Màster Interuniversitari en Seguretat de les TIC (MISTIC)

Trabajo Final de Máster
Primavera 2013

Elaboración de un Plan de Seguridad de la Información

OMAR CARAZO TORRES

TUTOR: ARSENIO TORTAJADA GALLEGO

RESUMEN

En el presente documento se realiza la elaboración de un plan de seguridad de la información a una empresa dedicada al sector de las tecnologías de la información. La elaboración de este proyecto consta de las diferentes etapas que componen la elaboración del plan de seguridad, y de un plan director de seguridad acorde a las necesidades de la empresa. Para ello se realiza un análisis de riesgos inicial, para identificar los activos críticos que podrían comprometer la continuidad del negocio en caso de incidente. Con este análisis inicial, posteriormente se analizaran las amenazas que pueden afectar a la empresa sujeta al análisis y con ello se obtendrán los resultados de los activos que se encuentran en riesgo potencial. A partir de estos resultados podrán diseñarse los proyectos necesarios para acercar a niveles óptimos la seguridad de los activos de la organización.

En el documento también se puede encontrar una auditoría interna y de cumplimiento con el objetivo de detectar la situación actual en la que se encuentra la organización y poder obtener un punto de partida a partir del cual comenzar a elaborar el plan de seguridad.

ÍNDICE

1. Resumen ejecutivo

1.1. Motivación del proyecto

Gurb S.A. es una empresa dedicada a dar soporte y ofrecer servicios a la Universidad Politécnica de Cataluña y donde, en estos momentos, se encuentra sumergida en el inicio de una profunda remodelación de su estructura en cuanto a seguridad de las tecnologías de la información se refiere. El objetivo principal de esta remodelación entorno a la seguridad de la información es mejorar la eficiencia y seguridad de los procesos de negocio de manera que se garantice el correcto funcionamiento cumpliendo con los estándares internacionales relacionados con la calidad de la seguridad de la información.

Gurb S.A. consciente de la necesidad de invertir esfuerzos en fortalecer la seguridad en el proceso de negocio, ha considerado oportuno realizar un análisis de la situación actual en la que se encuentra la empresa, de los riesgos y del impacto potencial que supone para el negocio. Este análisis será el comienzo para asentar unas bases para establecer unos criterios y directrices corporativas en materia de seguridad, que ayuden a mejorar de forma global los niveles corporativos en la seguridad de la información.

Para garantizar estos objetivos se ha decidido por definir un plan director de seguridad de la información, utilizando como marco estándar la ISO 27002:2005. A partir de este plan director, la ISO 27002:2005 y en base a un análisis de riesgos, será posible definir una serie de proyectos orientados a los dominios de la organización más vulnerables, con el objetivo de reducir los riesgos potenciales detectados. Todo este plan será incorporado dentro de un ciclo de mejora continua, tal como el que se presenta a continuación.

1.2. Enfoque del proyecto

Tal como se especificó en la motivación de la organización para implementar un plan director de la seguridad, este estará alineado con estándares como la ISO 27002:2005 y para realizar el análisis de riesgos la metodología en la que se basará el proceso será en MAGERIT.

Para realizar este análisis de riesgos se especificarán los activos de la organización orientados a soportar los procesos TI fundamentalmente, y a partir de ahí el alcance del proyecto será el reducir el riesgo de estos activos en caso de incidente o amenaza. Por tanto, el proyecto estará enfocado en identificar los activos críticos para la organización en primer lugar, a partir de la realización de un análisis de riesgos identificando las amenazas que pueden afectar a cada activo. A partir de este punto el plan director debería tener como referencia este análisis previo con el objetivo final de ejecutar los planes adecuados orientados a mejorar los niveles de seguridad de la información en la organización, de forma que todas las dimensiones de la seguridad estén los más próximas posibles a CMM5.

1.3. Conclusiones

Tal como se podrá ver a lo largo del proyecto, el estado inicial de la organización no es el más óptimo en cuanto a cuestiones de seguridad de la información se refiere. Por tanto, a partir del plan director se irán dictando ciertas mejoras que en el conjunto de todas ellas harán que la seguridad mejore en las cinco dimensiones de la seguridad.

Para garantizar la mejora de la seguridad en la organización, a partir de un análisis de la seguridad inicial, se definirán una serie de proyectos que ayudarán a conseguir ese estado óptimo deseado. En total, se ha estimado un conjunto de 3 años para completar esta serie de proyectos con un coste total de 18.900 € el primer año, 13.500€ el segundo año y 15.500 el último. Resultando en un coste total de todos los proyectos al cabo de los 3 años de 47.400 €.

A partir del análisis de riesgos inicial, se identificaron los principales riesgos para la organización, coincidiendo estos con los activos críticos para la continuidad de los procesos de negocio de la empresa, por tanto, los proyectos anteriormente citados, se concentraron principalmente en la seguridad de estos activos. Estos activos estaban enfocados en aplicaciones y servicios web, los cuales no disponían de las medidas de seguridad oportunas para afrontar un incidente o amenaza con seguridad y permitir que el negocio no se viera interrumpido.

Los esfuerzos de los proyectos no se enfocaron únicamente en intentar mitigar o reducir el riesgo que cierta amenaza podía causar sobre los activos críticos de la organización, sino que también fueron enfocados en reducir la frecuencia con que estos se producían.

Como resultado global se consiguió enfocar y mejorar la eficiencia de la organización en temas de la seguridad de la información, sin embargo, esto es un proceso cíclico en constante evolución y habría que continuar realizando análisis para detectar nuevos puntos críticos en la organización o realizando comprobaciones de seguridad pertinentes según detallen las políticas de seguridad.

2. Contextualización y documentación

1.1. Introducción

La empresa sobre la que se realizará el estudio la identificaremos a lo largo del presente documento como Gurb S.L .

Gurb S.A tiene por objetivo con esta actividad, promover la ejecución de prácticas de seguridad adecuadas y la posible implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001 para cubrir los servicios de soporte y servicios especializados, disponibles para los clientes.

1.2. Presentación de la empresa

Gurb S.A forma parte del convenio de empresas pertenecientes a la Universidad Politécnica de Cataluña (UPC), por tanto, todos sus clientes forman parte de este convenio y no de empresas o clientes externos. Esto significa que el principal cliente es la propia Universidad Politécnica de Cataluña en primera instancia, delegando trabajos destinados a mejorar o dar soporte a empresas pertenecientes a este convenio.

1.3. Actividad de negocio

La actividad principal de la empresa Gurb S.L es ofrecer diferentes servicios relacionados con las tecnologías de las TIC a otras empresas o fundaciones pertenecientes a la Universidad Politécnica de Cataluña. Estos servicios son los siguientes:

- Asesorar y dar soporte a las unidades estructurales de la Universidad Politécnica de Cataluña en los ámbitos de planificación estratégica i evaluación institucional y mejora de la certificación interna y externa de la calidad de su actividad.
- Realizar el seguimiento de la planificación académica de los profesores docentes e investigadores (PDI), el análisis de su actividad y evaluar los objetivos alcanzados del personal docente.
- Elaborar informes estadísticos, indicadores de actividad y de resultados en el análisis de datos que provienen de diferentes áreas de actividad de la universidad, realizando, posteriormente, la difusión con carácter oficial de las estadísticas generadas, tanto a nivel interno como externo.
- Diseñar, administrar, analizar y elaborar informes de resultados de encuestas de satisfacción y estudios de opinión de los agentes de interés sobre la actuación docente, oferta formativa y de servicios de la actividad de la universidad.
- Dar soporte a los diferentes órganos de gobierno de la universidad en los procesos de carácter transversal aportando información, análisis y estudios con el fin de realizar la difusión en los grupos de interés.

La sede principal de la empresa se encuentra en Barcelona, así como sus clientes.

1.4. Estructura organizativa

La empresa cuenta con 19 trabajadores distribuidos en el mismo edificio y planta, independientemente de las diferentes funciones que puedan desempeñar.

La distribución por áreas de la empresa es la siguiente:

Administrativo:

- La sección administrativa se encarga de la elaboración de los contratos laborales, de las gestiones con las administraciones y de la compra de material de oficina.

  Esta sección está compuesta únicamente por un trabajador

Desarrollo de soluciones tecnológicas:

- Son los encargados de desarrollar aplicaciones informáticas que ayuden a conseguir los objetivos fijados por el cliente. Otra de las principales funciones que desempeñan es la de dar soporte a las otras secciones con soluciones informáticas que ayuden a mejorar la productividad y tareas que desempeñan.

  El equipo de desarrolladores de soluciones tecnológicas lo conforman:

  - Responsable de sistemas
  - Responsable de desarrolladores
  - Cuatro desarrolladores
  - Especialista en sistemas

Estudios estadísticos y matemáticos:

- Los estudios estadísticos son realizados por personas formadas en matemáticas y estadística y tienen por objetivo principal realizar estudios de los datos que provienen de diferentes áreas de actividad de la universidad.

  El equipo de estudios estadísticos y matemáticos está formado por:

  - Dos personas especializadas en estudios matemáticos y estadísticos

Planificación estratégica y garantía de calidad:

- Encargados de asesorar y dar soporte a las unidades estructurales, así como de realizar el seguimiento de la planificación académica de los profesores docentes e investigadores (PDI) de la universidad.

  El equipo de planificación estratégica y garantía de calidad lo forman:

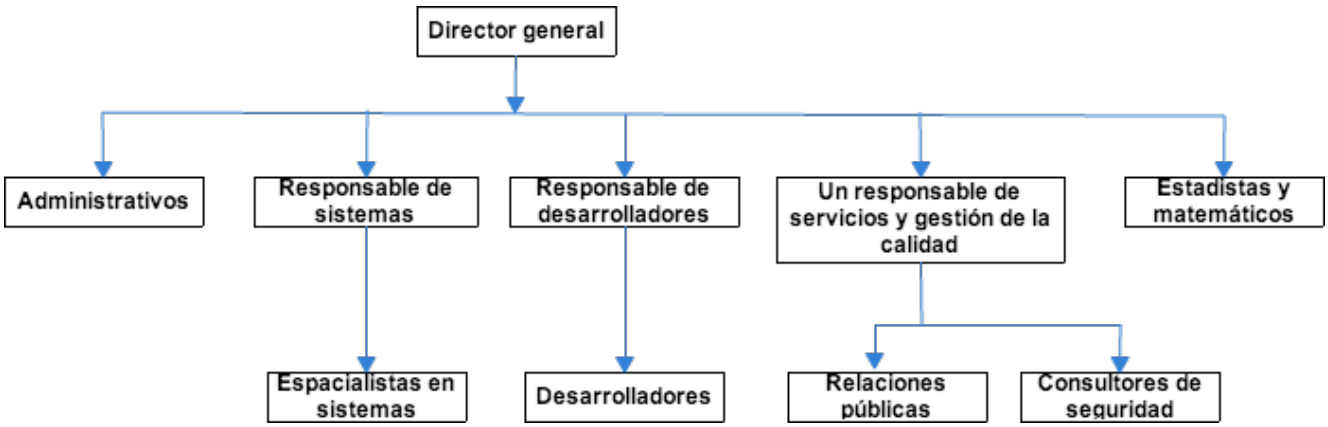
  - Un responsable de servicios y gestión de la calidad
  - Dos relaciones públicas

- Tres consultores de calidad

Por encima de las diferentes secciones existe un director general que es el responsable de que todas las áreas cumplan el grado de calidad y objetivos fijados por la empresa.

Los servicios de asistencia sanitaria están gestionados por la Universidad Politécnica de Cataluña (UPC), por tanto, los reconocimientos médicos, así como el controles se realizan de forma externa.

1.5. Organigrama de la empresa



1.6. Estado inicial de la seguridad

Actualmente, la empresa no cuenta con un departamento de seguridad ni tampoco tiene subcontratado una empresa externa que realice esta tarea. No obstante, cuenta con un soporte informático en caso de incidente del que se hace cargo la Universidad Politécnica de Cataluña, pero únicamente en casos de emergencia, sin tener ningún plan específico ni análisis de riesgos de la empresa específica en cuestión y como soporte de áreas especializadas para guiar en la resolución de problemas e incidentes.

El encargado de supervisar tareas relacionadas con al seguridad son los responsables TIC, que realizan esta tarea no como tarea principal, sino como complemente del buen funcionamiento para lograr los objetivos de las diferentes secciones. Por tanto, no se dispone de ningún SGSI implantado previamente.

Gestión de activos

La empresa no cuenta con un inventario de activos actualizados ni detallados según su función o importancia dentro de la organización de la empresa. Por tanto, tampoco están clasificados como demanda la ISO.

Cada trabajador dispone de un pc de sobremesa equipados con:

- Sistema operativo Windows XP
- Herramientas Office

- Antivirus

Todo el software utilizado dispone de las licencias pertinentes. Además se dispone de 2 impresoras para todos los trabajadores de la empresa.

La sala de servidores se encuentra en la misma sala de trabajo de la compañía, sin estar separada físicamente en otra sala o edificio. El acceso a esta habitación se encuentra custodiada por una llave de la que únicamente disponen copia los responsables TIC.

Seguridad relativa a los recursos humanos

Antes de entrar a trabajar, la persona que empieza las tareas para las que se contrató, ha de firmar un acuerdo de confidencialidad y no divulgación con el fin de evitar fugas de información confidencial de la empresa.

Cuando una persona es dada de baja de su puesto de trabajo, se le revocan los privilegios de acceso inmediatamente.

Seguridad física y controles de acceso

La empresa no dispone de ningún mecanismo de seguridad con el fin de identificar a las personas que acceden a las instalaciones. Debido a que es una empresa de tamaño pequeño , tampoco se dispone de tarjetas para invitados de manera que estos estén identificados.

En cuanto a los controles de acceso, cada usuario tiene asignado un identificador lógico que le permitirá acceder a su ordenador. Para acceder a los recursos compartidos del sistema, se utiliza el usuario dado de alta en el servidor LDAP, con sus permisos pertinentes según las funciones a realizar dentro de la empresa.

1.7. Motivación del plan de director

La confección del plan director será la base del proceso de mejora continua en materia de seguridad para la empresa y las actividades que desarrolla en ella, permitiendo conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales a los que se encuentra expuesta.

La elaboración del plan de director facilitará definir de manera clara cuál es la documentación normativa sobre las mejores prácticas en seguridad de la información, permitirá conocer también en todo momento cuál es la situación actual de la empresa y objetivos futuros para así poder mejorar esta situación.

De cara a poder cumplir estos objetivos:

- Se identificará y valorarán los activos corporativos como punto de inicio así como el análisis de riesgo correspondiente.
- Se evaluarán las amenazas y su clasificación en el ámbito corporativo.
- Se evaluará el nivel de cumplimiento de la ISO/IEC 27002 en la organización.

3. Anexo

3.1 Objetivos del plan director

3.1.1. Introducción

El plan director de seguridad constituye la hoja de ruta a seguir por parte de la empresa que se estudia en el presente documento, con el fin de gestionar de una forma adecuada la seguridad de toda la información y sistemas de la información, permitiendo, por un lado conocer perfectamente el estado en que nos encontramos en todo momento y, por el otro lado poder decidir claramente y con argumentos contrastados y estudiados en qué líneas se debería actuar de cara a mejorar la seguridad.

Gracias a estos dos puntos principales de los objetivos del plan director, se puede deducir claramente que el plan está enfocado a introducir el modelo de mejora continua y que aportará beneficios en la gestión de la seguridad de la información, permitiendo aproximarnos a la excelencia en este tema. Por tanto, Gurb S.L busca acercar la implementación de un Sistema de Gestión de la Información (SGSI) con base en la norma ISO/IEC 27001 para cubrir los soportes de servicios especializados.

3.1.2. Objetivos finales del plan de director

Se ha de resaltar que la empresa no dispone de personal especializado dentro de su plantilla y por tanto, tener en cuenta esta premisa en el desarrollo de la solución, así como el reducido número de trabajadores y equipos informáticos de los que dispone la empresa.

Una vez analizadas y revisadas las necesidades de la empresa, junto con la dirección y responsables de cada área se definen las líneas básicas del camino adecuado a seguir para mejorar la seguridad de la información y sus activos valiosos dentro de la empresa.

Por tanto, se han de tomar medidas de seguridad necesarias para minimizar los daños que puedan presentar la materialización de las diferentes amenazas a las que se encuentran expuestos estos activos valiosos y que podría repercutir en los niveles de confidencialidad, integridad y disponibilidad, afectando en un beneficio final para la organización. Entre las tareas destacables:

- Identificación de recursos críticos dentro de la operación Soporte y Servicios Especializados de Gurb S.L.
- La identificación de las amenazas y vulnerabilidades a las que están supeditados los procesos activos y críticos durante su operación.
- La estimación de la probabilidad de materialización de cada una de las amenazas identificadas al explotar vulnerabilidades existentes.
- La estimación del impacto de comprometer las operaciones del negocio y amenazar la seguridad de la información con la materialización de amenazas.
- La identificación de consecuencias por afectación interna o externa de las operaciones del negocio y la seguridad de la información de la compañía.

- La identificación de los controles que actualmente se tienen implementados y que permiten la mitigación en mayor o menor medida de las fuentes de riesgo.
- La estimación de los niveles de efectividad de los controles existentes.
- La estimación de los niveles de riesgo residual a los cuales aún se encuentra expuesta la operación.
- La identificación de hallazgos y recomendaciones de mejora.

Para poder dar un resultado eficiente, proactivo y preventivo es necesario implantar un sistema de gestión de la información (SGSI), el cual pueda ayudar a Gurb S.L. a emplazar sus esfuerzos en fines como:

- Disponer de las bases suficientes para establecer y mantener una política y estándares de seguridad de información que cubra toda la organización.
- Tener una metodología estándar de evaluación a procesos y actividades relacionados con la seguridad de la información.
- Establecer un programa de evaluación periódica de vulnerabilidades sobre los activos de la organización.
- Administrar conscientemente el programa de identificación y clasificación de activos de información.
- Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
- Identificar y monitorear vulnerabilidades reconocidas sobre funciones de los proveedores.
- Mejorar los procesos de control de incidentes de seguridad o violaciones de seguridad.
- Coordinar todas las funciones relacionadas a seguridad, como seguridad física, seguridad personal y seguridad de información,…
- Desarrollar y administrar con fundamento el presupuesto de seguridad de información.
- Generar y ejecutar programas periódicos de concienciación para comunicar aspectos básicos de seguridad de información y alineamientos.

Debido a la poca especialización en temas de seguridad en la compañía se dispensa facilitar los instrumentos suficientes para refinar compromisos a nivel de seguridad de la información a través de los diferentes roles y perfiles, como:

- **Operadores y usuarios:** Garantizar que el uso de los activos de la compañía y su información por parte de operadores y usuarios, es congruente con las órdenes administrativas, políticas, guías y reglas de la organización para mitigar riesgos y proteger adecuadamente los recursos. Adicionalmente, conocer los programas de entrenamiento y concienciación requeridos para estos perfiles.

- **Propietarios de la información:** Lograr que los propietarios sean responsables por definir, aprobar y autorizar los alineamientos de seguridad y cambios en sus sistemas, razón por la cual deben entender el rol que juegan en la administración de riesgos.

- **Administradores y Coordinadores de áreas:** Como responsables de la infraestructura y servicios de la compañía o custodios comprometidos con la apropiada implementación y monitoreo de los requerimientos de seguridad demandados por la alta dirección y los dueños de la información.

- **Analista de monitoreo e incidentes:** Contar con un responsable de consolidar log's y pistas de auditoría y definir procedimientos para monitorear los comportamientos

anormales o posibles incidentes y escalar en tiempos adecuados para tomar las medidas de contención necesarias o realizar investigaciones, junto con UPC, bajo un procedimiento de recolección de evidencia confiable sin afectar los derechos fundamentales de las personas.

- **Oficial de seguridad de la información:** Responsable en la introducción de una apropiada estructura y metodología para ayudar a identificar, evaluar y minimizar los riesgos de los sistemas que soportan la misión de la organización y cumpliendo funciones como:
    - Liderar y coordinar la implementación de políticas de seguridad de la información.
    - Evaluar y coordinar la implementación de controles.
    - Monitorear cambios significativos en los riesgos que afecten los activos de información.
    - Identificar necesidades y recursos necesarios para el mantenimiento de los niveles de seguridad adecuados.
    - Identificar las necesidades de formación, capacitación o concienciación.
    - Actuar como asesor de la seguridad de la información.
    - Responder al comité de seguridad de la información sobre el estado de la investigación y monitoreo de incidentes de seguridad.
    - Presentar informes periódicos del estado de la seguridad.

- **Comité de seguridad de la información:** Para que pueda estar conformado por los líderes o responsables de las diferentes áreas de la organización y determine, apruebe y de seguimiento a políticas, planes y proyectos que requiera la entidad en materia de seguridad de la información y respondiendo por actividades.

- **Alta dirección:** Lograr que la alta dirección o director general, pueda mantener y apoyar formalmente los proyectos y directrices a nivel de seguridad de la información a fin de garantizar la participación de todas las partes interesadas y sancionar los incumplimientos.

Se utilizará el modelo de buenas prácticas para mejorar la seguridad de la información la normativa ISO 27002, estándar de referencia muy extendido y valorado en el análisis y gestión de la seguridad de la información para organizaciones que han querido implantar un sistema de gestión de la seguridad de la información. La principal ventaja de esta normativa respecto otros modelos es que se basa en la información y no únicamente en un punto de vista informático. Dispone de un conjunto de controles que son aplicables prácticamente para cualquier organización.

3.1.3. Mecanismos de ejecución

Los mecanismos con los que contará el plan director para hacer viable su ejecución son:

Sensibilizar a la dirección de cada área especializada y en concreto a la alta dirección para promover una metodología estándar con fundamentos lógicos soportados en la normativa reconocida internacionalmente para el desarrollo de un programa de riesgos efectivo y trasversal a toda la organización con ventajas como:

- Unificación de criterios de evaluación y valoración.
- Lenguaje común entre las áreas .

- Cuadros de mandos unificados con métricas e indicadores claros.
- Toma de decisiones rápida y objetiva.

Por otra parte, fomentar el uso de técnicas de recolección de información para la consolidación de la información sobre las áreas operacionales de la empresa:

Cuestionarios: El personal responsable por la valoración de riesgos desarrolla cuestionarios para recoger información sobre los controles administrativos y operacionales planeados o utilizados por las diferentes dependencias de la organización.

Entrevistas en sitio: Las entrevistas en sitio con personal idóneo (con experiencia y conocimiento de sus funciones y contratiempos manejados) de los procesos con el objeto de obtener información útil para la valoración de riesgos. Las visitas en sitio también son contempladas para valorar áreas y ambientes de trabajo.

Revisión de documentos: La documentación de ejercicios anteriores, procesos, normas, directrices, formatos, plantillas de control, bitácoras, informes de auditorías previas, proveen excelente información acerca de los controles usados y planeados por la organización.

Herramientas de escaneo: Mediante el uso de herramientas, técnicas y métodos proactivos, se recolecta información complementaria y validación de perfiles y configuraciones individuales sobre recursos tecnológicos.

Finalmente, auxiliar a la empresa en el desarrollo y manejo de una técnica de selección de controles y medidas de seguridad efectivas con el objeto de instaurar un mapa de ruta que proporcione mejoras a los niveles de seguridad involucrados en los procesos de almacenamiento y transporte seguro de la información mediante un Sistema de Gestión de la Seguridad de la Información formalmente establecido.

3.2 Análisis diferencial

En este punto el objetivo es definir un estado inicial de cómo se encuentra la empresa y hacia dónde deseamos llegar para cumplir los objetivos marcados en cuanto a seguridad de la información.

3.2.1 Política de seguridad

Dado que la empresa no dispone de ninguna política de seguridad ni directiva parecida, actualizada y reconocida por los trabajadores, el objetivo principal será la creación de una política adecuada para la empresa y ,donde marcará las pautas a seguir por los trabajadores para preservar la seguridad de la información. Junto con la política, se definirán las bases del que será el Sistema de Gestión de Seguridad de la Información.

3.2.2 Aspectos organizativos de la seguridad de la información

En cuanto a aspectos organizativos de la seguridad de la información, y siguiendo la ISO/IEC 27002:2005, este apartado queda dividido en dos objetivos a organizar, por un lado la organización interna y la de terceros.

En cuanto a organización interna se deberían establecer estructuras de gestión adecuadas para iniciar y controlar la implementación de la seguridad de la información dentro de la empresa. Para llevar a cabo este punto, se han de asignar roles y perfiles con el fin de definir responsables en la gestión de la información. Esta tarea recaería sobre el *comité de seguridad* de la información. Otra tarea del comité de seguridad de la información sería la de realizar un seguimiento continuo para supervisar la elaboración del plan y seguir un plan de mejora.

En cuanto a la seguridad en los accesos de terceros, se ha de mantener la seguridad de que los recursos de tratamiento de la información y de los activos de la organización sean accesibles por terceros, controlando su acceso a los dispositivos. También se ha de implantar medidas de evaluación de riesgo para determinar las implicaciones sobre la seguridad y las medidas de control que requiere el negocio cuando un tercero accede a los recursos de información.

Actualmente la compañía dispone de soporte por parte de la UPC y sus grupos de seguridad en caso de incidente, a los cuales puede acudir en busca de ayuda. Estos grupos son gestionados por UPC independientemente y tienen su propia organización dependiendo del ámbito de actuación y donde estos, están bien definidos.

3.2.3 Clasificación y control de activos

La compañía Gurb S.L. no dispone actualmente de ninguna clasificación de activos o controles sobre el uso indebido de estos. Por tanto, es vital para el buen funcionamiento del sistema implantar este tipo de controles y clasificación de activos.

Junto con la política de seguridad, se identificarán, documentarán e implementarán regulaciones enfocados al uso adecuado de los activos, quedando definidas también las directrices de clasificación de activos.

Uno de los mecanismos de ejecución detallados en el plan director era la de obtener información de los activos críticos mediante entrevistas y consultas directamente con los trabajadores de la compañía. Ya que el número de estos es reducido, se pueden tener entrevistas individuales con ellos para determinar los activos críticos para cada uno de ellos, con el fin de obtener un mapa de los activos y recursos esenciales y valiosos para el correcto funcionamiento de la información y funciones de la compañía. Una vez asignados los activos se han de asignar responsabilidades de mantenimiento de los controles apropiados.

De la información obtenida, se debería obtener una clasificación en función del valor, requisitos legales, sensibilidad y criticidad para la compañía. El nivel de protección de la información puede ser determinado analizando la confidencialidad, integridad y disponibilidad, entre otros requisitos, para la información considerada.

3.2.4 Seguridad ligada a los recursos humanos

Actualmente la compañía, al contratar a personal nuevo firma un contrato de confidencialidad acerca de la información y recursos que pueda gestionar durante su estancia en el puesto. También se le asigna un usuario y privilegios adecuados al puesto al que ha sido designado, con el fin de proteger la información que está fuera de su competencia o que pueda obtener información que sensible para cometer un fraude o hurto. En cuanto a la contratación, no existe un estándar que seguir, sino que es el responsable de cada área de realizar las entrevistas a los empleados destinados a su zona de responsabilidad. Se ha de tener en cuenta que UPC ofrece soporte en cuanto a la contratación, por tanto, la responsabilidad en este punto es compartida.

Entre las funciones a seguir por la compañía en materia de seguridad de los recursos estas deberían proteger los activos de un acceso no autorizado, tal como se viene haciendo. Asegurar que la responsabilidad sea asignada al individuo para tomar acciones o reportar eventos de seguridad o eventos potenciales u otro riesgo para la compañía.

Actualmente no se recibe ningún tipo de formación o entrenamiento en términos de conocimiento y actuaciones regulares en políticas y procedimientos organizacionales relevantes en su función. Esta formación debería empezar con una inducción formal del proceso designado para introducir la política de seguridad de la compañía y las expectativas.

Otro punto a definir son los procesos disciplinarios para empleados que cometan aperturas en la seguridad, asegurándose que se reciba un correcto y justo tratamiento de los empleados por los hechos ocurridos y que han provocado dicha apertura.

Al finalizar el contrato, la compañía sí que revoca los permisos y activos que se le prestaron al empleado en el momento del contrato, con lo que los permisos y privilegios quedan anulados en el momento de la desvinculación contractual.

3.2.5 Seguridad física y del entorno

Actualmente los activos de la compañía se dividen en dos entornos. El primero es el material de oficina y diferente hardware para el funcionamiento de los servicios y el segundo, son los servidores para el funcionamiento de los servicios de soporte y buen funcionamiento de las diferentes áreas. Únicamente el segundo de los activos se encuentra en una zona restringida a los empleados y terceros. No obstante, no se tiene constancia de ningún método de control de acceso donde éstos queden registrados. En cuanto al resto de activos de la empresa físicos, no se tiene ningún control de acceso ni registro de las personas que acceden al recinto. Tampoco existe seguridad como cámaras o personal de seguridad.

En cuanto a la mejora de la seguridad del perímetro físicamente es difícil implementarla o mejorarla ya que, juntamente con la compañía, en el edificio o misma planta del mismo, conviven diferentes empresas.

Sin embargo, como objetivo en este punto estaría la de mejorar los métodos de acceso controlados y adecuados que aseguren el acceso al personal autorizado. Con el objetivo de reducir el riesgo de amenazas del entorno. También se debería proteger los equipos contra fallos de energía, seguridad del cableado que actualmente no se contemplan.

En cuanto a la seguridad de los equipos fuera de la compañía, no se contempla esta posibilidad ya que no es posible extraer material fuera de ella y los ordenadores que se desechan se realiza a través de la Universidad Politécnica de Cataluña que tiene un servicio para ello.

3.2.6 Gestión de comunicaciones y operaciones

Actualmente, cada responsable de cada área es responsable de su área únicamente y por encima de estos el director general, pero no existe ningún documento dónde se detalle la función de cada sección ni determine responsabilidades en algún aspecto o actuación en caso de incidente de seguridad. Por tanto, se debería establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de la información, como por ejemplo, el desarrollo de instrucciones apropiadas de operación y de procedimiento de respuesta ante incidentes.

Por otro lado, con el objetivo de minimizar el riesgo de fallos de los sistemas, es necesario una planificación para asegurar la disponibilidad de capacidad y de recursos para que los sistemas funcionen, además de documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos, ya que actualmente no se realiza.

Todos los usuarios disponen de su software antivirus en sus zonas de trabajo actualizado e instalado por los responsables TIC de la compañía, sin embargo, no existe ningún tipo de documentación que forme o eduque a los trabajadores en materias de protección contra software malicioso, política respecto al uso de software no autorizado o referente al riesgo de obtener software de lugares no reconocidos o peligrosos. Los empleados pueden acceder a estos lugares maliciosos, sin embargo el control de la red no pertenece a la compañía sino a la Universidad Politécnica que es la que la gestiona.

Uno de los puntos más sensibles a tener en cuenta y que actualmente no se realiza con un control o planificación adecuado y periódico y donde no existe documentación formal, actualizada ni con unas pautas y procedimientos revisados al respecto, son las copias de seguridad de toda la información esencial del negocio y que esta pueda recuperarse tras un desastre o fallo de los medios. También debería estar documentado el procedimiento de copia

de respaldo así como su recuperación y también el de uso adecuado de los medios de información.

La compañía, hoy por hoy, no monitoriza ningún tipo de tráfico que salga de la red que tiene asignada, ni tiene ningún control de los accesos que realizan sus empleados en la red. La UPC es la que gestiona la red y las comunicaciones.

3.2.7 Control de accesos

Tal como se comentó anteriormente, los accesos son controlados mediante los privilegios de accesos a la información, donde se controla que cada empleado únicamente pueda acceder a los recursos que le están destinados para su puesto de trabajo, sin revisar, en ningún periodo de tiempo, si cada usuario tiene los privilegios que le tocan para su puesto. Sin embargo, no está documentado y accesible para los empleados a modo de que sepan la política de la compañía. Tampoco está documentado y, por donde tampoco se aplica, una política de contraseñas robusta para acceder a los servicios de información.

En cuanto a la responsabilidad de los usuarios y compromiso de estos ante el buen mantenimiento y eficacia de las medidas de control y donde no existe ningún procedimiento ni documentación formal, actualizado y revisado periódicamente al respecto, por tanto es otro punto a implementar. Este procedimiento debería documentar pautas de los empleados como mantener el escritorio limpio, no permitir el acceso no autorizado a su zona de trabajo, una política de contraseñas robusta, no acceder a redes o sitios maliciosos que puedan comprometer los activos o información sensible.

3.2.8 Adquisición, desarrollo y mantenimiento de sistemas

Actualmente se cuenta con el buen hacer de los desarrolladores y especialistas en materia TIC en lo que a seguridad de las aplicaciones del sistema se refiere. Por este motivo es necesario diseñar medidas de control, tanto a la hora del diseño de las aplicaciones donde estas han de controlar factores de riesgo como la entrada y salida de datos, como controles criptográficos para proteger la información sometida a riesgo.

Otro punto a mejorar e implantar en el sistema de la compañía es la de asegurar la seguridad de los archivos del sistema, donde deberían existir procedimientos para controlar la instalación de software en sistemas operacionales o tener un procedimiento bien detallado y control sobre los datos de prueba, donde estos deben ser seleccionados, protegidos y controlados cuidadosamente. También hay que tener especial atención y cuidado con los accesos al código fuente de los programas para evitar los cambios no intencionales o de empleados que no tienen privilegios para ello. Por todo ello, además, es vital mantener e implantar, ya que no se realiza actualmente, una revisión de todo cambio al sistema con el fin de comprobar que no debilite la seguridad del sistema en general, así como un procedimiento de control de cambios.

3.2.9 Gestión de incidentes en la seguridad de información

La compañía no dispone de ningún sistema de reporte de eventos y debilidades de seguridad en estos momentos. Así pues, debería implementar los procedimientos adecuados para que todos los empleados y terceros involucrados por la compañía puedan reportar diferentes tipos

de eventos y debilidades que puedan tener un impacto en la seguridad de los activos. No obstante, en caso de infección o cualquier otro incidente de seguridad, se puede acudir a los servicios específicos de UPC destinados a estas tareas para obtener soporte especializado. Por este motivo los canales de gestión son los propios de UPC así que está debidamente implementado, la debilidad está en la comunicación interna de la propia compañía que no dispone de herramientas de reporte de eventos críticos.

De igual forma, para mantener y asegurar una efectiva y sólida respuesta de los incidentes debe establecerse un sistema de responsabilidades y procedimientos. También se ha de cuantificar mediante algún mecanismo eficiente, el costo de los incidentes en la seguridad de la información. Por otra parte, es importante monitorizar y controlar los eventos que vayan surgiendo en la compañía con el fin de tener evidencias sólidas y legales delante de cualquier procedimiento o acción legal que pueda surgir.

3.2.10 Gestión de continuidad de negocio

Es de vital importancia que la compañía implemente, ya que no dispone de ello, de un procedimiento de gestión de continuidad del negocio para reducir a niveles asumibles la interrupción causada por desastres y fallas de seguridad mediante controles preventivos y de recuperación.

Para esto, la compañía ha de identificar los procesos críticos de negocio (analizados en puntos anteriores) e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, …

La compañía debe analizar las consecuencias de los desastres, fallos de seguridad o pérdidas de servicio que puedan afectar a sus activos y una vez hecho esto, asegurarlos mediante un plan de contingencia que minimice los riesgos hasta niveles aceptables o asumibles para la compañía. Es obligación de la compañía realizar un análisis de la probabilidad de impacto y coste de recuperación del activo y coste del activo para analizar qué debe salvaguardar en primeras instancias o dónde destinar los recursos para ello. Una vez diseñados los planes de contingencias, deberían estar sometidos a controles y revisiones regularmente para asegurarse de su actualización y eficacia.

3.2.11 Cumplimiento

Debido a que la compañía pertenece al ámbito de la Universidad Politécnica de Cataluña, dispone del asesoramiento sobre requisitos legales específicos por parte de esta y que pone a su disposición en caso de necesitarse. Otro punto a tener en cuenta al redactar estos documentos y procedimientos es la protección de datos y la privacidad, donde debe ser asegurada en todo momento o, el mal uso de los recursos de tratamiento de la información personal con propósitos no autorizados, por ejemplo.

Junto con todos los procedimientos y documentos, los responsables deberían asegurarse que se cumplen todos estas regulaciones de seguridad dentro de su área de responsabilidad cumpliendo con las políticas y estándares de seguridad.

3.3 Tabla resumen del diseño diferencial

ANÁLISIS DIFERENCIAL	
5. POLÍTICA DE SEGURIDAD	
5.1 Política de seguridad de la información	
5.1.1 Documento de la política de seguridad de la información	L0 - No implementado / Inexistente
5.1.2 Revisión de la política de seguridad de la información	L0 - No implementado / Inexistente
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna	
6.1.1 Compromiso de la dirección con la seguridad de la información	L1 - Se ha hecho algo, manifestamente insuficiente
6.1.2 Coordinación de la seguridad de la información	L2 - Reproducible, pero intuitivo
6.1.3 Asignación de responsabilidades relativas a la seg. De la información	L1 - Se ha hecho algo, manifestamente insuficiente
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	L1 - Se ha hecho algo, manifestamente insuficiente
6.1.5 Acuerdo de confidencialidad	L3 - Proceso definido
6.1.6 Contacto con las autoridades	L4 - Gestionado y medible
6.1.7 Contacto con grupos de especial interés	L3 - Proceso definido
6.1.8 Revisión independiente de la seguridad de la información	L0 - No implementado / Inexistente
6.2 Terceros	
6.2.1 Identificación de los riesgos derivados del acceso de terceros	L1 - Se ha hecho algo, manifestamente insuficiente
6.2.2 Tratamiento de la seguridad en la relación con los clientes	L1 - Se ha hecho algo, manifestamente insuficiente
6.2.3 Tratamiento de la seguridad en contratos con terceros	L1 - Se ha hecho algo, manifestamente insuficiente
7. GESTIÓN DE ACTIVOS	
7.1 Responsabilidad sobre los activos	
7.1.1 Inventario de activos	L1 - Se ha hecho algo, manifestamente insuficiente
7.1.2 Propiedad de los activos	L2 - Reproducible, pero intuitivo
7.1.3 Uso aceptable de los activos	L2 - Reproducible, pero intuitivo
7.2 Clasificación de la información	
7.2.1 Directrices de clasificación	L1 - Se ha hecho algo, manifestamente insuficiente
7.2.2 Etiquetado y manipulado de la información	L1 - Se ha hecho algo, manifestamente insuficiente
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
8.1 Antes del empleo	
8.1.1 Funciones y responsabilidades	L2 - Reproducible, pero intuitivo

8.1.2 Investigación de antecedentes	L3 - Proceso definido
8.1.3 Términos y condiciones de contratación	L3 - Proceso definido
8.2 Durante el empleo	
8.2.1 Responsabilidades de la dirección	L2 - Reproducible, pero intuitivo
8.2.2 Concienciación, formación y capacitación en seguridad de la información	L2 - Reproducible, pero intuitivo
8.2.3 Proceso disciplinario	L2 - Reproducible, pero intuitivo
8.3 Cese del empleo o cambio de puesto de trabajo	
8.3.1 Responsabilidad del cese o cambio	L3 - Proceso definido
8.3.2 Devolución de activos	L4 - Gestionado y medible
8.3.3 Retirada de los derechos de acceso	L3 - Proceso definido
9. SEGURIDAD FÍSICA Y DEL ENTORNO	
9.1 Áreas seguras	
9.1.1 Perímetro de seguridad física	L3 - Proceso definido
9.1.2 Controles físicos de entrada	L1 - Se ha hecho algo, manifestamente insuficiente
9.1.3 Seguridad de oficinas, despachos e instalaciones	L3 - Proceso definido
9.1.4 Protección contra las amenazas externas y de origen ambiental	L3 - Proceso definido
9.1.5 Trabajo en áreas seguras	N.A. - No aplica
9.1.6 Áreas de acceso público y de carga y descarga	N.A. - No aplica
9.2 Seguridad de los equipos	
9.2.1 Emplazamiento y protección de equipos	L2 - Reproducible, pero intuitivo
9.2.2 Instalaciones de suministro	L2 - Reproducible, pero intuitivo
9.2.3 Seguridad del cableado	L3 - Proceso definido
9.2.4 Mantenimiento de los equipos	L1 - Se ha hecho algo, manifestamente insuficiente
9.2.5 Seguridad de los equipos fuera de las instalaciones	L1 - Se ha hecho algo, manifestamente insuficiente
9.2.6 Reutilización o retirada segura de equipos	L2 - Reproducible, pero intuitivo
9.2.7 Retirada de materiales propiedad de la empresa	L1 - Se ha hecho algo, manifestamente insuficiente
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
10.1 Responsabilidades y procedimientos de operación	
10.1.1 Documentación de los procedimientos de operación	L1 - Se ha hecho algo, manifestamente insuficiente
10.1.2 Gestión de cambios	L1 - Se ha hecho algo, manifestamente insuficiente
10.1.3 Segregación de tareas	L2 - Reproducible, pero intuitivo
10.1.4 Separación de los recursos de desarrollo, prueba y operación	L1 - Se ha hecho algo, manifestamente insuficiente
10.2 Gestión de la provisión de servicios por terceros	
10.2.1 Provisión de servicios	L3 - Proceso definido
10.2.2 Supervisión y revisión de los servicios prestados por terceros	L2 - Reproducible, pero intuitivo
10.2.3 Gestión del cambio en los servicios prestados por terceros	L2 - Reproducible, pero intuitivo

10.3 Planificación y aceptación del sistema	
10.3.1 Gestión de capacidades	L2 - Reproducible, pero intuitivo
10.3.2 Aceptación del sistema	L2 - Reproducible, pero intuitivo
10.4 Protección contra el código malicioso y descargable	
10.4.1 Controles contra el código malicioso	L3 - Proceso definido
10.4.2 Controles contra el código descargado en el cliente	N.A. - No aplica
10.5 Copias de seguridad	
10.5.1 Copias de seguridad de la información	L2 - Reproducible, pero intuitivo
10.6 Gestión de la seguridad de las redes	
10.6.1 Controles de red	L2 - Reproducible, pero intuitivo
10.6.2 Seguridad de los servicios de red	L2 - Reproducible, pero intuitivo
10.7 Manipulación de los soportes	
10.7.1 Gestión de soportes extraíbles	L1 - Se ha hecho algo, manifestamente insuficiente
10.7.2 Retirada de soportes	L2 - Reproducible, pero intuitivo
10.7.3 Procedimientos de manipulación de la información	L2 - Reproducible, pero intuitivo
10.7.4 Seguridad de la documentación del sistema	L2 - Reproducible, pero intuitivo
10.8 Intercambio de información	
10.8.1 Políticas y procedimientos de intercambio de información	L2 - Reproducible, pero intuitivo
10.8.2 Acuerdos de intercambio	L2 - Reproducible, pero intuitivo
10.8.3 Soportes físicos en tránsito	N.A. - No aplica
10.8.4 Mensajería eletrónica	L3 - Proceso definido
10.8.5 Sistemas de información empresariales	L2 - Reproducible, pero intuitivo
10.9 Servicios de comercio electrónico	
10.9.1 Comercio electrónico	N.A. - No aplica
10.9.2 Transacciones en línea	N.A. - No aplica
10.9.3 Información públicamente disponible	N.A. - No aplica
10.10 Supervisión	
10.10.1 Registros de auditoría	L2 - Reproducible, pero intuitivo
10.10.2 Supervisión del uso del sistema	L2 - Reproducible, pero intuitivo
10.10.3 Protección de la información de los registros	L2 - Reproducible, pero intuitivo
10.10.4 Registros de administración y operación	L3 - Proceso definido
10.10.5 Registro de fallos	L2 - Reproducible, pero intuitivo
10.10.6 Sincronización del reloj	L4 - Gestionado y medible
11. CONTROL DE ACCESO	
11.1 Requisitos de negocio para el control de acceso	
11.1.1 Política de control de acceso	L2 - Reproducible, pero intuitivo
11.2 Gestión de acceso de usuario	
11.2.1 Registro de usuario	L2 - Reproducible, pero intuitivo
11.2.2 Gestión de privilegios	L2 - Reproducible, pero intuitivo
11.2.3 Gestión de contraseñas de usuario	L2 - Reproducible, pero intuitivo
11.2.4 Revisión de los derechos de acceso de usuario	L1 - Se ha hecho algo, manifestamente

	insuficiente
11.3 Responsabilidades de usuario	
11.3.1 Uso de contraseñas	L2 - Reproducible, pero intuitivo
11.3.2 Equipo de usuario desatendido	L1 - Se ha hecho algo, manifestamente insuficiente
11.3.3 Política de puestos de trabajo despejados y pantalla limpia	L1 - Se ha hecho algo, manifestamente insuficiente
11.4 Control de acceso a la red	
11.4.1 Política de uso de los servicios de red	L2 - Reproducible, pero intuitivo
11.4.2 Autenticación de usuario para conexiones externas	L1 - Se ha hecho algo, manifestamente insuficiente
11.4.3 Identificación de los equipos en red	L2 - Reproducible, pero intuitivo
11.4.4 Protección de los puertos de diagnóstico y configuración remotos	L3 - Proceso definido
11.4.5 Segregación de las redes	L2 - Reproducible, pero intuitivo
11.4.6 Control de la conexión a la red	L2 - Reproducible, pero intuitivo
11.4.7 Control de encaminamiento a la red	L3 - Proceso definido
11.5 Control de acceso al sistema operativo	
11.5.1 Procedimientos seguros de inicio de sesión	L2 - Reproducible, pero intuitivo
11.5.2 Identificación y autenticación de usuario	L4 - Gestionado y medible
11.5.3 Sistema de gestión de contraseñas	L1 - Se ha hecho algo, manifestamente insuficiente
11.5.4 Uso de los recursos del sistema	L1 - Se ha hecho algo, manifestamente insuficiente
11.5.5 Desconexión automática de la sesión	L2 - Reproducible, pero intuitivo
11.5.6 Limitación del tiempo de conexión	L1 - Se ha hecho algo, manifestamente insuficiente
11.6 Control de acceso a las aplicaciones y a la información	
11.6.1 Restricción del acceso a la información	L2 - Reproducible, pero intuitivo
11.6.2 Aislamiento de sistemas sensibles	L3 - Proceso definido
11.7 Ordenadores portátiles y teletrabajo	
11.7.1 Ordenadores portátiles y comunicaciones móviles	L1 - Se ha hecho algo, manifestamente insuficiente
11.7.2 Teletrabajo	L2 - Reproducible, pero intuitivo
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
12.1 Requisitos de seguridad de los sistemas de información	
12.1.1 Análisis y especificación de los requisitos de seguridad	L2 - Reproducible, pero intuitivo
12.2 Tratamiento correcto de las aplicaciones	
12.2.1 Validación de los datos de entrada	L2 - Reproducible, pero intuitivo
12.2.2 Control del procesamiento interno	L2 - Reproducible, pero intuitivo
12.2.3 Integridad de los mensajes	L2 - Reproducible, pero intuitivo
12.2.4 Validación de los datos de salida	L4 - Gestionado y medible
12.3 Controles criptográficos	
12.3.1 Política de uso de los controles criptográficos	L1 - Se ha hecho algo, manifestamente insuficiente
12.3.2 Gestión de claves	L1 - Se ha hecho algo, manifestamente insuficiente

12.4 Seguridad de los archivos de sistema	
12.4.1 Control del software en explotación	L2 - Reproducible, pero intuitivo
12.4.2 Protección de los datos de prueba del sistema	L1 - Se ha hecho algo, manifestamente insuficiente
12.4.3 Control de acceso al código fuente de los programas	L2 - Reproducible, pero intuitivo
12.5 Seguridad en los procesos de desarrollo y soporte	
12.5.1 Procedimientos de control de cambios	L1 - Se ha hecho algo, manifestamente insuficiente
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el SO	L2 - Reproducible, pero intuitivo
12.5.3 Restricciones a los cambios en los paquetes de software	L2 - Reproducible, pero intuitivo
12.5.4 Fugas de información	L2 - Reproducible, pero intuitivo
12.5.5 Externalización del desarrollo de software	N.A. - No aplica
12.6 Gestión de la vulnerabilidad técnica	
12.6.1 Control de las vulnerabilides técnicas	L2 - Reproducible, pero intuitivo
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
13.1 Notificación de eventos y puntos débiles de seguridad de la información	
13.1.1 Notificación de los eventos de seguridad de la información	L4 - Gestionado y medible
13.1.2 Notificación de puntos débiles de seguridad	L3 - Proceso definido
13.2 Gestión de incidentes y mejoras de seguridad de la información	
13.2.1 Responsabilidades y procedimientos	L2 - Reproducible, pero intuitivo
13.2.2 Aprendizaje de los incidentes de seguridad de la información	L2 - Reproducible, pero intuitivo
13.2.3 Recopilación de evidencias	L3 - Proceso definido
14. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocio	
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de negocio	L2 - Reproducible, pero intuitivo
14.1.2 Continuidad del negocio y evaluación de riesgos	L2 - Reproducible, pero intuitivo
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	L2 - Reproducible, pero intuitivo
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	L2 - Reproducible, pero intuitivo
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad	L1 - Se ha hecho algo, manifestamente insuficiente
15. CUMPLIMIENTO	
15.1 Cumplimiento de los requisitos legales	
15.1.1 Identificación de la legislación aplicable	L4 - Gestionado y medible
15.1.2 Derechos de propiedad intelectual (DPI)	L3 - Proceso definido
15.1.3 Protección de los documentos de la organización	L3 - Proceso definido
15.1.4 Protección de datos y privacidad de la información de carácter personal	L3 - Proceso definido
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	L1 - Se ha hecho algo, manifestamente insuficiente
15.1.6 Regulación de los controles criptográficos	L1 - Se ha hecho algo, manifestamente insuficiente

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	
15.2.1 Cumplimiento de las políticas y normas de seguridad	L1 - Se ha hecho algo, manifestamente insuficiente
15.2.2 Comprobación del cumplimiento técnico	L2 - Reproducible, pero intuitivo
15.3 Consideraciones sobre las auditorías de los sistemas de la información	
15.3.1 Controles de auditoría de los sistemas de información	L1 - Se ha hecho algo, manifestamente insuficiente
15.3.2 Protección de las herramientas de auditoría de los sistemas de la información	L1 - Se ha hecho algo, manifestamente insuficiente

LEYENDA
L0 - No implementado / Inexistente
L1 - Se ha hecho algo, manifestamente insuficiente
L2 - Reproducible, pero intuitivo
L3 - Proceso definido
L4 - Gestionado y medible
L5 – Optimizado

3.4 Análisis de riesgos

3.4.1 Introducción

En esta fase del documento el objetivo es evaluar todos los activos que se encuentran relacionados con la creación de Plan Director, considerando las dependencias existentes entre ellos y realizando una valoración sobre estos. De esta forma se definirá claramente un punto de salida de todos los activos, sean estos tangibles o no, dentro de la compañía y pudiendo analizar a qué amenazas podrían estar expuestos estos activos.

Una vez disponemos de un listado de las amenazas reales que pueden afectar a nuestros activos y extraídos de la **Guía Magerit**, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la compañía en caso de que se materialicen estas amenazas.

El impacto, junto con los resultados anteriormente explicados dará una serie de datos que nos permitirán priorizar el plan de acción y, al mismo tiempo, evaluar como se ve modificado este valor una vez se apliquen las contramedidas o bien, el riesgo que estamos dispuestos a asumir (riesgo residual) por parte de la compañía.

Como resultado de esta fase, podremos obtener:

- Un análisis detallado de los activos relevantes de seguridad de la empresa. [Punto 3.4.5]
- Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto. [Punto 3.4.6]
- El resultado final, será el impacto potencial que tendrá la materialización de las diferentes amenazas a las que están expuestos nuestros activos.

3.4.2 Inventario de activos

El primer punto para el análisis es estudiar los activos vinculados a la información. Es habitual agrupar los activos por grupos para ello. En nuestro caso, podemos agrupar los activos por grupos basándonos en la metodología MAGERIT. Por tanto, los grupos en los que nos centraremos son:

- **[L]** Instalaciones
- **[HW]** Hardware
- **[SW]** Aplicación
- **[D]** Datos
- **[COM]** Red
- **[S]** Servicios
- **[AUX]** Equipamiento auxiliar
- **[P]** Personal

Los resultados de este estudio se recogerán en una tabla que facilitará posteriores estudios. La tabla se dividirá en dos columnas donde se recogerá la información aquí dispuesta y

clasificada. Para la primera columna se encontrará el ámbito del activo con el objetivo de realizar las agrupaciones y, en la segunda columna se encontrará el activo concreto.

3.4.3 Valoración de los activos

Con la identificación de activos en relación a la seguridad de la información, hará falta valorar cada activo dentro de nuestra organización.

El objetivo final del proceso es tomar un conjunto de medidas que garanticen nuestros activos. El coste de estas medidas no ha de superar el coste del activo que se tiene que proteger, de otra forma no sería un activo rentable protegerlo, ya que sería más fácil substituirlo en caso contrario, por tanto, un punto por donde empezar es la asignación de un valor a los activos.

Para poder valorar un activo se han de tener en cuenta diferentes aspectos, como por ejemplo el coste de reposición, el valor del tiempo sin servicio, posibles penalizaciones, etc. Por tanto, para facilitar esta tarea, se propone la **metodología MAGERIT**, la cual realiza una valoración cualitativa en relación al valor que tiene el activo respecto a nuestra organización, que se completa con una valoración cuantitativa respecto a estas categorías cualitativas.

La tabla sobre la que se procederá a realizar la valoración de activos es la siguiente (Extraída de **Magerit**)

Valoración	Abreviatura	Valor
Muy Alta	MA	Valor > 200.000 € → 300.000€
Alto	A	100.000 € < valor > 200.000 € →150.000€
Medio	M	50.000 € < valor > 100.000 € →75.000€
Bajo	B	10.000 € < valor > 50.000 € →30.000€
Muy bajo	MB	Valor < 10.000 € → 10.000€

Esta tabla nos permitirá realizar la asignación de un valor a los activos en función de las categorías de la columna valoración y a su vez, tendremos un valor cuantitativo que viene representado por la columna Valor. Los valores de los activos no corresponderán a valores fijos, sino a un rango que estimará los límites del valor correspondiente.

Por otra parte, se tendrá que tener en cuenta que los activos están jerarquizados, es decir, se deberán identificar y valorar las dependencias entre activos. Se dice que un activo superior depende de otro activo inferior cuando las necesidades de seguridad del superior se muestran en las necesidades de seguridad del inferior, o dicho de otra manera, cuando la materialización de una amenaza en el activo inferior tiene consecuencias perjudiciales sobre el activo superior. Por tanto, será requisito analizar el árbol de dependencias o jerarquía entre activos. Este apartado referente a las dependencias, quedará reflejado en la tabla de activos en la columna dependencias.

3.4.4 Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración de los activos, se ha de indicar cuál es el aspecto de la seguridad más crítico. Esto será de gran ayuda en el momento de pensar en posibles medidas de prevención, ya que serán enfocadas en aquellos aspectos más críticos.

Una vez identificados los activos, se ha de realizar la valoración **ACIDT** de los mismos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso de negocio. Esta valoración nos permitirá, a posteriori, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto.

El valor que reciba el activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando el resto de activos subordinados a las necesidades de explotación y protección de la información. De esta manera, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede tener un valor diferente en cada uno de las diferentes dimensiones para la organización que deseamos analizar. Por esto, se ha de tener presente siempre que representa cada dimensión.

Las cinco dimensiones de las que se habla son:

- **[C] Confidencialidad**. Únicamente las personas autorizadas tienen acceso a la información sensible o privada.
- **[I] Integridad**. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización
- **[D] Disponibilidad**. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.
- **[A] Autenticidad**. Hay garantía de la identidad de los usuarios o procesos que gestionarán la información.
- **[T] No repudio**. Hay garantía de la autoría de una determinada acción y está asociada a quien ha producido esta acción.

Una vez detalladas las cinco dimensiones se ha de tener presente la escala en que se realizarán las valoraciones. En este caso se utilizará una escala de valoración de diez valores siguiendo los siguientes criterios.

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Daño irrelevante a la organización

3.4.5 Tabla resumen de valoración

Ámbito	Activo		Dependencias	Valor	Aspectos críticos				
					C	I	D	A	T
[L] Instalaciones	**[L.1]**	CPD	-	MA	8	9	10	8	8
	[L.2]	Sala oficinas	-	A	5	7	8		
[H] Hardware	**[H.1]**	Servidor de correo	[L.1], [H.4], [COM.1], [COM.3], [D.3], [SW.9], [S.1]	MB	7	7	8	8	8
	[H.2]	Servidor Web	[L.1], [H.4], [COM.1], [COM.3], [D.2], [SW.3], [SW.4], [SW.5], [S3]	B	9	9	9	8	8
	[H.3]	Servidor Bases de datos	[L.1], [H.4] [COM.1], [COM.3], [D.2], [SW.7], [D.5]	B	9	9	9	8	8
	[H.4]	Servidor Firewall primario	[L.1], [COM.1], [COM.3]	A	8	9	9	8	8
	[H.5]	Servidor logs	[L.1], [H.12], [COM.1], [COM.3], [SW.8], [D.1]	MB	8	8	7	8	8
	[H.6]	Terminales de usuario	[L.2], [H.12], [H.12], [H.7], [COM.1], [COM.2]	MB	5	7	7	8	7
	[H.7]	Switch	[L.1]	MB	8	9	9	8	8
	[H.8]	Servidor Aplicaciones	[L.1], [H.12], [COM.1], [COM.3], [SW.4], [SW.5], [D.2]	MB	8	9	7	7	7
	[H.9]	Servidor backup	[L.1], [H.12], [COM.1], [COM.3]	MB	8	9	9	8	8
	[H.10]	Impresora	[L.2]	MB			7		
	[H.11]	Impresora color	[L.2]	MB			7		
	[H.12]	Servidor Firewall DMZ	[L.1], [H.4],[COM.1], [COM.2]	M	8	9	9	8	8
[SW] Aplicación	**[SW.1]**	Aplicación OS	[H.6]	MB	5	7	7	8	7
	[SW.2]	Aplicaciones ofimática	[H.6]	MB	4	7	6	7	6
	[SW.3]	Aplicación estadística	[H.6]	B	5	7	6	8	7
	[SW.4]	Aplicación Docencia	[H.2]	M	9	9	9	8	8
	[SW.5]	Aplicación Libro de datos	[H.2]	M	9	9	9	8	8
	[SW.6]	Aplicación Antivirus	[SW.1]	MB	4	7	5	6	7
	[SW.7]	Aplicación BBDD Server	[H.3]	B	8	9	8	8	8
	[SW.8]	Aplicación de logs	[H.5]	MB	8	8	7	8	8
	[SW.9]	Aplicación de correo	[H.1]	B	7	7	8	8	8
[D] Datos	**[D.1]**	Datos logs	[SW.8]	B	8	8	6	8	8
	[D.2]	Datos aplicaciones	[SW.4], [SW.5]	MA	9	9	9	8	8
	[D.3]	Datos Servidor correo	[SW.9]	M	7	7	6	8	7
	[D.4]	Datos estadísticos	[SW.3]	A	5	7	6	7	6
	[D.5]	Datos Backup	[H.9]	A	8	9	8	6	7
[COM] Red	**[COM.1]**	Router primario	[L.1]	B	7	9	9	6	7
	[COM.2]	Línea intranet (DMZ)	[L.1]	M	6	8	6		
	[COM.3]	Línea principal Internet	[L.1]	M	7	8	7		
[S] Servicios	**[S.1]**	Servicio correo usuarios	[SW.9]	MB	7	7	8	7	7
	[S.2]	Servicio intranet	[H.12]	B	8	9	9	8	7
	[S.3]	Servicio Web	[SW.4], [SW.5]	A	6	8	8	8	7
	[S.4]	Servicio log	[SW.8]	MB	6	7	7	8	8
	[S.5]	Servicio estadísticas	[SW.1], [SW.3]	M	5	7	6	7	6

	[S.6]	Servicio aplicación Docencia	[SW.4]	A	7	8	9	8	8
	[S.7]	Servicio Libro de datos	[SW.5]	A	7	8	9	7	8
[AUX] Equipamiento auxiliar	**[AUX.1]**	Equipo climatización CPD	[L.1]	B			9		
	[AUX.2]	Equipos extintores	[L.1], [L.2]	MB			7		
	[AUX.3]	Equipo climatización oficina	[L.2]	B			6		
[P] Personal	**[P.1]**	Responsable de aplicaciones	-	M			8		
	[P.2]	Técnico servidores	-	B			6		
	[P.3]	Responsable servidores	-	M			7		
	[P.4]	Responsable BDD	-	M			7		
	[P.5]	Técnico de red	-	B			6		
	[P.6]	Técnico de aplicaciones	-	B			6		
	[P.7]	Personal no TIC	-	M			8		

Para la empresa lo más valioso son sus servicios web, compuestos por la aplicación de docencia y el libro de datos, que es donde se basa principalmente su actividad, por este motivo, una interrupción de estos servicios sería considerado grave por parte de la empresa. En el apartado de amenazas se intenta dividir los servicios y aplicaciones según la actividad de la empresa y su estructura lógica. Los servicios web están expuestos de cara a usuarios externos, lo que otorga un plus de criticidad a estos. El resto de aplicaciones y servicios se encuentra tras un firewall que filtra el contenido de la DMZ al área local y por tanto, se hace esta distinción en los siguientes apartados, donde se explicara en detalle.

Como aclaración de los diferentes valores, se ha procedido a valorar de manera valiosa, los activos que contienen información confidencial y penalizada como grave en caso de pérdida por la LOPD, ya que podrían identificar inequívocamente personas físicas, las cuales no autorizan en algunos casos la divulgación de estos datos. Estos activos son los servidores web (Aplicación docencia y libro de datos) y sus dependencias, ya que, en algunos casos, podrían contener información confidencial y sensible acerca de los usuarios, pudiendo identificarlos inequívocamente.

3.4.6 Análisis de amenazas

Las amenazas pueden afectar diferentes aspectos de la seguridad de los activos, por tanto, uno de nuestros objetivos es el análisis de qué amenazas pueden afectar los activos de nuestra organización. Una vez hecho esto se ha de estimar la vulnerabilidad de cada activo respecto a las amenazas potenciales y de esta manera la frecuencia estimada de estas.

El primer paso para realizar este análisis es disponer de una tabla de amenazas y, en nuestro caso en particular, nos basaremos en la guía de **Magerit** para obtener este listado de amenazas y las cruzaremos con los activos que hemos detallado en el punto anterior.

Magerit clasifica las amenazas según:

- *Desastres naturales.*
- *De origen industrial*
- *Errores i fallos no intencionados*
- *Ataques intencionados*

Posteriormente se ha de valorar la frecuencia con la que ocurre o puede materializarse una amenaza. Para valorar esto se utiliza la siguiente tabla de valores:

Valoración	Abreviatura	Valor	Descripción
Frecuencia Muy alta	MA	100	A diario
Frecuente	A	10	Mensual
Normal	M	1	Una vez al año
Poco frecuente	B	1/10	Cada varios años
Muy poco frecuente	MB	1/100	Casi nunca

Se toma como referencia el año natural, que le asignamos un valor de frecuencia medio de ocurrencia y a partir de ese punto podemos establecer el resto de valores en función de si aparecen más de un año, lo que tendrá un valor de frecuencia muy bajo o si se produce más, lo que aumentaría el valor. La escala de valores toma como referencia **Magerit**, concretamente en la Guía I.

Esta escala de valores está extraída de la metodología en la que nos basamos, que es **Magerit**, aunque modificando los valores para que se ajusten más a la edad de la organización en la que pueden ocurrir los hechos.

En último lugar, para valorar el impacto de las amenazas en los activos que tenemos definidos en base a una frecuencia, que acabamos de definir, deberemos asignar valores al impacto que produciría en la organización la materialización de la amenaza, este valor será estimado en tanto por ciento y se define en la siguiente tabla:

Valor	Impacto
100%	Muy Alto – MA
75%	Alto - A
50%	Medio – M
20%	Bajo – B
5%	Muy Bajo - MB

Como se ha explicado anteriormente, para el análisis de las amenazas se ha utilizado la Guía de **Magerit**, concretamente el apartado 5 de la Guía II. De esta guía se extrae la relación de amenazas según el activo afectado y la dimensión que dicha amenaza afecta.

Se hacen las siguientes aclaraciones adicionales para comprender la clasificación realizada:

- Se ha realizado la división o agrupación de activos según ámbito (Instalaciones, hardware, software,…). Sin embargo, por darle más sentido al análisis, en algunos de los ámbitos se ha procedido a agrupar los activos según quién accede a ellos. Como la organización que analizamos tiene como principales actividades servicios orientados a la web, se han dividido los activos que se acceden desde el exterior y los activos que únicamente se accede desde el interior, o que están detrás de una DMZ. Un ejemplo de esto sería una aplicación web, donde se accede a ella desde cualquier red mundial y un portátil o un sistema operativo, donde únicamente se puede acceder desde la red de la organización. También se ha de tener en cuenta que no todas las dimensiones de la seguridad se ven afectadas por una amenaza, existirán amenazas dirigidas a vulnerar la integridad de un sistema y en cambio otras, únicamente a la disponibilidad, así como combinaciones de varias dimensiones afectadas.

- Otra decisión ha sido la de separar los datos y servicios de logs del resto de servicios, ya que la función de esta se aleja del objetivo de los servicios ofrecidos por la organización y por tanto, no sería realista juzgarlos de igual forma y otorgar amenazas que no les involucran.

- Para cada uno de los activos y sus agrupaciones, se han intentado escoger las amenazas con más sentido, descartando algunas de las que aparecen en la guía de Magerit. Un

ejemplo de esto son en algunos casos amenazas que por estructura o lógica de la organización, estas no aplican. Se detallan algunas de estas en los siguientes puntos.

- La organización que se analiza depende en algunos aspectos de UPC y, por tanto, es UPC quien controla algunos puntos del sistema. Un ejemplo de esto es el punto A.11 'Acceso no autorizado', donde en ciertos puntos no tiene sentido ya que los usuarios acceden a algunos servicios vía LDAP, que es un servicio que mantiene y gestiona UPC y nuestra organización únicamente toma los resultados de este servicio de autenticación. Así pues, algunas amenazas relacionadas con el servicio de autenticación y vulnerabilidades que este pueda acarrear no se tienen en cuenta en algunos análisis.

- Otro de los servicios que UPC controla, son las comunicaciones externas de la organización. Es UPC quien se encarga de controlar y mitigar cualquier tipo de incidencia en la comunicación exterior.

- Cabe destacar que todos los trabajadores de la organización tienen acceso a activos y recursos de la empresa. Como se explicó en puntos anteriores donde se describe la organización, se realiza poca segregación de tareas dentro de la organización. Además, que debido al reducido número de trabajadores de la plantilla y a su tarea, todos deben poder acceder a buena parte de la información para consultas principalmente.

- Otro punto a tener en cuenta es el punto E.23 'Errores de mantenimiento' referido a los equipos auxiliares. La organización reside en un espacio alquilado ajeno a ella, por tanto, el mantenimiento de los equipos de seguridad como extintores o aire acondicionado, es ajeno a la organización y son los responsables del edificio los encargados de gestionar la seguridad de estos equipos.

- Existen valoraciones para la integridad que podrían ser más altas, el por qué no lo son es que la organización tiene (aunque mal definidas o deficientes) backups o copias de seguridad que mitigan la amenaza en parte. De igual forma, existen otras contramedidas para el resto de activos en frente de las amenazas.

- Los datos de las aplicaciones se han separado del resto de datos, ya que a estos datos se pueden acceder desde el exterior, porque son gestionados por los usuarios de la comunidad que tiene acceso a ella, por tanto no pueden tener el mismo nivel de impacto una amenaza sobre estos que sobre los datos que gestionan los trabajadores de la compañía, como por ejemplo los datos del sistema operativo, antivirus,…

Es decir, se ha intentado dar un poco de sentido a los datos, agrupando los activos según qué tipo de servicio ofrecen y quién podrá acceder a ellos. De esta manera, se enriquecen los números y se ajusta más a la realidad, ya que no es lo mismo acceder a un servicio interno como un antivirus, que a un servicio externo al que se puede acceder desde el exterior y manipular datos en ellos. Este es el motivo principal por el que se ha optado a agrupar los activos según las tablas que se presentan a continuación.

3.4.7 Tablas de amenazas

Instalaciones							
ID	**Activo**	**Frecuencia**	**A**	**C**	**I**	**D**	**T**
L.1	**CPD**	10				100%	
L.2	**Sala oficinas**	10				100%	
		Amenazas					
N.1	**Fuego**	1/100				100%	
N.2	**Daños por agua**	1/100				100%	
I.1	**Fuego**	1/100				100%	
I.2	**Daños por agua**	1/100				75%	
A.11	**Acceso no autorizado**	10				25%	
A.26	**Ataque destructivo**	1/10				75%	

Hardware							
ID	**Activo**	**Frecuencia**	**A**	**C**	**I**	**D**	**T**
[H.1]	**Servidor de correo**	1		50%	50%	100%	
[H.2]	**Servidor Web**	1		50%	50%	100%	
[H.3]	**Servidor Bases de datos**	1		50%	50%	100%	
[H.4]	**Servidor Firewall primario**	1		50%	50%	100%	
[H.5]	**Servidor logs**	1		50%	50%	100%	
[H.7]	**Switch**	1		50%	50%	100%	
[H.8]	**Servidor Aplicaciones**	1		50%	50%	100%	
[H.9]	**Servidor backup**	1		50%	50%	100%	
[H.12]	**Servidor Firewall DMZ**	1		50%	50%	100%	
		Amenazas					
N.1	**Fuego**	1/100				100%	
N.2	**Daños por agua**	1/100				100%	
I.1	**Fuego**	1/100				100%	
I.2	**Daños por agua**	1/100				75%	
I.4	**Contaminación electromagnética**	1/100				75%	
I.5	**Avería física o lógica**	1/10				50%	
I.6	**Corte suministro eléctrico**	1				75%	
I.7	**Condiciones inadecuadas de temperatura**	1/10				20%	
E.2	**Errores del administrador**	1		50%	50%	20%	
E.23	**Errores de mantenimiento**	1/10				20%	
E.25	**Pérdida de equipos**	1/10		20%		20%	
A.11	**Acceso no autorizado**	1/10		50%		20%	
A.23	**Manipulación de equipos**	1/10		50%		75%	
A.24	**Denegación de servicio**	1				100%	
A.25	**Robo**	1/100		50%		50%	

A.26	**Ataque destructivo**	1/100				100%	

Hardware oficina							
ID	**Activo**	**Frecuencia**	**A**	**C**	**I**	**D**	**T**
[H.6]	**Terminales de usuario**	1		50%		75%	
[H.10]	**Impresora**	1		50%		75%	
[H.11]	**Impresora color**	1		50%		75%	
		Amenazas					
N.1	**Fuego**	1/100				75%	
N.2	**Daños por agua**	1/100				75%	
I.1	**Fuego**	1/100				75%	
I.2	**Daños por agua**	1/100				75%	
I.4	**Contaminación electromagnética**	1/100				75%	
I.5	**Avería física o lógica**	1/10				50%	
I.6	**Corte suministro eléctrico**	1				75%	
I.7	**Condiciones inadecuadas de temperatura**	1/10				20%	
E.23	**Errores de mantenimiento**	1/10				20%	
E.25	**Pérdida de equipos**	1/10		20%		20%	
A.11	**Acceso no autorizado**	1/10		20%		20%	
A.23	**Manipulación de equipos**	1/10		50%		50%	
A.24	**Denegación de servicio**	1				75%	
A.25	**Robo**	1/100		20%		50%	
A.26	**Ataque destructivo**	1/100				75%	

Aplicación web / accesibles por usuarios externos							
ID	**Activo**	**Frecuencia**	**A**	**C**	**I**	**D**	**T**
[SW.4]	**Aplicación Docencia**	10		75%	100%	75%	
[SW.5]	**Aplicación Libro de datos**	10		75%	100%	75%	
[SW.7]	**Aplicación BBDD Server**	10		75%	100%	75%	
		Amenazas					
E.1	**Errores de los usuarios**	10		20%	20%	20%	
E.2	**Errores del administrador**	1		50%	20%	50%	
E.8	**Difusión de software dañino**	1/10		20%	20%	20%	
E.18	**Destrucción de la información**	1/10				20%	
E.19	**Fugas de información**	1/10		20%			
E.20	**Vulnerabilidades de los programas**	1		75%	50%	75%	
E.21	**Errores de mantenimiento**	1/10			100%	75%	
A.6	**Abuso de privilegios de acceso**	1/10		5%	5%	5%	
A.11	**Acceso no autorizado**	1/10		50%	20%		

A.15	Modificación deliberada de la información	1/10			20%		

Aplicaciones internas							
ID	Activo	Frecuencia	A	C	I	D	T
[SW.1]	Aplicación OS	1		50%	50%	75%	
[SW.2]	Aplicaciones ofimática	1		50%	50%	75%	
[SW.3]	Aplicación estadística	1		50%	50%	75%	
[SW.6]	Aplicación Antivirus	1		50%	50%	75%	
[SW.9]	Aplicación de correo	1		50%	50%	75%	
	Amenazas						
E.1	Errores de los usuarios	1		20%	20%	20%	
E.2	Errores del administrador	1		50%	20%	50%	
E.8	Difusión de software dañino	1/10		20%	20%	20%	
E.18	Destrucción de la información	1/10				20%	
E.19	Fugas de información	1/10		20%			
E.20	Vulnerabilidades de los programas	1		20%	50%	75%	
E.21	Errores de mantenimiento	1/10			50%	75%	
A.6	Abuso de privilegios de acceso	1/10		50%	20%	20%	
A.8	Disfusión de software dañino	1/10		20%	50%	75%	
A.11	Acceso no autorizado	1/10		20%	50%		
A.15	Modificación deliberada de la información	1/100			50%		
A.22	Manipulación de programas	1/100		20%	50%	75%	

Datos de los logs							
ID	Activo	Frecuencia	A	C	I	D	T
[D.1]	Datos logs	1/10		75%	50%	50%	75%
[SW.8]	Aplicación de logs	1/10		75%	50%	50%	75%
[S.4]	Servicio log	1/10		75%	50%	50%	75%
	Amenazas						
E.3	Errores de monitorización	1/10					50%
A.3	Manipulación de los logs	1/100					75%
A.4	Manipulación de la configuración	1/100		75%	50%	50%	
A.13	Repudio	1/10					50%
E.18	Destrucción de la información	1/10				50%	
E.19	Fugas de información	1/10		50%			
A.11	Acceso no autorizado	1/10		75%	50%		
A.15	Modificación deliberada de la información	1/10			50%		

Datos aplicaciones internas							
ID	Activo	Frecuencia	A	C	I	D	T
[D.3]	Datos Servidor correo	1		50%	50%	50%	
[D.4]	Datos estadísticos	1		50%	50%	50%	
[D.5]	Datos Backup	1		50%	50%	50%	
	Amenazas						
E.1	Errores de los usuarios	1		20%	20%	20%	
E.2	Errores del administrador	1/10		50%	50%	50%	
E.4	Errores de configuración	1/10			50%		
E.15	Alteración accidental de la información	1/10			20%		
E.18	Destrucción de la información	1/100				50%	
E.19	Fugas de información	1/10		20%			
A.5	Suplantación de identidad de usuario	1/10		20%	50%	20%	
A.6	Abuso de privilegio de acceso	1		20%	20%	20%	
A.11	Acceso no autorizado	1/100		50%	50%		
A.15	Modificación deliberada de la información	1/100			50%		
A.19	Divulgación de la información	1/10		20%			

Datos aplicaciones web							
ID	Activo	Frecuencia	A	C	I	D	T
[D.2]	Datos aplicaciones	10		75%	75%	50%	
	Amenazas						
E.1	Errores de los usuarios	10		20%	20%	20%	
E.2	Errores del administrador	1/10		75%	75%	50%	
E.4	Errores de configuración	1/10			75%		
E.15	Alteración accidental de la información	1/10			20%		
E.18	Destrucción de la información	1/100				50%	
E.19	Fugas de información	1/10		50%			
A.5	Suplantación de identidad de usuario	1/10		50%	50%	20%	
A.6	Abuso de privilegio de acceso	1		20%	20%	20%	
A.11	Acceso no autorizado	1/100		50%	75%		
A.15	Modificación deliberada de la información	1/100			50%		
A.19	Divulgación de la información	1/10		50%			

Comunicación							
ID	Activo	Frecuencia	A	C	I	D	T
[COM.1]	Router primario	10		75%	75%	100%	
[COM.2]	Línea intranet (DMZ)	10		75%	75%	100%	
[COM.3]	Línea principal Internet	10		75%	75%	100%	
	Amenazas						
I.8	Fallo de servicio de comunicaciones	1/10				100%	
E.2	Errores del administrador	1/10		50%	20%	100%	
E.15	Alteración accidental de la información	1/10			50%		
E.19	Fugas de información	1/10		20%			
A.7	Uso no previsto	10		20%	20%	75%	
A.9	Re-encaminamiento de mensajes	1		20%			
A.11	Acceso no autorizado	1/10		75%	20%		
A.14	Interceptación de la información	1/10		50%			
A.15	Modificación deliberada de la información	1/100			75%		
A.24	Denegación de servicio	1/10				100%	

Servicios							
ID	Activo	Frecuencia	A	C	I	D	T
[S.3]	Servicio Web	10	50%	50%	75%	75%	50%
[S.6]	Servicio aplicación Docencia	10	50%	50%	75%	75%	50%
[S.7]	Servicio Libro de datos	10	50%	50%	75%	75%	50%
	Amenazas						
E.1	Errores de los usuarios	10		20%	20%	20%	
E.2	Errores del administrador	1		50%	75%	50%	
E.15	Alteración accidental de la información	1			20%		
E.18	Destrucción de la información	1/10				75%	
E.19	Fugas de información	1/10		20%			
A.5	Suplantación de identidad del usuario	1/10	50%	50%	20%		
A.6	Abuso de privilegio de acceso	1		20%	50%	20%	
A.7	Uso no previsto	10		20%	20%	20%	
A.11	Acceso no autorizado	1/10		50%	75%		
A.13	Repudio	1/10					50%
A.15	Modificación deliberada de la información	1/100			75%		
A.19	Divulgación de información	1/100		50%			

Servicios internos							
ID	Activo	Frecuencia	A	C	I	D	T
[S.1]	Servicio correo usuarios	1	20%	20%	50%	50%	20%
[S.2]	Servicio intranet	1	20%	20%	50%	50%	20%
[S.5]	Servicio estadísticas	1	20%	20%	50%	50%	20%
	Amenazas						
E.1	Errores de los usuarios	1		20%	20%	20%	
E.2	Errores del administrador	1		5%	20%	50%	
E.15	Alteración accidental de la información	1			20%		
E.18	Destrucción de la información	1/10				50%	
E.19	Fugas de información	1/10		20%			
A.5	Suplantación de identidad del usuario	1/10	20%	5%	5%		
A.6	Abuso de privilegio de acceso	1		5%	20%	20%	
A.7	Uso no previsto	10		20%	20%	50%	
A.11	Acceso no autorizado	1/10		20%	50%		
A.13	Repudio	1/10					20%
A.15	Modificación deliberada de la información	1/100			50%		
A.19	Divulgación de información	1/100		20%			

Auxiliar							
ID	Activo	Frecuencia	A	C	I	D	T
[AUX.1]	Equipo climatización CPD	1				100%	
[AUX.2]	Equipos extintores	1				100%	
[AUX.3]	Equipo climatización oficina	1				100%	
	Amenazas						
N.1	Fuego	1/100				100%	
N.2	Daños por agua	1/100				100%	
I.1	Fuego	1/100				100%	
I.2	Daños por agua	1/100				100%	
I.6	Corte del suministro eléctrico	1				100%	
I.9	Interrupción de otros servicios y suministros esenciales	1				20%	
E.23	Errores de mantenimiento	1/100				0%	
E.25	Pérdida de equipos	1/100				50%	
A.23	Manipulación de los equipos	1/100				50%	
A.26	Ataques destructivos	1/100				100%	

Personal							
ID	Activo	Frecuencia	A	C	I	D	T
[P.1]	Responsable de aplicaciones	1		50%	100%	100%	
[P.2]	Técnico servidores	1		50%	100%	100%	
[P.3]	Responsable servidores	1		50%	100%	100%	
[P.4]	Responsable BDD	1		50%	100%	100%	
[P.5]	Técnico de red	1		50%	100%	100%	
[P.6]	Técnico de aplicaciones	1		50%	100%	100%	
[P.7]	Personal no TIC	1		50%	100%	100%	
		Amenazas					
E.7	Deficiencias en la organización	1				50%	
E.19	Fugas de información	1/10		50%			
E.28	Indisponibilidad del personal	1/100				50%	
A.29	Extorsión	1/100		50%	100%	100%	
A.30	Ingeniería social	1/10		50%	20%	50%	

En las tablas anteriores se pueden ver detalladas la degradación de los activos en función del impacto al materializarse una amenaza, así como la frecuencia de ocurrencia de estas.

El valor del impacto escogido para cada activo, será el máximo del impacto de las amenazas que se pueden materializar sobre un activo determinado. Lo mismo pasa para la frecuencia (aunque en esta tabla no se calcula sobre la frecuencia), el valor escogido sobre la frecuencia será el peor caso, el peor escenario, y este será el valor más alto de ellos, ya que refleja las amenazas que se pueden materializar cada menor tiempo en la organización.

3.4.8 Impacto potencial

Una vez terminado el análisis de los activos, presentado en las tablas anteriores y el análisis de las amenazas, podemos calcular el impacto potencial que pueden suponer para la empresa la materialización de estas amenazas.

En este apartado y, para el cálculo del impacto, no se tienen en cuenta contramedidas, por tanto, el resultado que obtengamos de este cálculo se podrá extraer un valor de referencia que ayudará para determinar y priorizar un plan de acción. Al aplicar las contramedidas, este valor se verá modificado.

Para realizar el cálculo del impacto potencial, se utiliza la siguiente fórmula:

Impacto Potencial = Activo x Impacto

Donde, es el valor de cada dimensión y el impacto es la degradación en cada dimensión en la que se ve afectado el activo también en caso de materializarse. En la tabla siguiente se presentan los resultados:

ID	Activo	Valoración					Impacto					Impacto Potencial				
		c	i	d	a	t	c	i	d	a	t	c	i	d	a	t
[L.1]	CPD	8	9	10	8	8			100%					10		
[L.2]	Sala oficinas	5	7	8					100%					8		
[H.1]	Servidor de correo	7	7	8	8	8	50%	50%	100%			3,5	3,5	8		
[H.2]	Servidor Web	9	9	9	8	8	50%	50%	100%			4,5	4,5	9		
[H.3]	Servidor Bases de datos	9	9	9	8	8	50%	50%	100%			4,5	4,5	9		
[H.4]	Servidor Firewall primario	8	9	9	8	8	50%	50%	100%			4	4,5	9		
[H.5]	Servidor logs	8	8	7	8	8	50%	50%	100%			4	4	7		
[H.6]	Terminales de usuario	5	7	7	8	7	50%		75%			2,5		5,25		
[H.7]	Switch	8	9	9	8	8	50%	50%	100%			4	4,5	9		
[H.8]	Servidor Aplicaciones	8	9	7	7	7	50%	50%	100%			4	4,5	7		
[H.9]	Servidor backup	8	9	9	8	8	50%	50%	100%			4	4,5	9		
[H.10]	Impresora			7			50%		75%					5,25		
[H.11]	Impresora color			7			50%		75%					5,25		
[H.12]	Servidor Firewall DMZ	8	9	9	8	8	50%	50%	100%			4	4,5	9		
[SW.1]	Aplicación OS	5	7	7	8	7	50%	50%	75%			2,5	3,5	5,25		
[SW.2]	Aplicaciones ofimática	4	7	6	7	6	50%	50%	75%			2	3,5	4,5		
[SW.3]	Aplicación estadística	5	7	6	8	7	50%	50%	75%			2,5	3,5	4,5		
[SW.4]	Aplicación Docencia	9	9	9	8	8	75%	100%	75%			6,75	9	6,75		
[SW.5]	Aplicación Libro de datos	9	9	9	8	8	75%	100%	75%			6,75	9	6,75		
[SW.6]	Aplicación Antivirus	4	7	5	6	7	50%	50%	75%			2	3,5	3,75		
[SW.7]	Aplicación BBDD Server	8	9	8	8	8	75%	100%	75%			6	9	6		
[SW.8]	Aplicación de logs	8	8	7	8	8	75%	50%	50%		75%	6	4	3,5		6
[SW.9]	Aplicación de correo	7	7	8	8	8	50%	50%	75%			3,5	3,5	6		
[D.1]	Datos logs	8	8	6	8	8	75%	50%	50%		75%	6	4	3		6
[D.2]	Datos aplicaciones	9	9	9	8	8	75%	75%	50%			6,75	6,75	4,5		
[D.3]	Datos Servidor correo	7	7	6	8	7	50%	50%	50%			3,5	3,5	3		
[D.4]	Datos estadísticos	5	7	6	7	6	50%	50%	50%			2,5	3,5	3		
[D.5]	Datos Backup	8	9	8	6	7	50%	50%	50%			4	4,5	4		
[COM.1]	Router primario	7	9	9	6	7	75%	75%	100%			5,25	6,75	9		
[COM.2]	Línea intranet (DMZ)	6	8	6			75%	75%	100%			4,5	6	6		
[COM.3]	Línea principal Internet	7	8	7			75%	75%	100%			5,25	6	7		
[S.1]	Servicio correo usuarios	7	7	8	7	7	20%	50%	50%	20%	20%	1,4	3,5	4	1,4	1,4
[S.2]	Servicio intranet	8	9	9	8	7	20%	50%	50%	20%	20%	1,6	4,5	4,5	1,6	1,4
[S.3]	Servicio Web	6	8	8	8	7	50%	75%	75%	50%	50%	3	6	6	4	3,5
[S.4]	Servicio log	6	7	7	8	8	75%	50%	50%		75%	4,5	3,5	3,5		6
[S.5]	Servicio estadísticas	5	7	6	7	6	20%	50%	50%	20%	20%	1	3,5	3	1,4	1,2
[S.6]	Servicio aplicación Docencia	7	8	9	8	8	50%	75%	75%	50%	50%	3,5	6	6,75	4	4

[S.7]	Servicio Libro de datos	7	8	9	7	8	50%	75%	75%	50%	50%	3,5	6	6,75	3,5	4
[AUX.1]	Equipo climatización CPD			9					100%					9		
[AUX.2]	Equipos extintores			7					100%					7		
[AUX.3]	Equipo climatización oficina			6					100%					6		
[P.1]	Responsable de aplicaciones			8			50%	100%	100%					8		
[P.2]	Técnico servidores			6			50%	100%	100%					6		
[P.3]	Responsable servidores			7			50%	100%	100%					7		
[P.4]	Responsable BDD			7			50%	100%	100%					7		
[P.5]	Técnico de red			6			50%	100%	100%					6		
[P.6]	Técnico de aplicaciones			6			50%	100%	100%					6		
[P.7]	Personal no TIC			8			50%	100%	100%					8		

3.4.9 Nivel de riesgo aceptable y residual

Una vez conocemos el impacto potencial causado por un activo y su impacto en el sistema, es posible obtener el riesgo integrando la frecuencia con que se puede dar un hecho concreto en nuestros sistemas. Podríamos afirmar que si:

Riesgo = Impacto Potencial * Frecuencia

Podemos afirmar que el riesgo será mayor cuanto mayor sea el impacto y mayor la frecuencia de ocurrencia.

Es necesario definir un límite a partir del cual podremos decidir si asumimos un riesgo o por el contrario decidimos no asumirlo y por tanto aplicar los controles. Al definir un nivel de riesgo, se definirá una línea sobre la cual se divide lo que puede suponer una amenaza para la organización y lo que no y donde:

- Lo que supere este nivel aceptable deberá ser tratado por la organización de manera que tome controles oportunos para reducir este riesgo.
- Lo que no supere el riesgo aceptable no supondrá una amenaza importante para la organización.

El objetivo es reducir los riesgos que superan el nivel aceptable y aprobado por la dirección de la organización. Reducir todos los riesgos a cero es una tarea complicada y prácticamente imposible, no obstante, siempre se pueden concentrar los esfuerzos en mitigar el impacto de una amenaza lo máximo posible. Posteriormente a haber aplicado los controles pertinentes, el riego que todavía continua existiendo es el riesgo residual.

Por tanto, el primer paso para establecer un nivel de riesgo aceptable es tener la tabla con los cálculos pertinentes según cada activo, calculado tal como se especifica en la fórmula anterior. Una vez tenemos los resultados, para calcular el riesgo aceptable para nuestra organización, hemos definido la siguiente metodología:

Riesgo aceptable = Valor Activo * Impacto * Frecuencia

Donde:

- **Valor Activo** → Los activos son valorados del 1 al 10, siendo 10 un daño muy grave a la organización y 0 un daño irrelevante. El valor escogido es 5, ya que es el valor medio de lo que empieza a ser un daño importante en la organización. Cualquier activo por encima de este valor comienza a ser un activo crítico para el desempeño y continuidad de negocio.

- **Impacto** → El impacto se valora en porcentajes, siendo estos 100% un impacto Muy alto para la organización y 5% un impacto muy bajo. Por tanto, se considera que todo lo que está por encima del 50% de impacto en la organización ha de comenzar a tratarse especialmente.

- **Frecuencia** → La frecuencia de ocurrencia de una determinada amenaza a la organización marca otro punto a tener en cuenta a la hora de calcular el riesgo aceptable. Se ha escogido una frecuencia de ocurrencia de amenaza 10, o sea, amenazas que se materializan al menos una vez al mes, mensuales. A partir de este valor se considera que no es aceptable, por tanto este es el límite para la frecuencia de ocurrencia.

Por tanto el valor del riesgo aceptable es:

Riesgo aceptable = 5 x 10 x 50% = 25

Este valor podría sufrir ajustes según los valores resultantes del cálculo del riesgo, es decir, el resultado de esta fórmula no es un resultado vinculante ni absoluto, sino que se puede ver ajustado a los resultados obtenidos para conseguir mayor afinamiento en la detección de aquellos activos potencialmente en riesgo.

Con toda esta información detallamos a continuación los valores del cálculo del riesgo así como los valores que quedan detectados por encima del valor de riesgo aceptable para la organización en color rojo:

ID	Activo	Frecuencia	Impacto Potencial					Riesgo Acumulado				
			c	i	d	a	t	c	i	d	a	t
[L.1]	CPD	10			10					100		
[L.2]	Sala oficinas	10			8					80		
[H.1]	Servidor de correo	1	3,5	3,5	8			3,5	3,5	8		
[H.2]	Servidor Web	1	4,5	4,5	9			4,5	4,5	9		
[H.3]	Servidor Bases de datos	1	4,5	4,5	9			4,5	4,5	9		
[H.4]	Servidor Firewall primario	1	4	4,5	9			4	4,5	9		
[H.5]	Servidor logs	1	4	4	7			4	4	7		
[H.6]	Terminales de usuario	1	2,5		5,25			2,5		5,25		
[H.7]	Switch	1	4	4,5	9			4	4,5	9		
[H.8]	Servidor Aplicaciones	1	4	4,5	7			4	4,5	7		
[H.9]	Servidor backup	1	4	4,5	9			4	4,5	9		
[H.10]	Impresora	1			5,25					5,25		
[H.11]	Impresora color	1			5,25					5,25		
[H.12]	Servidor Firewall DMZ	1	4	4,5	9			4	4,5	9		
[SW.1]	Aplicación OS	1	2,5	3,5	5,25			2,5	3,5	5,25		
[SW.2]	Aplicaciones ofimática	1	2	3,5	4,5			2	3,5	4,5		
[SW.3]	Aplicación estadística	1	2,5	3,5	4,5			2,5	3,5	4,5		
[SW.4]	Aplicación Docencia	10	6,75	9	6,75			67,5	90	67,5		
[SW.5]	Aplicación Libro de datos	10	6,75	9	6,75			67,5	90	67,5		
[SW.6]	Aplicación Antivirus	1	2	3,5	3,75			2	3,5	3,75		
[SW.7]	Aplicación BBDD Server	10	6	9	6			60	90	60		
[SW.8]	Aplicación de logs	0,1	6	4	3,5		6	0,6	0,4	0,35		0,6
[SW.9]	Aplicación de correo	1	3,5	3,5	6			3,5	3,5	6		
[D.1]	Datos logs	0,1	6	4	3		6	0,6	0,4	0,3		0,6
[D.2]	Datos aplicaciones	10	6,75	6,75	4,5			67,5	67,5	45		
[D.3]	Datos Servidor correo	1	3,5	3,5	3			3,5	3,5	3		
[D.4]	Datos estadísticos	1	2,5	3,5	3			2,5	3,5	3		
[D.5]	Datos Backup	1	4	4,5	4			4	4,5	4		
[COM.1]	Router primario	10	5,25	6,75	9			52,5	67,5	90		
[COM.2]	Línea intranet (DMZ)	10	4,5	6	6			45	60	60		
[COM.3]	Línea principal Internet	10	5,25	6	7			52,5	60	70		
[S.1]	Servicio correo usuarios	1	1,4	3,5	4	1,4	1,4	1,4	3,5	4	1,4	1,4
[S.2]	Servicio intranet	1	1,6	4,5	4,5	1,6	1,4	1,6	4,5	4,5	1,6	1,4

[S.3]	**Servicio Web**	10	3	6	6	4	3,5	30	60	60	40	35	
[S.4]	**Servicio log**	0,1	4,5	3,5	3,5		6	0,45	0,35	0,35		0,6	
[S.5]	**Servicio estadísticas**	1	1	3,5	3	1,4	1,2	1	3,5	3	1,4	1,2	
[S.6]	**Servicio aplicación Docencia**	10	3,5	6	6,75	4	4	35	60	67,5	40	40	
[S.7]	**Servicio Libro de datos**	10	3,5	6	6,75	3,5	4	35	60	67,5	35	40	
[AUX.1]	**Equipo climatización CPD**	1			9					9			
[AUX.2]	**Equipos extintores**	1			7					7			
[AUX.3]	**Equipo climatización oficina**	1			6					6			
[P.1]	**Responsable de aplicaciones**	1			8					8			
[P.2]	**Técnico servidores**	1			6					6			
[P.3]	**Responsable servidores**	1			7					7			
[P.4]	**Responsable BDD**	1			7					7			
[P.5]	**Técnico de red**	1			6					6			
[P.6]	**Técnico de aplicaciones**	1			6					6			
[P.7]	**Personal no TIC**	1			8					8			

3.4.10 Resultados

En la tabla anterior se pueden ver los resultados del riesgo, producto del impacto potencial por la frecuencia. Se puede ver como han quedado definidos como por encima del riesgo aceptable justamente aquellos activos que están relacionados con el servicio principal que desarrolla la organización. Estos servicios son los que están abiertos a internet y a los usuarios que están registrados para acceder a ella. Estos activo son la aplicación de docencia, el libro de datos y la base de datos que los gestiona, a partir de estos, todos los activos relacionados con ellos, como el servidor web o los propios datos de las aplicaciones también son considerados críticos y actualmente se encuentran por encima del riesgo aceptable.

A continuación se muestran los resultados asociados a los servicios que tiene la organización disponibles, de forma que se pueda interpretar el riesgo que tienen asociados con el fin de discernir los servicios a tener en cuenta y sobre los que sería importante aplicar controles con el fin de mitigar el riesgo:

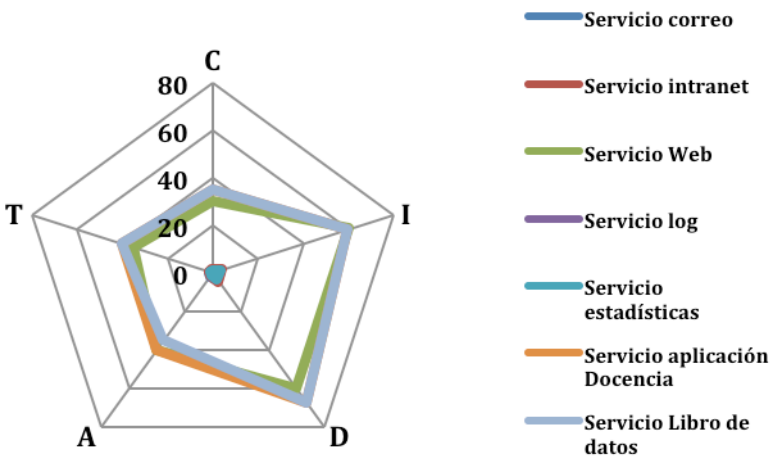


Gráfico representativo del riesgo de los servicios de la empresa

Los datos de las aplicaciones, además, contienen datos confidenciales que podrían identificar inequívocamente a una persona física, por lo tanto están sometidos a un riesgo adicional. Tal como se explica en apartados enteriores, aunque no existe un procedimiento formal, estructurado y actualizado, la empresa realiza ciertas medidas para garantizar la confidencial o integridad de los datos, como por ejemplos, las copias de seguridad. En el siguiente gráfico puede aplicarse la diferencia entre el riesgo de los datos:

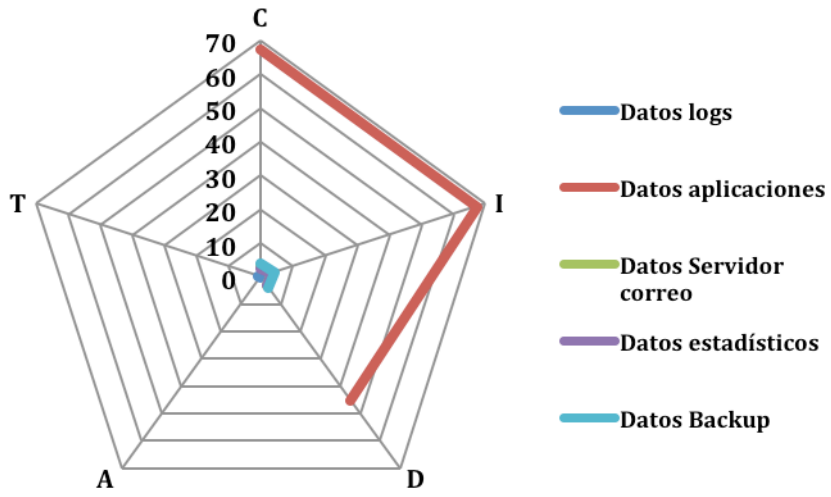


Gráfico representativo del riesgo de los datos de la empresa

Tal como se explica, los datos de la empresa relacionados con las aplicaciones (Aplicación de docencia y libro de datos) son categorizados como muy sensible por la LOPD y lo explicado anteriormente. Además, estos datos son accesibles desde el exterior, ya que forman la parte central de las aplicaciones web y cualquier fuga de información, error que permita a un atacante acceder a ellos mediante algún ataque web por ejemplo o pérdida de los mismos, supondría un gran impacto y riesgo en la organización. De ahí la importancia de estos datos y la importancia de preservar su integridad y confidencialidad. El resto de datos son de un uso más interno y menos confidencial, por eso el motivo de que el riesgo no sea tan elevado, ya que en caso de pérdida la actividad de negocio de la empresa no peligraría como si se vieran involucrados los datos de las aplicaciones.

En cuanto a las aplicaciones que gestiona la organización, siguen el mismo patrón que han seguido todos los activos hasta ahora, diferenciando las aplicaciones que son accesibles desde el exterior y las que no lo son. Que se pueda acceder desde el exterior no debería ser determinante para el riesgo de los activos de la organización, sin embargo, en este caso coinciden esas aplicaciones con las más críticas e importantes para la continuidad de negocio, que son la aplicación de docencia, la aplicación libro de datos y la base de datos que gestiona las conexiones de los datos con ambas y absorbe las peticiones de los usuarios. A continuación se muestra un gráfico del riesgo que suponen las aplicaciones en la empresa.

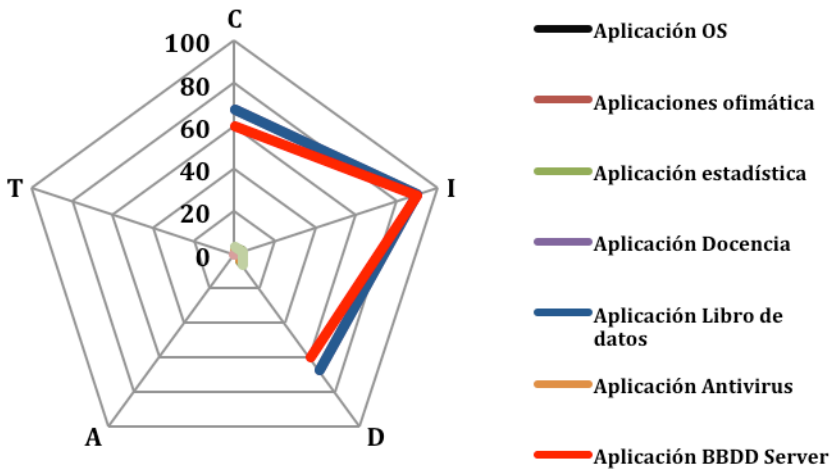


Gráfico representativo del riesgo de las aplicaciones de la empresa

Dada que la principal actividad de la organización son los servicios web, la comunicación que facilita esto, como el router primario o la línea de conexión a la red son activos fundamentales para llevar a cabo la actividad de negocio. De igual manera la línea interna que proporciona conectividad entre los trabajadores y de estos al exterior es importante para mantener todas las áreas de la empresa conectada y operativa para responder en caso de incidente. Continuación se presenta un gráfico representativo de las áreas de riesgo respecto de los activos de comunicación:

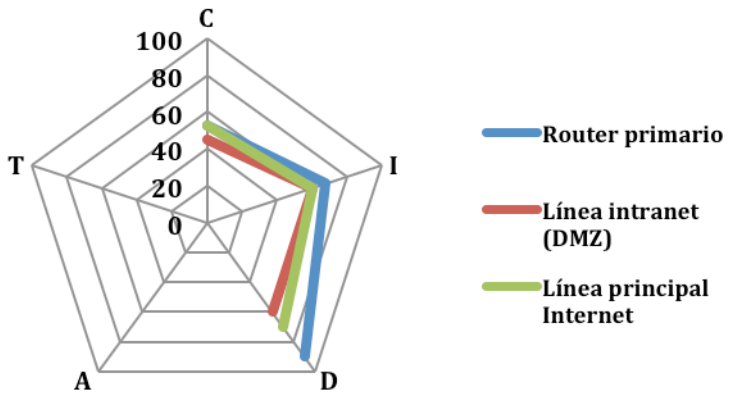


Gráfico representativo del riesgo de comunicaciones de la empresa

Otro de los activos que tienen un riesgo por encima de lo aceptable son el CPD y la sala de oficinas, ya que es el centro neurálgico de las operaciones de la empresa, en caso de pérdida de estas salas, donde se encuentran todos los servidores y datos, causaría el cese de la actividad de la empresa de forma inmediata, ya que no existen otras salas de réplica listas para dar soporte de forma inmediata ni replicación de los datos fuera de estas dos instalaciones.

El resto de activos se encuentran por debajo del nivel de riesgo aceptable coincidiendo con activos que se encuentran principalmente para uso interno o bien dan soporte a otros servicios como el caso del hardware.

En cuanto a las dimensiones de la seguridad más afectadas por las amenazas, nos encontramos con el siguiente gráfico explicativo:

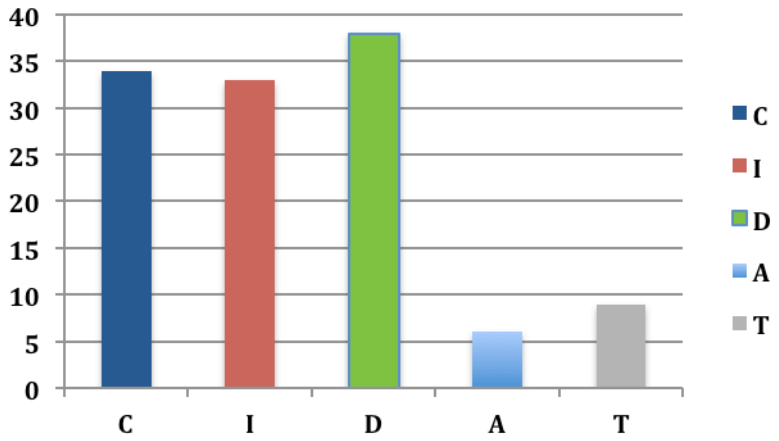


Gráfico representativo de las dimensiones de la seguridad afectadas

Tal como se puede ver en el gráfico, las dimensiones de la seguridad más afectadas por las amenazas son la confidencialidad, la integridad y la disponibilidad de los datos, siendo esta última la que más amenazas pueden afectarla. Esto puede dar una idea de en qué dimensiones habrá que dedicar más esfuerzos para asegurar la continuidad de negocio, ya que la mayoría de amenazas van destinadas a estos valores.

Los controles que se apliquen para intentar reducir los riesgos presentados afectaran de manera significativa los valores actuales, en concreto, nuestros esfuerzos han de ir dirigidos a intentar reducir y mitigar en la medida de lo posible los activos que están por encima del riesgo aceptable para la organización.

3.5 Auditoría de cumplimiento

3.5.1 Introducción

En este punto se ha analizado la empresa desde el punto de vista de sus activos, cómo está organizada, las amenazas y un análisis de riesgos donde se puede ver cómo afectan estas y el impacto que tienen sobre la organización.

En este apartado se evaluará hasta que punta la empresa cumple con las buenas prácticas en materia de seguridad. Esto se hará utilizando como guía la ISO/IEC 27002:2005 basándonos en el marco de control del estado de la seguridad.

3.5.2 Metodología

La ISO/IEC 27002:2005 servirá como marco de control del estado de la seguridad. En total, la ISO/IEC 27002:2005 agrupa 133 controles o medidas preventivas sobre "buenas prácticas" para la gestión de la seguridad de la información, organizados en 11 áreas y 39 objetivos de control. Este estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de las organizaciones.

Existen diferentes aspectos, para los cuales las medidas preventivas actúan reduciendo el riesgo y que son conocidos como controles ISO/IEC 27002:2005 o cualquier catálogo. Estos son en general:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política personal
- Solicitudes técnicas (Software, hardware o comunicaciones).
- Seguridad física.

La protección integral, por las diferentes amenazas, requiere de una combinación de medidas preventivas sobre cada uno de los aspectos.

3.5.3 Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad según los diferentes dominios de control y los 133 controles planteados por la ISO.

A modo de resumen, los dominios que se han de analizar y que componen la ISO/IEC 27002:2005 son:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos

- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

El estudio ha de realizar una revisión de los 133 controles planteados por la norma a cumplir, con los diferentes objetivo de control. Esta estimación se realizará según la siguiente tabla, que se basa en el modelo de madurez de la capacidad (CMM):

Efectividad	CMM	Significado	Descripción
0%	**L0**	**Inexistente**	Carencia completa de cualquier proceso que se reconozca. No se ha reconocido que exista ningún problema a resolver
10%	**L1**	**Inicial / Ad-hoc**	Estado inicial donde el éxito de las actividades de los procesos se basa en la mayor parte de las veces en un esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	**Reproducible pero intuitivo**	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea. Se normalizan las “buenas prácticas” a base de experiencia y método. No hay comunicación o entretenimiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	**Proceso definido**	La organización participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entretenimiento.
95%	**L4**	**Gestionado y medible**	Se puede seguir con indicaciones numéricos y estadísticos la evolución de los

			procesos. Se dispone de tecnología para automatizar el flujo de trabajo, teniendo herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	**Optimizado**	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunas y se optimizan los procesos

3.5.4 Resultados por dominio según ISO/IEC 27002:2005

A continuación se muestran los resultados obtenidos en cada control de la ISO según el dominio al que pertenecen. Los resultados son en función de la valoración detallada en apartados anteriores con el fin de analizar la madurez de los controles.

CONTROL	ESTADO
5. POLÍTICA DE SEGURIDAD	**10%**
5.1 Política de seguridad de la información	**10%**
5.1.1 Documento de la política de seguridad de la información	10%
5.1.2 Revisión de la política de seguridad de la información	0%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**40%**
6.1 Organización interna	**50%**
6.1.1 Compromiso de la dirección con la seguridad de la información	30%
6.1.2 Coordinación de la seguridad de la información	60%
6.1.3 Asignación de responsabilidades relativas a la seg. De la información	25%
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	30%
6.1.5 Acuerdo de confidencialidad	95%
6.1.6 Contacto con las autoridades	75%
6.1.7 Contacto con grupos de especial interés	90%
6.1.8 Revisión independiente de la seguridad de la información	0%
6.2 Terceros	**30%**
6.2.1 Identificación de los riesgos derivados del acceso de terceros	30%
6.2.2 Tratamiento de la seguridad en la relación con los clientes	25%
6.2.3 Tratamiento de la seguridad en contratos con terceros	35%
7. GESTIÓN DE ACTIVOS	**30%**
7.1 Responsabilidad sobre los activos	**45%**
7.1.1 Inventario de activos	25%
7.1.2 Propiedad de los activos	60%
7.1.3 Uso aceptable de los activos	50%
7.2 Clasificación de la información	**15%**
7.2.1 Directrices de clasificación	20%
7.2.2 Etiquetado y manipulado de la información	10%

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**65%**
8.1 Antes del empleo	**73%**
8.1.1 Funciones y responsabilidades	40%
8.1.2 Investigación de antecedentes	90%
8.1.3 Términos y condiciones de contratación	90%
8.2 Durante el empleo	**30%**
8.2.1 Responsabilidades de la dirección	30%
8.2.2 Concienciación, formación y capacitación en seguridad de la información	20%
8.2.3 Proceso disciplinario	40%
8.3 Cese del empleo o cambio de puesto de trabajo	**91%**
8.3.1 Responsabilidad del cese o cambio	90%
8.3.2 Devolución de activos	95%
8.3.3 Retirada de los derechos de acceso	90%
9. SEGURIDAD FÍSICA Y DEL ENTORNO	**40%**
9.1 Áreas seguras	**52%**
9.1.1 Perímetro de seguridad física	80%
9.1.2 Controles físicos de entrada	10%
9.1.3 Seguridad de oficinas, despachos e instalaciones	30%
9.1.4 Protección contra las amenazas externas y de origen ambiental	90%
9.1.5 Trabajo en áreas seguras	
9.1.6 Áreas de acceso público y de carga y descarga	
9.2 Seguridad de los equipos	**28%**
9.2.1 Emplazamiento y protección de equipos	30%
9.2.2 Instalaciones de suministro	50%
9.2.3 Seguridad del cableado	70%
9.2.4 Mantenimiento de los equipos	10%
9.2.5 Seguridad de los equipos fuera de las instalaciones	10%
9.2.6 Reutilización o retirada segura de equipos	20%
9.2.7 Retirada de materiales propiedad de la empresa	10%
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	**50%**
10.1 Responsabilidades y procedimientos de operación	**15%**
10.1.1 Documentación de los procedimientos de operación	10%
10.1.2 Gestión de cambios	10%
10.1.3 Segregación de tareas	30%
10.1.4 Separación de los recursos de desarrollo, prueba y operación	10%
10.2 Gestión de la provisión de servicios por terceros	**50%**
10.2.1 Provisión de servicios	70%
10.2.2 Supervisión y revisión de los servicios prestados por terceros	50%
10.2.3 Gestión del cambio en los servicios prestados por terceros	30%
10.3 Planificación y aceptación del sistema	**40%**
10.3.1 Gestión de capacidades	30%
10.3.2 Aceptación del sistema	50%
10.4 Protección contra el código malicioso y descargable	**90%**
10.4.1 Controles contra el código malicioso	90%
10.4.2 Controles contra el código descargado en el cliente	

10.5 Copias de seguridad	**30%**
10.5.1 Copias de seguridad de la información	30%
10.6 Gestión de la seguridad de las redes	**45%**
10.6.1 Controles de red	40%
10.6.2 Seguridad de los servicios de red	50%
10.7 Manipulación de los soportes	**47%**
10.7.1 Gestión de soportes extraíbles	10%
10.7.2 Retirada de soportes	50%
10.7.3 Procedimientos de manipulación de la información	60%
10.7.4 Seguridad de la documentación del sistema	70%
10.8 Intercambio de información	**70%**
10.8.1 Políticas y procedimientos de intercambio de información	70%
10.8.2 Acuerdos de intercambio	70%
10.8.3 Soportes físicos en tránsito	
10.8.4 Mensajería electrónica	80%
10.8.5 Sistemas de información empresariales	60%
10.9 Servicios de comercio electrónico	
10.9.1 Comercio electrónico	
10.9.2 Transacciones en línea	
10.9.3 Información públicamente disponible	
10.10 Supervisión	**70%**
10.10.1 Registros de auditoría	60%
10.10.2 Supervisión del uso del sistema	70%
10.10.3 Protección de la información de los registros	50%
10.10.4 Registros de administración y operación	90%
10.10.5 Registro de fallos	50%
10.10.6 Sincronización del reloj	95%
11. CONTROL DE ACCESO	**30%**
11.1 Requisitos de negocio para el control de acceso	**30%**
11.1.1 Política de control de acceso	30%
11.2 Gestión de acceso de usuario	**27%**
11.2.1 Registro de usuario	20%
11.2.2 Gestión de privilegios	30%
11.2.3 Gestión de contraseñas de usuario	50%
11.2.4 Revisión de los derechos de acceso de usuario	10%
11.3 Responsabilidades de usuario	**18%**
11.3.1 Uso de contraseñas	25%
11.3.2 Equipo de usuario desatendido	10%
11.3.3 Política de puestos de trabajo despejados y pantalla limpia	20%
11.4 Control de acceso a la red	**54%**
11.4.1 Política de uso de los servicios de red	40%
11.4.2 Autenticación de usuario para conexiones externas	20%
11.4.3 Identificación de los equipos en red	50%
11.4.4 Protección de los puertos de diagnóstico y configuración remotos	80%
11.4.5 Segregación de las redes	50%

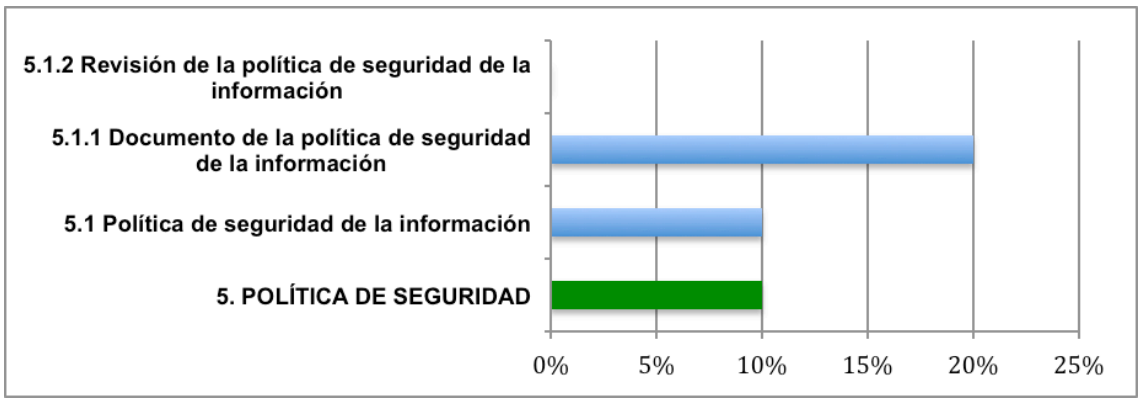
11.4.6 Control de la conexión a la red	60%
11.4.7 Control de encaminamiento a la red	80%
11.5 Control de acceso al sistema operativo	**28%**
11.5.1 Procedimientos seguros de inicio de sesión	30%
11.5.2 Identificación y autenticación de usuario	90%
11.5.3 Sistema de gestión de contraseñas	10%
11.5.4 Uso de los recursos del sistema	10%
11.5.5 Desconexión automática de la sesión	20%
11.5.6 Limitación del tiempo de conexión	10%
11.6 Control de acceso a las aplicaciones y a la información	**55%**
11.6.1 Restricción del acceso a la información	30%
11.6.2 Aislamiento de sistemas sensibles	80%
11.7 Ordenadores portátiles y teletrabajo	**15%**
11.7.1 Ordenadores portátiles y comunicaciones móviles	10%
11.7.2 Teletrabajo	20%
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**25%**
12.1 Requisitos de seguridad de los sistemas de información	**20%**
12.1.1 Análisis y especificación de los requisitos de seguridad	20%
12.2 Tratamiento correcto de las aplicaciones	**42%**
12.2.1 Validación de los datos de entrada	30%
12.2.2 Control del procesamiento interno	30%
12.2.3 Integridad de los mensajes	20%
12.2.4 Validación de los datos de salida	90%
12.3 Controles criptográficos	**10%**
12.3.1 Política de uso de los controles criptográficos	10%
12.3.2 Gestión de claves	10%
12.4 Seguridad de los archivos de sistema	**16%**
12.4.1 Control del software en explotación	20%
12.4.2 Protección de los datos de prueba del sistema	10%
12.4.3 Control de acceso al código fuente de los programas	20%
12.5 Seguridad en los procesos de desarrollo y soporte	**22%**
12.5.1 Procedimientos de control de cambios	10%
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el SO	20%
12.5.3 Restricciones a los cambios en los paquetes de software	20%
12.5.4 Fugas de información	40%
12.5.5 Externalización del desarrollo de software	
12.6 Gestión de la vulnerabilidad técnica	**40%**
12.6.1 Control de las vulnerabilidades técnicas	40%
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**70%**
13.1 Notificación de eventos y puntos débiles de seguridad de la información	**80%**
13.1.1 Notificación de los eventos de seguridad de la información	90%
13.1.2 Notificación de puntos débiles de seguridad	70%
13.2 Gestión de incidentes y mejoras de seguridad de la información	**63%**
13.2.1 Responsabilidades y procedimientos	50%

13.2.2 Aprendizaje de los incidentes de seguridad de la información	70%
13.2.3 Recopilación de evidencias	70%
14. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	**30%**
14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocio	**30%**
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de negocio	40%
14.1.2 Continuidad del negocio y evaluación de riesgos	20%
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	50%
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	20%
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad	15%
15. CUMPLIMIENTO	**30%**
15.1 Cumplimiento de los requisitos legales	**62%**
15.1.1 Identificación de la legislación aplicable	90%
15.1.2 Derechos de propiedad intelectual (DPI)	80%
15.1.3 Protección de los documentos de la organización	70%
15.1.4 Protección de datos y privacidad de la información de carácter personal	80%
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	40%
15.1.6 Regulación de los controles criptográficos	10%
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	**15%**
15.2.1 Cumplimiento de las políticas y normas de seguridad	10%
15.2.2 Comprobación del cumplimiento técnico	20%
15.3 Consideraciones sobre las auditorías de los sistemas de la información	**10%**
15.3.1 Controles de auditoría de los sistemas de información	10%
15.3.2 Protección de las herramientas de auditoría de los sistemas de la información	10%

3.5.5 Presentación de resultados

En este apartado se presentan los resultados del análisis de madurez anteriormente especificado. Para ello, la mejor manera de ver los resultados es analizando los resultados por dominio, de manera que se pueda ver claramente los diferentes controles de cada dominio el estado que presentan de forma gráfica.

5. Política de seguridad



Tal como se puede ver en el gráfico de barras, no existe una política de seguridad bien definida en general en ningún aspecto. Al no existir una política de seguridad formal y completa en la organización, tampoco existe una revisión sobre ella, por lo que este dominio de la ISO/IEC 27002:2005 sería uno de los objetivos a mejorar, primeramente creando una política de seguridad adecuada para la organización y seguidamente estableciendo unos periodos de revisión de la misma para actualizarla de manera paralela a los cambios que pueda ir sufriendo la organización.

Como principales puntos a destacar por parte de la política de seguridad, esta debería:

- establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. La gerencia debería aprobar, publicar y comunicar a todos los empleados en la forma adecuada, un documento de política de seguridad de la información.

- El otro objetivo principal de la política es llevar un control, revisándola a intervalos previamente definidos y planificados o, en caso de cambios significantes, con el fin de asegurar su uso continuo, adecuación y efectividad.

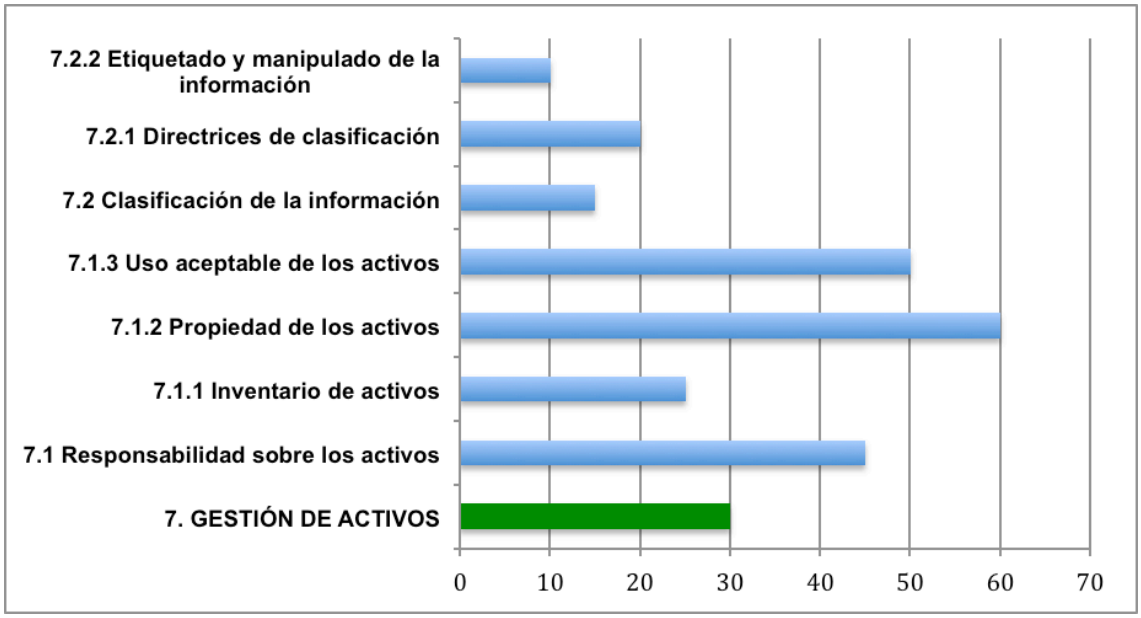
6. Aspectos organizativos de la seguridad de la información

En cuanto a los aspectos organizativos de la información se podría decir que es un dominio de contrastes, ya que hay controles que se encuentran muy bien implementados y otros en cambio están por trabajar. En cuanto a los que están con buenos porcentajes, tienen su razón de ser en el que la organización tiene algunos servicios que los gestiona y coordina UPC, que es de quien depende y por tanto. En cambio otros como la revisión independiente de la seguridad, simplemente no se realiza ya que no existe ningún procedimiento de auditoría, ni de gestión de continuidad de negocio, mantenimiento de sistemas e información, etc que pueda ayudar a asegurar la información y llevar mejor gestión sobre ella. La asignación de responsabilidades entre otros, también está en ni nivel bastante bajo, lo que puede repercutir en muchos otros controles.

Por tanto, en la organización interna se deberían establecer estructuras de gestión adecuadas para iniciar y controlar la implementación de la seguridad de la información dentro de la empresa. Para llevar a cabo este punto, se han de asignar roles y perfiles con el fin de definir responsables en la gestión de la información. Esta tarea recaería sobre el *comité de seguridad* de la información. Otra tarea del comité de seguridad de la información sería la de realizar un seguimiento continuo para supervisar la elaboración del plan y seguir un plan de mejora

En cuanto a los subdominios puede verse como la organización interna está ligeramente a mejor nivel que no la de terceros, sin embargo, ninguna de las dos está por encima del 50% del nivel, lo que deja bastante margen de mejora en este dominio.

7. Gestión de activos

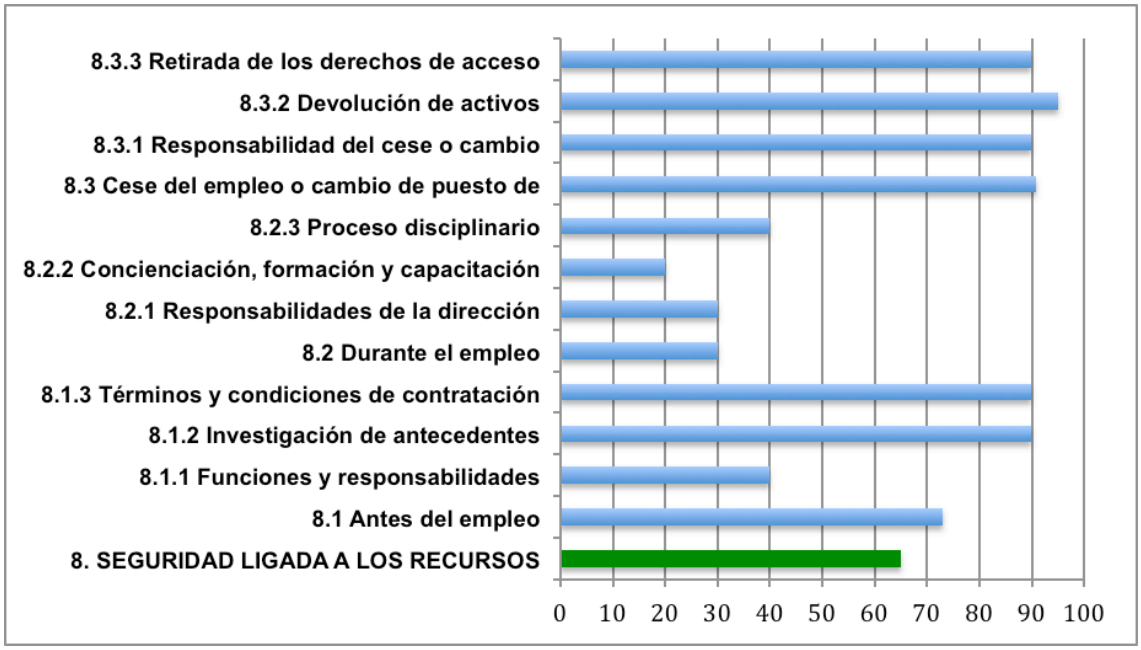


La gestión de activos no obtiene buenos resultados a nivel general, por tanto, la organización ha de intentar enfocar sus esfuerzos en realizar una gestión de los activos más importante de manera que se intenten alcanzar niveles aceptables. La media de los valores de los diferentes controles es de un 30% lo que es un resultado muy pobre como para no poner remedio en todas las líneas en general. El único control que está por encima del 50% sería la propiedad de los activos, sin embargo, también está lejos de niveles óptimos.

Uno de los mecanismos de ejecución detallados en el plan director era la de obtener información de los activos críticos mediante entrevistas y consultas directamente con los trabajadores de la compañía.

De la información obtenida, se debería obtener una clasificación en función del valor, requisitos legales, sensibilidad y criticidad para la compañía. El nivel de protección de la información puede ser determinado analizando la confidencialidad, integridad y disponibilidad, entre otros requisitos, para la información considerada.

8. Seguridad ligada a los recursos humanos



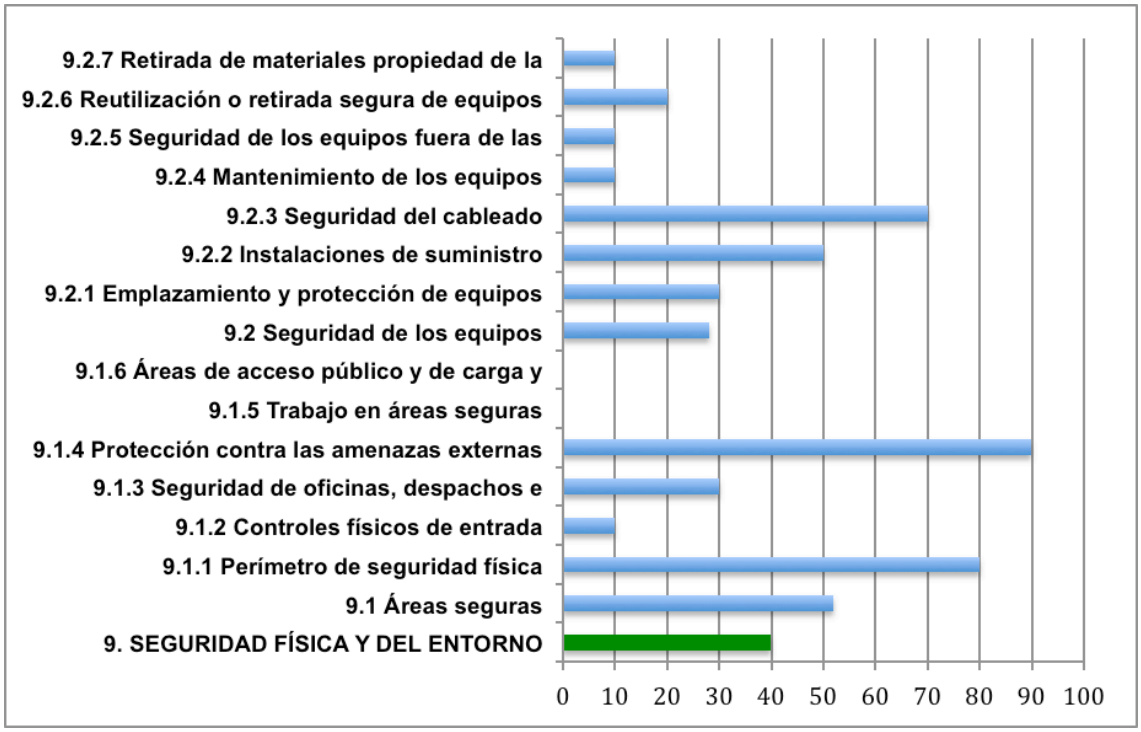
La seguridad de los recursos humanos está en líneas generales por encima del 50% del nivel total, lo que es un nivel aceptable pero no suficiente como para no invertir esfuerzos en mejorar este apartado. Que este dominio tenga mejores niveles en general en todas las líneas (salvo en algunas) es debido a que UPC gestiona parte de los recursos humanos en colaboración con la empresa. Sin embargo, existen controles donde la organización tiene deficiencias que hacen que no en líneas generales penalice el resultado final. Estos controles están relacionados con las responsabilidades, roles y gestiones que debería tener cada trabajador de la organización, así como formación o procedimientos de control, disciplinarios que ayuden a mejorar la seguridad de los recursos humanos.

Actualmente no se recibe ningún tipo de formación o entrenamiento en términos de conocimiento y actuaciones regulares en políticas y procedimientos organizacionales relevantes en su función. Esta formación debería empezar con una inducción formal del proceso designado para introducir la política de seguridad de la compañía y las expectativas.

Otro punto a definir son los procesos disciplinarios para empleados que cometan aperturas en la seguridad, asegurándose que se reciba un correcto y justo tratamiento de los empleados por los hechos ocurridos y que han provocado dicha apertura.

Se puede observar como entre los dos grandes subdominios, el correspondiente a los controles ligados a antes del empleo y el cese del mismo, están mejor valorados que durante el empleo, el cual por motivos de responsabilidades y procedimientos no está bien definido y hace que descienda la media notablemente.

9. Seguridad física y del entorno



Hay que destacar que la organización está ubicada en un espacio alquilado compartido por otras empresas con sus respectivas oficinas, con lo que ciertos servicios como el de la seguridad medioambiental o las paredes corren a cargo también del propietario del espacio. Por este motivo la protección contra amenazas externas o el perímetro de seguridad física o el cableado tienen las características necesarias para tener valores cercanos al óptimo. Sin embargo, la empresa se ve penalizada en otros en la mayoría del resto de aspectos y que será principalmente donde concentrar las fuerzas para mejorar los niveles presentados.

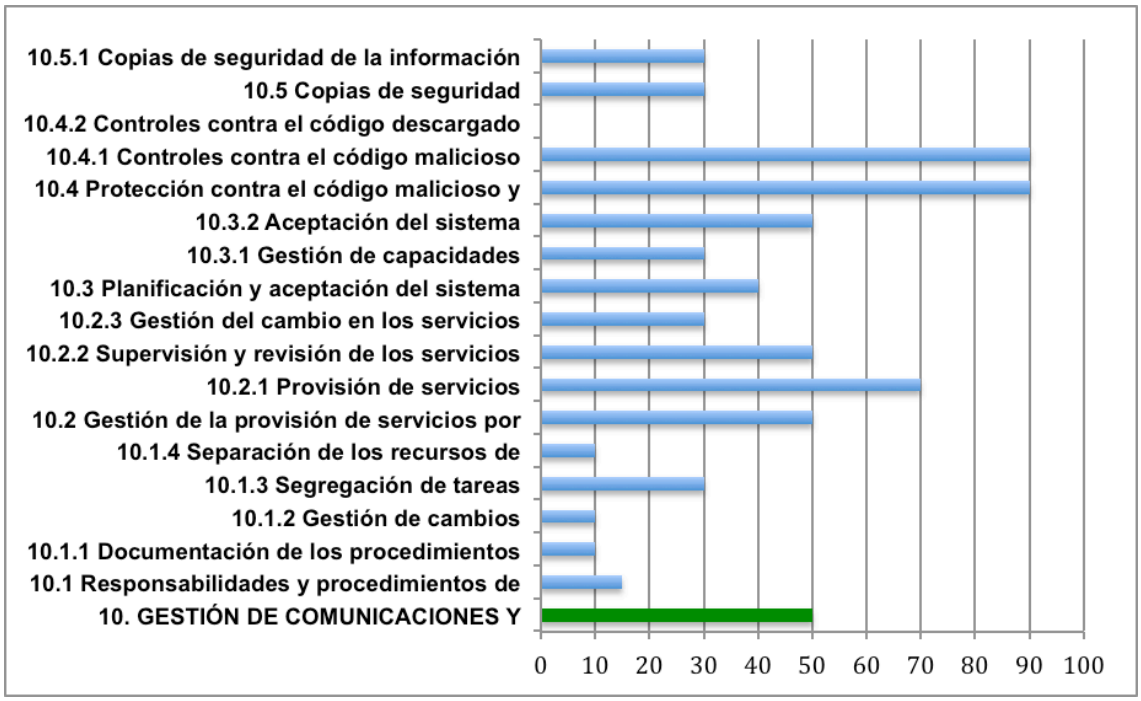
De esta ecuación no se ha tenido en cuenta las áreas de acceso público o el trabajo en áreas seguras ya que no aplica y por tanto su cálculo está fuera del resultado, de todas formas se ha mantenido el control en el gráfico.

En cuanto a la seguridad de los equipos fuera de la compañía, no se contempla esta posibilidad ya que no es posible extraer material fuera de ella y los ordenadores que se desechan se realiza a través de la Universidad Politécnica de Cataluña que tiene un servicio para ello, por lo tanto, en este apartado haría falta formalizar el procedimiento y ponerlo en conocimiento de los trabajadores de la organización informando que es un servicio que se puede realizar a través de un tercero, aún y así debe reforzarse este control.

En cuanto a los subdominios, se puede apreciar como las áreas seguras tienen mejores resultados que la seguridad de los equipos, los cuales están por debajo del 30%.

10. Gestión de las comunicaciones y operaciones

Este dominio se ha divido en dos gráficos ya que era demasiado grande para analizarlo en uno solo y de esta forma se puede ver de forma más clara.



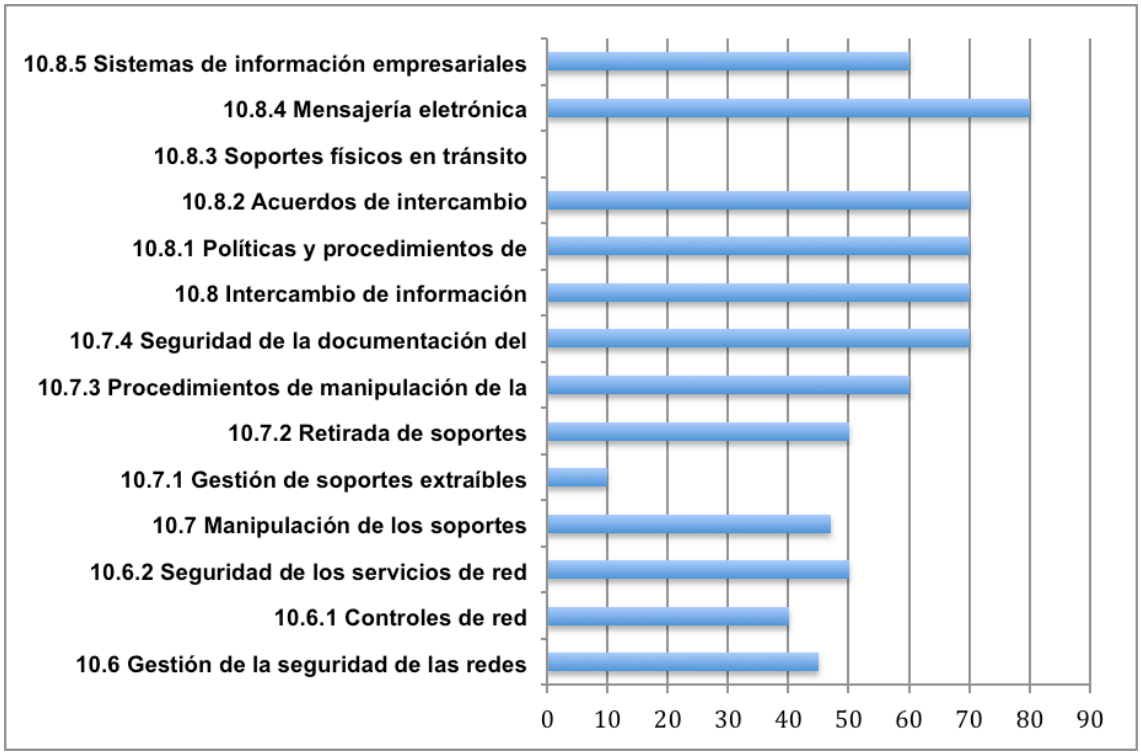
Actualmente, cada responsable de cada área es responsable de su área únicamente y por encima de estos el director general, pero no existe ningún documento dónde se detalle la función de cada sección ni determine responsabilidades en algún aspecto o actuación en caso de incidente de seguridad.

Se puede ver como hay valores dispares, algunos controles están en valores óptimos y en cambio otros están prácticamente sin haberse tenido en cuenta. Este fuerte contraste es el que hace que el valor general del dominio no se encuentre más allá del 50%.

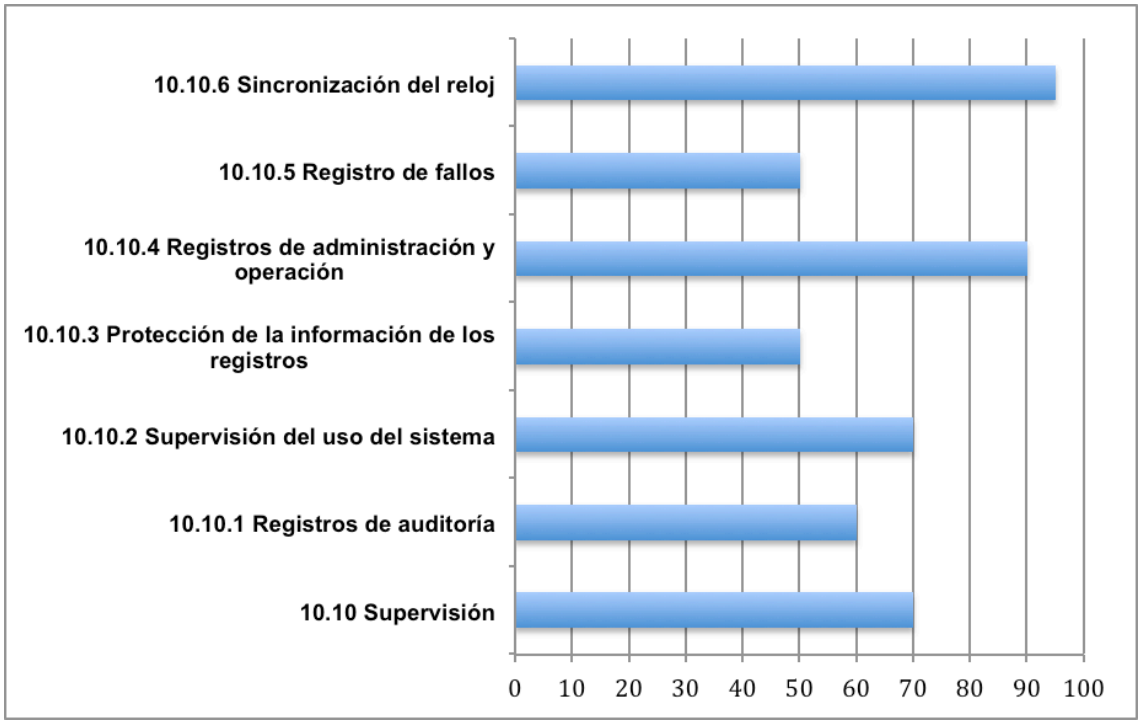
Se puede ver como controles importantes como la definición de responsabilidades o documentación de procedimientos o las copias de seguridad, están muy por debajo de valores aceptables.

Uno de los puntos más sensibles a tener en cuenta y que actualmente no se realiza con un control o planificación adecuado y periódico y donde no existe documentación formal, actualizada ni con unas pautas y procedimientos revisados al respecto, son las copias de seguridad de toda la información esencial del negocio y que esta pueda recuperarse tras un desastre o fallo de los medios. También debería estar documentado el procedimiento de copia de respaldo así como su recuperación y también el de uso adecuado de los medios de información.

La compañía, hoy por hoy, no monitoriza ningún tipo de tráfico que salga de la red que tiene asignada, ni tiene ningún control de los accesos que realizan sus empleados en la red. La UPC es la que gestiona la red y las comunicaciones, sin embargo sí que debería implementar controles que detecten y protejan la entrada de intrusiones en primera instancia.

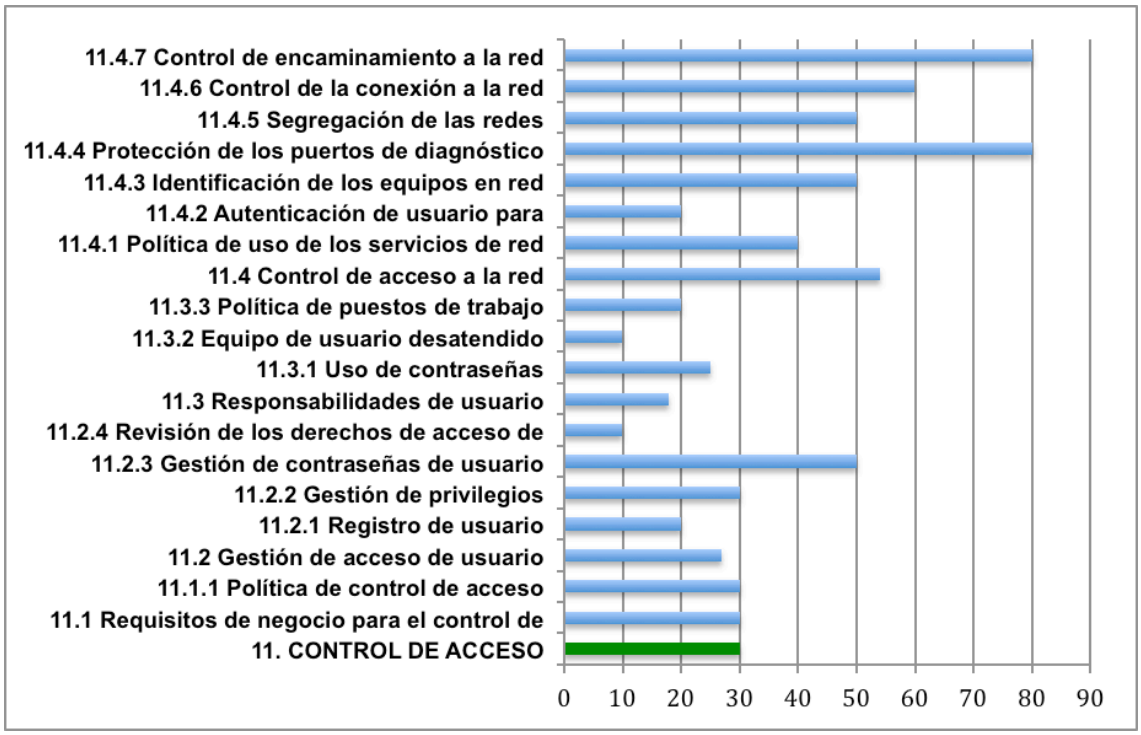


Los siguientes controles del mismo dominio parecen más homogéneos en cuanto a resultados, excepto ciertos controles de red que hacen que disminuya la media en general un poco ya que se encuentran por debajo del 50%. Los controles que no tienen porcentaje en este momento es porque no aplica y por tanto, también se ha sacado de la ecuación y los resultados.



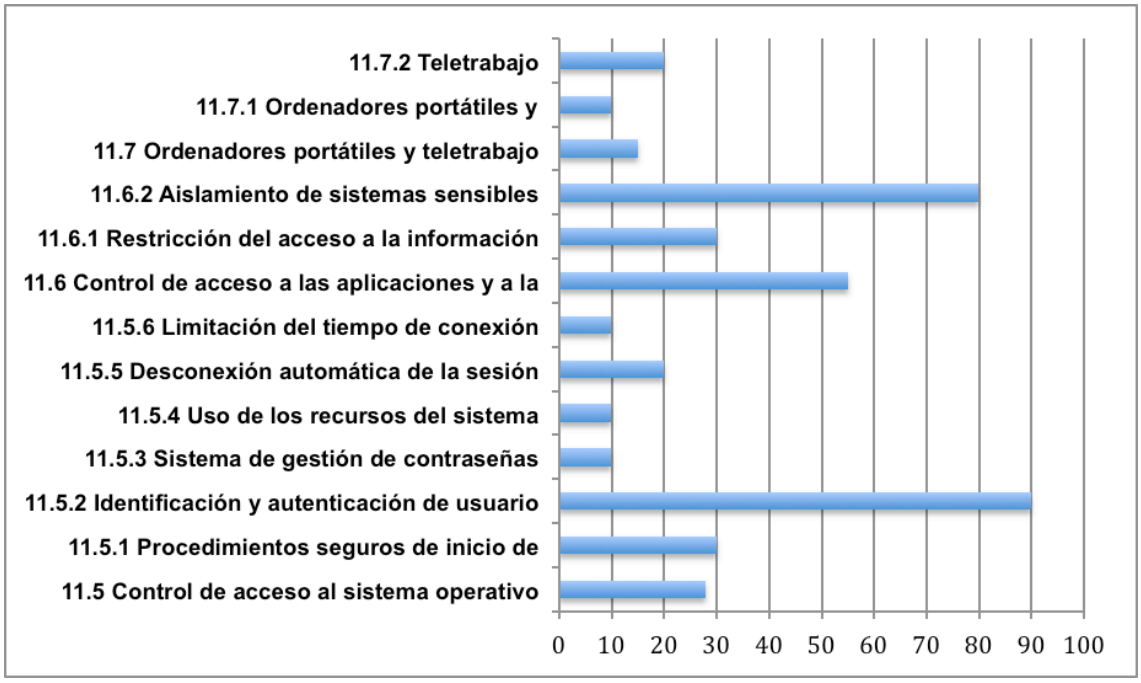
Los últimos controles del dominio 10 de la ISO parecen estar más parejos entre ellos y todos por encima del 50%, por lo que a priori estos no serían los principales controles en los que concentrar nuestros esfuerzos para mejorar la seguridad de la información.

11. Controles de acceso



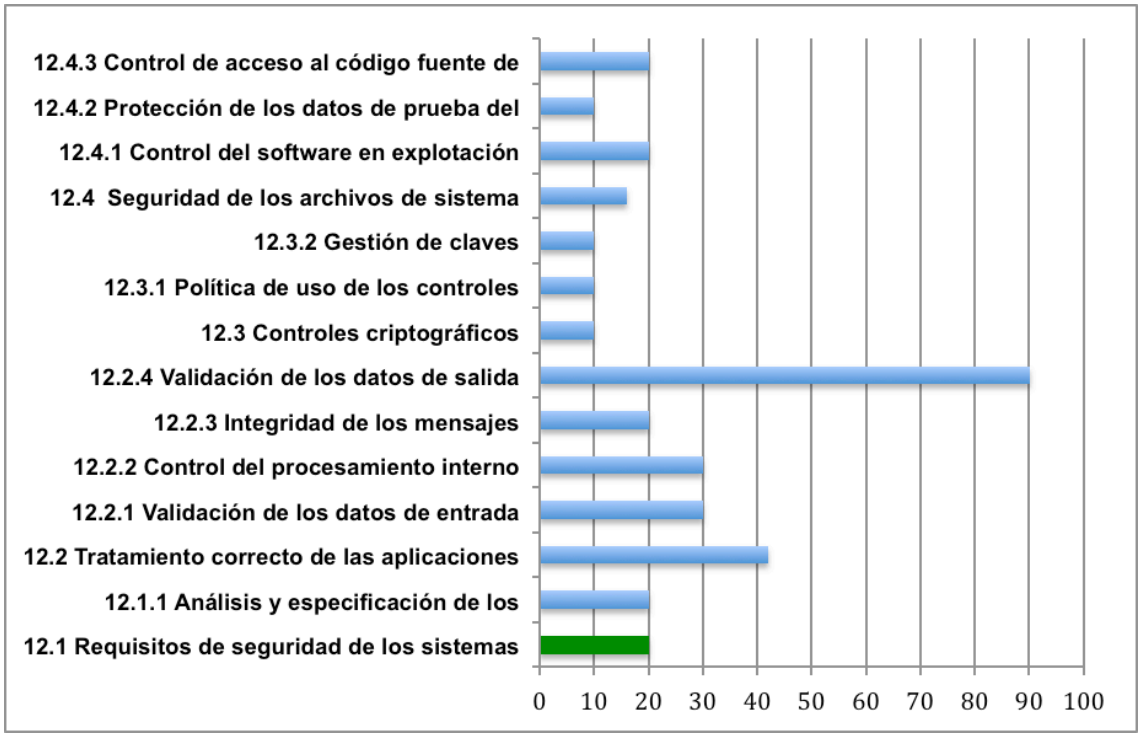
Tal como se aprecia en el gráfico, la media total del dominio es del 30%, por lo que el nivel de los controles no son aceptables y en general lejos del nivel óptimo que requeriría la organización. Algunos controles sí que están cerca de los niveles óptimos debido a que son controles donde UPC ayuda a la gestión y control de los mismos, por tanto la responsabilidad es compartida y se nota que se recibe soporte especializado en algunos puntos.

En cuanto a la responsabilidad de los usuarios y compromiso de estos ante el buen mantenimiento y eficacia de las medidas de control y donde no existe ningún procedimiento ni documentación formal, actualizado y revisado periódicamente al respecto, por tanto es otro punto a implementar. Este procedimiento debería documentar pautas de los empleados como mantener el escritorio limpio, no permitir el acceso no autorizado a su zona de trabajo, una política de contraseñas robusta, no acceder a redes o sitios maliciosos que puedan comprometer los activos o información sensible.



En los siguientes controles del mismo dominio se aprecia aún más el contraste entre los controles donde UPC presta soporte y en cuales no. En concreto la identificación y autenticación del usuario se utiliza el sistema de acceso de UPC en primera instancia, para acceder a los servicios. Sin embargo es responsabilidad a posterior, de la organización el gestionar el buen uso de estos accesos.

12. Adquisición, desarrollo y mantenimiento de sistemas de información

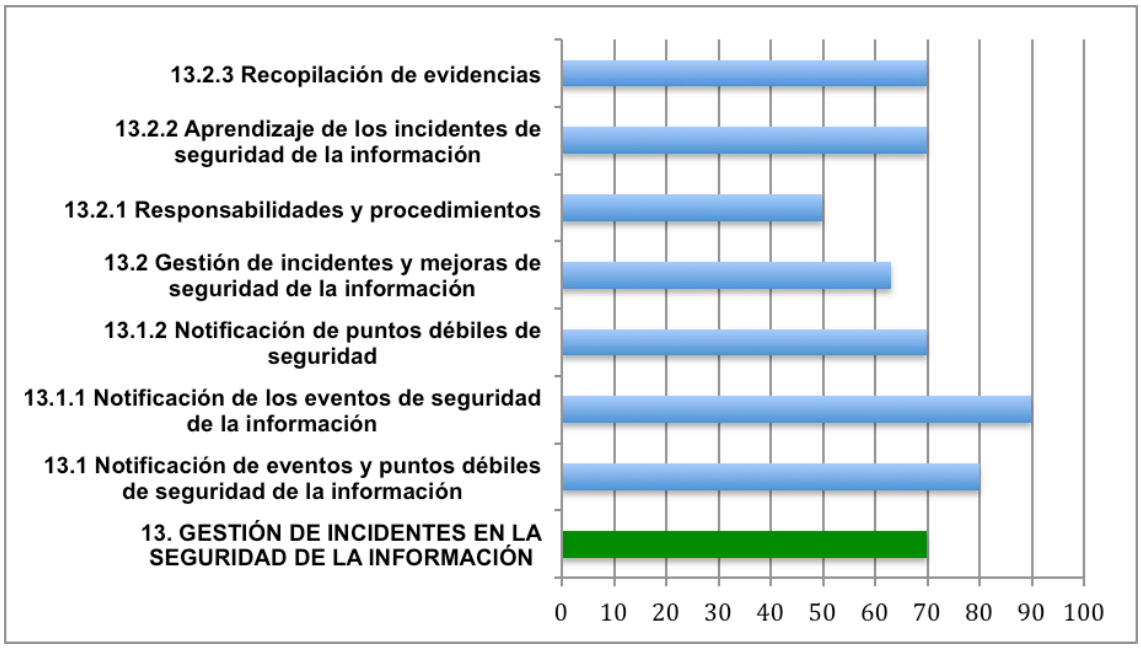


En este dominio destaca por tener unos niveles en general muy bajos, ya que carece la organización de ningún tipo de procedimiento de buenas prácticas o seguimiento a la hora de llevar a cabo los servicios, sin embargo, uno de los controles sí que está en niveles óptimos.

Esto es debido que los datos de salida que se ven devueltos al usuario son verificados de forma exhaustiva con el fin de comprobar que sean correctos, ya que parte de las principales líneas de negocio de la organización son aplicaciones web de consulta, por tanto, sería de vital importancia que las consultas devueltas sean correctas. Sin embargo, en el resto de controles cabe una mejora importante en cuanto a seguridad de la información se refiere.

Otro punto a mejorar e implantar en el sistema de la compañía es la de asegurar la seguridad de los archivos del sistema, donde deberían existir procedimientos para controlar la instalación de software en sistemas operacionales o tener un procedimiento bien detallado y control sobre los datos de prueba, donde estos deben ser seleccionados, protegidos y controlados cuidadosamente. También hay que tener especial atención y cuidado con los accesos al código fuente de los programas para evitar los cambios no intencionales o de empleados que no tienen privilegios para ello.

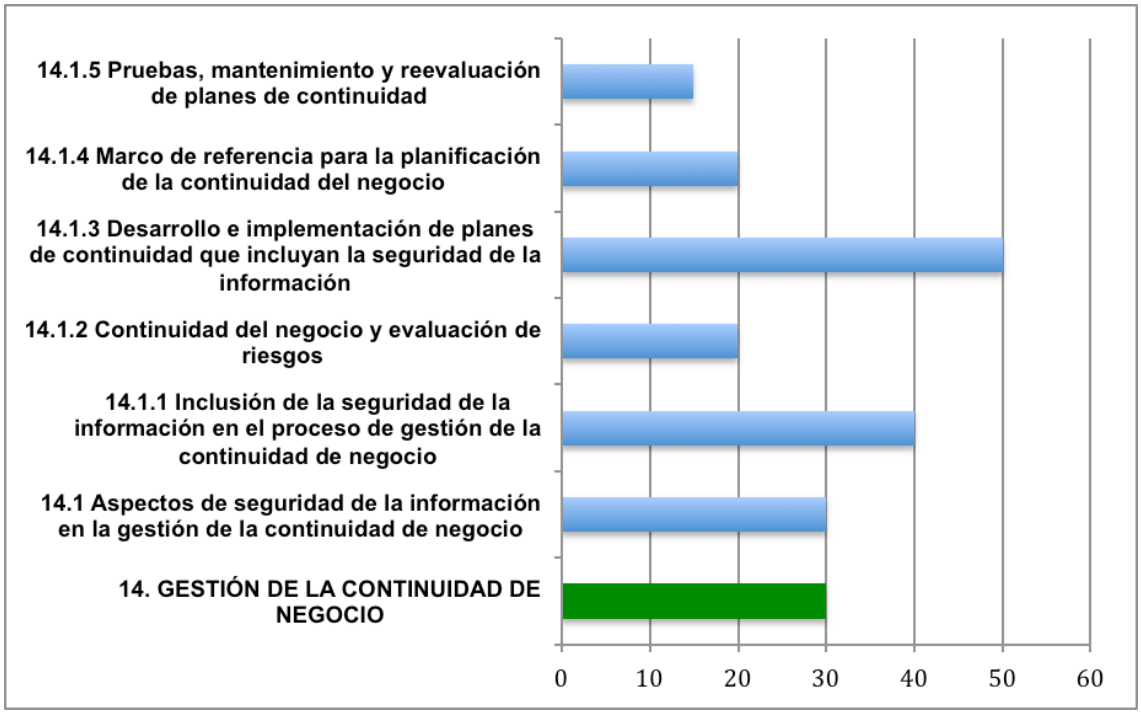
13. Gestión de incidentes



Tal como se puede ver en el gráfico, el dominio 13 está bastante compensado con buenos niveles en todos los controles de forma general. Esto tiene su explicación en que estos controles están relacionados con soporte que obtiene la empresa por parte de la UPC en la respuesta de incidentes, con lo que todos los controles están ciertamente en mejor estado que en la gran mayoría del resto de dominios.

De igual forma, para mantener y asegurar una efectiva y sólida respuesta de los incidentes debe establecerse un sistema de responsabilidades y procedimientos. También se ha de cuantificar mediante algún mecanismo eficiente, el costo de los incidentes en la seguridad de la información.

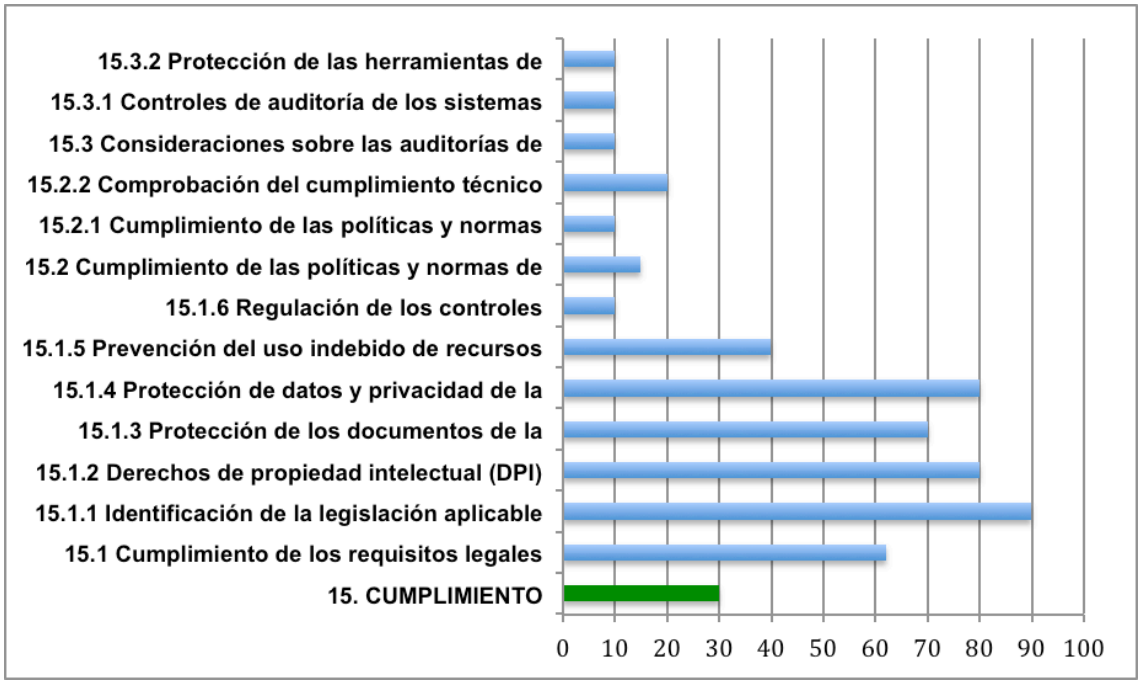
14. Gestión de la continuidad de negocio



A diferencia del dominio anterior, este se encuentra a niveles muy bajos en líneas generales, donde el control que mejor estado presenta únicamente llega al 50% del nivel, resultando el global en un 30%. No existe ningún control o controles que devalúen o descompensen algún control en general, sino que todos están en general muy por debajo del nivel deseado, por tanto, la organización deberá centrar sus esfuerzos en reforzar planes y procedimientos relacionados con la continuidad de negocio en caso de incidente.

Es de vital importancia que la compañía implemente, ya que no dispone de ello, de un procedimiento de gestión de continuidad del negocio para reducir a niveles asumibles la interrupción causada por desastres y fallas de seguridad mediante controles preventivos y de recuperación. Para esto, la compañía ha de identificar los procesos críticos de negocio (analizados en puntos anteriores) e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, …

15. Cumplimiento

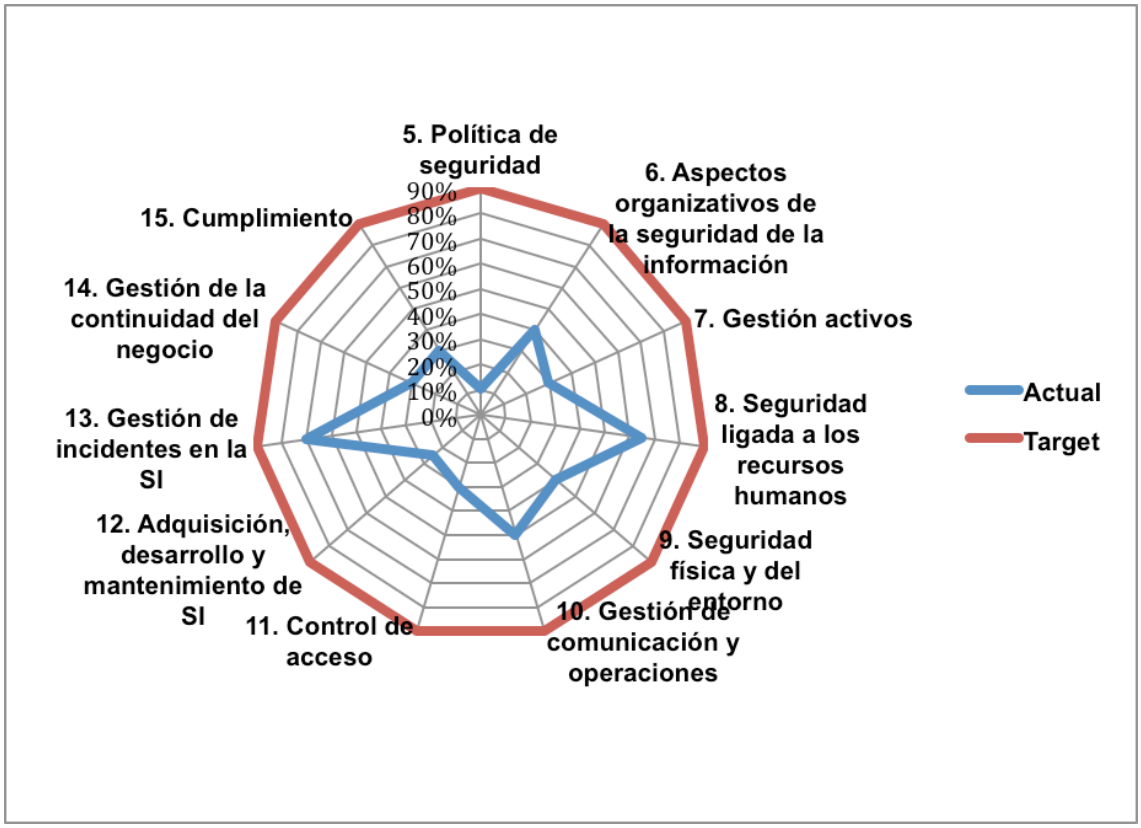


En cuanto al cumplimiento, se puede observar que hay controles que están en muy buenos niveles, incluso en estado óptimo, sin embargo el nivel medio del dominio es del 30%. Esto es debido a que existen controles que están en muy mal estado, contrarrestando los controles que están en nivel óptimo.

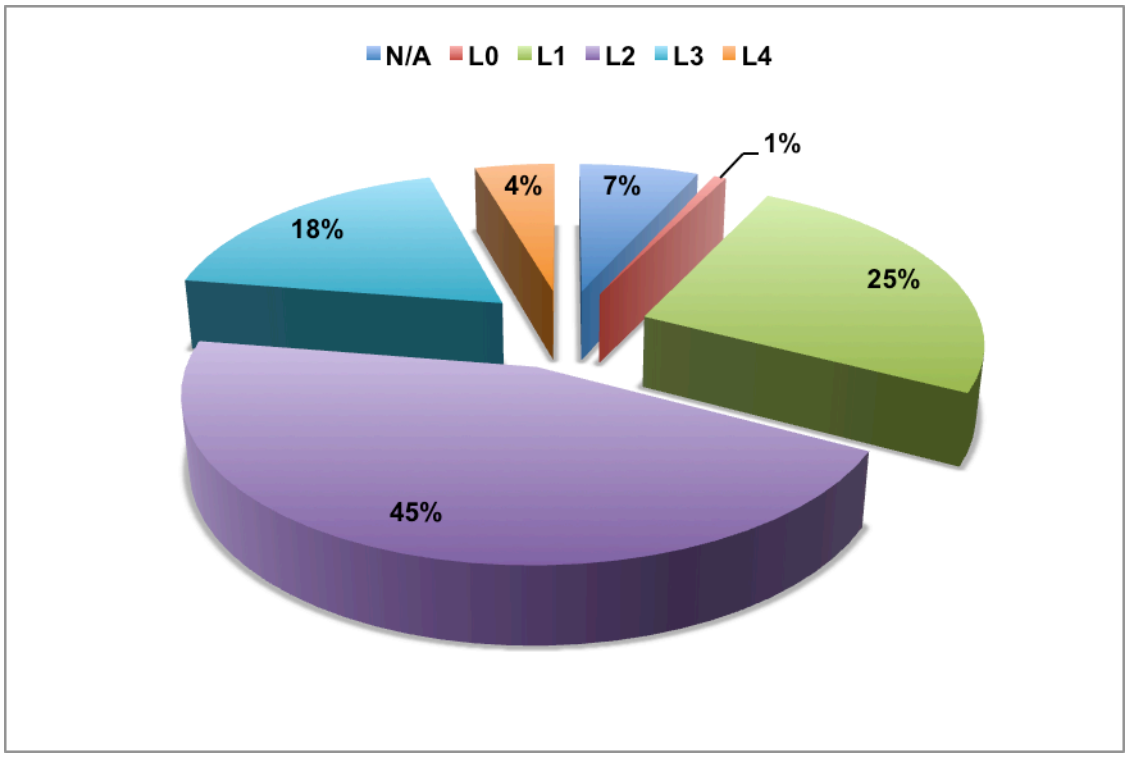
Es contrastable el estado del subdominio 15.1 que hace referencia a los requisitos legales, con el 15.2 que hace referencia al cumplimiento de las políticas y normas de seguridad, donde esta está muy por debajo de la primera, dejando patente que la organización tiene mejores niveles en cuanto a requisitos legales que en cuanto a las políticas y normas técnicas de seguridad de la información.

Debido a que la compañía pertenece al ámbito de la Universidad Politécnica de Cataluña, dispone del asesoramiento sobre requisitos legales específicos por parte de esta y que pone a su disposición en caso de necesitarse, a parte de ofrecer el soporte adecuado en estos temas.

Gráfico radial de los diferentes niveles de los dominios de la ISO 27002:2005



En porcentajes respecto a los diferentes niveles de madurez de la capacidad (CMM), los controles de que dispone la empresa tienen la siguiente distribución:



Se puede observar en términos generales, como el nivel de madurez predominante es el L2, correspondiente a niveles Reproducibles pero intuitivos, lo que significa por definición:

- Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea.

- Se normalizan las “buenas prácticas” a base de experiencia y método.

- No hay comunicación o entretenimiento formal, las responsabilidades quedan a cargo de cada individuo.

- Se depende del grado de conocimiento de cada individuo.

Lo que significa que no existen modelos formales o estándares que puedan adoptar los trabajadores para resolver y trabajar todos de la misma manera, de manera que los resultados no son eficientes, ya que se deja todo bajo la responsabilidad del buen hacer del trabajador.

Preocupante para la organización es también que el nivel L1 sea el segundo con más porcentajes en el análisis, lo que implica que la empresa dispone de pocos controles en niveles aceptables para mantener y asegurar la seguridad de la información. Sería deseable aumentar los niveles de los controles que se encuentran tanto en L2 como en L1, al menos hasta niveles de madurez correspondientes a L3.

L3 y L4 serían los niveles más deseables, pero también los más escasos en la organización, ya que ni sumándolos alcanzan el nivel de los controles que se encuentran en un estado L1 de madurez.

Por tanto, los esfuerzos de la organización deben ir enfocados a mejorar estos niveles de madurez de modo que la mayoría de ellos se encuentren en niveles óptimos, minimizando o reduciendo prácticamente a 0 el número de controles que se encuentren en niveles L1 y los de L2 lo máximo que sea posible. Para ello será necesario realizar los análisis de riesgos pertinentes y crear los proyectos necesarios para corregir las desviaciones que nos arrojen los resultados de los análisis.

3.6 Propuestas de proyectos

3.6.1 Introducción

Una vez realizado el análisis de riesgos y obtenido las amenazas, impacto y riesgo en nuestros activos, se dispone de un conocimiento más amplio y exacto del estado de la organización. No obstante, uno de los objetivos primordiales es reducir el riesgo existente en la organización y mitigando el impacto de las amenazas hasta conseguir el estado de cumplimiento de madurez óptimo de los diferentes dominios indicados en la ISO.

Por tanto, en este nivel se plantean diferentes propuestas de proyectos que pueden ayudar a conseguir este nivel óptimo que se persigue en toda organización. La consecución de estos objetivos está pensada para que se realice en los próximos **3 años**.

También se ha tenido en cuenta no realizar un excesivo número de proyectos ya que la empresa es pequeña, con poco personal y recursos, por lo que se ha intentado hacer algo realista dado el número de personas cualificadas que podrían dedicar tiempo a los proyectos sin desatender totalmente los servicios habituales ofrecidos.

3.6.2 Propuestas

En este apartado se describen las propuestas de proyectos que podrían ayudar a mitigar en lo máximo de lo posible el riesgo actual de la organización y evolucionar hacia el cumplimiento de la ISO hasta niveles adecuados.

Los proyectos planteados serán los resultantes de agrupar un conjunto de recomendaciones identificadas, en la fase de análisis de riesgos, para facilitar su ejecución. Se incidirá no únicamente en la mejora de la gestión de la seguridad, sino también en posibles beneficios colaterales como pueden ser la optimización de recursos, mejora de la gestión de procesos y tecnologías presentes en la organización.

Se ha procedido a realizar “fichas” de proyectos donde se especifica un identificador para cada proyecto, el nombre y el ámbito al que pertenece (si es documentación, gestión, un proyecto de control, implementación de alguna tecnología, etc.). Se realiza una pequeña descripción del proyecto escogido, así como los objetivos o mejoras que puede aportar a la organización.

También se detalla qué dominio de la ISO 27000 está relacionado con el control detallado a forma de intentar llevar cierto control sobre los diferentes aspectos de la seguridad que se intentan mitigar. Únicamente se ha detallado el control de la ISO que más relacionado está directamente con el proyecto en cuestión, sin embargo, otros proyectos podrían afectar indirectamente o en menor medida a un determinado control.

Como complemento, los controles están relacionados con unos activos que se ven afectados por estos, de manera que, según el análisis de riesgos realizado en apartados anteriores, se especifica qué grupo de activos se ven favorecidos por la salvaguarda aplicada, es decir, si existe mejora por parte del proyecto en los riesgos detectados en el análisis de riesgos anterior.

Para el cálculo del coste que supondría un proyecto, se ha procedido a sumar los costes que tendría por un lado la mano de obra de los empleados que realizarán el proyecto, así como, en caso de que fuera necesario, el coste del hardware o soluciones privadas de software requeridas para llevar a cabo el proyecto. Los empleados que realizan dichos proyectos no están a horario completo en todos los proyectos, sino que dedican tiempo de su jornada a realizar este proyecto mientras realizan las tareas propias de su trabajo.

A continuación se presentan las fichas de los proyectos que deberían implementarse para mejorar la seguridad de la información de la organización.

ID:	**DOC001**
Nombre Propuesta:	**Política de seguridad**
Ámbito:	**Documentación**
Detalles	

Descripción

Es necesario la creación y formalización de un documento de seguridad donde se especifiquen y detallen los requisitos que debe seguir la organización conjuntamente con la normativa de seguridad vigente española para la gestión de los datos de carácter confidencial, para conseguir preservar la confidencialidad, integridad y disponibilidad de los recursos de la organización.

Este documento será de obligado cumplimiento y deberá estar al alcance de cualquier trabajador de la empresa, ya que en el se especifican las pautas a seguir para preservar la seguridad de los datos y recursos de la organización.

Este documento deberá revisarse y actualizarse periódicamente para adecuarse a los cambios que puedan surgir en la organización.

Controles / Objetivos:

- Creación y mantenimiento de una política de seguridad de los sistemas de información actualizada.
- Adecuación a la legislación española vigente para la gestión de datos de carácter confidencial.
- Formalización de procesos y gestión de los usuarios sobre los recursos de la organización, como:
    - Controles de acceso adecuados al rol del usuario.
    - Procedimientos de seguridad claramente definido.
    - Roles especificados y detallados para la gestión de la información, etc.
    - Responsabilidades de los trabajadores.
- Concienciación del usuario sobre temas de seguridad de la información.
- Reducción del riesgo por desconocimiento de los controles o respuesta a incidentes.
- Buenas prácticas por parte de los usuarios.
- Grado de despliegue y adopción de la política en la organización.

Dominio ISO relacionado	5.1 Política de seguridad
Activos del AARR afectados	El conjunto de todos los activos de la organización
Tiempo estimado	3 meses / borrador – 6 meses / primera versión
Coste	

Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Coste total	5.500 €

ID:	**D0C002**
Nombre Propuesta:	**Documento del plan de continuidad de negocio (BCP)**
Ámbito:	**Documentación**
Detalles	

Descripción

Es necesario la creación y formalización de un documento que garantice la continuidad de negocio, juntamente con el seguimiento del mismo apoyado de pruebas periódicas por parte de las partes que lo integran.

Este plan de continuidad de negocio surge a partir del análisis de riesgos y por parte del comité de seguridad para gestionar la situación en caso de que se materialicen las amenazas sobre los activos de la organización y, mas en concreto, en aquellos activos que son más importantes para la continuidad del negocio.

El plan sufrirá un seguimiento continuo por parte de las partes implicadas para evolucionar y poner en práctica el plan para afrontar de manera óptima las posibles amenazas que puedan surgir.

Controles / Objetivos:

- Elaboración y formalización de un plan de continuidad de negocio.
- Evolución y seguimiento de dicho plan.
- Preparación adecuada de respuesta en caso de incidente.
- Personal preparado y con conocimiento para gestionar posibles incidentes producidos por amenazas en la organización.
- Minimización del impacto de las amenazas.
- Conocimiento del riesgo al que están expuestos los recursos de la organización.
- Anticipación ante una situación adversa o crítica que pueda surgir en la organización.
- Porcentajes de unidades organizativas con planes de continuidad en cada una de las fases del ciclo de vida.

Dominio ISO relacionado	14.1 Aspectos de la gestión de continuidad de negocio
Activos del AARR afectados	El conjunto de todos los activos de la organización
Tiempo	6 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Coste total	6.000 €

ID:	**DOC003**
Nombre Propuesta:	**Documento mantenimiento de sistemas**
Ámbito:	**Documentación**
Detalles	

Descripción

Es necesario definir una serie de documentos donde se especifique, las necesidades y objetivos de llevar a cabo una serie de buenas practicas en cuanto al funcionamiento y mantenimiento de los sistemas de información, identificando e implantando regulaciones para el uso adecuado de la información y los activos asociados.

En estos documentos también debe especificarse el mantenimiento que es necesario realizar en los sistemas para que estos puedan ofrecer, durante su vida útil, el servicio para el que está orientado, así como las diferentes salvaguardas que son necesarias para mitigar ciertas amenazas.

Este documento, debe ser sometido a revisión de forma periódica para estar en consonancia con las actualizaciones que puedan surgir en la organización.

Controles / Objetivos:

- Elaboración de una guía de buenas prácticas para el correcto uso de los sistemas de información por parte del personal de la organización.
- Elaboración de histórico sobre los sistemas y su actualización.
- Listado de las salvaguardas necesarias para los activos.
- Documentación de los responsables de llevar a cabo este mantenimiento.
- Mejor gestión y previsión de posibles amenazas futuras.

Dominio ISO relacionado	7.1 Responsabilidad sobre los activos 9.2 Seguridad de los equipos
Activos del AARR afectados	El conjunto de todos los activos de la organización
Tiempo	3 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	3.500 €

ID:	**DOC004**
Nombre Propuesta:	**Listado de activos**
Ámbito:	**Documentación**
Detalles	

Descripción

Será necesario disponer de un listado de los activos de que dispone la organización, organizados según funcionalidad y ámbito al que corresponden. Junto con el listado, debería constar una descripción del activo, la función que desempeña, el ámbito al que hace referencia y el propietario, el cual será el responsable de su mantenimiento o responsable en caso de incidencia de actuar como esté definido en el documento de seguridad.

Esta lista de activos deberá someterse a revisión de forma periódica para incorporar los nuevos activos que se añaden al sistema o bien para actualizarlos en caso de que alguno deje de dar soporte.

Controles / Objetivo:

- Mantener una lista de los activos que forman el sistema de información.
- Clasificar los activos según el ámbito al que afectan, así como el responsable.
- Tener un listado de activos medible y analizable.

Dominio ISO relacionado	7.1 Responsabilidad sobre los activos
Activos del AARR afectados	Complemento de otros proyectos
Tiempo	1 mes
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	1.500 €

ID:	**PREV001**
Nombre Propuesta:	**Gestión de los Backup de los sistemas**
Ámbito:	**Prevención (Proactivo)**
Detalles	

Descripción

Para evitar la pérdida de datos en caso de incidente en la organización, será necesario realizar copias de seguridad de los sistemas de información. Para realizar esta tarea será necesario establecer una sería de buenas prácticas y una guía formalizada donde se especifique cómo realizar esta tarea y su periocidad, así como el lugar de almacenamiento de estas copias para que esté guardada en lugar seguro en caso de que el CPD sufriera un incidente.

Esta gestión de las copias de seguridad deberá tener un asignado un responsable encargado de mantener y gestionar las copias, así como de revisar la gestión de forma periódica para establecer los cambios que sean necesarios.

Controles / Objetivo:

- Con esto se intenta mitigar la pérdida de datos por materialización de alguna amenaza.
- Disponer de un procedimiento gestionado de copias de seguridad.
- Previsión de pérdida de información por mal uso de esta, materialización de amenaza o error humano.

Dominio ISO relacionado	10.5 Copias de seguridad
Activos del AARR afectados	Datos de la organización
Tiempo	2 meses
Coste	

Recurso	Horas de trabajo por parte del personal de la organización. Hardware. Soportes o servidores remotos para almacenar las copias.
Dedicación	Dedicación a tiempo completo por parte de los responsables
Cote total	4.000 €

ID:	**CON001**
Nombre Propuesta:	**Gestión de acceso al CPD**
Ámbito:	**Control de permisos**
Detalles	

Descripción

Es importante gestionar y controlar el acceso de los trabajadores al CPD, ya que es en este donde se controla toda la actividad de la organización y se gestionan los sistemas. Es por este motivo que se debe establecer una política y unas medidas de acceso a esta sala.

Actualmente el CPD no tiene medidas de acceso ni control alguno, por lo que se deberían tomar las medidas adecuadas para instalar un control de acceso físico que únicamente permita a las personas autorizadas su entrada a el. Por otra parte, también debería registrarse el acceso al CPD de manera que se pueda llevar un histórico de cuándo se accedió y quién accedió al CPD. La revisión de esta información, así como la revisión de las políticas de acceso al CPD, son importantes para mantener un control periódico con el fin de verificar que la gestión de accesos es la correcta.

Controles / Objetivos:

- Instalar un sistema de gestión de accesos físico que permita acceder al CPD únicamente a las personas con autorización el acceso.
- Gestionar un histórico de accesos para llevar el control del mismo.
- Aumento de la seguridad en la zona más crítica de los sistemas de la organización.
- Mayor control y seguridad de las personas que pueden acceder al CPD.
- Procedimientos y controles formalizados y claros.
- Identificar los intentos fallidos de acceso.
- Deshabilitar los accesos de las personas que se les retira la autorización.

Dominio ISO relacionado	9.1 Áreas seguras
Activos del AARR afectados	Acceso al CPD
Tiempo	6 meses
Coste	

Recurso	Horas de trabajo por parte del personal de la organización. Hardware. Dispositivos de lectura de accesos. Software. Plataforma de registro de accesos.
Dedicación	Dedicación parcial por parte del personal y responsables
Cote total	9.000 €

ID:	**CON002**
Nombre Propuesta:	**Gestión de roles, responsabilidades y accesos**
Ámbito:	**Control de permisos**
Detalles	

Descripción

Es necesario establecer una serie de roles según área de actuación del personal de la empresa para poder gestionar a posteriori los accesos a los recursos, de manera que estos puedan estar controlados y gestionados de manera más eficiente. La gestión de accesos en este caso está limitada a los recursos de la organización, de manera que no todos los trabajadores de la organización tengan los mismos privilegios sobre todos los recursos.

La gestión de roles, responsabilidades y accesos será de vital importancia a la hora de saber quién es el responsable de gestionar ciertos incidentes, proyectos o acciones en la organización a forma de garantizar una eficiente respuesta.

Será necesario someter a revisión periódica los controles de acceso para comprobar que estos se adecuan al nivel del empleado según esté autorizado y según la empresa vaya evolucionando.

Controles / Objetivo:

- Disminución de los riesgos por uso indebido de los recursos de la organización.
- Formalización de accesos según nivel de autorización de los empleados.
- Disminución de los riesgos de modificación de datos por errores o desconocimiento de los empleados.
- Control e histórico de los accesos de los usuarios según rol.
- Implantación de estructura de gestión para controlar e incitar la implantación de sistemas de la información.

Dominio ISO relacionado	6.1 Organización interna 11.1 Requisitos de negocio para el control de acceso 11.2 Gestión de accesos de usuario 11.6 Control de acceso a las aplicaciones y a la información 13 Gestión de incidentes
Activos del AARR afectados	Servicios, Aplicaciones, Software, Servidores y Datos.
Tiempo	4 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	4.200 €

ID:	PRO001
Nombre Propuesta:	Procedimiento de programación segura
Ámbito:	Procedimientos
Detalles	

Descripción

Es esencial desarrollar un procedimiento de programación segura para evitar errores en la programación y que estos surjan una vez el código se encuentra en producción, lo que facilitaría que atacantes remotos aprovecharan estos errores para provocar errores en el sistema o bien obtener datos confidenciales.

Estos procedimientos han de detallar una forma segura de programar, donde se contemplen diferentes entornos seguros en los que llevar a cabo la actividad sin que los sistemas se vean afectados ni los usuarios no autorizados tengan acceso a esta. De esta forma, una vez se ha desarrollado el software, este está en disposición de probarse y por último de ponerse en producción.

El objetivo de este procedimiento es el de dotar de una zona segura y controlada a los programadores de aplicaciones para que puedan desarrollar de forma segura sin afectar al software ni a los datos de la organización, a la vez que se mejora la puesta a punto y se evitan errores una vez en producción.

Deberían someterse a revisión periódicamente los accesos de los usuarios a las zonas de programación segura para comprobar que estos son correctos o bien para actualizarse en la línea de los cambios que puedan surgir en la organización.

Controles / Objetivo:

- Disminución del riesgo por errores de programación.
- Disminución del impacto de las amenazas relacionadas con errores en el código que comprometan la confidencialidad e integridad de los datos.
- Desarrollo de un procedimiento formalizado sobre el ciclo de desarrollo del software (Fase de Pre-Producción).
- Gestión de los usuarios que acceden a las zonas seguras y tienen permiso para ello.
- Utilización de plataforma comuna para el desarrollo de aplicaciones.
- Mayor seguridad en el tratado de la información.
- Aplicar estándares de seguridad (NIS, CIS, etc).
- Integrar las mejoras de seguridad en las actividades de gestión de cambios.

Dominio ISO relacionado	12.4 Seguridad de los ficheros del sistema 12.5 Seguridad en los procesos de desarrollo y soporte
Activos del AARR afectados	Servicios, Datos y Aplicaciones
Tiempo	3 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	2.500 €

ID:	**PRO002**
Nombre Propuesta:	**Procedimiento de pruebas del software**
Ámbito:	**Procedimientos**
Detalles	

Descripción

Este procedimiento va ligado al procedimiento PRO001 donde se define un entorno de programación segura. Por tanto, este procedimiento va a posteriori, donde se define un nuevo entorno de pruebas del software para poder controlar los posibles errores y defectos que tenga el software antes de ponerse en producción. Al realizar las pruebas en un entorno especializado es posible identificar y corregir desviaciones antes de que el software se encuentre en producción, a la vez que se mitiga el impacto que estos errores puedan tener sobre los activos y recursos de la organización.

Este procedimiento de pruebas debería también especificar qué usuarios tienen acceso para poder probar el software en busca de vulnerabilidades en el código. Así mismo, también se deberían especificar revisiones de estos controles para comprobar que las autorizaciones van en la misma línea de evolución que la organización.

Controles / Objetivo:

- Elaboración de procedimiento para realizar pruebas adecuadas a los proyectos de desarrollo.
- Guía de pruebas a realizar para considerar un producto seguro.
- Disminución del riesgo por errores en la programación.
- Disminución de errores provocados por los usuarios y donde podrían afectar a la confidencialidad o integridad de los datos.
- Desarrollo de un procedimiento formalizado sobre el ciclo de desarrollo del software (Fase de pruebas).
- Mayor seguridad en el tratado de la información.
- Minimización del impacto de las amenazas que afectan al código.
- Aplicar estándares de seguridad (NIS, CIS, etc).
- Integrar las mejoras de seguridad en las actividades de gestión de cambios.

Dominio ISO relacionado	12.2 Tratamiento correcto de las aplicaciones 12.4 Seguridad de los ficheros del sistema 12.5 Seguridad en los procesos de desarrollo y soporte
Activos del AARR afectados	Servicios, Datos y Aplicaciones
Tiempo	2 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	2.500 €

ID:	**PRO003**
Nombre Propuesta:	**Procedimiento de cumplimiento de normas y requisitos legales**
Ámbito:	**Procedimiento**
Detalles	

Descripción

La organización ha de disponer de un procedimiento formalizado donde se detallen una serie de normas que los empleados deben conocer y poner en práctica. En estos procedimientos se han de detallar temas como:

- El uso correcto de los activos de la organización.
- Posibles sanciones en caso de incumplimiento de algunas de las normas especificadas en otros documentos o procedimientos.
- Identificación de la legislación aplicable.
- Revisiones de auditorías para comprobar el funcionamiento de las políticas de seguridad y otros procedimientos.

Los trabajadores de la organización deben conocer estos procedimientos y haber dado el consentimiento sobre ellos antes de firmar el contrato. Igualmente, estos procedimientos han de estar al alcance de cualquier trabajador y estarán sometidos a revisiones periódicas para actualizarse en la misma dirección que lo hace la empresa.

Controles / Objetivo:

- Disminución de los riesgos por uso indebido de los recursos de la organización.
- Garantía del cumplimiento de los procedimientos expuestos por la organización.
- Alinear los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de cumplimiento legal, regulador, etc.

Dominio ISO relacionado	15.1 Cumplimiento de los requisitos legales 15.2 Cumplimiento de las políticas y normas de seguridad
Activos del AARR afectados	El conjunto de todos los activos de la organización
Tiempo	3 meses
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación parcial por parte del personal y responsables.
Cote total	3.000 €

ID:	**PRO004**
Nombre Propuesta:	**Auditorías de seguridad**
Ámbito:	**Procedimiento**
Detalles	

Descripción

La organización ha de realizar auditorías de seguridad técnicas de forma periódica en sus sistemas para comprobar el estado en que se encuentran sus servicios. Estas auditorías deberían reflejar lo vulnerables que son sus servicios de cara a atacantes externos que intenten aprovechar los agujeros de seguridad para comprometer la confidencialidad,

integridad o disponibilidad de los datos.

Estas auditorías de seguridad técnicas deberían correr a cargo de una entidad externa a la organización, de manera que no disponga de información adicional sobre ella y de esta forma la auditoría se pueda ajustar más a la realidad.

Controles / Objetivo:

- Prevención de posibles ataques futuros.
- Disminución del riesgo causado por amenazas orientadas a los servicios y aplicaciones.
- Balance del estado en que se encuentran los servicios respecto a seguridad.
- Aplicar estándares de seguridad (NIS, CIS, etc).
- Aplicar auditorías de TI cualificadas (ISO, ITIL, CMM, etc).
- Aplicar ISOs con marcos orientados a auditorías internas del SGSI.

Dominio ISO relacionado	12.6 Gestión de la vulnerabilidad técnica 15.3 Consideraciones sobre las auditorías de SI
Activos del AARR afectados	Servicios, aplicaciones, software y datos
Tiempo	1 mes
Coste	
Recurso	Horas de trabajo por parte del personal externo de la organización.
Dedicación	Dedicación completa por parte del personal externo.
Cote total	4.000 €

ID:	**IMP001**
Nombre Propuesta:	**Implantación Firewall de aplicación**
Ámbito:	**Implantación**
Detalles	

Descripción

Las principales actividades de negocio de la organización se basan en aplicaciones web, por tanto es lógico que muchas de las amenazas provengan de usuarios externos a través de estos servicios. Es por este motivo que es necesaria la implantación de una solución que gestione y controle las peticiones que se realicen sobre los aplicativos, impidiendo que tráfico malicioso afecte los sistemas y ponga en peligro la integridad, disponibilidad y confidencialidad de los datos.

La implantación de un firewall de aplicación es un complemento más de seguridad, sin substituir otros dispositivos o procedimientos de seguridad. Este firewall de aplicación deberá tener asignado un responsable que se encargue de verificar las alertas que se generan, así como de actualizarlo de forma periódica.

Controles / Objetivo:

- Disminución del impacto por amenazas relacionadas con vulnerabilidades orientadas a aplicaciones web, como inyecciones o código malicioso.
- Mayor seguridad en el tratamiento de la información ante ataques informáticos.
- Servicio actualizado con las técnicas actuales de ataques.

- Nuevo servicio de detección de ataques e intrusiones.
- Monitorización de posibles ataques contra las aplicaciones web.
- Implantar estándares, directrices y procedimientos de seguridad técnicos para la seguridad de las redes.

Dominio ISO relacionado	10.6 Gestión de la seguridad de las redes
Activos del AARR afectados	Servicios y aplicaciones
Tiempo	5 días
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación completa por parte del personal y responsables.
Cote total	500 €

ID:	**IMP002**
Nombre Propuesta:	**Implantación Sistema de detección de intrusos**
Ámbito:	**Implantación**
Detalles	

Descripción

Las principales actividades de negocio de la organización se basan en aplicaciones web, es decir, servicios orientados a usuarios externos. Es por este motivo que es necesario disponer de dispositivos que sean capaces de detectar y mitigar posibles intrusiones en el sistema antes de que causen alteración en los datos u obtengan información confidencial.

Es importante analizar la actividad que se genera en la red de forma periódica para comprobar que no ha habido intrusiones no autorizadas y que dicha actividad en la red queda registrada ,para que en caso de incidente, se tengan las suficientes muestras para comprender qué fue lo sucedido y poder solucionarlo o prevenirlo en acciones futuras.

Mejoras / Objetivo:

- Disminución del impacto por amenazas relacionadas con vulnerabilidades orientadas a aplicaciones web
- Asegurar la seguridad de las infraestructuras y de la información de la organización.
- Servicio actualizado con las técnicas actuales de ataques.
- Nuevo servicio de detección de ataques e intrusiones.
- Monitorización de posibles ataques contra las aplicaciones web.
- Implantar estándares, directrices y procedimientos de seguridad técnicos para la seguridad de las redes.

Dominio ISO relacionado	10.6 Gestión de la seguridad de las redes
Activos del AARR afectados	Servicios y aplicaciones
Tiempo	10 días
Coste	
Recurso	Horas de trabajo por parte del personal de la organización.
Dedicación	Dedicación completa por parte del personal y responsables.
Cote total	1.200 €

3.6.3 Planificación de los proyectos

Para conocer el tiempo y el coste económico de los controles seleccionados, se procede primeramente a realizar un diagrama temporal, donde se especificarán los proyectos que se llevarán a cabo en cada periodo de tiempo.

Los proyectos se han dividido en el tiempo, organizándolos según prioridad para la empresa, intentando implantar los proyectos que reducen el riesgo de áreas o activos más críticos o sensibles para la organización en primer lugar. Siendo los proyectos divididos por años:

1er año (2014):

- *Gestión de los Backup de los sistemas*
- *Gestión de acceso al CPD*
- *Gestión de roles y accesos*
- *Implantación Firewall de aplicación*
- *Implantación Sistema de detección de intrusos*

2do año (2015):

- *Procedimiento de programación segura*
- *Procedimiento de pruebas del software*
- *Procedimiento de cumplimiento de normas y requisitos legales*
- *Política de seguridad*

3er año (2016)

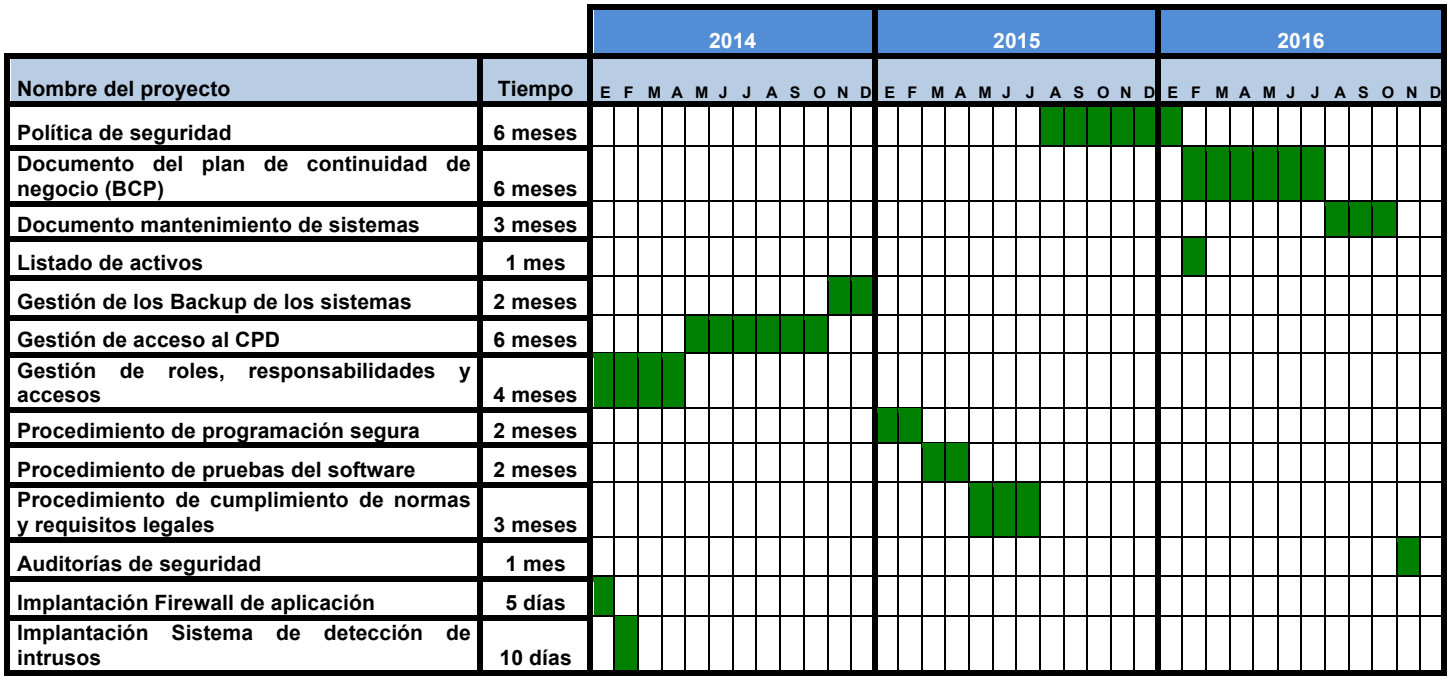
- *Documento del plan de continuidad de negocio (BCP)*
- *Documento mantenimiento de sistemas*
- *Listado de activos*
- *Auditorías de seguridad*

La razón de escoger estos proyectos en el primer año, ha sido que el CPD es el centro neurálgico de la actividad de la empresa y este, no se encuentra regulado el acceso ni por medidas lógicas ni físicas importantes y por tanto, cualquier usuario podría acceder a el sin que quede constancia en el sistema. Esto cobra más importancia si la empresa no dispone de una gestión adecuada y formal de copias de seguridad, lo que incrementa el riesgo a perder datos o información sensible. Es por este motivo, que se ha preferido implantar estos controles en primer lugar para asegurar la zona más crítica de la organización en primer lugar. En cuanto a la implantación de firewall de aplicación y a los IDS ha sido por una razón similar, ya que el negocio principal de la organización se basa en aplicaciones y servicios web, con lo que intentar controlar y mitigar en la medida de los posible ataques externos que puedan vulnerar la confidencialidad, disponibilidad e integridad de los datos es fundamental.

La mayoría de errores eran por parte de los usuarios o bien por tener errores en el código por no llevar a cabo una correcta gestión en el ciclo de desarrollo del software, por ese motivo, después de haber fortificado el CPD y los accesos externos, se ha creído conveniente desarrollar unos procedimientos de programación segura y de pruebas del software adecuada para mitigar errores de los usuarios y de los propios empleados.

El tercer año está destinado a la documentación de la organización referente a procedimientos y activos de la organización, así como una auditoría para comprobar la seguridad de los sistemas de información.

A continuación, se muestra el diagrama temporal con los proyectos organizados en el tiempo:



Nombre del proyecto	Tiempo
Política de seguridad	6 meses
Documento del plan de continuidad de negocio (BCP)	6 meses
Documento mantenimiento de sistemas	3 meses
Listado de activos	1 mes
Gestión de los Backup de los sistemas	2 meses
Gestión de acceso al CPD	6 meses
Gestión de roles, responsabilidades y accesos	4 meses
Procedimiento de programación segura	2 meses
Procedimiento de pruebas del software	2 meses
Procedimiento de cumplimiento de normas y requisitos legales	3 meses
Auditorías de seguridad	1 mes
Implantación Firewall de aplicación	5 días
Implantación Sistema de detección de intrusos	10 días

Tal como se muestra en el diagrama, alguna de las tareas pueden realizarse en paralelo ya que las personas que se encargan de esa tarea no son las mismas. Por ejemplo, los responsables y dirección de la organización puede encargarse de gestionar y organizar los roles necesarios para el acceso al CPD y a los sistemas de información mientras los técnicos implantan las medidas tecnológicas como el AWF y el IDS. También se realiza en paralelo el documento del plan de continuidad y la lista de activos, ya que son tareas que se pueden realizar en paralelo.

3.6.4 Planificación económica

En cuanto a la planificación económica se especifican los gastos que se llevarán a tiempo durante el período en el que se aplicarán los controles seleccionados para mitigar o reducir en la medida de los posible los riesgos detectados en el análisis de riesgos.

Se ha procedido a dividir los gastos por años, según el gasto que se hizo cada año correspondiendo a los controles implantados en aquel periodo de tiempo. Los proyectos se contabilizan a partir del año que empiezan, es decir, un proyecto puede empezar en 2015 pero acabar en 2016, no obstante, entra en el presupuesto del año en el que empieza, el 2015. El resultado es:

1er año (2014) → *18.900 €*
2do año (2015) → *13.500 €*
3er año (2016) → *15.000 €*

Total → **47.400 €**

Tal como se puede observar, el mayor desembolso se realizar el primer año, donde se implementan las medidas más urgentes para la organización y sus servicios. No obstante, todos los años están bastante parejos y repartidos durante los 3 años sin que haya unas diferencias demasiado acusadas entre años.

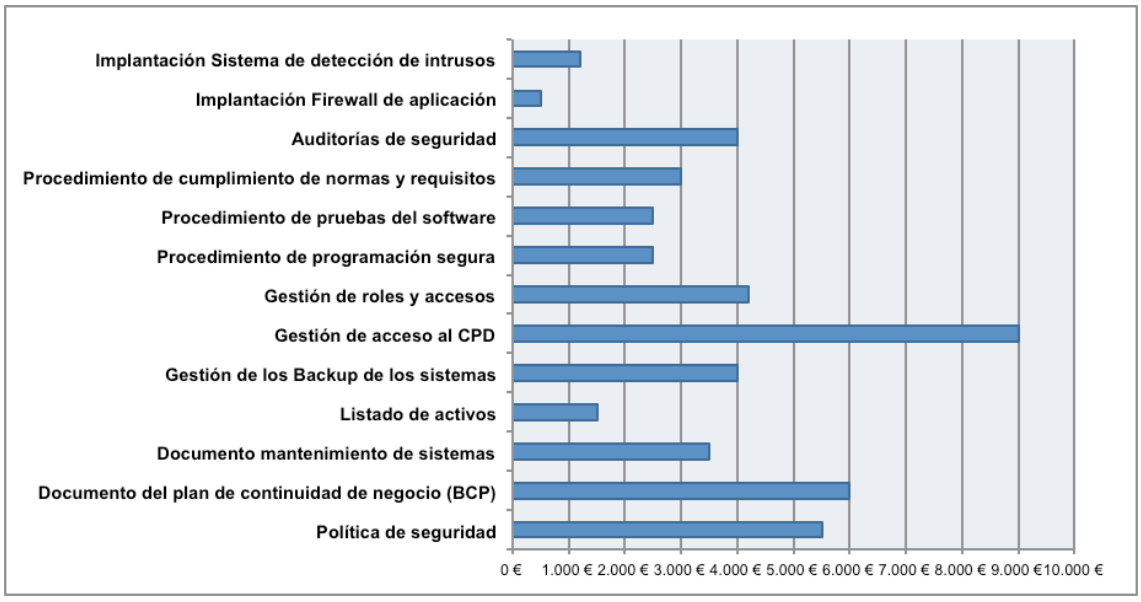
El resumen de los proyectos y coste de ellos divido en años es el siguiente:

1er año (2014)	
Gestión de los Backup de los sistemas	4.000 €
Gestión de acceso al CPD	9.000 €
Gestión de roles y accesos	4.200 €
Implantación Firewall de aplicación	500 €
Implantación Sistema de detección de intrusos	1.200 €

2do año (2015)	
Procedimiento de programación segura	2.500 €
Procedimiento de pruebas del software	2.500 €
Procedimiento de cumplimiento de normas y requisitos legales	3.000 €
Política de seguridad	5.500 €

3er año (2016)	
Documento del plan de continuidad de negocio (BCP)	6.000 €
Documento mantenimiento de sistemas	3.500 €
Listado de activos	1.500 €
Auditorías de seguridad	4.000 €

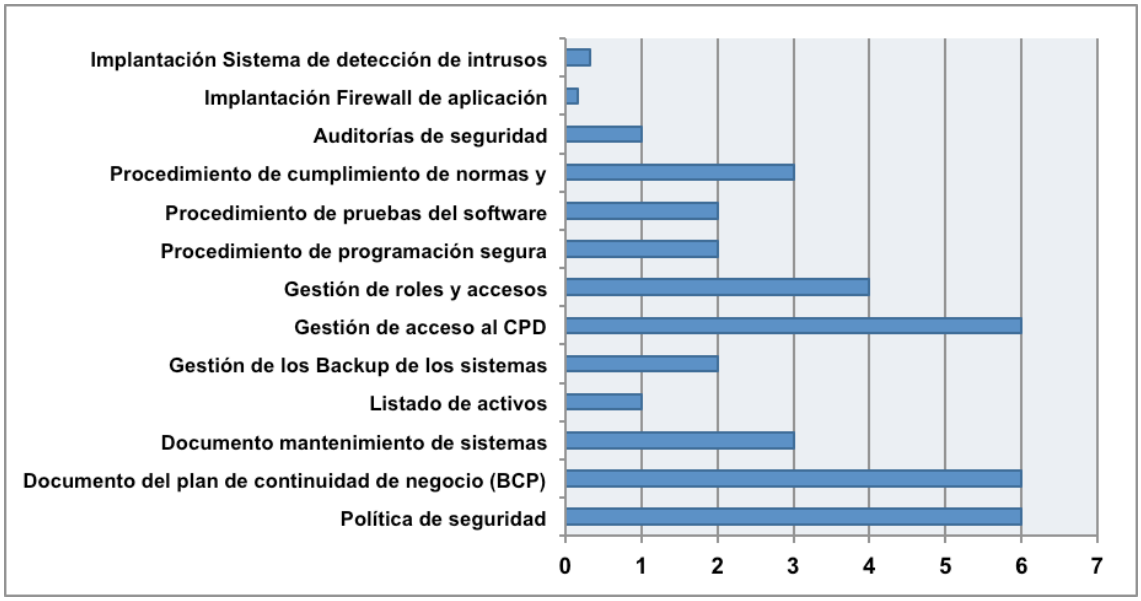
A continuación, se desglosa en una gráfica de barras los diferentes proyectos realizados así como su coste, con el fin de diferenciarlos entre ellos claramente.



Se puede apreciar que, con diferencia, el proyecto que más ha costado a la organización ha sido el de la gestión al CPD, ya que no únicamente se trata de gestionar tiempo de los empleados para realizar el proyecto, sino que se ha de adquirir nuevo hardware y software para gestionar el acceso físico a la vez que se registra este acceso en un histórico. Por otra parte, tiene sentido que el acceso al CPD sea de los proyectos más caros ya que también es el activo más crítico del que dispone sin protección alguna la organización.

En segunda posición como proyectos más caros, se encuentra la creación de la política de seguridad y la creación del documento de continuidad de negocio, los cuales son los más largos en tiempo y de ahí el incremento del coste. Se ha de tener en cuenta que los proyectos que se realizan, a excepción de la gestión de acceso al CPD, el resto de proyectos no comporta la adquisición de complementos adicionales como hardware y de ahí que no se incrementen en exceso los costes. La implementación del firewall de aplicación o IDS, se pueden encontrar este tipo de software de forma gratuita en la red, con lo que el coste acaba derivando únicamente en el coste del recurso que lo implanta, en este caso, trabajadores de la organización.

En el siguiente gráfico se desglosan los proyectos por meses de duración.



Se puede observar como coinciden con el gráfico anterior los costes con los tiempos, siendo la gestión al CPD y la documentación del plan de continuidad y la política de seguridad los proyectos que más duran, todos 6 meses. Tanto la implantación del firewall de aplicación como del IDS son proyectos que no llegan a un mes de duración, coincidiendo de nuevo los más cortos en el tiempo con los que menos presupuesto se destina a ellos.

Esto no tiene por qué ser de esta manera siempre, en este caso coincide, pero se podría haber dado el caso de un proyecto que no tiene demasiada duración, sin embargo al haberse de contratar fuera o comprar un determinado producto al final resulta en un alto coste. Un ejemplo es la auditoría de seguridad, donde únicamente dura un mes, sin embargo, como se ha de contratar de manera externa a la organización, los costes son más elevados pero la duración es tan solo de un mes.

3.6.5 Evolución del impacto y el riesgo

A raíz de la creación de una serie de proyectos que intentan añadir unas mejoras en la seguridad de la información de la organización, se han visto repercutidos de manera positiva los resultados del análisis de riesgo realizado en etapas anteriores, concretamente, tanto el impacto potencial como el riesgo acumulado han sufrido una serie de modificaciones positivas para la organización.

Concretamente, la introducción de los roles y controles de acceso, tanto a entornos físicos como a lógicos, así como la creación de unas pautas de buenas prácticas, programación segura y procedimientos de pruebas del software en pre-producción y de la realización de copias de seguridad, han contribuido notablemente a reducir el impacto de las amenazas en el sistema. Sin obviar documentos como la política de seguridad o el plan de continuidad de negocio que ayudan a mejorar el conjunto de todos los activos así como su seguridad frente a determinadas amenazas.

Por tanto, el impacto potencial de las amenazas sobre los activos de la organización, sufre un ajuste en cuanto a los valores que nos ayudan a determinar el impacto que una amenaza afectaría a los sistemas de información. En la siguiente tabla se puede observar el impacto potencial que se tenía antes de realizar los proyectos, y al lado, el impacto potencial reajustado una vez se han creado y definido los proyectos.

Únicamente se muestran los activos que habían sido detectados en el cálculo del riesgo acumulado, con valores por encima del valor aceptable

ID	Activo	Impacto Potencial					Impacto potencial después proyectos				
		c	i	d	a	t	c	i	d	a	t
[L.1]	CPD	10					7,5				
[L.2]	Sala oficinas	8					6				
[SW.4]	Aplicación Docencia	6,75	9	6,75			4,5	4,5	4,5		
[SW.5]	Aplicación Libro de datos	6,75	9	6,75			4,5	4,5	4,5		
[SW.7]	Aplicación BBDD Server	6	9	6			4	4,5	4		
[D.2]	Datos aplicaciones	6,75	6,75	4,5			1,8	4,5	1,8		
[COM.1]	Router primario	5,25	6,75	9			3,5	6,75	6,76		
[COM.2]	Línea intranet (DMZ)	4,5	6	6			3	6	4,5		
[COM.3]	Línea principal Internet	5,45	6	7			3,5	6	5,25		
[S.3]	Servicio Web	3	6	6	4	3,5	1,2	4	6	1,6	3,5
[S.6]	Servicio aplicación Docencia	3,5	6	6,75	4	4	1,4	4	6,75	1,6	4
[S.7]	Servicio Libro de datos	3,5	6	6,75	3,5	4	31,4	4	6,75	1,4	4

Tal como se observa en la tabla anterior, en cuanto a las dimensiones de la seguridad, los valores del impacto potencial han sido reducidos significativamente en la mayoría de los campos.

Sin embargo, un factor donde han influido positivamente la creación de los proyectos ha sido en la frecuencia de materialización de las amenazas. Por ejemplo, el CPD antes de la creación de roles y permisos de acceso, junto con mecanismos de autenticación físicos, podía acceder cualquier persona a el sin demasiada complicación, después de la creación de los proyectos

esto se ha solucionado y únicamente personas con tarjeta y autorización podrían acceder, por tanto, la frecuencia con la que se materializa una amenaza es inferior. Esto es extrapolable al resto de amenazas donde la frecuencia en la que estas se materializaban ha sido reducida de forma considerable, lo que ayuda a mitigar el riesgo acumulable final.

En la siguiente tabla se vuelve a mostrar una comparativa donde se puede ver el riesgo acumulado que tenía la organización en el primer análisis realizado y al lado el riesgo acumulado nuevo, teniendo en cuenta los proyectos creados. También se puede ver la nueva frecuencia en la que se materializan las amenazas. De igual forma que la tabla anterior, únicamente se muestran los activos que tenían un riesgo acumulado por encima del valor aceptable para la organización.

ID	Activo	Frecuencia	Riesgo Acumulado					Riesgo Acumulado después proyectos				
			c	i	d	a	t	c	i	d	a	t
[L.1]	CPD	1,00			100			7,50				
[L.2]	Sala oficinas	1,00			80			6				
[SW.4]	Aplicación Docencia	1,00	67,5	90	67,5			4,5	4,5	4,5		
[SW.5]	Aplicación Libro de datos	1,00	67,5	90	67,5			4,5	4,5	4,5		
[SW.7]	Aplicación BBDD Server	1,00	60	90	60			4	4,5	4		
[D.2]	Datos aplicaciones	1,00	67,5	67,5	45			1,8	4,5	1,8		
[COM.1]	Router primario	1,00	52,5	67,5	90			3,5	6,75	6,75		
[COM.2]	Línea intranet (DMZ)	1,00	45	60	60			3	6	4,5		
[COM.3]	Línea principal Internet	1,00	52,5	60	70			3,5	6	5,25		
[S.3]	Servicio Web	1,00	30	60	60	40	35	3	1,6	1,6	1,6	3,5
[S.6]	Servicio aplicación Docencia	1,00	35	60	67,5	40	40	3,5	1,6	1,8	1,6	4
[S.7]	Servicio Libro de datos	0,10	35	60	67,5	35	40	0,35	0,16	0,18	0,14	0,4

Anteriormente existían amenazas que se materializaban de forma repetida de forma mensual, con los proyectos creados esto se ha reducido y no se dispone de ninguna amenaza que se materialice de forma mensual repetidamente, lo que reduce drásticamente el riesgo para la organización.

Todas las dimensiones de la seguridad han sufrido mejoras con la creación de los proyectos, reduciendo sus niveles de riesgo y del impacto potencial, excepto el no repudio, el cual no ha sufrido mejoras significativas al crear los nuevos proyectos como sí lo ha sufrido la integridad o la confidencialidad de los datos, los aspectos que más podían preocupar a la organización dada su actividad.

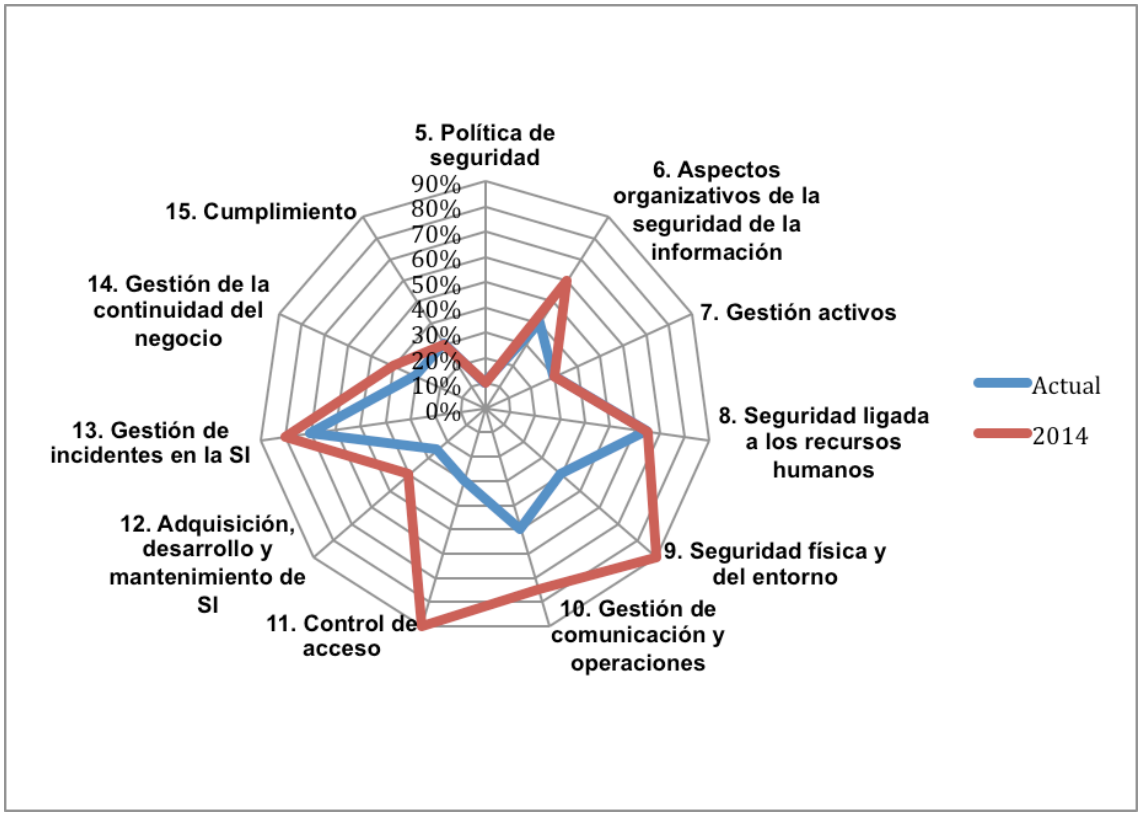
En esta evolución del impacto y del riesgo no se tienen en cuenta nuevos activos que puedan haberse introducido a raíz de la creación de los nuevos proyectos, únicamente se contempla el estudio de la evolución de los activos que ya se encontraban en la organización con antelación a la creación de los proyectos. Para el siguiente análisis de riesgo sí que habría que definir los nuevos activos de la organización entre los que se encontrarían los activos nuevos debido a la creación de los proyectos.

3.6.6 Evolución del nivel de cumplimiento de la ISO

El nivel de cumplimiento de la ISO, a raíz de la incorporación de las modificaciones repercute directamente en cada uno de los diferentes dominios de la ISO a medida que se van implantando y se alcanza con ello cada vez un punto más óptimo de seguridad en el sistema.

Se ha considerado que el máximo posible será un 90% ya que todavía quedarían cosas por retocar y mejorar para conseguir un modelo óptimo para la seguridad, siempre habrá mejoras que realizar y puntos a reforzar conforme surjan nuevas amenazas, vulnerabilidades y se realicen nuevos análisis de riesgos.

Desglosando la evolución por años se puede apreciar de una forma más clara la evolución de los controles y el cumplimiento de la ISO. Por eso, en el siguiente gráfico se muestra el estado actual y lo que se prevee que quede implantado en la organización para el 2014:

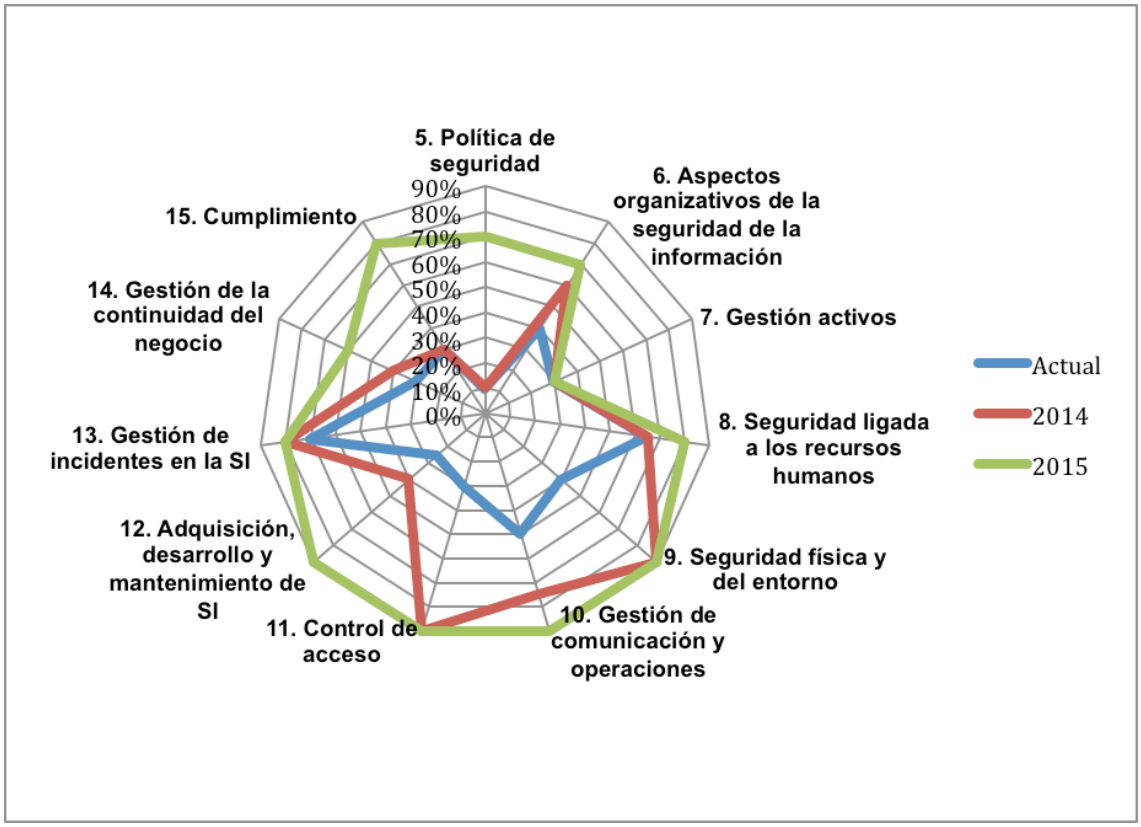


Tal como se ha visto en los apartados anteriores, donde se hacía más enfasis era en la creación de controles de acceso para el CPD así como roles de acceso a los servicios y recursos de la organización, es por este motivo que justamente el grado de cumplimiento de la ISO respecto a los dominios del control de acceso y la seguridad física de los activos y recursos queda cumplido en el primer año. La gestión de incidentes que puedan ocurrir en la red por algún tipo de intrusión se gestiona a través de UPC, ya que la red y los routers es su campo de control contra los incidentes, así como también dispone de su centro de respuestas a incidentes, por tanto, sufre mejora con los proyectos en el ámbito de la creación de roles y responsabilidades, los cuales, dependiendo del tipo de incidente que pudiera surgir en la

organización serán los encargados de cara área donde estos ocurran de ponerse en contacto con los órganos pertinentes.

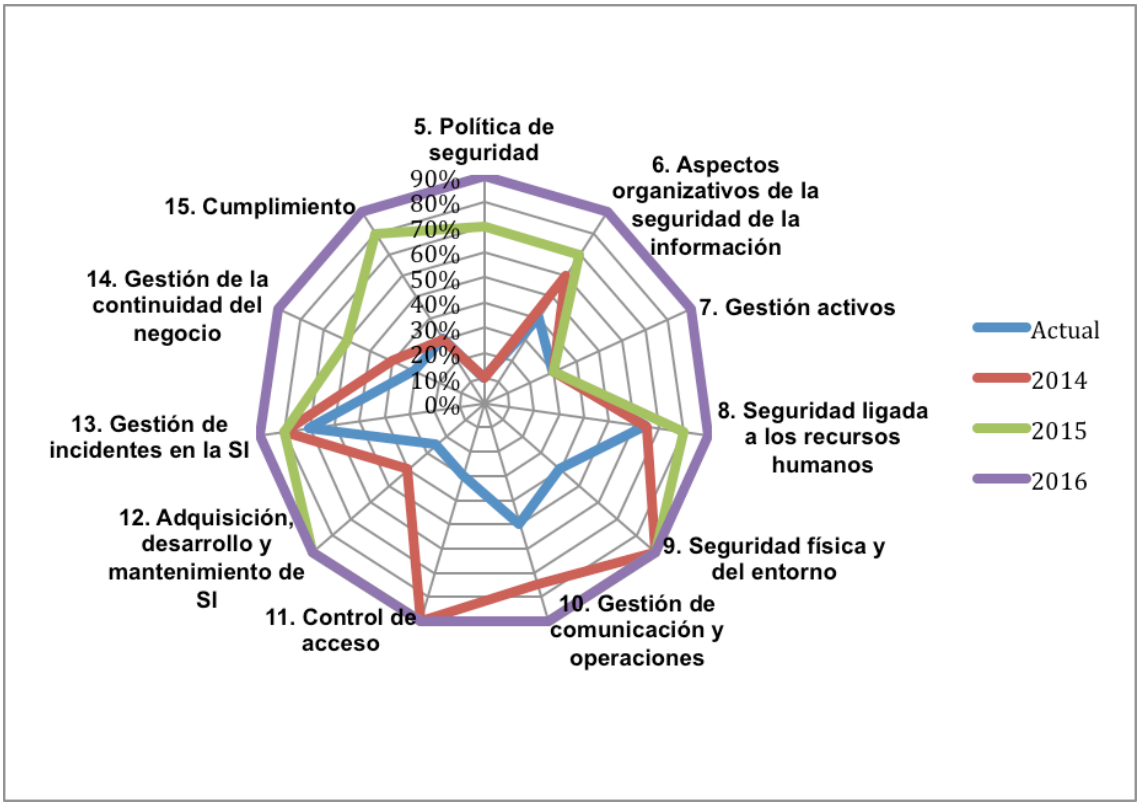
A continuación, durante el 2015, se implantan más proyectos que mejoran aspectos de la seguridad que era de vital importancia incorporar mejoras debido al carácter de negocio que tiene la organización.

La adquisición, desarrollo y mantenimiento de los SI era uno de los aspectos más críticos para la organización debido a su servicio y que menos protección tenía. Esto se puede ver como actualmente tiene un 20% únicamente de cobertura y pasa al 90% en el 2015.



Durante el 2015 puede verse una ampliación importante en todos los dominios de la ISO, esto es debido a que prácticamente la totalidad de los proyectos han sido terminados o comenzados, a excepción de algunos claro. La política de seguridad empiza en el 2015 para terminar en el 2016, por tanto, los cambios más significativos en este aspecto se empiezan a notar a partir del siguiente año. Existen proyectos, sobretodo de procedimiento que se culminan en el 2015 que afectan indirectamente, a otros controles de la ISO, pero que no están centrados en ellos exclusivamente, de ahí que haya unos cuantos controles que no experimenten una gran mejora, esto es debido a que estos proyectos se enfocan principalmente en otros controles.

Para el siguiente año, los esfuerzos han sido concentrados en terminar la política de seguridad, realizar una gestión de los activos, realizar proyectos orientados al cumplimiento y reforzar la gestión de la continuidad de negocio, por tanto, el objetivo sería adquirir un nivel óptimo y aceptable en la totalidad de dominios de la ISO, quedando el gráfico de evolución de la siguiente manera:



En este año ocurre lo mismo que en anteriores, se realizan proyectos orientados a controles especificos donde se persigue una mejora importante y, así se muestra en la ficha de proyectos, no obstante, estos proyectos pueden afectar de manera mínima otros controles de la ISO, aunque no de suficiente manera como para notar una mejoría aceptable como si de un proyecto enfocado a un control determinado se tratase.

En cuanto al periodo actual, lo que mejor estado presentaba es el estado de la seguridad ligada a los recursos humanos debido a que algunos de estos puntos se realizan de forma externalizada a través de UPC, que es quien gestiona los recursos humanos, por tanto la seguridad es compartida o mínima de la empresa y la gestión de incidentes, que también se gestionaba de forma externalizada por parte de UPC. Por tanto, estos dos puntos necesitaban unos precedimientos documentados y formalizados donde se detallen de forma adecuada los roles y responsabilidades para responder de forma eficiente y una política de seguridad y documento de continuidad.

3.7 Política de seguridad

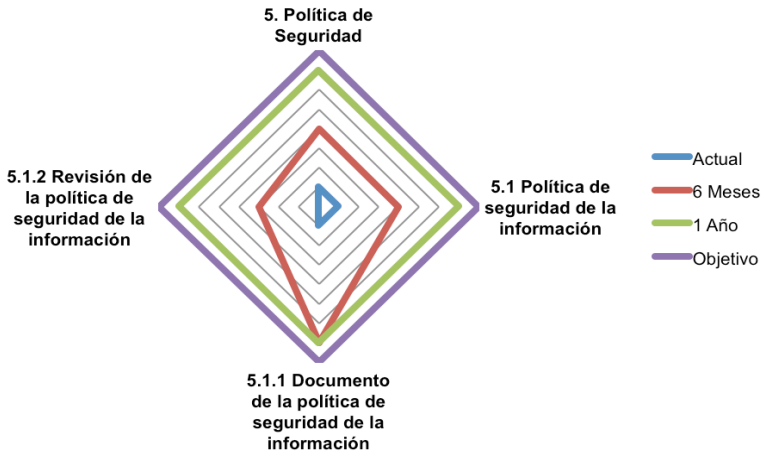
Actualmente, no existe ningún documento identificable con una política de seguridad actualizada y completa en la organización, ni tampoco al alcance y conocimiento de todos los empleados de esta misma. Por este motivo, uno de los objetivos principales, es la creación de una política de seguridad bien definida y actualizada, con el fin de tener implicada a toda la organización en temas de seguridad de la información.

La política de seguridad es un documento donde se especifican unas pautas a seguir por la organización con el objetivo de proteger los activos que hacen posible llevar a cabo la actividad y servicios de la organización. Por este motivo, es importante que la organización establezca procedimientos para preservar la confidencialidad, integridad y disponibilidad de los datos, especialmente en las áreas más críticas para la actividad de la misma, tal como se especifica en el alcance del Plan Director, especificado en puntos anteriores. Por otro lado, en este documento de seguridad, debería establecerse las pautas de seguridad adecuadas para que el personal de la organización se sensibilice con estas buenas prácticas y sea un activo importante en lo que la seguridad de los activos críticos se refiere.

La política de seguridad deberá someterse a revisión para reflejar los diferentes cambios que puedan surgir, como por ejemplo de activos, procedimientos, de carácter legislativo, etc. Con el fin de adecuarse a los cambios que van surgiendo en el conjunto de la organización y su actividad y por ende, pueda seguir manteniendo un nivel de seguridad aceptable sobre los activos que dan sentido al servicio ofrecido.

Esta política de seguridad debería aplicarse y ponerse al alcance de todo el personal de la organización a corto plazo, con el objetivo de aplicar las mejoras pertinentes en toda la organización tal como se especifique. Posteriormente debería someterse a revisión por parte de la gerencia y responsables, de manera permanente, para reflejar los cambios en la organización.

En el siguiente gráfico se muestra un estado de la política de seguridad actual y la estimación de lo que se podría esperar entorno a su elaboración en el próximo año. Se han escogido los mismos puntos que existen especificados en la ISO 27001



3.8 Procedimiento de auditoría interna

Actualmente no se realiza ningún proceso ni procedimiento de auditoría interna debido a la disponibilidad y conocimientos del personal (ni tampoco se realiza ningún tipo de auditoría externa). Por tanto, uno de los principales objetivos será la definición de unos procedimientos de auditoría interna que facilite unos reportes identificando que áreas necesitan implementar o focalizar los esfuerzos de la organización para mejorar el sistema de información.

Estas auditorías deberían realizarse de forma periódica con una frecuencia de al menos cada 6 meses y bajo el control del responsable de los sistemas de información, el cual será la personalidad máxima encargada de estas tareas debido a que será el responsable también de conocer los procesos críticos para la organización y las áreas a auditar correspondientes.

Metodología

Estas auditorías deberían realizarse por personas cualificadas para ello y que tengan independencia del proceso que se va a auditar. Por este motivo, es importante que los auditores no formen parte de ningún proceso de la organización y por tanto, sean externas a estas. Además, el auditor ha de estar al corriente de las diferentes leyes y normas que puedan ser de aplicación en el organismo auditado así como velar por su cumplimiento. También deberá conocer los activos, salvaguardas, procedimientos y todo tipo de información relevante para llevar a cabo la tarea del auditor de forma adecuada.

Adicionalmente el auditor, ha de conocer, en caso de que existan, los resultados de auditorías previas que se puedan haber realizado, así como sus resultados. También debe ser consciente y conocer perfectamente el alcance de la auditoría y sistemas que ha de revisar, sin salirse del objetivo y procesos definidos previamente antes de empezar la auditoría. Al finalizar el trabajo, deberá entregar a los organismos pertinentes los resultados de la auditoría, de forma confidencial.

Resultados

El informe de resultados debe reflejar las observaciones, evidencias, recomendaciones y por último las conclusiones, referente al trabajo de auditoría llevado a cabo. Es un documento de carácter confidencial y que debe llegar a los responsables de la organización para que sean conscientes de los desvíos en temas de seguridad de la información que ha sufrido la organización.

Es tarea del responsable de los sistemas auditados de la organización de tomar responsabilidades sobre los resultados detectados en la auditoría, así como de tomar precauciones y correcciones oportunas sobre las vulnerabilidades y amenazas detalladas en el informe en un tiempo limitado.

Una vez verificado el informe por los responsables y tomado las acciones correctivas pertinentes, se ha de realizar un seguimiento sobre estas acciones para comprobar que los errores han sido solucionados, si más no mitigados en la medida de los posible.

3.9 Procedimiento de revisión por la dirección

Objetivo

Este documento tiene por objeto establecer las actividades para realizar las revisiones por la Dirección que tiene como finalidad:

- Analizar la información de gestión disponible para obtener conclusiones sobre el desempeño del Sistema de Gestión de Calidad.
- Determinar acciones correctoras y recursos necesarios para corregir posibles desvíos en relación con los objetivos de la compañía.
- Validar la Política y Objetivos de Calidad de la compañía.
- Analizar la sostenibilidad a medio y largo plazo del Sistema de Gestión a partir de sus Fortalezas, Debilidades, Amenazas y Oportunidades de desarrollo
- Determinar planes de mejora para aumentar el desempeño en materia de posicionamiento, ingresos, RR físicos y financieros, personal, procesos, servicios al cliente y el sistema de gestión de calidad.

La dirección debe revisar el SGSI de la organización a intervalos planificados(por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad.

Esta revisión debe incluir oportunidades de evaluación para la mejora y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información.

Alcance

Este procedimiento aplica para todos los procesos del sistema de gestión de la calidad, para los diferentes subsistemas, componentes, y para los componentes del sistema de desarrollo administrativo. Comienza con la citación a reunión del Comité de Calidad para revisión del sistema y termina con la incorporación de correctivos para asegurar el cumplimiento del plan de acción adoptado en la revisión.

Puntos de entrada de revisión por la dirección

Las entradas para la revisión por la dirección deben incluir:

1. resultados de auditorias y revisiones del SGSI;
2. retroalimentación de las partes interesadas;
3. técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
4. estado de acciones preventivas y correctivas;
5. vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
6. resultados de mediciones realizadas;
7. acciones de seguimiento de las revisiones por la dirección previas;
8. cualquier cambio que pudiera afectar el SGSI; y
9. recomendaciones para la mejora.

Resultados de la revisión por la dirección

El resultado de la revisión por la dirección debe incluir cualquier decisión y acción relacionada con:

1. la mejora de la eficacia del SGSI;
2. la actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
3. la modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    a. requerimientos comerciales;
    b. requerimientos de seguridad;
    c. procesos comerciales que afectan los requerimientos comerciales existentes;
    d. requerimientos reguladores o legales;
    e. obligaciones contractuales; y
    f. niveles de riesgo y/o criterio de aceptación del riesgo.
4. necesidades recursos;
5. de mejora: de cómo se mide la efectividad de los controles.

3.10 Roles y responsabilidades

El sistema de Gestión de la seguridad de la información ha de estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el sistema. En este documento se detallan los diferentes roles y responsabilidades para llevar a cabo un correcto funcionamiento y gestión de la seguridad de la información.

Definimos uno a uno los diferentes roles con sus responsabilidades, teniendo en cuenta que los empleados de la compañía son reducidos y poco especializados en seguridad, ya que sus áreas de competencia están lejos de los temas informáticos y seguridad de la información.

El comité de dirección presenta las siguientes funciones:

- Tener la seguridad de la información como un punto fijo en la agenda del comité de dirección de la compañía.
- Nombrar los miembros del comité de seguridad de la información y dotarle de todo el soporte y recursos necesarios junto con las directrices de trabajo.
- Aprobar la política, las normas y responsabilidades en materia de seguridad.
- Determinar el límite de riesgo aceptable en materia de seguridad.
- Analizar los posibles riesgos introducidos por los cambios en las funciones o en el funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el plan de seguridad de la información que recoja los principales proyectos e iniciativas en la materia.

El comité de seguridad de la información se encarga de:

- Implantar las directrices del comité de dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar al comité de dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas.
- Validar el plan de seguridad de la información y presentarlo para aprobación del comité de dirección.
- Supervisar la implantación y realizar el seguimiento.
- Comprobar que se cumpla la legislación que sea aplicable en materia de seguridad.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de comando de la seguridad de la información y de la evolución del SGSI.

Por otro lado, se define de forma genérica algunas de las tareas a realizar por el nivel operativo, que es donde se encuentran los perfiles más activos dentro del sistema de gestión

de la información y de cada departamento en concreto. Es habitual que las valoraciones sean formuladas directamente por estas personas ya que conocen directamente el impacto sobre sus departamentos y sus activos.

Por tanto, podríamos definir las siguientes tareas:

- Clasificar la información de la cual son responsables según la criticidad que esta tenga para la compañía en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio, trazabilidad e impacto mediático, determinando el uso que se hará de la información y quien puede acceder.
- Tener conocimiento de la normativa general o sectorial aplicable a la información de la cual son responsables, incluyendo la normativa vigente en materia de protección de datos de carácter personal.
- Realizar el seguimiento del estado de la seguridad de los sistemas de información que traten la información de la que son responsables y gestionar la mitigación de riesgos dentro de su nivel de decisión.
- Implicarse y definir procedimientos alternativos en caso de indisponibilidad del sistema o falta de integridad de la información.
- Colaborar con las revisiones y el seguimiento durante la realización del proyecto.
- Cumplir las políticas, normas y procedimientos en materia de seguridad de la información.

3.11 Metodología de análisis de riesgos

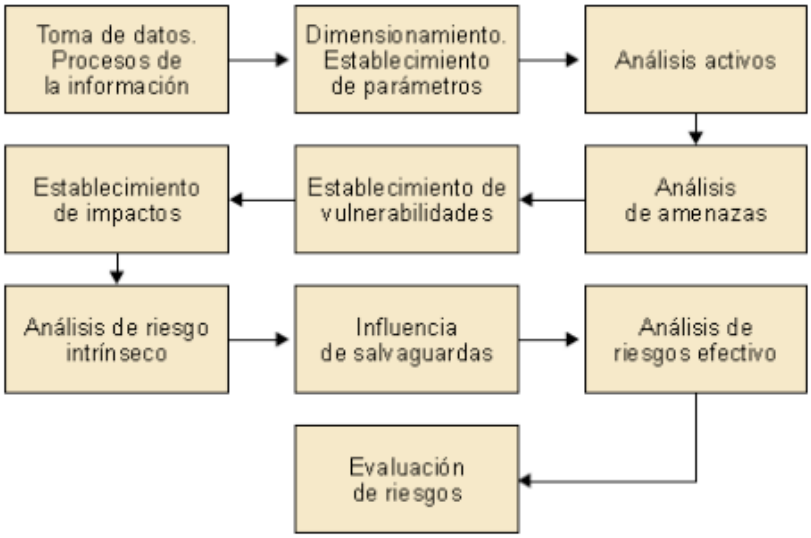
La metodología que se implementará será Magerit, que fue elaborada por el MAP (Ministerio de Administraciones Públicas) con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos. Con posterioridad ha sido aplicable a cualquier organización.

Esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente, lo que tiene una ventaja y un inconveniente:

- El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Esto hace que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- Por el contrario, el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

Fases de Magerit

Esta metodología posee una herramienta que permite la aplicación Magerit de forma directa. Magerit sigue un proceso hasta llegar a la elaboración e identificación de todos los riesgos de una organización. Las fases son las siguientes:



Establecimiento de parámetros

En este apartado se definen los parámetros que se utilizarán durante todo el proceso de análisis de riesgos. Los parámetros que deben identificarse son los siguientes:

- Valor de los activos
- Vulnerabilidad
- Impacto
- Efectividad de control de seguridad

Analizándolos uno a uno:

- Los *activos* que han de ser analizados son aquellos que requiere la organización para llevar a cabo los procesos propios de la misma.
  Para llevar a cabo la valoración deben establecerse diferentes grupos de **activos según su valor**. A cada uno de estos rangos se le asigna un valor estimado que será el que se utilice para todos los activos cuya valoración económica se corresponda con ese rango de valores.

  A la hora de asignar una valoración a cada activo debe tenerse en consideración lo siguiente:

  - El valor de reposición es el valor que tiene para la organización reponer ese activo en caso de que se pierda o de que no pueda ser utilizado.

  - El valor de configuración es el tiempo que se necesita desde que se adquiere el nuevo activo hasta que se configura o se pone a punto para que pueda utilizarse para la función que desarrolla el activo.

  - El valor del uso del activo es el valor que pierde la organización durante el tiempo que no puede utilizar dicho activo para la función que desarrolla.

  - El valor de pérdida de oportunidad es el valor que pierde potencialmente la organización por no poder disponer de dicho activo durante un tiempo.

3.12 Gestión de indicadores

Indicadores por dominio
5. POLÍTICA DE SEGURIDAD
5.1 Política de seguridad de la información
Grado de despliegue y adopción de políticas en toda la organización.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
6.1 Organización interna
Número de revisiones por la dirección realizadas, respecto de las planificadas.
Porcentaje de centros de responsabilidad asociados a procesos de negocio que han implementado una estrategia para mantener dentro de los umbrales explícitamente aceptados por la dirección del servicio.
6.2 Terceros
Número de incidentes o eventos asociados a terceros
7. GESTIÓN DE ACTIVOS
7.1 Responsabilidad sobre los activos
Porcentaje de los activos de información 1 anali ados en cada fase
Porcentaje de los activos de información crítica 4 para los que se implementó los planes de tratamiento de riesgos de seguridad de la información y se mantuvo estos
7.2 Clasificación de la información
Porcentaje de los activos de información en cada categoría de clasificación
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
8.1 Antes del empleo
Porcentaje del personal nuevo (funcionarios, 3ó4 contratistas, consultores, etc.) que han sido investigados y han aprobado, de acuerdo a las políticas de la institución, antes de comenzar a trabajar
8.2 Durante el empleo
Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, activos e inactivos
8.3 Cese del empleo o cambio de puesto d tr bajo
Porcentaje de activos devueltos
Media de tiempo en la retirada de accesos
9. SEGURIDAD FÍSICA Y DEL ENTORNO
9.1 Áreas seguras
Número de revisiones periódicas de seguridad física de las instalaciones
9.2 Seguridad de los equipos
Mantenimientos a los dispositivos de las instalaciones en relación a los planificados.
Mantenimientos a los equipos efectuados en relación a los planificados.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Responsabilidades y procedimientos de operació
P rcentaje de implementaciones de soluciones a vulnerabilidades de sistemas
Porcentaje de implementación actualizaciones sistemas.
Porcentaje de solicitudes atendidas referentes a cambios
10.2 Gestión de la provisión de servicios por terceros
Evaluación de los costos del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio.
Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega y costos
10.3 Planificación y aceptación del sistema
Porcent je de proyectos Implementados
10.4 Protección contra el código malicioso y descargable
Porcentaje de código malicioso no detectado
Número de descargas por parte de los usuarios no permitido y efectuado
10.5 Copias de seguridad
Porcentaje de backups con éxito de sistemas críticos e importantes
10.6 Gestión de la seguridad de las redes
Número de incidencias de seguridad de red en el mes
10.7 Manipulación de los soportes
Evaluación de medidas de seguridad adoptadas para la gestión de soportes
10.8 Intercambio de información
Evaluación de medidas de seguridad adoptadas en el intercambio de información
10.10 Supervisión
Número/porcentaje de eventos o incidentes de seg ridad que han sido correctamente registrados y analizados
11. CONTROL DE ACCESO
11.1 Requisitos de negocio para el control de acceso
Evaluación de consistencia entre lo establecido en la política y la clasificación de criticidad de activos
11.2 Gestión de acceso de usuario
Porcentaje de usuarios con contraseñas débiles
Número de incidentes relacionados con privilegios mal asignados
11.3 Responsabilidades de usuario
Porcentaje de usuarios/puestos de trabajo cuyas responsabilidades en seguridad de la información se encuentran formalmente aceptadas
11.4 Control de acceso a la red
Evaluación de logs y estadísticas identificando la relación numérica entre vulnerabilidades aprovechadas e intentos de accesos o ataques bloqueados y repelidos
11.5 Co trol de acceso al sistema operativo
Nivel de existencia de registro seguro
Nivel de existencia de contraseñas robustas
Nivel de existencia de técnicas de autenticación
Nivel de existencia de cierre de sesiones inactivas
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

12.2 Tratamiento correcto de las aplicaciones
Porcentaje de sistemas para los cuales los controles de validación de datos se han definido e implementado, y se han demostrado eficaces mediante pruebas
12.4 Seguridad de los archivos de sistema
Porcentaje de sistemas evaluados conformes en relación a la norma iva de seguridad existente en estas materias respecto a aquellos que no han sido evaluados, o no han aprobado la normativa
12.5 Seguridad en los procesos de desarrollo y soporte
Porcentaje de procesos de cambios que se han realizado conforme a la normativa existente al respecto, en relación al total de cambios solicitados y realizados
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
13.1 Notificación de eventos y puntos débiles de seguridad de la información
Número de notificac ón de eventos de seguridad de la información
Número de notificación de puntos débiles de seguridad
13.2 Gestión de incidentes y mejoras de seguridad de la información
Número de evidencias recopiladas
14. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO
14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocio
Porcentaje de centros de responsabilidad con planes de continuidad del negocio que han sido adecuadamente documentados y probados con pruebas dentro de los últimos 12 meses.
15. CUMPLIMIENTO
15.1 Cumplimiento de los requisitos legales
Número de requerimientos legales agrupados y analizados por estado y nivel de significación o riesgo
Número de políticas internas y otros requerimientos agrupados y analizados por estado y nivel de significación o riesgo
Porcentaje revisiones de cumplimiento de SI sin registros de incumplimientos substanciales de los controles.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico
Porcentaje revisiones de cumplimiento de SI sin registros de incumplimientos substanciales de los controles
15.3 Consideraciones sobre las auditorías de los sistemas de la información
Número de recomendaciones de auditoría agrupados y analizados por estado y nivel de significación o riesgo
Porcentaje de hallazgos de auditoría de SI que se han resuelto y cerrado, respecto del total que se abrió en el mismo período.

3.13 Declaración de aplicabilidad

DECLARACIÓN DE APLICABILIDAD		
9. SEGURIDAD FÍSICA Y DEL ENTORNO		
9.1 Áreas seguras		
9.1.5 Trabajo en áreas seguras	N.A. - No aplica	El lugar es alquilado, por tanto seguridad de la zona no aplica a los controles de la empresa
9.1.6 Áreas de acceso público y de carga y descarga	N.A. - No aplica	No existen tales zonas en el negocio de la empresa
9.2 Seguridad de los equipos		
9.2.5 Seguridad de los equipos fuera de las instalaciones	N.A. - No aplica	No es posible extraer material de la empresa, no existen tampoco máquinas con ese fin.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES		
10.6 Gestión de la seguridad de las redes		
10.6.1 Controles de red	N.A. - No aplica	La red no forma parte de los controles de la empresa, ya que la red es parte de UPC y por tanto, es esta quien controla su perímetro.
10.9 Servicios de comercio electrónico		
10.9.1 Comercio electrónico	N.A. - No aplica	La empresa no tiene negocios electrónicos
10.9.2 Transacciones en línea	N.A. - No aplica	La empresa no tiene negocios electrónicos ni relacionados con transacciones económicas en línea
11. CONTROL DE ACCESO		
11.4 Control de acceso a la red		
11.4.2 Autenticación de usuario para conexiones externas	N.A. - No aplica	No exsite posibilidad de acceso remoto a los recursos
11.4.7 Control de encaminamiento a la red	N.A. - No aplica	La red no forma parte de los controles de la empresa, ya que la red es parte de UPC y por tanto, es esta quien controla su perímetro.