proveedor de servicios *cloud* para estos clientes [7]. Es decir, una misma compañía puede ser al mismo tiempo proveedor y cliente de servicios *cloud*. Ese es exactamente el caso que nos ocupa en este proyecto.

Según se especifica en el apartado 4.3 de la norma, el cliente de servicios *cloud* debe considerar los riesgos específicos de este tipo de entornos. Una vez seleccionado el servicio *cloud*, el cliente debería gestionar el manejo de su información para cumplir con los requisitos de seguridad de la información que tiene el propio cliente. Esto significa que, aunque la compañía centre todos sus esfuerzos en proteger la información alojada en su infraestructura, debe ser el cliente quien se encargue de gestionar la seguridad de la información que maneja en el CMS, así como de otros aspectos tales como cumplimientos legales, por ejemplo, RGPD.

De manera análoga, la compañía como cliente deberá estudiar el servicio *cloud* contratado y la seguridad de la información que ofrece para adaptar sus procesos según corresponda de forma que se garantice la seguridad de la información lo máximo posible.

Con el fin de mostrar de un vistazo las interfaces y dependencias del SGSI, se muestra el siguiente diagrama.

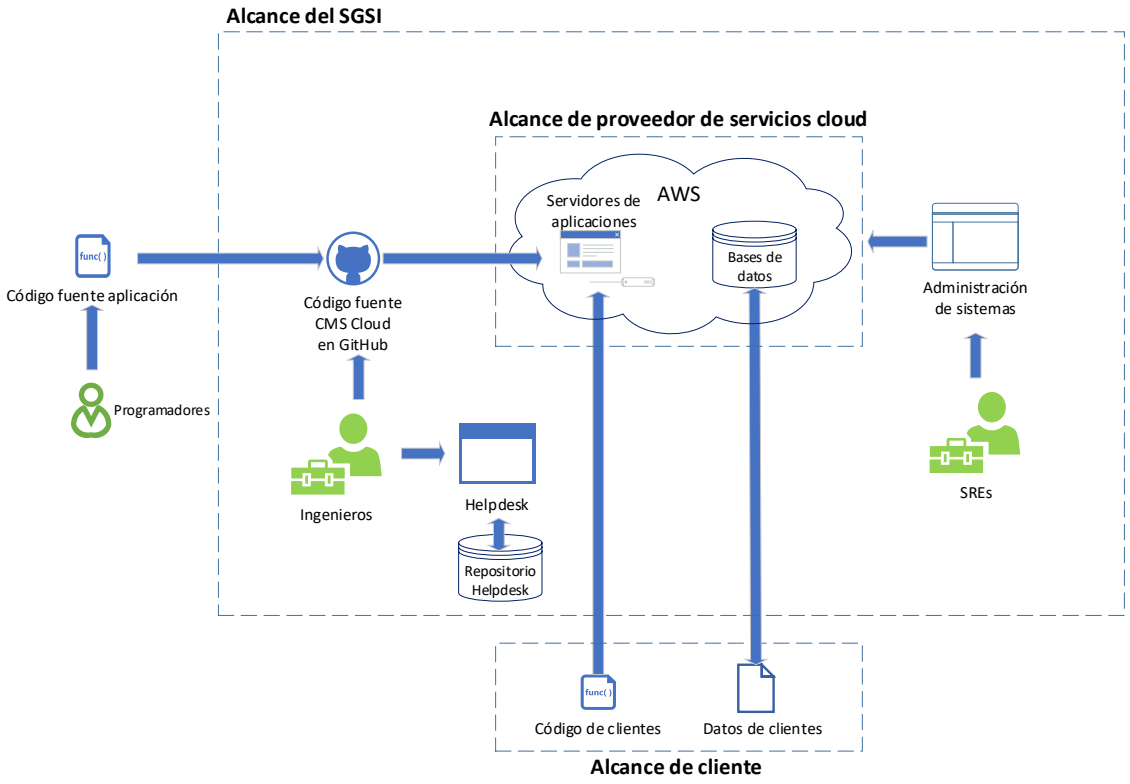

Figura 9. Alcance del SGSI. Fuente: Elaboración propia

Alcance del proveedor de servicios cloud

Dentro de este recuadro se encuentran los servicios que son suministrados por el proveedor de servicios *cloud*. La información estará fuera del alcance de la compañía por lo que, como se explicó anteriormente, se deberán asumir los riesgos que esto supone, conocer las prácticas de seguridad llevadas a cabo por el proveedor y aplicar las medidas necesarias que mitiguen los riesgos derivados del alojamiento *cloud*. En el caso de estudio, el proveedor de servicios es AWS, quien sostiene llevar a cabo el cumplimiento de la ISO 27001 e ISO 27017 entre otras [8].

Alcance del cliente

En el recuadro que muestra el alcance del cliente se puede ver cómo tanto el código propio que añade al software original y que puede realizar tratamiento y procesamiento de información, como los propios datos que los clientes intercambian con la aplicación, estarían fuera del alcance del SGSI. Será el propio cliente quien tiene que aplicar las medidas de seguridad necesarias a estos elementos para garantizar la seguridad de la información. Estas medias tendrán una magnitud apropiada, basándose en la seguridad de la información aportada por la compañía con la que han contratado el servicio *cloud*.

3.2.3. Aprobación y revisión del alcance del SGSI

El alcance del SGSI descrito hasta ahora tendrá que ser revisado y aprobado por la alta dirección de la compañía y el comité de seguridad. Así mismo se monitorizará su adecuación a las necesidades del resto de las partes interesadas y con las interfaces anteriormente mostradas.

Dado que en el mundo de la tecnología las condiciones son muy cambiantes y las compañías están en un proceso constante de adaptación, también será necesario que el alcance del SGSI sea revisado periódicamente de forma anual o semestral por parte de los miembros del comité de seguridad para identificar nuevas necesidades que puedan surgir, así como redundancias que puedan ser limitadas.

3.3. Liderazgo

3.3.1. Liderazgo y compromiso

La dirección de la compañía promoverá su compromiso con el SGSI a través de toda la compañía liderando las siguientes acciones:

- Establecer una política de seguridad que cumpla con los objetivos tanto de seguridad de la información como los estratégicos de la compañía. Esta política se detallará en el siguiente apartado.
- Proporcionar en todo momento los recursos necesarios para la implantación del SGSI
- Comprobar periódicamente que el SGSI cumple con su objetivo
- Manifestar la importancia de la seguridad de la información y promoviéndola entre las personas para dar como resultado un SGSI eficaz.
- Promover los principios de mejora continua para el SGSI
- Atribuir responsabilidades en materia de seguridad entre el personal de dirección de áreas internas de la compañía.

3.3.2. Política de seguridad de la información

Para cumplir con la norma ISO 27001 en este apartado, la alta dirección de la compañía, o su representación mediante el comité de seguridad, deben establecer y aprobar una política de seguridad de la información adecuada al propósito de la organización que incluya los objetivos de seguridad de la información que se han de cumplir. La política, además, debe mostrar el compromiso de cumplir con los requisitos aplicables a la seguridad de la información y de mejora continua. Por último, la organización se asegurará de que el documento de esta política sea accesible para todos los interesados dentro de la compañía y se comunique de forma que todos conozcan su existencia y queden claras sus responsabilidades y obligaciones [5].

Siguiendo estas directrices marcadas por la norma 27001, y tomando como referencia los controles indicados en la norma ISO 27002, se propone que la alta dirección establezca la política de seguridad que considere los siguientes requisitos [9]:

3.3.2.1. Estrategia de negocio

La política de seguridad debe considerar el principal objetivo estratégico de la compañía, que es ofrecer las máximas garantías de seguridad en la solución *cloud* para así, mostrarse más atractivos de cara al sector de clientes que son reticentes a las soluciones *cloud* por miedo a que no se cumplan las medidas de seguridad apropiadas. Por ello, la política debe remarcar el concepto de seguridad de la información, indicando que se van a implementar los controles propuestos por la norma ISO27001 de cara a garantizar la seguridad de la información en sus tres dimensiones, confidencialidad, integridad y disponibilidad, para todas las actividades y procesos involucrados en el área de explotación *cloud*. En este sentido, al tratarse de una solución *cloud* en la que según las características del servicio ofertado y, de acuerdo con lo establecido en la norma ISO 27017, la compañía se comportaría como cliente de servicios *cloud* ya que subcontrata el hosting y *cloud computing* a servicios AWS y a su vez, como proveedor de servicios *cloud* ante sus clientes a quienes le ofrece una plataforma de servicios sobre los anteriores. Siguiendo la indicación de la ISO 27017, en lo que respecta al perfil de la compañía como cliente de servicios *cloud*, los niveles de seguridad ofrecidos por la compañía de *cloud computing* (AWS) deben ser aceptables y en concordancia con el nivel de seguridad que la compañía quiere implementar en el SGSI, teniendo en cuenta que la información almacenada en el mismo o los activos son susceptibles de ser gestionados por el proveedor *cloud* o sus administradores y tener en cuenta las diferentes localizaciones geográficas en que sistema de información podría ser almacenado por el proveedor. Como proveedor del servicio *cloud*, la política deberá mostrar los requisitos de seguridad tanto del diseño e implementación del servicio ofrecido, riesgos debidos a divulgación de información confidencial dentro de la compañía, acceso de los ingenieros/SREs a la información/activos, procedimientos de seguridad en accesos, comunicaciones de brechas de seguridad y cambios de gestión, acceso y protección de los datos del usuario y seguridad de virtualización [7].

Además, se asignarán las responsabilidades generales y específicas a cada uno de los roles definidos dentro del contexto del proyecto y se establecerán los procesos para la gestión de desviaciones y excepciones.

La política de seguridad incluirá los objetivos de seguridad de la información o indicará la forma de establecerlos en base a un marco de referencia. Estos objetivos serán determinados en última instancia por la compañía a la hora de redactar la política de seguridad. Para ejemplificar cómo podrían determinarse los objetivos de seguridad del SGS, se agrupan en las siguientes categorías [10]:

Protección

Se incluyen en esta categoría todos los objetivos relacionados con la protección de los activos de la compañía que contienen información. Esto es de vital importancia para fortalecer el sistema garantizando que solo los usuarios autorizados tengan acceso a estos activos. Para ello se debe definir qué tipos de usuario existen en el sistema y qué tipos de acceso podrían darse. Ejemplos de estos objetivos serían los siguientes:

- Las instancias en AWS serán inaccesibles excepto para los administradores: Únicamente un empleado con cargo SRE podrá acceder al sistema de administración de instancias AWS.
- Las bases de datos en AWS serán inaccesibles excepto para los administradores: Las bases de datos contenidas en instancias RSD serán accesibles solo por usuarios SRE de la subárea DBA

Autenticación

Estos objetivos engloban todas las acciones enfocadas en evitar la suplantación de identidad. A continuación, se enumeran ejemplos de este tipo de objetivos y cómo se podrían conseguir.

- Las conexiones con el servidor deben ser seguras: Todas las conexiones se harán mediante SSL e intercambiando el certificado de la compañía
- Nadie más que el empleado accede a su computador: Los portátiles con los que trabajan los empleados tendrán sistemas de autenticación biométrica y complementariamente, se activará la autenticación de doble factor del sistema operativo
- El sistema garantizará que únicamente el cliente se conecta a sus instancias: La conexión de los clientes a la aplicación requiere de autenticación de doble factor.
- La contraseña debe ser personal y no transferirse bajo ningún concepto: Política de mesa despejada prohibiendo totalmente la existencia de contraseñas apuntadas tanto en formato físico (papel) como lógico (ficheros en el escritorio…)

Autorización

Los objetivos de autorización tienen que ver con el nivel de acceso a la información y recursos. Ejemplos de objetivos de este tipo serían:

- El cuadro de mandos ofrecerá la información mínima relevante al usuario conectado: Los clientes únicamente podrán acceder a los datos de sus instancias en la aplicación cuadro de mandos y no a los de otros clientes.
- Los SRE accederán a las instancias determinadas para cumplir sus funciones: La consola de administración no mostrará por defecto todas las instancias, se tendrán que habilitar específicamente permisos de acceso para aquellas a las cuales pueden acceder.

Integridad

Esta clasificación de objetivos se centra en mantener la integridad de la información en todo momento. Será importante que los objetivos cubran los datos, el sistema y las transacciones llevadas a cabo garantizando el no repudio.

- Comprobación de no repudio en las órdenes del cuadro de mandos
- Cifrado de la información de las bases de datos
- Respaldo de la información ante posibles incidentes: copias de seguridad

Auditoría

Los objetivos centrados en la monitorización de incidentes de seguridad con el fin de tomar medidas para evitar que se vuelvan a producir en el futuro. Ejemplos de objetivos de esta categoría serían:

- Controlar el acceso al sistema de cuadro de mandos: Se auditarán todas las operaciones de acceso en el módulo indicando IP, ubicación, fecha y hora del acceso.
- Controlar cumplimiento de la ISO27001: auditorías internas

3.3.2.2. Normativa y legislación aplicable

Se asegurará el cumplimiento de la legislación vigente en lo que respecta al reglamento general de protección de datos y cualquier otra normativa o legislación que pueda aplicar al producirse una movilidad geográfica del almacenamiento de la información debida a la localización del proveedor de servicios de *cloud computing* (AWS).

La política de seguridad debe contemplar los requisitos legales impuestos por la normativa y legislación aplicable. Principalmente, incidirá en el cumplimiento del reglamento general de protección de datos (RGPD) en todas aquellas actividades que involucren el tratamiento de datos de carácter personal. Es importante que se realice un análisis de la información almacenada en los sistemas de información y se evalúe su naturaleza de acuerdo con lo propuesto por dicho reglamento.

Roles según el RGPD

El escenario propuesto para este trabajo tiene la particularidad de que la información va a ser alojada externamente a través de un proveedor de servicios en la nube. Por ello, la política debe contemplar adecuadamente los aspectos que podrían ser ambiguos en lo relativo al tratamiento de los datos.

El RGPD define dos actores para el tratamiento de datos [11]:

- Responsable del tratamiento es el que decide sobre el contenido, uso y finalidad del tratamiento.
- Encargado del tratamiento es quien trata los datos personales por cuenta del responsable del tratamiento (RGDP, cap. 1, artículo 4)

En un entorno *cloud*, el prestador de servicios, en este caso la compañía en estudio asumiría el papel de encargado del tratamiento y sería el cliente final el responsable del tratamiento de datos personales.

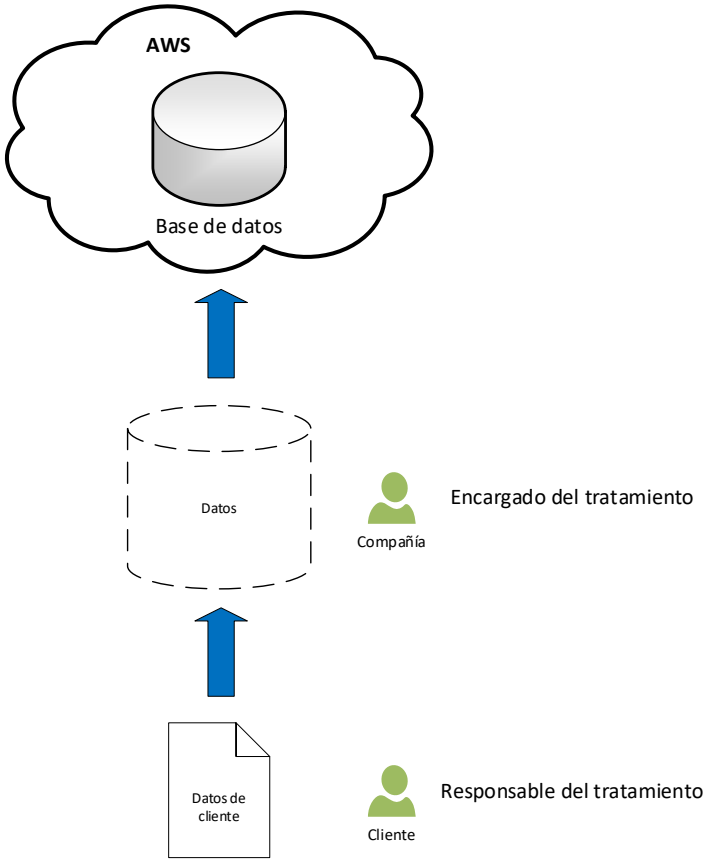

Figura 10. Responsable y encargado del tratamiento. Fuente: Elaboración propia

Es importante que esto se especifique de forma clara y concisa en la política de seguridad con el fin de adecuarse rigurosamente a la normativa en protección de datos.

Transferencias internacionales de datos

Existe la particularidad de que los entornos *cloud* podrían ubicarse en diferentes localizaciones, suponiendo lo que el RGPD traduce como una transferencia internacional de datos personales. En este sentido, la política de seguridad de la compañía debe ser muy precisa acerca de las ubicaciones en las que se va a alojar la información de sus clientes y de cómo se afrontarán posibles transferencias de datos.

La compañía contrata el servicio de computación en la nube a AWS, convirtiéndose en cliente de servicios *cloud*, por lo que en el caso de que el prestador subcontratase servicios de hosting, por ejemplo, bajo un escenario de alta demanda, se podrían producir transferencias internacionales de datos involuntarias.

La política de seguridad deberá contemplar este escenario y establecer las condiciones que deberán especificarse en el contrato con el proveedor acerca de los países en los que se desarrollan sus servicios, las acciones que se pueden tomar en el caso de que intervengan subcontratistas y los acuerdos contractuales a los que se puede llegar con ellos. Además, de cara al cliente final, la compañía es proveedora de servicios *cloud*, por lo que, como proveedor se debe contemplar en la política de seguridad los mecanismos de información a los clientes en caso de que se produzca un escenario de transferencia de datos internacionales debido a subcontrataciones o cambios en el modelo de servicio del proveedor.

Ejercicio de derechos LOPDGDD

Según el RGPD, es el responsable del tratamiento quien debe garantizar a los interesados el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. En este sentido la política de seguridad de la empresa únicamente debe recomendar que se facilite la colaboración para que estos derechos puedan ser ejercidos.

3.3.2.3. Entorno actual y previsto de amenazas para la seguridad de la información

Se tendrán en cuenta los requisitos propios del entorno específico, anteriormente mencionados y cubiertos por la norma ISO27017, además de las amenazas para la seguridad de la información específicas que se verán más adelante en el capítulo dedicado a la gestión de riesgos.

La política se dividirá en diferentes sub políticas más específicas que implementen los controles adecuados a su ámbito de aplicación. En el escenario propuesto, se contempla la elaboración de las siguientes políticas específicas:

- Control de acceso
    - Control de acceso al entorno *cloud* AWS
    - Control de acceso a equipos informáticos
    - Control de acceso físico al área de explotación de la compañía y subáreas
- Clasificación de la información del sistema *cloud*
- Copias de seguridad
    - En la nube
    - En el entorno local o CPD
- Privacidad y protección de la información
- Cumplimiento legal

- Usuario
    - Uso correcto de activos
    - Mesa despejada y pantalla limpia
    - Dispositivos móviles, extraíbles y teletrabajo
    - Software de terceros: instalación y uso
    - Transferencias de datos

Para garantizar el ciclo de mejora continua, la política se revisará anualmente y se establecerán actividades formativas para que todos los actores involucrados en el SGS.

3.3.3. Roles, responsabilidades y autoridades

La dirección de la compañía designará los siguientes roles de seguridad [12] a los que asignará la autoridad y responsabilidad correspondiente y se comunicará de forma oficial dentro de la compañía.

Estas responsabilidades asignadas garantizarán que se asegure que el SGSI cumple la norma ISO 27001 y dotará de los mecanismos para informar del comportamiento del SGSI.

Comité de seguridad

Compuesto por directivos de diferentes áreas de la empresa para tomar decisiones relacionadas con la seguridad. Concretamente sus funciones serán las siguientes:

- Validará y aprobará la política de seguridad
- Comprobar el estado de seguridad mediante análisis de riesgos o auditorías
- Aprobar los proyectos relacionados con la mejora de la seguridad

Estará compuesto por:

- Responsable de comunicaciones y sistemas
- Responsable de asesoría legal
- Un responsable de cada área de negocio

Responsable de información y servicios

En el caso de estudio se trata del responsable del área de servicio *cloud*. Sus funciones son las siguientes:

- Definir los requisitos de seguridad del servicio de explotación del CMS en *cloud* y la información que este maneja para garantizar la seguridad en todas sus dimensiones: Disponibilidad, Integridad y Confidencialidad.
- Tienen que asegurar que los empleados de su área de servicio cumplen las normas de protección de la información y se responsabilizan de los medios empleados

Responsable de sistemas y comunicaciones

En el caso de estudio se trata del responsable del sistema *cloud* que se encarga de garantizar que todos los servicios alojados en los servidores de AWS estén funcionando correctamente en todo momento. Sus funciones son las siguientes:

- Hacer más seguros los sistemas informáticos mediante su correcta configuración y mantenimiento.
- Aplicar medidas de *backup* y restauración de información.

- Monitorizar y supervisar los sistemas para detectar cualquier fallo de seguridad.
- Aplicar medidas de seguridad a los procesos de administración y operación.

Responsable de seguridad
Se encarga de coordinar y garantizar que se toman medidas de seguridad, no necesariamente se encarga de aplicarlas. Son funciones concretas son:

- Conocer en todo momento el estado de seguridad de los sistemas de información.
- Coordinar y establecer el plan director de seguridad.
- Coordinar y establecer el plan de continuidad de negocio.

Usuarios
Cualquier empleado dentro de la compañía que haga uso de alguna forma de los sistemas de información será encargado de cumplir con lo establecido en la política de seguridad de la información aprobada por la dirección, así como las normas y protocolos establecidos por sus responsables según se ha definido en los apartados anteriores.

3.4. Planificación: Análisis de riesgos

Siguiendo con los pasos que propone la ISO 27001, se muestra ahora la planificación del SGSI que propone realizar el análisis de riesgos y su posterior plan de tratamiento. Siguiendo lo aprendido durante las asignaturas cursadas en este máster, se va a utilizar la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT con la ayuda de la herramienta proporcionada en la asignatura de seguridad de informática avanzada.

3.4.1. Inventario de activos

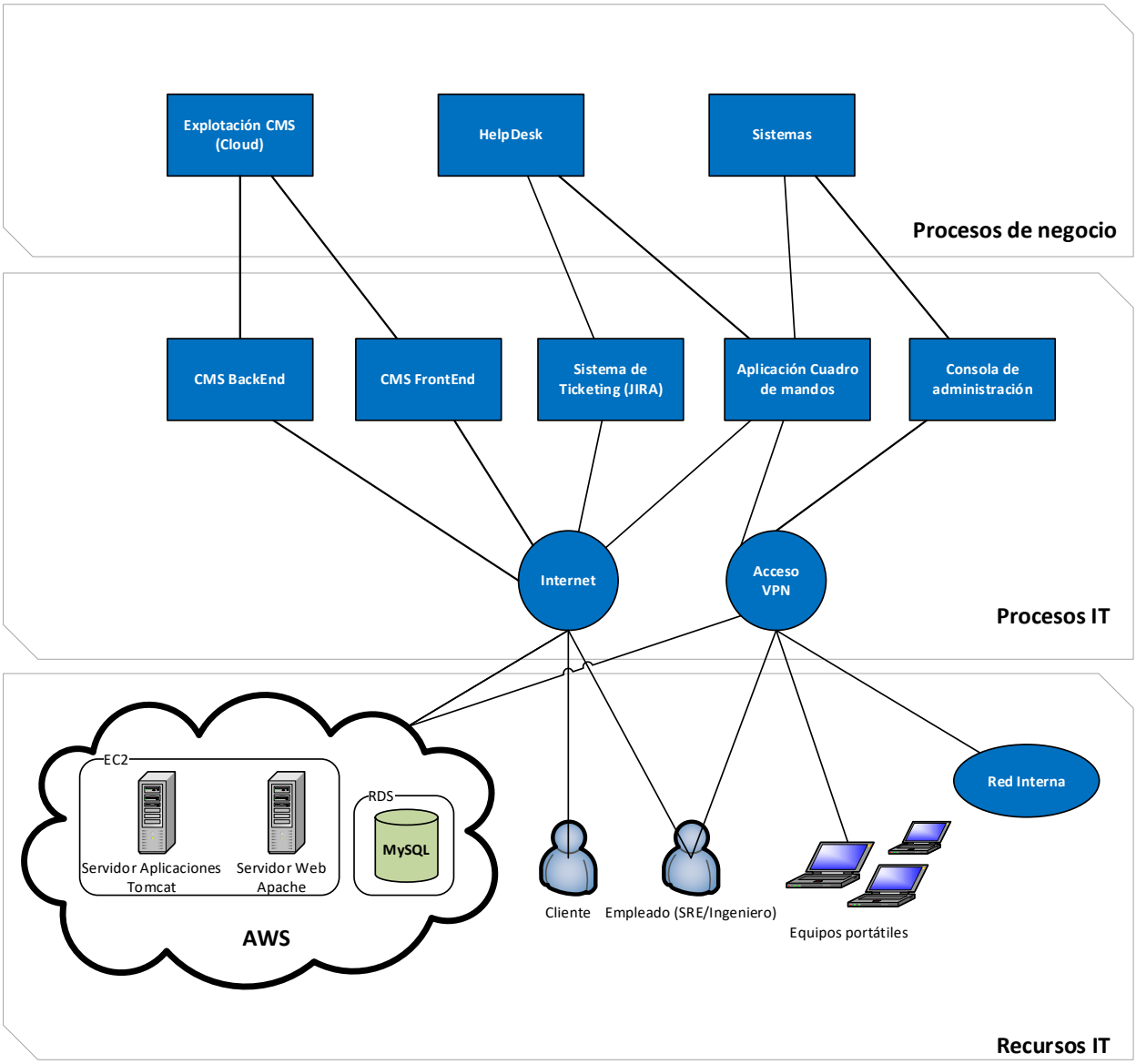

Figura 11. Mapa de activos. Fuente: Elaboración propia

3.4.1.1. Procesos de negocio

En este punto se describen los procesos de negocio incluidos en el inventario de activos.

Explotación CMS (*cloud*)

Es el proceso de negoción de explotación del software creado por la compañía en su versión *cloud*

Helpsdesk

Este proceso de negocio consiste en la atención de peticiones de clientes cloud a través de un sistema de *ticketing* (JIRA). Se encargan de resolución de dudas e incidencias.

Sistemas

Este proceso de negocio comprende la administración de los sistemas en la nube, tanto las aplicaciones propias desplegadas en la nube como las propias instancias de AWS. Permiten la

escalabilidad y alta disponibilidad de los sistemas mediante su monitorización y un sistema de alertas.

3.4.1.2. Procesos IT

Aquí entran los canales, tecnologías y aplicaciones con las que se realiza el tratamiento de datos.

CMS *backend*

Es la parte de *backend* del CMS, utilizado normalmente por los empleados de la empresa cliente para gestionar sus contenidos, añadir funcionalidades, configurar el sistema a medida y crear las plantillas de visualización de contenidos.

CMS *frontend*

Es la parte *frontend* del CMS. Las configuraciones, plantillas y contenidos gestionados en la parte *frontend* serán transferidos a esta para ser publicados y accesibles para los clientes generales.

Sistema de *ticketing* JIRA

Es la aplicación que se utiliza para registrar peticiones por parte de los clientes que serán resueltas por los ingenieros de la compañía, a veces en colaboración con el equipo de SREs.

Aplicación Cuadro de mandos

Es la aplicación que administra las instancias de la aplicación CMS desplegadas, permite revisar su estado y realizar operaciones de administración como reinicio, ampliar capacidades, gestión de *backup* o monitorización de recursos. Será accedida tanto por los clientes como por los SREs.

Consola de administración

Es la consola con la que los SRE administran las instancias *cloud* de AWS.

Internet

Se utiliza internet para acceder a las aplicaciones y servicios anteriormente descritos.

Acceso VPN

Los trabajadores de la compañía accederán mediante la red privada virtual a las aplicaciones de administración de sistemas.

3.4.1.3. Recursos IT

Cliente

Son los clientes de la compañía que harán uso de los servicios *cloud* ofertados. Accederán a las aplicaciones web del CMS (*frontend* y *backend*) así como al cuadro de mandos

Equipos portátiles

Son los equipos de trabajo con los que los miembros de la compañía acceden a los sistemas de administración y aplicaciones de la compañía.

Empleado (SRE/Ingeniero)

Son los empleados de la compañía, tanto los ingenieros que dan soporte a través de *helpdesk* como los SRE que se encargan de que los sistemas estén siempre en perfecto funcionamiento.

Instancias en AWS

Tal y como se describe en la ISO 27017 apartado 8.1.1 [7], el inventario de activos del cliente de servicios *cloud* debe tener en cuenta la información y activos asociados almacenados en dicho entorno *cloud*. Por tanto, se tienen en cuenta las instancias alojadas en los servicios *cloud* de AWS. Estas son:

- **EC2:** instancia de computación en la nube que aloja el servidor de aplicaciones tomcat y el servidor web apache.
- **RDS:** instancia que aloja el servicio de bases de datos relacional MySQL. Es donde se almacenan los datos manejados por el CMS y por tanto donde el grueso de la información es gestionado.

3.4.2. Valoración de activos

Utilizando la herramienta proporcionada en la asignatura de seguridad informática avanzada se han valorado los activos de los tres niveles para obtener finalmente el valor de los recursos IT que se tratarán en el análisis de riesgos.

Valor de negocio

En primer lugar, se ha dado un valor a la compañía de 400.000.000€. A partir de este valor y del cálculo realizado por los valores en la siguiente matriz se obtiene el valor de negocio de cada uno de los procesos de negocio mostrados en el mapa de activos.

Procesos de Negocio	Explotación CMS Cloud	Helpdesk	Administración de sistemas	Factor de Negocio	Valor de Negocio
Explotación CMS Cloud		10,0	5,0	**15,0**	**292.682.927 €**
Helpdesk	0,1		0,2	**0,3**	**5.853.659 €**
Administración de sistemas	0,2	5,0		**5,2**	**101.463.415 €**

Tabla 1. Valor de negocio

Los valores en azul son auto calculados por la herramienta mientras que los negros se han asignado a partir del análisis realizado de la compañía y se explican a continuación. El valor dado puede ser uno de los siguientes:

- 10 Si la línea es mucho más importante que la columna
- 5 Si la línea es más importante que la columna
- 1 Si la línea es igual de importante que la columna
- 0,2 Si la línea es menos importante que la columna
- 0,1 Si la línea es mucho menos importante que la columna

Por tanto, se ha considerado que la explotación *cloud* del CMS es mucho más importante que el proceso de negocio de *Helpdesk*, ya que este es un proceso que lo complementa, pero por si solo no tiene mayor importancia. En segundo lugar, se ha valorado que la explotación *cloud* del CMS es un proceso de negocio más importante que la administración de sistemas debido, en este caso a que es necesario para la explotación del CMS. Finalmente, se ha considerado que *Helpdesk* es un proceso de negocio de menor importancia que la administración de sistemas ya que como se ha explicado, es una proceso que complementa y da valor añadido a la los otros dos, pero la administración de sistemas cobra mayor importancia ya que se encarga de mantener todo en funcionamiento, incluyendo el propio proceso de negocio *Helpdesk*.

Valor de negocio por dimensión de seguridad

La metodología de análisis de riesgos MAGERIT propone 5 dimensiones de la seguridad y la herramienta utilizada añade protección de datos: Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad y Protección de datos (DICATPd). El siguiente paso en el análisis de riesgos realizado con la herramienta es asignar para cada una de las dimensiones descritas anteriormente, un valor correspondiente a cada uno de los procesos de negocio de la compañía. Este valor puede ser no aplica, alto, medio o bajo.

En el análisis llevado a cabo se han asignado los siguientes valores de acuerdo con la naturaleza de cada proceso de negocio:

Procesos de negocio	Niveles					
	D	I	C	A	T	Pd
Explotación CMS Cloud	3 - Alto	3 - Alto	3 - Alto	0 - NA	2 - Medio	3 - Alto
Helpdesk	3 - Alto	3 - Alto	2 - Medio	2 - Medio	3 - Alto	2 - Medio
Administración de sistemas	3 - Alto	2 - Medio	1 - Bajo	2 - Medio	2 - Medio	0 - NA

Tabla 2. Niveles DICATPd de negocio

Como se puede observar, el proceso de explotación *cloud* del CMS tiene valores altos en casi todas las dimensiones, pues es de vital importancia garantizar su disponibilidad, la integridad de la información que almacena, la confidencialidad y el nivel adecuado de protección de datos. No aplica la autenticidad porque en este sentido, es el cliente quien tiene que velar por que la información que almacene sea auténtica. La trazabilidad también es importante para detectar todas las acciones que se han llevado a cabo con la información de este proceso.

El proceso de *Helpdesk* se ha considerado que tiene valor alto para la disponibilidad e integridad ya que son dimensiones clave debido a que su disponibilidad es esencial y la integridad de la información que contiene. El nivel de trazabilidad también es alto ya que es muy necesario poder trazar la información en este proceso.

Para administración de sistemas se tiene un valor alto de disponibilidad porque esta dimensión cobra especial importancia en este proceso de negocio.

A partir de los valores dados en la tabla anterior, la herramienta auto calcula los valores de cada proceso de negocio por dimensión de seguridad quedando como se muestra en la siguiente tabla.

Procesos de negocio	Valores					
	D	I	C	A	T	Pd
Explotación CMS Cloud	292.682.927 €	292.682.927 €	292.682.927 €	0 €	193.170.732 €	292.682.927 €
Helpdesk	5.853.659 €	5.853.659 €	3.863.415 €	3.863.415 €	5.853.659 €	3.863.415 €
Administración de sistemas	101.463.415 €	66.965.854 €	33.482.927 €	66.965.854 €	66.965.854 €	0 €
Cantidad	400.000.000 €	365.502.439 €	330.029.268 €	70.829.268 €	265.990.244 €	296.546.341 €

Tabla 3. Valor de negocio DICATPd

Se observa que en aquellas dimensiones cuyo valor se ha considerado alto para el proceso de negocio el valor corresponde al 100% del valor calculado en el apartado anterior, mientras que si el valor asignado es no aplica, se tiene un valor de 0€.

Valor de los procesos IT

Para calcular el valor de los procesos de IT se ha utilizado la tabla correspondiente de la herramienta en la que hay que asignar valores en función de la necesidad del proceso de TI para el proceso de negocio. Concretamente se ha seguido el siguiente criterio a la hora de asignar valores:

- 9 Si el proceso de T.I es absolutamente necesario para el proceso de negocio
- 3 Si el proceso de T.I es necesario para el proceso del negocio
- 1 Si el proceso de T.I es sólo útil para el proceso de negocio
- 0 Si el proceso de T.I no es útil para el proceso de negocio

	Valor de T.I	**2.346.109 €**	**2.346.109 €**	**738.676 €**	**952.381 €**	**961.672 €**	**2.373.984 €**	**241.580 €**
	Proceso I.T	CMS Back	CMS Front	Sistema de *ticketing* (JIRA)	Aplicación Cuadro de mandos	Consola de administración	Internet	Acceso VPN
Proceso de Negocio	**Valor de Negocio**							
Explotación CMS Cloud	**292.682.927 €**	9	9	3	3	1	9	0
Helpdesk	**5.853.659 €**	3	3	9	3	1	9	0
Administración de sistemas	**101.463.415 €**	3	3	0	3	9	3	3

Tabla 4. Cálculo del valor de los procesos IT

Para simplificar los resultados obtenidos del cálculo anterior se muestra la siguiente tabla:

Proceso I.T	CMS Back	CMS Front	Sistema de *ticketing* (JIRA)	Aplicación Cuadro de mandos	Consola de administración	Internet	Acceso VPN
Valor de T.I	**2.346.109 €**	**2.346.109 €**	**738.676 €**	**952.381 €**	**961.672 €**	**2.373.984 €**	**241.580 €**

Tabla 5. Valor de activos IT

De los valores anteriores se deduce que los procesos de mayor valor son los relacionados con el CMS, sus variantes *backend* y *frontend*, así como Internet ya que es el medio de acceso utilizado.

Valor de los recursos IT

La última valoración de activos corresponde a los recursos IT. Para ello se ha utilizado la tabla correspondiente de la herramienta en la que se han asignado los valores según el siguiente criterio:

- 6 Si la pérdida del recurso de T.I es muy significativa para el proceso TI
- 4 Si la pérdida del recurso de T.I es significativa para el proceso TI
- 2 Si la pérdida del recurso de TI sólo agrega carga de trabajo en el proceso TI
- 1 Si la pérdida del recurso de TI sólo agrega una pequeña carga de trabajo
- 0 Si la pérdida del recurso de T.I no es significativa para el proceso TI

	Valor Recursos T.I	**1.001.936 €**	**950.390 €**	**400.199 €**	**273.326 €**	**965.655 €**	**630.496 €**	**965.655 €**
	Recursos de T.I	Cliente	Empleado (SRE/Ingeniero)	Equipos portátiles	Red Interna	Servidores Tomcat (EC2 AWS)	Servidores Apache (EC2 AWS)	Servidores MySQL (RDS AWS)
Proceso T. I	**IT Value**							
CMS *Backend*	**2.346.109 €**	6	4	0	0	6	2	6
CMS *Frontend*	**2.346.109 €**	6	4	0	0	6	4	6
Sistema de *ticketing* (JIRA)	**738.676 €**	6	6	4	0	0	0	0
Aplicación Cuadro de mandos	**952.381 €**	0	0	4	4	4	4	4
Consola de administración	**961.672 €**	0	6	4	4	4	4	4
Internet	**2.373.984 €**	4	4	2	1	2	2	2
Acceso VPN	**241.580 €**	0	6	6	6	0	0	0

Tabla 6. Cálculo del valor de los recursos IT

Si se pierde el cliente, supone un gran efecto en los procesos CMS (*frontend* y *backend*) y el sistema de *ticketing* JIRA. La pérdida de los empleados sería significativa para para los procesos CMS y muy significativa para la consola de administración. Todos recursos que tiene que ver con el acceso VPN notaría, una pérdida significativa al perderse esta. El proceso TI Internet está involucrado en todos ellos con mayor o menor importancia dado que al fin y al cabo todos harán uso de este proceso.

Finalmente, a modo de resumen de la tabla anterior, se muestran los valores obtenidos para los recursos TI:

Recursos de T.I	Cliente	Empleado (SRE/ Ingeniero)	Equipos portátiles	Red Interna	Servidores Tomcat (EC2 AWS)	Servidores Apache (EC2 AWS)	Servidores MySQL (RDS AWS)
Valor	1.001.936 €	950.390 €	400.199 €	273.326 €	965.655 €	630.496 €	965.655 €

Tabla 7. Valor de los recursos IT

Se da mayor valor al cliente, los servidores de aplicaciones y bases de datos, así como a los empleados especializados en el área *cloud*.

3.4.3. Análisis de las amenazas

Del catálogo de amenazas proporcionado por MAGERIT (ver Anexo A. Catálogo de amenazas MAGERIT) se recogen aquellas que, tras el análisis de riesgo, se ha valorado que pueden materializarse en el sistema propuesto. El siguiente listado resumen muestra, para cada amenaza, su dificultad de explotación, el activo al que está asociada y el daño que podría ocasionar a la compañía si se llegase a materializar.

El listado completo con la descripción de las amenazas, su efecto en la compañía y las justificaciones de cada valor asignado se puede consultar en el Anexo B. Análisis de Riesgos

Dificultad de explotación (L)	**Asignación de riesgo**		**Daño para la organización (D)**
Nivel	**Amenaza**	**Activo (Recurso IT)**	**Nivel**
5 - Muy Baja	[N.*] Otros desastres naturales	Servidores Tomcat (EC2 AWS)	3 - Alto
5 - Muy Baja	[N.*] Otros desastres naturales	Servidores Apache (EC2 AWS)	2 - Medio
5 - Muy Baja	[N.*] Otros desastres naturales	Servidores MySQL (RDS AWS)	3 - Alto
5 - Muy Baja	[I.1] Fuego	Servidores MySQL (RDS AWS)	4 - Muy Alto
4 - Baja	[I.5] Avería de origen físico o lógico	Servidores Tomcat (EC2 AWS)	3 - Alto
4 - Baja	[I.5] Avería de origen físico o lógico	Servidores MySQL (RDS AWS)	4 - Muy Alto
4 - Baja	[I.6] Corte del suministro eléctrico	Servidores MySQL (RDS AWS)	4 - Muy Alto
4 - Baja	[I.8] Fallo de servicios de comunicaciones	Servidores Apache (EC2 AWS)	3 - Alto
4 - Baja	[I.9] Interrupción de otros servicios y suministros esenciales.	Servidores MySQL (RDS AWS)	3 - Alto
3 - Media	[E.1] Errores de los usuarios	Servidores MySQL (RDS AWS)	2 - Medio
4 - Baja	[E.2] Errores del administrador.	Servidores MySQL (RDS AWS)	3 - Alto
4 - Baja	[E.2] Errores del administrador.	Servidores Tomcat (EC2 AWS)	3 - Alto

4 - Baja	[E.4] Errores o manipulación de la configuración	Servidores Tomcat (EC2 AWS)	3 - Alto
4 - Baja	[E.4] Errores o manipulación de la configuración	Servidores MySQL (RDS AWS)	3 - Alto
4 - Baja	[A.5] Suplantación de la identidad del usuario	Cliente	3 - Alto
3 - Media	[A.6] Abuso de privilegios de acceso	Empleado (SRE/Ingeniero)	3 - Alto
4 - Baja	[E.8] Difusión de software dañino.	Servidores Tomcat (EC2 AWS)	3 - Alto
4 - Baja	[E.18] Destrucción de información	Servidores MySQL (RDS AWS)	3 - Alto
4 - Baja	[E.19] Fugas o revelación de información.	Empleado (SRE/Ingeniero)	3 - Alto
4 - Baja	[E.20] Vulnerabilidades de los programas (software).	Servidores Tomcat (EC2 AWS)	3 - Alto
4 - Baja	[E.21] Errores de mantenimiento / actualización de programas (software)	Equipos portátiles	2 - Medio
4 - Baja	[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)	Equipos portátiles	2 - Medio
4 - Baja	[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	Servidores Apache (EC2 AWS)	3 - Alto
4 - Baja	[E.25] Robo o Pérdida de equipos	Equipos portátiles	3 - Alto
5 - Muy Baja	[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas	Servidores MySQL (RDS AWS)	3 - Alto
4 - Baja	[Pd.8] Divulgación que origina incumplimiento en el deber de secreto	Empleado (SRE/Ingeniero)	3 - Alto
4 - Baja	[A.11] Acceso no autorizado.	Servidores MySQL (RDS AWS)	3 - Alto
4 - Baja	[A.12] Análisis de tráfico	Red Interna	2 - Medio
4 - Baja	[A.14] Interceptación de información (escucha).	Red Interna	3 - Alto

4 - Baja	[A.26] Ataque destructivo	Servidores Tomcat (EC2 AWS)	3 - Alto
4 - Baja	[A.26] Ataque destructivo	Servidores MySQL (RDS AWS)	3 - Alto

Tabla 8. Amenazas

3.4.4. Cálculo de riesgo

Tras asignar los valores de probabilidad de ocurrencia de la amenaza e impacto causado, se calculará el riesgo asociado como:

$$riesgo = valor\ del\ activo\ x\ probabilidad\ x\ impacto$$

Con esta fórmula y los datos anteriormente registrados en la herramienta para el análisis de riesgos, se han calculado los riesgos agrupados por dimensión de seguridad y por amenazas.

3.4.4.1. Riesgos por dimensión de la seguridad

La siguiente tabla muestra los resultados obtenidos del análisis de riesgos agrupados por dimensión de seguridad. En la primera fila se muestran los porcentajes según los valores de los activos y en la segunda, se muestra el riesgo asociado a cada una de las dimensiones de seguridad

Riesgos por dimensión de seguridad						
	D	**I**	**C**	**A**	**T**	**Pd**
Perfil DICAT organización	20%	22%	20%	4%	16%	18%
Riesgo	31%	24%	16%	17%	6%	6%

Tabla 9. Riesgos por dimensión de seguridad

Como se puede observar, las dimensiones de seguridad que asumirían más riesgos son la disponibilidad y la integridad con un 31% y 24% respectivamente. Estos valores son los esperados dados los datos que han sido previamente asignados a las amenazas durante el análisis (véase Tabla 2. Niveles DICATPd de negocio) donde estas dimensiones recibían el valor alto en mayoría y los valores más elevados como resultado.

La explicación de estos resultados reside en la propia naturaleza del proyecto, al tratarse de un CMS alojado en la nube, lo primordial es la disponibilidad total de la información, así como su integridad. De ahí que estos valores hayan sido los que más puntuación han obtenido tras ser analizados con la herramienta.

Para ilustras de forma gráfica los resultados obtenidos, se muestran en las siguientes gráficas.

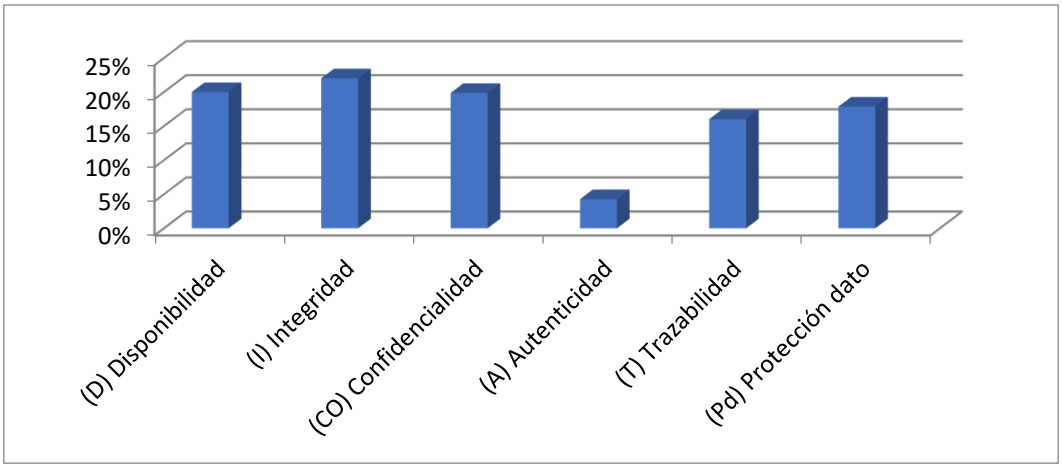

Figura 12. Valor de los activos por dimensión de seguridad. Fuente: Elaboración propia

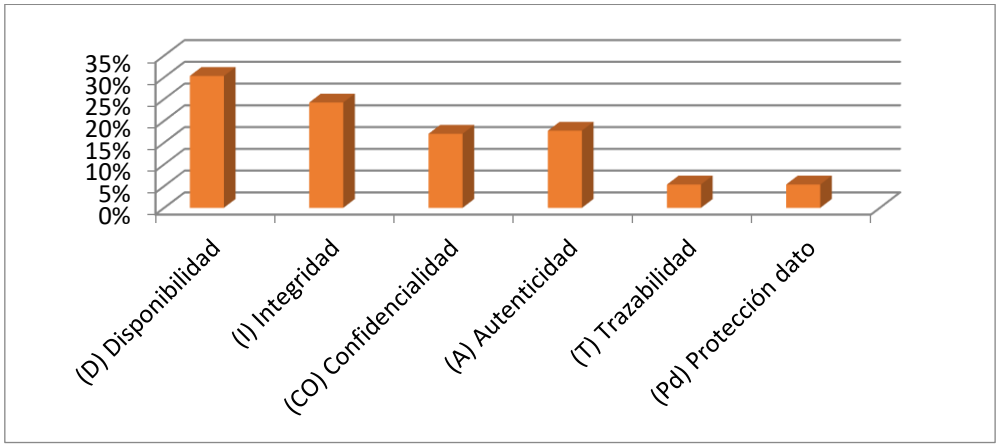

Figura 13. Riesgo por dimensión de seguridad. Fuente: Elaboración propia

Finalmente se muestran las cantidades asociadas a los datos vistos en las gráficas anteriores.

Riesgo							
	D	**I**	**C**	**A**	**T**	**Pd**	**Global**
Valor activos negocio	400.000.000 €	365.502.439 €	330.029.268 €	70.829.268 €	265.990.244 €	296.546.341 €	400.000.000 €
Valor activos TI	5.187.656 €	4.829.773 €	4.462.370 €	733.625 €	3.443.898 €	4.115.014 €	5.187.656 €
Riesgo residual	2.313.522 €	1.759.123 €	1.201.424 €	1.256.286 €	416.924 €	416.924 €	6.947.279 €

Tabla 10. Detalle de riesgos por dimensión de seguridad

3.4.4.2. Riesgos de las amenazas

La gráfica mostrada más abajo detalla los valores de los riesgos asociados a cada una de las amenazas que del catálogo de MAGERIT que aplican al presente proyecto.

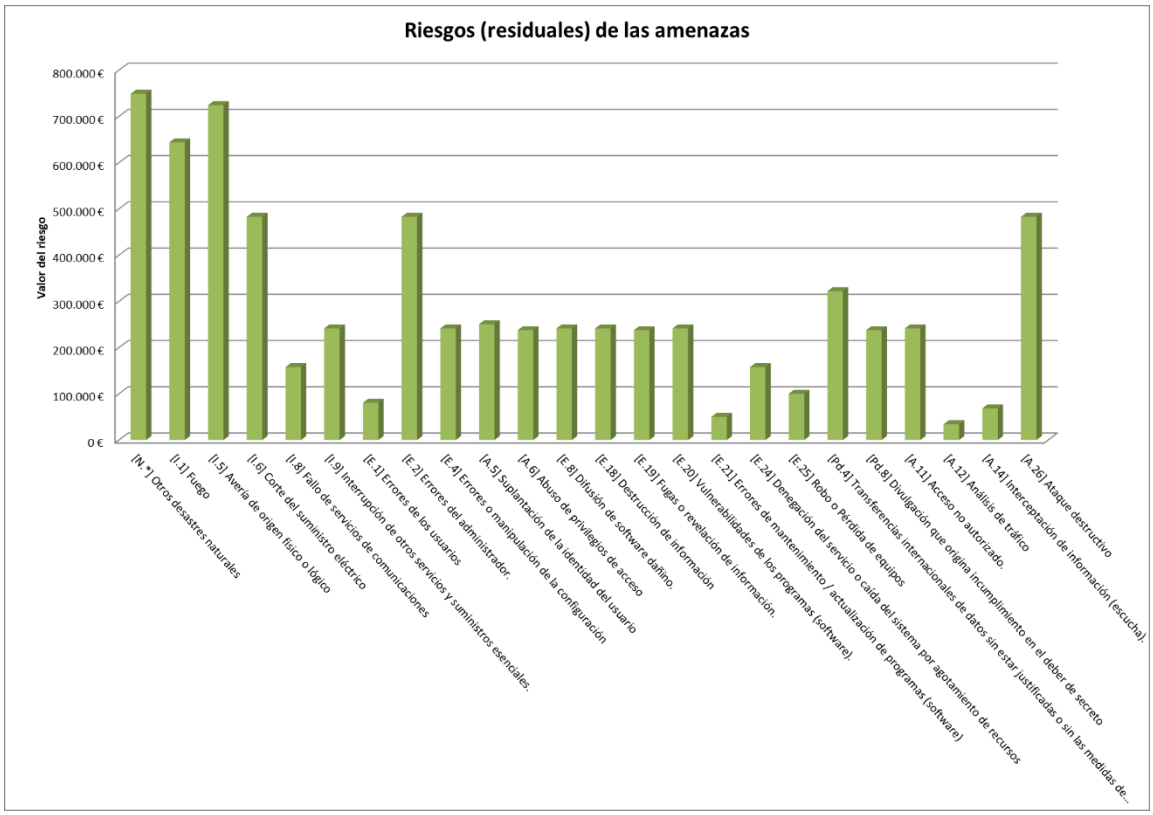

Figura 14. Riesgos de las amenazas. Fuente: Elaboración propia

De la gráfica anterior se deduce que las amenazas asociadas a la pérdida física de recursos y averías o cortes de suministros serían las que más daños producirían ya que podrían afectar directamente al cliente y/o al servicio recibido. Además, muestran especial importancia aquellas amenazas relacionadas con fallos en el software y su administración.

Estos resultados tienen sentido en el escenario de estudio pues en un sistema basado en servicios *cloud*, los accidentes externos que ocasionen la pérdida de recursos son los que más riesgo suponen para la empresa ya que implicaría la pérdida directa de estos. La compañía al ser, a su vez, clientes de servicios *cloud* (AWS), se encuentra que monitorizar y controlar estas situaciones queda fuera de su alcance y tiene que confiar en las buenas prácticas que el proveedor asegura en su contrato.

La importancia de los errores en el administrador reside en que un fallo supondría la pérdida de servicio de los clientes, que podría ocasionar pérdidas cuantiosas tanto a la compañía como al propio cliente. Por ejemplo, por incumplimiento del acuerdo de nivel de servicio,

En el Anexo C. Tabla de riesgos por amenaza, se muestran los detalles de los riesgos por amenaza con mayor nivel de detalle y los valores calculados correspondientemente.

3.5. Gestión de riesgos

Una vez evaluados los riesgos para la compañía siguiendo la metodología MAGERIT, se proponen las salvaguardas asociadas y el plan de tratamiento de riesgos con aquellos proyectos de seguridad de la información que se llevarán a cabo.

3.5.1. Definición de salvaguardas

Para reducir los riesgos anteriormente calculados se proponen una serie de salvaguardas que se agrupan en proyectos de seguridad. En este apartado, se analizará, para cada uno de ellos, su viabilidad en base al coste que supone la aplicación de la salvaguarda en comparación con el beneficio que supone su implantación.

A continuación, se desglosan los diferentes proyectos de seguridad y las salvaguardas que pertenecen a cada uno de ellos.

3.5.1.1. Alta disponibilidad

Este proyecto de seguridad recoge todas las salvaguardas encargadas de asegurar que los sistemas de información, concretamente los servidores Tomcat alojados en instancias EC2 donde se despliegan las aplicaciones CMS y los servidores de bases de datos alojados en instancias RDS, siempre estén disponibles y su contenido no se pierda. Para ello, se propone la siguiente salvaguarda:

- **Ampliación de zonas AWS**: Aplicar esta salvaguarda significaría tener entornos disponibles para replicar los existentes en diferentes zonas dentro de la misma región contratada para que, si se materializa alguna de las amenazas que hace perder algunos de los sistemas de información, se pudiera acceder a él desde la réplica de otra zona. El coste de esta salvaguarda es considerable debido a la contratación de más capacidad para replicar el contenido de cada zona y además el coste de administrar y mantener las nuevas zonas a nivel técnico.

3.5.1.2. Copias de seguridad

Se encarga de agrupar las salvaguardas que tienen que ver con la creación de copias de seguridad, su administración y procedimientos de respaldo y restauración en casos de pérdida de información o su integridad. A continuación, se enumeran las diferentes salvaguardas de este proyecto.

- **Contratación de AWS *Backup***: Consiste en la contratación de la herramienta que provee AWS para la creación, automatización y administración de copias de seguridad. Esta salvaguarda supone un coste notable ya que además de la contratación del servicio, debe existir personal cualificado al cargo de la administración de esta herramienta.
- **Procedimiento de respaldo**: Consiste en el diseño e implementación de procedimientos de respaldo encargados de guardar las copias de seguridad de los sistemas de información
- **Procedimiento de restauración segura de *Backup***: Consiste en el diseño e implementación de procedimientos de restauración de copias de seguridad en aquellos entornos que la información se haya degradado.

3.5.1.3. Seguridad de Aplicación

Recoge las salvaguardas correspondientes a la implementación de mecanismos de seguridad en la aplicación que permitan reducir su vulnerabilidad ante amenazas de diversa índole. Estas son las salvaguardas que se contemplan en este proyecto.

- **Cifrar los datos de las instancias RDS:** Se aplicará cifrado en las instancias RDS para que los datos no puedan ser leídos e interpretados por personas externas. Esta herramienta la provee AWS y necesitará de empleados cualificados capaces de hacer uso de ella.
- **Implementar autenticación de doble factor:** Se implementará un control de doble factor de autenticación para el acceso a las aplicaciones, de esta forma se reduce el riesgo de que entre una persona que no debe.
- **Implementar sistema de trazado de todas las acciones realizadas por un usuario:** Se implementará un sistema que guarde trazas de todas las acciones realizadas por un usuario, sea común o administrador.
- **Creación de diferentes entornos para realizar pruebas exhaustivas:** Se crearán entornos de pruebas anteriores al de producción y la batería de pruebas correspondiente para asegurar que no hay errores en las aplicaciones antes de desplegarlas en producción.
- **Implementar capa de seguridad contra los ataques más comunes:** Se implementará un sistema de filtros de peticiones que intercepten aquellos ataques más comunes como Inyección de SQL, denegación de servicio, *cross-site* scripting…
- **Utilización de AWS IAM**: Hacer uso de esta herramienta permite administrar el acceso a los servicios y recursos de AWS de forma segura [13].
- **Contratación de AWS Shield Advanced**: Contratar este servicio que sirve para mitigar ataques de denegación de servicio [13].

3.5.1.4. Formación

Aquí se agrupan las salvaguardas correspondientes a la formación y concienciación de personal o clientes.

- **Training especializado para empleados**: Acciones formativas para empleados que contemplan todos los aspectos técnicos avanzados para que puedan ejecutar sus tareas con el mayor conocimiento posible mitigando posibles errores.
- **Training especializado para clientes**: Acciones formativas para clientes que van a ser usuarios de la aplicación, cuyo contenido se basa en conceptos avanzados de uso para mejorar su comprensión de la aplicación y mitigar posibles errores.
- **Plan de concienciación**: Actividades organizadas por la compañía para sus empleados cuyo objetivo es promover sus valores, buenas prácticas en el manejo de instalaciones y herramientas y todos los aspectos de seguridad pertinentes incluyendo contraseñas, cifrado de datos en equipos, copias de seguridad etc.

3.5.1.5. Ciberseguridad

El proyecto ciberseguridad recoge las salvaguardas que tienen que ver con la red interna de la empresa y el software de terceros que se utiliza en la compañía. Las salvaguardas correspondientes a este proyecto son las siguientes.

- **Actualizaciones de software de empleados**: Se mantendrá actualizado en la última versión todo el software utilizado por los empleados de la compañía. Para ello se tendrán que adquirir las licencias necesarias y disponer de personal cualificado que se encargue de gestionar estas actualizaciones e inventariar todos los equipos de empleados y software instalado en cada uno de ellos.
- **Cifrar los datos que viajan por la red interna**: Se implementarán los controles y herramientas para hacer que todos los datos que viajan por la red interna de la empresa circulen cifrados.

3.5.1.6. Cumplimiento

Se encarga de garantizar el cumplimiento de las normas de seguridad de la información en los sistemas de la compañía. Recopila todas las salvaguardas que se centran en el cumplimiento de alguna normativa. Las salvaguardas que se han establecido para este proyecto se muestran a continuación.

- **Control de regiones de las instancias RDS**: Se llevará a cabo un control exhaustivo sobre la ubicación de los datos en las instancias RDS, con la información pertinente a los clientes para evitar en todo momento transferencias internacionales de datos no deseadas/contempladas.
- **Administrar el cifrado de los datos de las instancias RDS**: Consiste en mantener el cifrado de instancias de bases de datos de manera que los empleados no puedan visualizar contenidos de las bases de los clientes para garantizar así que no puedan divulgarse y cumplan con la normativa aplicable en cada caso.

3.5.2. Valoración de las salvaguardas

Una vez se han definido las salvaguardas y agrupado en proyectos, se estudia la viabilidad de su implementación en función del coste anual de mantenimiento de cada una en relación con el valor de reducción de riesgo calculado por la herramienta utilizada en base a valores establecidos de porcentaje de reducción de riesgo para cada una de las dimensiones de la seguridad.

Según la relación entre ambos valores se muestra en verde aquellas salvaguardas que merece la pena implementar ya que su coste de mantenimiento anual es menor que el beneficio que conlleva.

Salvaguarda	Proyecto	Coste Anual de Mantenimiento	Reducción de riesgo	Amenaza
Ampliación de zonas AWS	Alta disponibilidad	30.000 €	14.977 €	[N.*] Otros desastres naturales
Contratación AWS Backup	Copias de seguridad	60.000 €	386.262 €	[I.1] Fuego
Procedimientos de respaldo	Copias de seguridad	21.000 €	579.393 €	[I.5] Avería de origen físico o lógico
Procedimiento de restauración segura de Backup	Copias de seguridad	24.000 €	386.262 €	[I.6] Corte del suministro eléctrico
Ampliación de zonas AWS	Alta disponibilidad	150.000 €	78.812 €	[I.8] Fallo de servicios de comunicaciones
Ampliación de zonas AWS	Alta disponibilidad	150.000 €	120.707 €	[I.9] Interrupción de otros servicios y suministros esenciales.
Cifrar los datos de las instancias RDS	Seguridad de aplicación	30.000 €	213.838 €	[E.19] Fugas o revelación de información.

Training especializado para empleados	Formación	24.000 €	96.565 €	[E.2] Errores del administrador.
Implementar autenticación de doble factor	Seguridad de aplicación	75.000 €	75.145 €	[A.5] Suplantación de la identidad del usuario
Implementar sistema de trazado de todas las acciones realizadas por un usuario	Seguridad de aplicación	120.000 €	166.318 €	[A.6] Abuso de privilegios de acceso
Creación de diferentes entornos previos a producción en los que se lleven a cabo pruebas exhaustivas	Seguridad de aplicación	30.000 €	48.283 €	[E.8] Difusión de software dañino.
Contratación AWS Backup	Copias de seguridad	60.000 €	193.131 €	[E.18] Destrucción de información
Contratación de AWS Shield	Seguridad de aplicación	60.000 €	126.099 €	[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos
Implementar capa de seguridad contra los ataques más comunes	Seguridad de aplicación	15.000 €	24.141 €	[E.20] Vulnerabilidades de los programas (software).
Actualizaciones de software de empleados	Ciberseguridad	15.000 €	7.504 €	[E.21] Errores de mantenimiento / actualización de programas (software)
Actualizaciones de software de empleados	Ciberseguridad	15.000 €	0 €	[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)
Cifrar los datos que viajan por la red	Ciberseguridad	60.000 €	54.665 €	[A.14] Interceptación de información (escucha).
Utilización de AWS IAM	Seguridad de aplicación	6.000 €	144.848 €	[A.11] Acceso no autorizado.
Plan de concienciación	Formación	4.500 €	40.020 €	[E.25] Robo o Pérdida de equipos
Control de regiones de las instancias RDS	Cumplimiento	6.000 €	160.942 €	[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas

Administrar el cifrado de los datos de las instancias RDS	Cumplimiento	15.000 €	190.078 €	[Pd.8] Divulgación que origina incumplimiento en el deber de secreto
Training especializado para clientes	Formación	30.000 €	32.188 €	[E.1] Errores de los usuarios
Training especializado para empleados	Formación	24.000 €	96.565 €	[E.4] Errores o manipulación de la configuración
Ampliación zona AWS	Alta disponibilidad	150.000 €	144.848 €	[A.26] Ataque destructivo
Cantidad		1.174.500 €		

Tabla 11. Salvaguardas

3.5.3. Plan de tratamiento de riesgos

Según los datos que nos proporciona la tabla anterior, se incluirán en el plan de tratamiento de riesgos los proyectos que son viables. En el Anexo D. Plan de tratamiento de riesgos, se muestran los detalles de estos proyectos y su plazo estimado de ejecución. A modo de resumen se muestra el siguiente diagrama de dependencias de los proyectos del plan de tratamiento de riesgos.

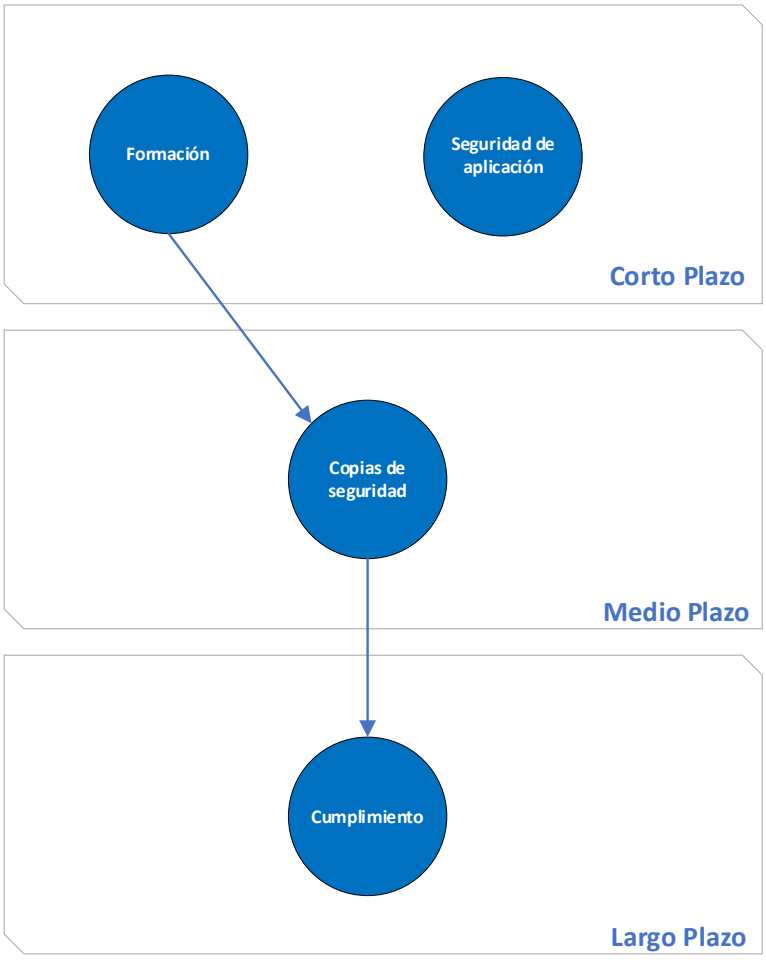

Figura 15. Plan de tratamiento de riesgos. Fuente: Elaboración propia

3.5.4. Controles implementados en el plan de tratamiento de riesgos

El apartado 6.1.3 c) de la norma ISO 27001 establece que se tiene que verificar que se implementen los controles necesarios recogidos en el anexo A de dicha norma [5]. Para ello, se van a desglosar los proyectos de seguridad del plan de tratamiento de riesgos y los controles que implementa cada uno de ellos. También se van a revisar los controles añadidos por la norma ISO 27017 [7] que complementan los establecidos por la norma ISO 27001 pero enfocan el escenario de servicios en la nube que es caso de este estudio.

3.5.4.1. Copias de seguridad.

Norma	Control	Descripción
ISO 27001	A.6.1.5	La gestión del proyecto tratará la seguridad de la información de acuerdo con sus particularidades y sin importar la naturaleza de este.
ISO 27001	A.8.2.3	La manipulación de la información se realizará siguiendo los procedimientos adoptados de acuerdo con la clasificación establecida.
ISO 27001	A.12.3.1	Se harán copias de seguridad de las bases de datos de acuerdo a la política de copias de seguridad de la compañía
ISO 27001	A.17.2.1	Se realizarán las copias de seguridad que sean necesarias de cada instancia RDS para garantizar su disponibilidad

Tabla 12. Controles implementados por el proyecto Copias de seguridad

3.5.4.2. Seguridad de aplicación

Norma	Control	Descripción
ISO 27001	A.6.1.5	La gestión del proyecto tratará la seguridad de la información de acuerdo con sus particularidades y sin importar la naturaleza de este.
ISO 27001	A.9.1.1	Se establecerá una política de acceso que debe cumplir los requisitos del negocio y de la seguridad de la información
ISO 27001	A.9.1.2	Se implementarán los controles de acceso basados en roles para permitir que los usuarios únicamente tengan acceso a aquellas áreas de información de su competencia
ISO 27001	A.9.2.1	Se implementará una funcionalidad para alta y baja de usuarios de acuerdo con el procedimiento forma establecido en la política. Esta funcionalidad permitirá asignar permisos a los usuarios.
ISO 27001	A.9.2.2	Se implementará una funcionalidad para asignar/revocar permisos de acceso
ISO 27001	A.9.2.3	La funcionalidad que permite administrar usuarios y sus permisos será implementada de tal forma que únicamente pueda ser accedida por usuario administrador o *root*.
ISO 27001	A.9.2.4	El sistema de autenticación a implementar deberá generar aleatoriamente la contraseña de los nuevos usuarios o aquellos que desean modificarla de acuerdo con el procedimiento formal establecido por la compañía
ISO 27001	A.9.4.1	Las funcionalidades de las aplicaciones y el acceso a la información estarán implementadas en base al sistema de permisos descrito anteriormente
ISO 27001	A.9.4.2	Se implementará un proceso de autenticación de doble factor
ISO 27001	A.9.4.3	La funcionalidad de control de acceso requerirá y genera contraseñas seguras que contengan una longitud mínima de caracteres e incluyan letras mayúsculas, minúsculas, números y signos de puntuación.
ISO 27001	A.9.4.4	La funcionalidad de control de acceso no permitirá crear cuentas de administrador. Las cuentas de administrador o *root* estarán limitadas y sólo se podrá crear un número limitado según el procedimiento establecido
ISO 27001	A.9.4.5	Existirá un control de acceso con usuario y contraseña para acceder a los diferentes entornos que se van a crear para probar el código fuente

		antes de ser desplegado en producción, así como a las ramas de git donde se aloja el código.
ISO 27001	A.10.1.1	El cifrado de las instancias RDS se hará de acuerdo con lo establecido en la política sobre el uso de controles criptográficos para proteger la información
ISO 27001	A.10.1.2	Las claves de cifrado utilizadas para cifrar las instancias RDS se manejarán de acuerdo con la política sobre uso, duración y protección de las claves de cifrado durante todo su ciclo de vida
ISO 27001	A.12.1.4	Se crearán entornos separados para entornos de desarrollo, pruebas, preproducción y producción
ISO 27001	A.12.2.1	Se implementará una capa de seguridad contra las amenazas más comunes
ISO 27001	A.12.4.1	Se implementará un sistema de trazabilidad de todas las acciones realizadas por un usuario
ISO 27001	A.12.4.2	Se implementarán los mecanismos necesarios para que los registros del sistema de trazabilidad no puedan ser manipulados (clave publica)
ISO 27001	A.12.4.3	El sistema de trazabilidad registrará todas las acciones realizadas por los usuarios incluyendo los administradores
ISO 27001	A.12.4.4	El sistema de trazabilidad utilizará el horario oficial establecido por la política de la empresa
ISO 27001	A.12.5.1	El paso del software por los diferentes entornos permitirá controlar la instalación final del mismo en producción
ISO 27001	A.14.1.1	Para el desarrollo de las aplicaciones se incluirán los relacionados con la seguridad de la información
ISO 27001	A.14.1.2	La información contenida en las bases de datos de los clientes será asegurada mediante su cifrado
ISO 27001	A.14.1.3	Las medidas de seguridad implementadas en este proyecto añadirán protección a información manejada en las transacciones que realizan
ISO 27001	A.14.2.1	El desarrollo de las aplicaciones y funcionalidades añadidas seguirá las reglas de desarrollo de la compañía que establecen los mecanismos seguros para el desarrollo de software
ISO 27001	A.14.2.2	El control de cambios en el desarrollo de software se gestionará mediante la herramienta git
ISO 27001	A.14.2.3	Cualquier cambio que se realice en un entorno será probado en los nuevos entornos de pruebas, incluyendo el cambio del sistema operativo
ISO 27001	A.14.2.4	Cualquier cambio deberá ser probado y aprobado mediante los procedimientos de la compañía utilizando la herramienta git
ISO 27001	A.14.2.6	Los desarrollos se llevarán siempre bajo el entorno de desarrollo seguro provisto por la compañía
ISO 27001	A.14.2.8	Se realizarán pruebas funcionales de seguridad en los entornos creados para ello
ISO 27001	A.14.2.9	Se realizarán pruebas de aceptación tras actualizar o añadir nuevos componentes software en los nuevos entornos creados para ello
ISO 27001	A.14.3.1	Se implementarán los procedimientos para garantizar que todos los datos que se usarán en los entornos de prueba serán enmascarados
ISO 27001	A.18.1.4	Se garantizará la privacidad y protección de la información contenida en las bases de datos mediante su cifrado
ISO 27001	A.18.1.5	Los controles criptográficos se ajustarán a las regulaciones pertinentes
ISO 27017	CLD.9.5.1	Siempre se utilizarán instancias independientes para los clientes de forma que no se comparten los datos de diferentes clientes en una misma instancia
ISO 27017	CLD.9.5.2	Se cerrarán todos los puertos de acceso a las máquinas virtuales que conforman los entornos de pruebas. También se implementarán controles de trazabilidad, cifrado y autenticación de doble factor.

Tabla 13. Controles implementados por el proyecto Seguridad de aplicación

3.5.4.3. Formación

Norma	Control	Descripción
ISO 27001	A.6.1.5	La gestión del proyecto tratará la seguridad de la información de acuerdo con sus particularidades y sin importar la naturaleza de este.
ISO 27001	A.7.2.1	La formación para empleados remarcará la exigencia de aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
ISO 27001	A.7.2.2	Las actividades formativas tanto para empleados como para clientes incluirán contenidos para concienciar y capacitar en la seguridad de la información y, además, se irán actualizando para adaptarse a la actualidad.
ISO 27001	A.9.3.1	En la formación a empleados se requerirá a los usuarios el cumplimiento de las prácticas establecidas por la compañía para el manejo de la información secreta de autenticación
ISO 27001	A.11.2.8	En la formación a empleados se remarcarán las normas de seguridad que deben aplicarse cuando se deja un equipo desatendido
ISO 27001	A.11.2.9	En la formación a empleados se remarcarán las normas de seguridad que deben aplicarse en el puesto de trabajo incluyendo la política de puesto de trabajo despejado y pantalla limpia
ISO 27017	CLD.6.3.1	Como proveedores de servicio *cloud* se utilizarán las formaciones a clientes para comunicar y compartir la documentación acerca de la seguridad de la información pertinente, dejando claro roles, responsabilidades y controles que el cliente debe implementar como usuario del servicio *cloud*.
ISO 27017	CLD.8.1.5	Como proveedores de servicio *cloud* se utilizarán las formaciones a clientes para comunicar y compartir la documentación existente acerca del proceso de devolución/eliminación de activos del cliente en el entorno *cloud* como consecuencia de la finalización del contrato.
ISO 27017	CLD.12.1.5	Como proveedores de servicio *cloud* se utilizarán las formaciones a clientes para comunicar y compartir la documentación acerca de los procesos y operaciones críticas.
ISO 27017	CLD.12.4.5	Como proveedores de servicio *cloud* se utilizarán las formaciones a clientes para comunicar y compartir la documentación acerca del manejo de la aplicación cuadro de mandos que permite la monitorización de las instancias.

Tabla 14. Controles implementados por el proyecto Formación

3.5.4.4. Cumplimiento

Norma	Control	Descripción
ISO 27001	A.6.1.5	La gestión del proyecto tratará la seguridad de la información de acuerdo con sus particularidades y sin importar la naturaleza de este.
ISO 27001	A.13.2.1	Se establecerás políticas, procedimientos y controles para proteger el intercambio de información entre instancias AWS cumpliendo con la normativa
ISO 27001	A.13.2.2	Se establecerán acuerdos con los clientes y proveedores de servicios para garantizar el intercambio seguro de información cumpliendo con la normativa
ISO 27001	A.18.1.5	Los controles criptográficos se ajustarán a las regulaciones pertinentes mediante la administración del cifrado de las bases de datos en las instancias RDS
ISO 27001	A.18.2.3	Este proyecto se encargará de verificar el cumplimiento de las políticas y normas de seguridad de la información establecidas por la compañía

Tabla 15. Controles implementados por el proyecto Cumplimiento

3.5.5. Otros controles implementados en el SGSI

Cabe destacar que existen otros controles que también estarían incluidos en el SGSI pero que por su naturaleza están fuera de los proyectos de seguridad dentro del plan de tratamiento de riesgos, por lo que no se han mostrado en el apartado anterior. Se resumen en la siguiente tabla todos los controles que serían implementados por el SGSI.

Norma	Control	Descripción
ISO 27001	A.5	Políticas de seguridad
ISO 27001	A.6.1	Organización Interna
ISO 27001	A.6.2	Dispositivos móviles y teletrabajo
ISO 27001	A.8	Gestión de activos
ISO 27001	A.9	Control de acceso
ISO 27001	A.11	Seguridad física y del entorno
ISO 27001	A.12	Seguridad de las operaciones
ISO 27001	A.13	Seguridad de las comunicaciones
ISO 27001	A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información
ISO 27001	A.15	Relación con proveedores: Importante en este escenario en el que existe una cadena de suministro entre cliente, compañía y prestador de servicios (AWS)
ISO 27001	A.16	Gestión de incidentes de seguridad de la información
ISO 27001	A.17	Aspectos de seguridad de la información para la gestión de continuidad del negocio
ISO 27001	A.18	Cumplimiento

Tabla 16. Controles ISO 27001

3.6. Objetivos de seguridad de la información

Siguiendo el apartado 6.2 de la ISO27001, la compañía establece, a grandes rasgos, los objetivos de seguridad de la información a largo plazo:

- Diseño e implantación de un Sistema de Gestión de Seguridad de la Información que cubra el proceso de explotación del software en su versión *cloud*, incluyendo las actividades y tareas que comprende dicho proceso.
- Cumplimiento de la norma ISO27001 en el SGSI mencionado en el punto anterior
- Establecer un sistema de mejora continua para mantener el SGSI y el cumplimiento de la norma aplicable en seguridad de la información
- Establecer procedimientos de recuperación y continuidad de negocio que sean dinámicos y adaptables al cliente y su entorno.
- Revisión y evaluación periódica de condiciones contractuales con proveedores y valoración de alternativas que garanticen mayores niveles de cumplimiento en lo relativo a normativa de seguridad.

3.7. Soporte, operación, evaluación y mejora continua

Una vez diseñado el SGSI, la ISO27001 propone las siguientes medidas para la implantación y mejora continua del SGSI. Se muestra a continuación qué acciones se llevarán a cabo para cumplir con estos apartados de la norma.

3.7.1. Soporte

La compañía proporcionará todos los medios y recursos necesarios para establecer, implementar, mantener y mejorar el SGSI. Se valorará la competencia del personal en lo que respecta a su relación con el SGS, se realizarán acciones formativas y de concienciación sobre la importancia de la seguridad de la información y el SGSI. Se comunicará oficialmente toda la información relevante acerca del SGSI y se proporcionará documentación que se revisará y actualizará periódicamente.

3.7.2. Operación

Se planificarán, implementará y controlarán todos los procesos indicados en el plan de tratamiento de riesgos, así como los necesarios para la consecución de los objetivos de seguridad de la información especificados en el apartado anterior. Se implementarán los controles establecidos en el plan de tratamiento de riesgos para llevar a cabo la apreciación de riesgos que será documentada correspondientemente.

3.7.3. Evaluación

La compañía se asegurará de monitorizar el desempeño de la seguridad de la información y verificar que el SGSI es eficaz. Se programarán auditorías internas periódicas con el fin de evaluar si el SGSI cumple con los requisitos de la compañía y los de la norma ISO27001.

Además, se establecerán revisiones periódicas por parte de la dirección para validar la adecuación, eficacia y conveniencia del SGSI de modo continuo.

3.7.4. Mejora continua

Establecer las acciones correctivas a llevar a cabo tras detectar una no conformidad que garanticen su control, corrección y afrontar las consecuencias, además de la eliminación de las causas que dieron lugar a la no conformidad.

Garantizar la mejora continua la eficacia, idoneidad y adecuación del SGSI.

4. Conclusiones

Combinando los conocimientos adquiridos durante el estudio de este máster y el trabajo de investigación realizado para este proyecto en las áreas de servicios *cloud* y seguridad de la información, se ha podido desarrollar el diseño de un Sistema de Gestión de la Seguridad de la Información para un área específica de una compañía.

El SGSI diseñado se encuentra en una fase inicial, necesitaría implantarse y pasar por el proceso de mejora continua para alcanzar cierta madurez que lo haga más robusto. Por esta razón, es muy importante enfatizar el cumplimiento del ciclo de Deming en los sistemas de gestión, ya que tienen que adaptarse constantemente a las necesidades cambiantes del mundo actual. Esto cobra mayor sentido en un ámbito como el de la seguridad de la información, donde constantemente pueden aparecer nuevas amenazas que pongan en riesgo la continuidad del negocio.

Los resultados obtenidos tras realizar el análisis de riesgos siguiendo la metodología MAGERIT ponen de manifiesto que el tratamiento de riesgos no se centrará en los activos de información que forman parte de la infraestructura tecnológica, es decir, los que están alojados en servicios *cloud*. Esto demuestra que, si el proveedor de servicios *cloud* garantiza en sus prácticas un cumplimiento mínimo de los estándares de seguridad de la información actuales, la compañía que contrata el servicio se liberaría en gran parte del tratamiento de dichos riesgos, lo que supone un beneficio en cuestión de ahorro de tiempo, dinero y esfuerzo dedicado, por ejemplo, a proteger la seguridad física de las instalaciones. De esta forma únicamente se deberán enfocar en proteger la información que manejan de acuerdo con el RGPD y verificar que el proveedor de servicios cumple con estos estándares. Esta es una de las razones de peso, por las que hoy en día cada vez más empresas contratan este tipo de servicios.

La importancia de las normas y estándares en materia de seguridad de la información y su aplicación dentro de los sistemas de gestión de las compañías es vital ya que son una herramienta imprescindible para lograr la implementación de sistemas de gestión de seguridad de la información eficaces.

Las normas de estandarización, como las de la familia ISO 27000, tratan de abarcar todos los posibles escenarios que pueden darse en una compañía. Es trabajo de estas, identificar cuáles de ellas se van a aplicar en su entorno y qué controles se deberán implementar. Para ello, las auditorías de cumplimiento internas pueden ayudar bastante a cuantificar el grado de cumplimiento de su SGSI. En este sentido, repasar algunos informes de este tipo de auditorías durante la investigación para este proyecto me ayudó bastante a comprender qué se espera de un SGSI y cómo seleccionar los controles aplicables al entorno dado.

5. Trabajos futuros

El presente trabajo plantea una serie de líneas de trabajo adicionales que podrían ser tratadas en futuros proyectos o trabajos de investigación.

- Elaborar una política de seguridad completa para el entorno dado.
- Diseñar la auditoría de cumplimiento de las normas ISO 27001 e ISO 27017 para el SGSI diseñado en este proyecto
- Ampliar cumplimiento ISO 27001 al área de explotación *on premises* / desarrollo / global en la compañía
- Desarrollar los proyectos de seguridad recogidos en el plan de tratamiento de riesgos.
- Medir la madurez del SGSI utilizando COBIT

Bibliografía

[1] AEPD, «Agencia española de protección de datos,» 2018. [En línea]. Available: https://www.aepd.es/es/documento/guia-cloud-clientes.pdf-0. [Último acceso: Junio 2021].

[2] Varios, «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. [Último acceso: Junio 2021].

[3] K.-b. -. K. B. (http://www.bulsuk.com), «PDCA Cycle,» [En línea]. Available: https://commons.wikimedia.org/wiki/File:PDCA_Cycle.svg. [Último acceso: Junio 2021].

[4] «Cobit y la seguridad de la información,» 6 Diciembre 2018. [En línea]. Available: https://www.pmg-ssi.com/2018/12/como-se-relaciona-cobit-5-y-la-seguridad-de-la-informacion/. [Último acceso: Julio 2021].

[5] UNE-EN, *ISO-27001,* 2017.

[6] Administración Electrónica, «MAGERIT,» Octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: Julio 2021].

[7] ISO 27017, *ISO 27017,* 2021.

[8] Amazon, «Amazon Web Services Compliance,» [En línea]. Available: https://aws.amazon.com/es/compliance/programs/.

[9] UNE-EN, *ISO-27002,* 2017.

[10] «Norma ISO27001.es,» [En línea]. Available: https://normaiso27001.es/. [Último acceso: Mayo 2021].

[11] Agencia española de protección de datos, «AEPD,» [En línea]. Available: https://www.aepd.es/sites/default/files/2019-09/guia-cloud-prestadores.pdf. [Último acceso: Junio 2021].

[12] P.-C. Valcarcel Lucas, *Apuntes Seguridad Informática Avanzada,* Máster en dirección de proyectos informáticos, 2019.

[13] Amazon, «Documentación de AWS,» Junio 2021. [En línea]. Available: https://aws.amazon.com/.

[14] V. M. Orrego, «Revista Pensamiento Americano,» 2011. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/47441491/57-53-1-PB.pdf?1469232962=&response-content-disposition=inline%3B+filename%3DLa_gestion_en_la_seguridad_de_la_informa.pdf&E

xpires=1624910167&Signature=PsGwyDXGBXAoLtvYYSK7jZkBPjA9p8m35q-R2zZEHyVgn4yieiLDEQ1Hg. [Último acceso: 2021].

[15] AWS, «AWS Risk and compliance,» Enero 2016. [En línea]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/aws-risk-and-compliance-program.html. [Último acceso: Junio 2021].

Anexo A. Catálogo de amenazas MAGERIT

[N] Desastres naturales	[N.1] Fuego.
	[N.2] Daños por agua
	[N.*] Otros desastres naturales
[I] De origen industrial	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación mecánica
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios y suministros esenciales.
	[I.10] Degradación de los soportes de almacenamiento de la información
	[I.11] Emanaciones electromagnéticas.
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios
	[E.2] Errores del administrador.
	[E.3] Errores o manipulación de registros de actividad (log)
	[E.4] Errores o manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[E.7] Uso no previsto
	[E.8] Difusión de software dañino.
	[E.9] Errores de re-encaminamiento.
	[E.10] Errores o alteración de secuencia
	[E.18] Destrucción de información
	[E.19] Fugas o revelación de información.
	[E.20] Vulnerabilidades de los programas (software).
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.22] Manipulación de programas.

	[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos
	[E.25] Robo o Pérdida de equipos
(Pd) Amenazas relacionadas con el cumplimiento	[Pd.1] Ataque a los derechos de los afectados (ARCO, información, consentimiento, portabilidad)
	[Pd.2] Carencia de legitimación en el tratamiento de la información
	[Pd.3] Falta de transparencia en el tratamiento de la información
	[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas
	[Pd.5] Incumplimiento del Principio de Calidad de los datos
	[Pd.6] Falta de control de los tratamientos derivados de un inadecuado registro y notificación
	[Pd.7] Incumplimiento de las medidas de seguridad
	[Pd.8] Divulgación que origina incumplimiento en el deber de secreto
	[Pd.9] Errores de los usuarios o en el tratamiento de la información por falta de sensibilización y conocimiento experto de la normativa
	[Pd.10] Errores, pérdidas de información, incumplimiento medidas de seguridad por un control, gestión o elección deficiente del Encargado del Tratamiento
[A] Ataques intencionados	[A.11] Acceso no autorizado.
	[A.12] Análisis de tráfico
	[A.13] Repudio
	[A.14] Interceptación de información (escucha).
	[A.26] Ataque destructivo
	[A.27] Ocupación enemiga
	[E.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)

Anexo B. Análisis de Riesgos

La siguiente tabla muestra el detalle del análisis de riesgos realizado en la fase de planificación del SGSI. Con la ayuda de la herramienta proporcionada en la asignatura de Seguridad Informática Avanzada de este mismo máster.

En ella se muestran las siguientes columnas:

- **Vulnerabilidad**: la vulnerabilidad que se analiza.
- **Explicación**: Detalle de cómo podría manifestarse y afectar a la compañía en estudio.
- **Dificultad de explotación – Nivel**: Expresa la probabilidad de que la amenaza se materialice.
- **Dificultad de explotación – Explicación:** Razonamiento del valor anterior.
- **Amenaza:** Amenaza dentro del catálogo de MAGERIT.
- **Activo:** Recurso de TI sobre el que se manifiesta la amenaza.
- **Daño para la organización – Nivel**: Expresa el daño que causaría la amenaza a la compañía.
- **Daño para la organización – Explicación**: Razonamiento del valor anterior.
- **Identificador**: Donde se ha encontrado la información para dar los valores anteriores.

		Dificultad de explotación (L)		Asignación de riesgo		Daño para la organización (D)		
Vulnerabilidad	**Explicación**	**Nivel**	**Explicación**	**Amenaza**	**Activo (Recurso IT)**	**Nivel**	**Explicación**	**Identificador**
La ubicación donde se encuentren las instancias EC2 que despliegan los servidores de aplicaciones pueden ser vulnerables a desastres naturales.	Inundaciones, temperaturas extremas, terremotos o cualquier otro desastre natural podría destruir los servidores sobre los que se despliegan las instancias EC2	5 - Muy Baja	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales.	[N.*] Otros desastres naturales	Servidores Tomcat (EC2 AWS)	3 - Alto	El cliente perdería servicio	Documento Amazon web services risk and compliance [15]
La ubicación donde se encuentren las instancias EC2 que despliegan los servidores web pueden ser vulnerables a desastres naturales.	Inundaciones, temperaturas extremas, terremotos o cualquier otro desastre natural podría destruir los servidores sobre los que se despliegan las instancias EC2	5 - Muy Baja	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales.	[N.*] Otros desastres naturales	Servidores Apache (EC2 AWS)	2 - Medio	Se podrían dar retrasos en la atención de peticiones en caso de sobrecarga	Documento Amazon web services risk and compliance [15]
La ubicación donde se encuentren las instancias RDS que despliegan los servidores mysql pueden ser vulnerables a desastres naturales.	Inundaciones, temperaturas extremas, terremotos o cualquier otro desastre natural podría destruir los servidores sobre los que se despliegan las instancias RDS	5 - Muy Baja	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales.	[N.*] Otros desastres naturales	Servidores MySQL (RDS AWS)	3 - Alto	Se perderían datos del cliente	Documento Amazon web services risk and compliance [15]
Se puede producir un incendio en las instalaciones donde se almacenan las bases de datos mysql	Si esto ocurre se producirían pérdidas de datos de los clientes	5 - Muy Baja	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales.	[I.1] Fuego	Servidores MySQL (RDS AWS)	4 - Muy Alto	Se perderían datos del cliente	Documento Amazon web services risk and compliance [15]

Avería que afecte a los servidores de aplicaciones o a las aplicaciones desplegadas en ellos (CMS front y back)	Si esto ocurre se produciría pérdida de funcionalidad	4 - Baja	No es común que se produzcan fallos de este tipo en los entornos de producción ya que se prueban concienzudamente	[I.5] Avería de origen físico o lógico	Servidores Tomcat (EC2 AWS)	3 - Alto	Un funcionamiento anómalo podría producir afectar a la integridad de los datos manejados	Documento Amazon web services risk and compliance [15]
Avería que afecte a los servidores de bases de datos	Si esto ocurre se producirían pérdidas de datos de los clientes	4 - Baja	No es común que se produzcan fallos de este tipo en los entornos de producción ya que se prueban concienzudamente	[I.5] Avería de origen físico o lógico	Servidores MySQL (RDS AWS)	4 - Muy Alto	Se perderían datos del cliente	Documento Amazon web services risk and compliance [15]
Corte del suministro eléctrico dejaría sin alimentación a los servidores de bases de datos	Si esto ocurre podrían quedarse pendientes transacciones y producir un estado corrupto de los daatos	4 - Baja	El equipo de AWS está protegido frente a interrupciones de los servicios públicos de conformidad con la norma ISO 27001.	[I.6] Corte del suministro eléctrico	Servidores MySQL (RDS AWS)	4 - Muy Alto	Se perderían datos del cliente	Documento Amazon web services risk and compliance [15]
Fallan los servicios de cominicaciones y no es posible acceder a los servicios de aplicación	No habría acceso a la aplicación	4 - Baja	El equipo de AWS está protegido frente a interrupciones de los servicios públicos de conformidad con la norma ISO 27001.	[I.8] Fallo de servicios de comunicaciones	Servidores Apache (EC2 AWS)	3 - Alto	Puede afectar a la compañía si ocurre en momentos en los que se genere un gran volumen de negocio	Documento Amazon web services risk and compliance [15]
Falla o se ve interrumpido algún servicio o suministro esencial	La base de datos puede ser súbitamente terminada	4 - Baja	El equipo de AWS está protegido frente a interrupciones de los servicios públicos de conformidad con la norma ISO 27001.	[I.9] Interrupción de otros servicios y suministros esenciales.	Servidores MySQL (RDS AWS)	3 - Alto	Un funcionamiento anómalo podría producir afectar a la integridad de los datos manejados	Documento Amazon web services risk and compliance [15]
Los usuarios cometen errores al manejar la aplicación	La información puede verse comprometida por estos errores (borrados accidentales, sobreescritura de registros…)	3 - Media	Los usuarios con permisos de modificación de registros deben haberse formado	[E.1] Errores de los usuarios	Servidores MySQL (RDS AWS)	2 - Medio	Un error de un usuario podría conllevar la pérdida de información	Política interna de la compañía
El administrador comete un error al manipular las instancias de los servidores de aplicaciones	Un error de administración de sistemas puede conllevar a un mal despliegue de las aplicaciones o versiones incorrectas ejecutándose	4 - Baja	Los empleados reciben formación y los cambios en instancias deben aprobarse por varios miembros del equipo	[E.2] Errores del administrador.	Servidores MySQL (RDS AWS)	3 - Alto	Un error en la administración de las aplicaciones podría conllevar a la pérdida de funcionalidad	Política interna de la compañía

El administrador comete un error al manipular las instancias de los servidores de bases de datos	Un error de administración de base de datos puede llevar a la imposibilidad de acceso a la misma o la pérdida de datos existentes	4 - Baja	Los empleados reciben formación y los cambios en instancias deben aprobarse por varios miembros del equipo	[E.2] Errores del administrador.	Servidores Tomcat (EC2 AWS)	3 - Alto	Un error en las instancias RDS provocaría pérdidas de información	Política interna de la compañía
La configuración de las aplicaciones es defectuosa	Un error de configuración de aplicaciones puede conllevar a un mal despliegue de las aplicaciones o versiones incorrectas ejecutándose	4 - Baja	Los empleados reciben formación y los cambios en configuración deben aprobarse por varios miembros del equipo	[E.4] Errores o manipulación de la configuración	Servidores Tomcat (EC2 AWS)	3 - Alto	Un error en la configuración de los servidores de aplicaciones podría conllevar a la pérdida de funcionalidad	Política interna de la compañía
La configuración de las bases de datos es defectuosa	Un error de configuración de base de datos puede llevar a la imposibilidad de acceso a la misma o la pérdida de datos existentes	4 - Baja	Los empleados reciben formación y los cambios en configuración deben aprobarse por varios miembros del equipo	[E.4] Errores o manipulación de la configuración	Servidores MySQL (RDS AWS)	3 - Alto	Se perdería información	Política interna de la compañía
Un tercero puede acceder a las instancias del CMS con los datos de acceso del cliente	Si el acceso a la aplicación no tiene las medidas de seguridad adecuadas un tercero podría hacerse con las credenciales de un usuario y suplantar su identidad	4 - Baja	Existe un sistema de autenticación de doble factor por el que es bastante complicado que se pueda acceder con datos de otra persona	[A.5] Suplantación de la identidad del usuario	Cliente	3 - Alto	Se podría actuar de forma malintencionada en el nombre de otro usuario	Política interna de la compañía
Un usuario con privilegios de administración abusa de estos para adquirir información a la que no debe acceder	Los administradores SRE con privilegios de acceso total podrían acceder a los datos de la instancia de algún cliente	3 - Media	Existe un compromiso de confidencialidad para todos los empleados, pero este podría romperse por parte de alguno de ellos	[A.6] Abuso de privilegios de acceso	Empleado (SRE/Ingeniero)	3 - Alto	Se podría acceder a información sensible de algún cliente	Política interna de la compañía
Se despliega una pieza de software dañino en la solución cloud del CMS	En algún despliegue de una nueva versión del CMS se incluye alguna funcionalidad que resulta ser dañina no intencionadamente	4 - Baja	Existen controles y pruebas estrictas antes de que el software sea desplegado	[E.8] Difusión de software dañino.	Servidores Tomcat (EC2 AWS)	3 - Alto	El software dañino afectaría a los clientes con el riesgo de perderlos y ganar mala reputación	Política interna de la compañía
Se destruye información contenida en las bases de datos de las instancias RDS	Por algún error no intencionado, la información de las bases de datos se destruye.	4 - Baja	Existen controles antes de realizar este tipo de operaciones	[E.18] Destrucción de información	Servidores MySQL (RDS AWS)	3 - Alto	Se perdería información	Política interna de la compañía

La información contenida en las instancias RDS es revelada o filtrada por algún usuario	La información de alguna de las instancias de un cliente es accedida y revelada por un empleado con privilegios de acceso de administración	4 - Baja	Existe un compromiso de confidencialidad para todos los empleados, pero este podría romperse por parte de alguno de ellos	[E.19] Fugas o revelación de información.	Empleado (SRE/Ingeniero)	3 - Alto	Se perdería la confidencialidad y se podría acceder a información sensible de algún cliente	Política interna de la compañía
El software podría tener vulnerabilidades	Vulnerabilidades en el software podrían permitir un ataque	4 - Baja	Existen controles y pruebas estrictas antes de que el software sea desplegado	[E.20] Vulnerabilidades de los programas (software).	Servidores Tomcat (EC2 AWS)	3 - Alto	Un ataque afectaría a los clientes con el riesgo de perderlos y ganar mala reputación	Política interna de la compañía
El software utilizado en los equipos de los trabajadores no es mantenido o actualizado correctamente	Se utilizan versiones antiguas o no correctamente actualizadas del software	4 - Baja	Existe una política de actualizaciones de software en la que se obliga a tener siempre instaladas las últimas versiones recomendadas por el departamento de seguridad de la información	[E.21] Errores de mantenimiento / actualización de programas (software)	Equipos portátiles	2 - Medio	Los errores en la actualización o mantenimiento podrían provocar fallos de seguridad	Política interna de la compañía
El software utilizado en los equipos de los trabajadores no es mantenido o actualizado correctamente debido a su manipulación	Se utilizan versiones antiguas o no correctamente actualizadas del software	4 - Baja	Existe una política de actualizaciones de software en la que se obliga a tener siempre instaladas las últimas versiones recomendadas por el departamento de seguridad de la información	[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)	Equipos portátiles	2 - Medio	Los errores en la actualización o mantenimiento podrían provocar fallos de seguridad	Política interna de la compañía
La aplicación no puede atender peticiones debido a una caida provocada por alta demanda	Se produce una alta demanda de peticiones que provoca que los recursos no sean suficientes para atenderlas y se interrumple el servicio	4 - Baja	AWS ofrece posibilidad de autoescalado para garantizar la alta disponibilidad	[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	Servidores Apache (EC2 AWS)	3 - Alto	El cliente podría perder actividad en su negocio	Documento Amazon web services risk and compliance [15]

Los equipos portátiles de trabajo de los SREs se pierden o son robados	El robo de estos puede implicar la pérdida importante de información ya sea de la compañía de algún cliente o alguna funcionalidad implementada que aún no se ha subido a los repositorios comunes	4 - Baja	El personal ha pasado por un proceso de formación y concienciación de la importancia de guardar a buen recaudo los equipos	[E.25] Robo o Pérdida de equipos	Equipos portátiles	3 - Alto	Habría que comprar equipos nuevos y se podría perder información con valor en los equipos extraviados	Política interna de la compañía
Los datos son transferidos a otro país donde la legislación es diferente	Al estar en un entorno cloud, por razones de mantenimiento o necesidades para garantizar la capacidad, los datos contenidos en las instancias RDS podrían ser alojados en uno de los servidores de otro país cuya legislación difiera del país d eorigen	5 - Muy Baja	Los clientes pueden designar en qué región física se ubicarán sus datos. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales.	[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas	Servidores MySQL (RDS AWS)	3 - Alto	Un no cumplimento de este tipo podría suponer una sanción importante	Documento Amazon web services risk and compliance [15]
Datos protegidos son divulgados	Los datos de carácter protegido en una de las instancias de un cliente son accedidos y divulgados por un empleado con privilegios de acceso de administración	4 - Baja	Existe un compromiso de confidencialidad para todos los empleados, pero este podría romperse por parte de alguno de ellos	[Pd.8] Divulgación que origina incumplimiento en el deber de secreto	Empleado (SRE/Ingeniero)	3 - Alto	Un no cumplimento de este tipo podría suponer una sanción importante	Política interna de la compañía
Se accede sin autorización a los datos de las instancias RDS	Se accede desde el exterior a los datos de las bases de datos de las instancias RDS, por parte de los empleados de AWS	4 - Baja	Según la política de AWS: No accedemos a su contenido ni lo usamos para ningún otro fin sin su consentimiento. En ningún momento utilizamos su contenido ni extraemos información para marketing o publicidad.	[A.11] Acceso no autorizado.	Servidores MySQL (RDS AWS)	3 - Alto	Supondría un fallo en el mantenimiento de la confidencialidad de la información del cliente	https://aws.amazon.com/es/compliance/data-privacy-faq/

Se analiza el tráfico de la red para establecer unos comportamientos o conocer qué se está haciendo	Se podría analizar el tráfico de información que viaja a través de la red de la compañía con fines malintencionados	4 - Baja	La red interna implementa los mecanismos de seguridad que impiden el acceso a terceros, sería muy dificil que esta situación se diese	[A.12] Análisis de tráfico	Red Interna	2 - Medio	Se podrían conocer detalles internos de la compañía a través del análisis de tráfico	Política interna de la compañía
Se accede a datos que viajan por la red	Mediante una herramienta de escucha o sniffer se podrían interceptar datos que viajan por la red interna de la compañía	4 - Baja	Los datos viajan cifrados	[A.14] Interceptación de información (escucha).	Red Interna	3 - Alto	Información confidencial podría caer en manos de terceros comprometiendo a la compañía	Política interna de la compañía
Un ataque destructivo contra los servidores de aplicaciones	Un atacante podría tratar de destruir la información de los servidores de aplicaciones	4 - Baja	AWS provee de mecanismos de seguridad ante ataques	[A.26] Ataque destructivo	Servidores Tomcat (EC2 AWS)	3 - Alto	Se perdería información de las aplicaciones	Documento Amazon web services risk and compliance [15]
Un ataque destructivo contra las bases de datos intenta eliminar toda la información de los clientes	Un atacante podría tratar de destruir la información de las bases de datos	4 - Baja	AWS provee de mecanismos de seguridad ante ataques	[A.26] Ataque destructivo	Servidores MySQL (RDS AWS)	3 - Alto	Se perdería información de los clientes	Documento Amazon web services risk and compliance [15]

Anexo C. Tabla de riesgos por amenaza

Amenaza	Riesgo	D	I	C	A	T	Cu
[N.1] Fuego.	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[N.2] Daños por agua	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[N.*] Otros desastres naturales	748.852 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.1] Fuego	643.770 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.2] Daños por agua	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.*] Desastres industriales	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.3] Contaminación mecánica	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.4] Contaminación electromagnética	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.5] Avería de origen físico o lógico	724.241 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.6] Corte del suministro eléctrico	482.827 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.7] Condiciones inadecuadas de temperatura o humedad	0 €	0,6	0,2	0,0	0,2	0,0	0,0
[I.8] Fallo de servicios de comunicaciones	157.624 €	1,0	0,0	0,0	0,0	0,0	0,0
[I.9] Interrupción de otros servicios y suministros esenciales.	241.414 €	1,0	0,0	0,0	0,0	0,0	0,0
[I.10] Degradación de los soportes de almacenamiento de la información	0 €	0,0	0,5	0,0	0,5	0,0	0,0
[I.11] Emanaciones electromagnéticas.	0 €	0,0	0,0	1,0	0,0	0,0	0,0
[E.1] Errores de los usuarios	80.471 €	0,1	0,3	0,3	0,3	0,0	0,0
[E.2] Errores del administrador.	482.827 €	0,1	0,3	0,3	0,3	0,0	0,0
[E.3] Errores o manipulación de registros de actividad (log)	0 €	0,0	0,0	0,0	0,0	0,0	0,0
[E.4] Errores o manipulación de la configuración	241.414 €	0,0	0,5	0,0	0,5	0,0	0,0
[A.5] Suplantación de la identidad del usuario	250.484 €	0,0	0,4	0,2	0,4	0,0	0,0
[A.6] Abuso de privilegios de acceso	237.597 €	0,0	0,4	0,2	0,4	0,0	0,0
[E.7] Uso no previsto	0 €	0,0	0,4	0,2	0,4	0,0	0,0
[E.8] Difusión de software dañino.	643.770 €	0,1	0,3	0,3	0,3	0,0	0,0
[E.9] Errores de re-encaminamiento.	0 €	0,0	0,0	1,0	0,0	0,0	0,0
[E.10] Errores o alteración de secuencia	0 €	0,0	0,5	0,0	0,5	0,0	0,0
[E.18] Destrucción de información	241.414 €	0,0	0,8	0,0	0,2	0,0	0,0
[E.19] Fugas o revelación de información.	237.597 €	0,0	0,0	1,0	0,0	0,0	0,0
[E.20] Vulnerabilidades de los programas (software).	241.414 €	0,0	0,3	0,6	0,1	0,0	0,0
[E.21] Errores de mantenimiento / actualización de programas (software)	50.025 €	0,0	0,6	0,2	0,2	0,0	0,0
[A.22] Manipulación de programas.	0 €	0,0	0,4	0,2	0,4	0,0	0,0
[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)	0 €	0,0	0,4	0,2	0,4	0,0	0,0
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	157.624 €	1,0	0,0	0,0	0,0	0,0	0,0
[E.25] Robo o Pérdida de equipos	100.050 €	0,2	0,0	0,8	0,0	0,0	0,0
[Pd.1] Ataque a los derechos de los afectados (ARCO, información, consentimiento, portabilidad)	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.2] Carencia de legitimación en el tratamiento de la información	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.3] Falta de transparencia en el tratamiento de la información	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas	321.885 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.5] Incumplimiento del Principio de Calidad de los datos	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.6] Falta de control de los tratamientos derivados de un inadecuado registro y notificación	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.7] Incumplimiento de las medidas de seguridad	0 €	0,0	0,0	0,6	0,0	0,4	0,4
[Pd.8] Divulgación que origina incumplimiento en el deber de secreto	237.597 €	0,0	0,0	0,6	0,0	0,4	0,4
[Pd.9] Errores de los usuarios o en el tratamiento de la información por falta de sensibilización y conocimiento experto de la normativa	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[Pd.10] Errores, pérdidas de información, incumplimiento medidas de seguridad por un control, gestión o elección deficiente del Encargado del Tratamiento	0 €	0,0	0,0	0,0	0,0	1,0	1,0
[A.11] Acceso no autorizado.	241.414 €	0,0	0,4	0,6	0,0	0,0	0,0
[A.12] Análisis de tráfico	34.166 €	0,0	0,0	1,0	0,0	0,0	0,0
[A.13] Repudio	0 €	0,0	0,0	0,0	1,0	0,0	0,0
[A.14] Interceptación de información (escucha).	68.331 €	0,0	0,0	1,0	0,0	0,0	0,0
[A.26] Ataque destructivo	482.827 €	0,2	0,6	0,0	0,2	0,0	0,0
[A.27] Ocupación enemiga	0 €	0,1	0,3	0,5	0,1	0,0	0,0
[E.28] Indisponibilidad del personal	0 €	1,0	0,0	0,0	0,0	0,0	0,0
[A.29] Extorsión	0 €	0,0	0,2	0,6	0,2	0,0	0,0
[A.30] Ingeniería social (picaresca)	0 €	0,0	0,0	1,0	0,0	0,0	0,0

Anexo D. Plan de tratamiento de riesgos

ID Proyecto	Activos (ámbito)	Riesgos del proyecto	Recursos	Responsable	Comienzo (Corto, Medio o Largo Plazo)
Copias de seguridad	Servidores de bases datos MySQL en instancias RDS de AWS	Perturbar el funcionamiento normal de los sistemas en producción	550.000 €	SREs	2- Medio Plazo
Formación	Empleados (ingenieros/SREs), clientes	Falta de interés de los participantes hace que la formación pierda su efectividad	275.000 €	Dirección general, RRHH	1 - Corto Plazo
Seguridad de aplicación	Servidores de bases datos MySQL en instancias RDS de AWS, Servidores de aplicaciones Tomcat en instancias EC2 de AWS	Errores en las implementaciones, mal uso y curva de aprendizaje de las herramientas de cifrado e IAM	1.120.000 €	SREs	1 - Corto Plazo
Cumplimiento	Servidores de bases datos MySQL en instancias RDS de AWS	La comunicación con el cliente puede no ser clara y concisa. Desconocimiento de las tecnologías de cifrado en AWS	70.000 €	SREs	3 - Largo Plazo