UOC Universitat Oberta de Catalunya www.uoc.edu
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili
UIB Universitat de les Illes Balears

Master interuniversitario en Seguridad de las TIC

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 EN LA EMPRESA GESPA

Autor: *José Francisco Romano Herrera*
Director: *Antonio José Segovia Henares*
Fecha presentación: junio 2019

Agradecimientos:

A mi esposa Toñi y a mis hijos Laura, José Francisco y Adrián.

Resumen:

La información es uno de los principales activos de una gran parte de las empresas a nivel mundial. Por ese motivo, es importante tomar las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, disponibilidad e integridad de dicha información.

Para poder proteger adecuadamente la información, es necesario seguir una serie de recomendaciones técnicas y organizativas que hagan que se alcance un nivel adecuado de seguridad de la información de nuestra compañía.

El presente trabajo trata de describir el proceso de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), incluyendo todas las tareas, documentos, procedimientos y medidas organizativas necesarias para cumplir con lo establecido en la norma ISO/IEC 27001:2013, ya que como está demostrado, es una herramienta imprescindible desde el punto de vista de la seguridad, al ofrecernos una visión tanto global como detallada de la seguridad de la información de nuestra empresa en la fase inicial, las medidas necesarias que hay que adoptar para corregir las deficiencias y la situación final después de la aplicación de los proyectos emprendidos.

A la finalización del proceso de implantación de la ISO 27001:2013 se han generado una serie de documentos que formarán parte del sistema de gestión documental del SGSI.

Abstract:

Information is one of the most important assets for the majority of the word´s companies. For this reason, it is important to take the necessary technical and organizational measures to guarantee the confidentiality, availability and integrity of such information.

In order to adequately protect the information, it is necessary to follow some technical and organizational recommendations to achieve de adequate level of security information in our company.

This work tries to describe the Information Security Management System (ISMS) implementation process, including all the tasks, documents, procedures and organizational measures necessary to comply with SO/IEC 27001:2013, since it is demonstrated, it is an essential tool from the point of view of security, because it offers us a global and detailed vision of our company´s security information in the initial phase, the necessary measures that there are to adopt to correct the deficiencies and the final situation after the implementation of the projects undertaken.

At the end of the implementation process of ISO 27001:2013, some documents that will be part of the document management system in the ISMS have been generated.

Tabla de Contenido

1 SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1 INTRODUCCIÓN

Los datos, o de forma más genérica la información, es uno de los activos que forman parte del legado tanto de las personas físicas, como de las empresas, organizaciones o estados, y como tal, tienen que ser protegidos contra la publicación, pérdida, robo o apropiación indebida por parte de grupos de la competencia o grupos criminales que pretendan sacar provecho de los mismos.

Hasta hace relativamente poco tiempo, la información se encontraba principalmente en soporte físico (papel, diapositivas, fotografías etc.), por lo que la protección de la información se centraba en evitar el acceso no autorizado tanto en la fase de almacenamiento, manejo o transporte de dicha información. Esta protección se basaba en la seguridad física y el control de acceso a la misma (seguridad perimetral, cajas fuertes, armarios de seguridad, zonas de trabajo de acceso restringido etc.), pero hoy en día, con la proliferación de los medios digitales para el almacenamiento, manejo y transporte de datos, se hace necesaria una nueva estrategia de defensa y protección de la información.

En un mundo digital como el que en la actualidad nos encontramos, el concepto de protección ya no se limita al control del acceso a la información para garantizar la confidencialidad, sino que hay que garantizar también la disponibilidad, trazabilidad, integridad y autenticidad de los datos, por lo que hay que dotarse de los medios técnicos y procedimentales necesarios para conseguir esa protección.

Ante la amplitud y complejidad de las amenazas y de los sistemas de manejo de la información, se hizo necesario crear unos estándares y normas que ayudaran al control y gestión de la seguridad de la información. Entre las normas internacionales más conocida están las normas de la familia ISO 27000, y más concretamente la ISO 27001 y la ISO 27002, que son las que vamos a usar a lo largo del presente trabajo.

Una vez que se ha decidido la norma y los códigos de buenas prácticas que se van a seguir para garantizar la seguridad de la información, es necesario crear el Plan Director de Seguridad, que es el documento que establece lo que hay que hacer para alcanzar el grado de seguridad requerido por la empresa de acuerdo a sus características propias, y conseguir los objetivos marcados por la dirección.

El presente trabajo pretende realizar el Plan de Implementación de la ISO 27001:13 a la empresa GESPA, para lo que se realizará un estudio en profundidad de la situación inicial y se elaborarán los informes correspondientes y las recomendaciones necesarias para conseguir que el sistema obtenga la certificación de acuerdo a la ISO 27001:2013.

1.2 DEFINICIONES DE TÉRMINOS

En este apartado se recogen las definiciones de los términos utilizados en este trabajo. Las definiciones y términos están recogidas de la ISO 27000.

- control de acceso:

Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

- ataque:

Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo.

- atributo:

Propiedad o característica de un objeto que es cuantitativa o cualitativamente distinguible por medios humanos o automáticos.

- auditoría:

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- alcance de la auditoría:

Extensión y límites de una auditoría.

- autenticación:

Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma.

- autenticidad:

Propiedad consistente en que una entidad es lo que dice ser.

- disponibilidad:

Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

- medida básica:

Medida definida por medio de un atributo y el método para cuantificar.

- competencia:

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

- confidencialidad:

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

- conformidad:

Cumplimiento de un requisito.

.

- consecuencia:

Resultado de un suceso que afecta a los objetivos.

- mejora continua:

Actividad recurrente para mejorar el desempeño.

- control:

Medida que modifica un riesgo.

- objetivo de control:

Declaración que describe lo que se quiere lograr como resultado de la implementación de controles

- corrección:

Acción para eliminar una no conformidad detectada.

- acción correctiva:

Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir.

- datos:

Conjunto de valores asociados a medidas básicas, medidas derivadas y/o indicadores

- información documentada:

Información que una organización tiene que controlar y mantener, y el medio en el que está contenida.

- evento:

Ocurrencia o cambio de un conjunto particular de circunstancias.

- dirección ejecutiva:

Persona o grupo de personas en la(s) que los órganos de gobierno han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la organización.

- gobernanza de la seguridad de la información:

Sistema mediante el cual una organización dirige y supervisa las actividades de seguridad de la información.

- órgano de gobierno:

Conjunto de personas que responden y rinden cuentas del desempeña de la organización

- indicador:

Medida que proporciona una estimación o una evaluación usando un modelo analítico para satisfacer unas determinadas necesidades de información.

- recursos (instalaciones) de tratamiento de información:

Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

- seguridad de la información:

Preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

- continuidad de la seguridad de la información:

Procesos y procedimientos para asegurar la continuidad de las actividades relacionadas con la seguridad de la información.

- evento o suceso de seguridad de la información:

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información , un fallo de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

- incidente de seguridad de la información:

Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

- gestión de incidentes de seguridad de la información:

Procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información.

- sistema de información:

Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

- integridad:

Propiedad de exactitud y completitud.

- parte interesada:

Persona u organización que puede afectar, estar afectada. o percibir que está afectada por una decisión o actividad.

- contexto interno:

Entorno interno en el que la organización busca alcanzar sus objetivos.

- proyecto del SGSI:

Actividades estructuradas llevadas a cabo por una organización para implementar un SGSI.

- nivel de riesgo:

Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.

- sistema de gestión:

Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos

- medida:

Variable a la que se le asigna un valor como resultado de una medición.

- no conformidad:

Incumplimiento de un requisito.

- no repudio:

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.

- objetivo:

Resultado a lograr.

- política:

Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.

- proceso:

Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

- fiabilidad:

Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

- requisito:

Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.

- riesgo residual:

Riesgo remanente después del tratamiento del riesgo.

- riesgo:

Efecto de la incertidumbre sobre la consecución de los objetivos.

- aceptación del riesgo:

Decisión informada en favor de tomar un riesgo particular.

- análisis del riesgo:

Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- apreciación del riesgo:

Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

- comunicación y consulta del riesgo:

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas, en relación con la gestión del riesgo.

- criterios de riesgo:

Términos de referencia respecto a los que se evalúa la importancia de un riesgo.

- evaluación del riesgo:

Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

- identificación del riesgo:

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos

- gestión del riesgo:

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

- proceso de gestión del riesgo:

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

- dueño del riesgo:

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

- tratamiento del riesgo:

Proceso destinado a modificar el riesgo.

- parte interesada:

Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

- amenaza:

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- vulnerabilidad:

Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

1.3 INTRODUCCIÓN A LA NORMA ISO 27001 Y LA ISO 27002

A lo largo de la historia, la preocupación por la salvaguarda de la información privada, comercial, militar etc. ha sido una constante en organismos, estados, instituciones y en general de todos los ciudadanos.

La forma de conservarla y de preservarla del posible robo, destrucción o revelación, se basaba en medidas de protección física como podían ser los dispositivos con cerraduras, cajas fuertes o el transporte mediante mensajeros armados.

Con el paso del tiempo se llega a la era digital, donde la información comienza a tratarse de forma masiva y con unos medios inexistentes hasta entonces.

Con la aparición de esta nueva forma de tratar, almacenar y transmitir la información, aparece una nueva forma de delincuencia basada en la explotación de las nuevas vulnerabilidades.

Como medida de protección ante este hecho, aparecen las primeras recomendaciones en el campo de la seguridad de la información. Así por ejemplo en el año 1995 la Biritish Standards Institution publica la BS 7799-1:1995 que eran unas recomendaciones, no una norma certificable.

A partir de esa primera aparición de estas recomendaciones, se comienza a trabajar en una nueva norma que fuese certificable, apareciendo en el año 1998, la BS 7799-2.

En el año 2000, la Organización Internacional para la Estandarización (ISO) saca la ISO 177999, que básicamente es la misma norma de la BS. En el año 2002 se publica una nueva versión de la norma que permitía la acreditación de empresas.

Será en el 2005 cuando aparezca la ISO 27001:2005 y la ISO 17799:2005, siendo la ISO 27001 una norma certificable, convirtiéndose en un estándar sobre la seguridad de la información a nivel internacional.

En 2007 se renombra la ISO 17799 y pasa a ser la ISO 27002:2005, y se hace una revisión de la ISO 27001, apareciendo la ISO 27001:2007.

Por último en 2013, se hace una nueva revisión a la ISO 27001, apareciendo la ISO 27001:2013, que tiene una serie de cambios bastante significativos con relación a versión anterior, como son:

- Desaparece la sección de "enfoque a procesos".
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Cambian los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Se incluye un nuevo dominio sobre "Relaciones con el Proveedor"

La ISO 27001:2013, se encuentra formada por dos partes, la primera está compuesta por 10 apartados

1. **Objeto y campo de aplicación:** Establece cuál es el contenido y finalidad de la norma.
2. **Normas para consulta:** Como norma de consulta se establece que se usará la ISO /IEC 27000, "Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad"
3. **Término y definiciones:** Establece que los términos y definiciones usados son los que aparecen en la norma ISO/IEC 27000.
4. **Contexto de la organización:** Se determinan las necesidades y expectativas de la organización, que afecten directa o indirectamente al sistema de gestión de la seguridad de la información.
5. **Liderazgo:** Se hace hincapié en la importancia que tiene que la alta dirección se involucre en el Sistema de Gestión de la Seguridad de la Información, y en todo lo relativo a la implantación y mantenimiento del SGSI.
6. **Planificación:** Trata sobre la evaluación y gestión de riesgos, así como los planes que hay que llevar a cabo para lograr hacer el análisis, evaluación y gestión de dichos riesgos.
7. **Soporte:** Trata sobre los recursos que la organización tiene que destinar a la Seguridad de la información para conseguir que lo previsto el Plan de Seguridad se lleve a buen término.
8. **Operación:** Trata sobre la forma en que la organización debe de planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de la seguridad de la información, así como de la apreciación y el tratamiento de los riesgos.
9. **Evaluación de desempeño:** En este apartado se trata de hacer un seguimiento, medición, análisis y evaluación del desempeño y eficacia, así como de las auditorías internas programadas y de la revisión del sistema de gestión de la seguridad de la información por parte de la dirección.
10. **Mejora:** Trata sobre las no conformidades, las acciones correctivas y la mejora continua.

En la otra parte, está el anexo A, en donde se establecen los objetivos de control y los controles de referencia y está formado por 14 dominios y 114 controles.

La ISO 27002:2013 es un estándar de seguridad de la información que proviene de la ISO/IEC 17799:2005, aunque no es una norma certificable, sino que es una guía de buenas prácticas, al contrario que la ISO 27001 que sí es certificable y especifica qué requisitos son necesarios para implantar mantener y mejorar el Sistema de Gestión de la Información.

Tal como se ha dicho antes, está formada por 14 dominios y 114 controles.

Los dominios son:

- Políticas de Seguridad
- Organización de la Seguridad de la Información
- Seguridad de los Recursos Humanos.
- Gestión de los Activos.
- Control de Accesos
- Cifrado
- Seguridad Física
- Seguridad de las Operaciones procedimientos y responsabilidades
- Seguridad de las Comunicaciones
- Adquisiciones de sistemas, desarrollo y mantenimiento.
- Relaciones con los Proveedores.
- Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
- Conformidad

La ISO 27002, no hace distinción entre los controles que son aplicables a una organización y los que no lo son.

1.4 OBJETIVOS DEL PLAN DIRECTOR.

Los objetivos del presente trabajo los podemos dividir en:

1.4.1 OBJETIVOS GENERALES.

Como objetivos generales están el aumento de la seguridad de los sistemas de información de la empresa y la obtención de la certificación de acuerdo a la norma ISO 27001:2013, para ello, se hará una evaluación de la empresa que determine su grado de cumplimiento, y se realizarán los cambios tanto operativos como técnicos que hagan que ésta pueda obtener la certificación.

Al final del proceso, se deberían de proponer unas recomendaciones que hiciesen que la empresa cumpliese con lo establecido en la norma.

Una vez obtenida la certificación, el objetivo final es el mantenimiento de la misma, para lo que se deberán de realizar las auditorías tanto internas como externas que se necesiten.

1.4.2 OBJETIVOS ESPECÍFICOS.

Como objetivos específicos del trabajo están:

- Conseguir una mayor conciencia de seguridad de los empleados.
- Aumento de los niveles de seguridad (confidencialidad, disponibilidad e integridad) de la información que maneja, almacena y transmite la empresa
- Conseguir mayor nivel de confianza de los clientes en nuestro sistema TIC.
- Reducir los incidentes de seguridad como son el robo o pérdida, de información o dispositivos.
- Obtener la certificación de la ISO 27001 para poder optar a ciertos proyectos.
- Aumento de la seguridad la transmisión de información y de las comunicaciones.

1.5 ALCANCE

Dentro alcance del Plan Director está la evaluación de todos los elementos y departamentos implicados en el almacenamiento, manejo y transmisión o transporte de la información, no estando incluido en el mismo, el análisis de los procedimientos operativos ni de explotación de la información.

Dado que en mayor o menor medida todos los departamentos manejan información, el estudio abarcará a toda la organización, y los procedimientos que se establezcan serán de obligado cumplimiento para todos los trabajadores del departamento afectado.

Como parte del alcance está el estudio del equipamiento hardware utilizado, su configuración, el software usado y las medidas de seguridad utilizadas para garantizar la confidencialidad, disponibilidad e integridad de la información, no formando parte del alcance del estudio, el análisis desde el punto de vista de la productividad, del material tanto hardware como software utilizado en la empresa ni los procedimientos operativos.

1.6 DESCRIPCIÓN CONTEXTUAL DE LA EMPRESA

La empresa objeto del estudio se dedica al diseño e instalación de sistemas de control industrial. Está ubicada en una zona industrial de Madrid capital, ocupando dos plantas de un edificio con una superficie total de 4.000 m^2.

Está compuesta por una plantilla de 115 trabajadores con una alta cualificación, de los cuales el 70% son ingenieros.

La empresa ha sufrido una serie de cambios en los últimos tiempos, debido sobre todo a la última crisis económica que afectó considerablemente a su contratación, y por lo tanto, al número de trabajadores.

El edificio dispone de un servicio de vigilancia durante las 24 horas del día, con un sistema de CCTV y de alarmas centralizado en la planta baja, desde donde se visualizan las distintas alarmas, se activan y desactivan zonas y se dan los permisos de acceso a los diferentes usuarios, de acuerdo a los roles facilitados por el departamento de recursos humanos.

El acceso al edificio se realiza a través de un único punto de entrada, donde hay un control de accesos con tornos y una persona en la recepción que controla que sólo las personas autorizadas pasan al edificio.

El acceso al CPD se realiza a través de un sistema de autenticación mediante tarjeta wiegand y huella dactilar, estando el acceso restringido al administrador del sistema, administrador de seguridad y Jefe de Seguridad. Además está equipado con un sistema de detección y extinción de incendios, así como de un sistema de aire acondicionado que mantiene la temperatura y la humedad dentro de los límites establecidos.

En determinadas salas y despachos se han instalado controles de acceso mediante tarjeta wiegand de proximidad.

En la planta baja se encuentran la zona de fabricación, montaje y prueba de equipos, mientras en la primera se encuentra la zona de oficinas, donde está la mayor parte de la actividad de la compañía, ya que es donde se halla el personal de administración, el de I+D, comercial, ingeniería y jefatura de proyectos. La mayor parte del personal se encuentra distribuido en un espacio abierto.

El personal no realiza teletrabajo, aunque a ciertas personas, como son los jefes de proyecto, se les permite el acceso en remoto al ERP de la empresa mediante conexión con VPN, del mismo modo, el personal desplazado que lleva a cabo las instalaciones y puesta a punto, también tiene acceso a ciertos servicios de la empresa a través de VPN.

Al personal que sale a “campo” se le equipa de un ordenador portátil con Windows 7 o Windows 10, software de ofimática, antivirus, navegador Explorer y Firefox, antivirus kaspersky, aplicación cliente para acceso al ERP de la empresa y, dependiendo del perfil del usuario, algún tipo de aplicativo que necesite para realizar labores técnicas, además se le dota de un teléfono móvil con sistema

operativo android en el que se han instalado y configurado aplicaciones predeterminadas por la empresa. Al personal de oficina se le suele proveer de un ordenador de sobremesa con Windows 7 o Windows 10 y las aplicaciones de ofimática, navegador Explorer y Firefox, antivirus Kaspersky, Acrobat reader y el software de gestión necesario.

Se da la circunstancia de que a los usuarios de los portátiles se les otorga privilegios de administrador, ya que en determinadas circunstancias, mientras realizan las labores técnicas, necesitan esos privilegios.

Hay que hacer notar que tanto en los equipos portátiles como en los de sobremesa, no existe un control sobre los dispositivos USB que se les conecta, lo que puede suponer un peligro para la empresa.

Para las comunicaciones voz, a cada puesto de trabajo se le dota de un teléfono digital CISCO IP PHONE 7942.

Aunque más adelante se volverá sobre el equipamiento de la empresa cuando hagamos la valoración de activos, de forma resumida, se puede decir que éste está formada por:

- Red de área local con 2 routers y 4 switches de CISCO
- Un firewall.
- Red wifi para trabajadores.
- Red wifi para visitas.
- 1 servidor de proyectos y comercial.
- 1 servidor para desarrollo.
- 1 servidor de aplicación para administración y financiero.
- 1 servidor de impresión.
- 1 Sistema de backup.
- 80 portátiles.
- 35 ordenadores de sobremesa
- Paquete Gsuite de Google, que incluye correo electrónico, Drive, Calendar, Contactos etc.

1.7 ESTRUCTURA DE LA RED

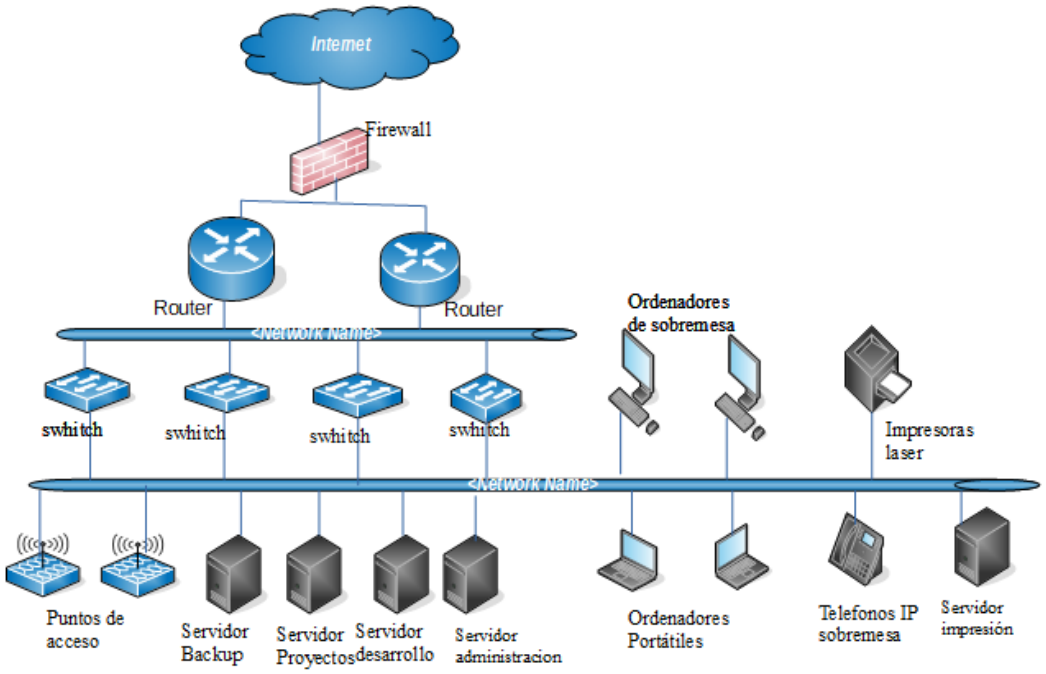


Ilustración 1 Estructura de red.

1.8 ORGANIGRAMA DE LA EMPRESA

El organigrama de la empresa es:

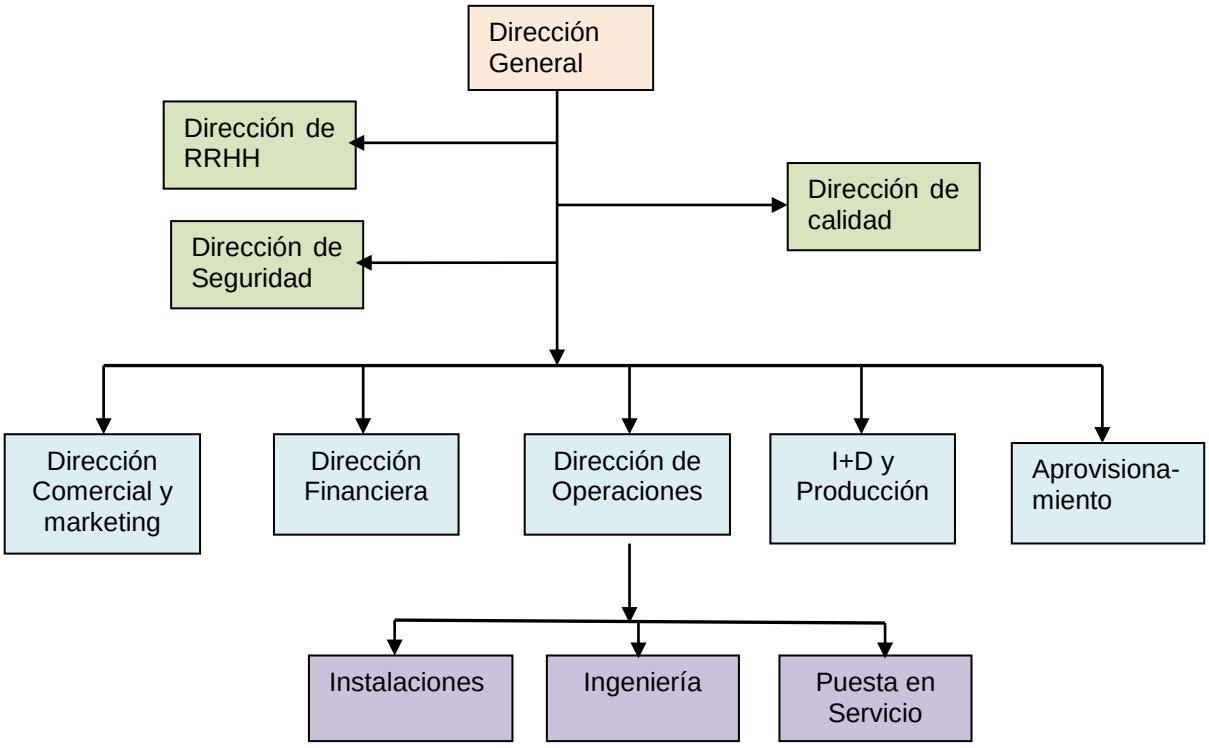


Figura 2 Organigrama de la compañía

La estructura de la empresa está orientada a la ejecución “llave en mano” de proyectos, abarcando desde el desarrollo de nuevos elementos que se necesiten en el mercado del control industrial, hasta la elaboración del proyecto de ejecución, instalación y puesta en servicio.

En la actualidad se están explorando nuevos mercados tanto desde el punto de vista tecnológico como de nuevos países. En concreto se está introduciendo en el mundo de la seguridad física, dada la similitud que existe entre el control industrial y los sistemas de recepción de alarmas y envío de órdenes de control a los diferentes componentes del sistema. Sólo cambian los sensores, el HMI y los procedimientos de actuación.

La responsabilidad última de la empresa recae sobre la Dirección General, quien a su vez se ve apoyada por el comité de dirección. Los cometidos de las distintas direcciones son:

- Dirección de Recursos Humanos: Es el responsable de todo lo relativo a contratación de personal, políticas de incentivos, gestión de nóminas, Prevención de Riesgos Laborales, formación, etc.
  En esta dirección también se encuadra el departamento de servicios generales e informática de cuyo responsable depende la gestión y explotación de dichos servicios.

- Dirección de Seguridad: Tiene bajo su responsabilidad todo lo relativo a la seguridad de la información y la protección de los activos de la empresa.

- Dirección de Calidad: La empresa dispone de los certificados de calidad ISO 9001:2015, ISO 14001 y OHSAS 18001. Es la dirección encargada de que todos los procesos productivos de la compañía se desarrollen de acuerdo a las normas de calidad y a los procedimientos establecidos por ésta. Tiene a la vez la responsabilidad de las auditorías internas de calidad y de la gestión de las auditorías externas.

- Dirección Comercial y marketing: Es donde recae la responsabilidad de conseguir nuevos contratos y explorar nuevos mercados. Está formado por el director comercial, 3 administrativos, 8 ingenieros de ofertas y 6 comerciales que se encargan de los clientes según la zona adjudicada a nivel mundial.

- Dirección financiera: Tiene la responsabilidad de realizar la gestión económica de la empresa, estando entre sus cometidos, el pago de facturas a proveedores, análisis financiero mensual, previsiones de caja, emisión y cobro de las facturas a los clientes etc.

- Dirección de Operaciones: Es donde se encuentra el mayor volumen de personal de la empresa. En esta dirección se está encuadrada:

- la Ingeniería de Ejecución cuya misión es la elaborar los proyectos técnicos de las obras que hay que ejecutar

- el departamento de instalaciones, que son los encargados de ejecutar las obras en campo y hacer la preinstalación de elementos antes de enviarlos a las instalaciones, como pueden ser los racks, cuadros de control, cuadros eléctricos etc.

- el departamento de puesta en servicio, formado por el personal técnico que realiza la puesta en marcha y la configuración de las instalaciones.

- I+D y Producción: Es el encargado de realizar los nuevos desarrollos de los elementos de control, así como la fabricación de las tarjetas necesarias para la ejecución de los proyectos.

- Aprovisionamiento: Es el departamento responsable de evaluar a nuevos proveedores, hacer los pedidos y gestionar el almacén de la empresa.

1.9 PLANIFICACIÓN DEL PROYECTO

La planificación de las actividades del presente Trabajo Fin de Master, viene marcado por los requerimientos temporales para la presentación de los diferentes entregables.

El trabajo se ha dividido en fases, de tal forma que con la finalización de cada una de ellas, y la entrega del material requerido, se va avanzando de forma secuencial, cumpliendo cada uno de los hitos marcados.

En el siguiente diagrama de Gantt, se refleja la planificación prevista para la realización de este TFM.

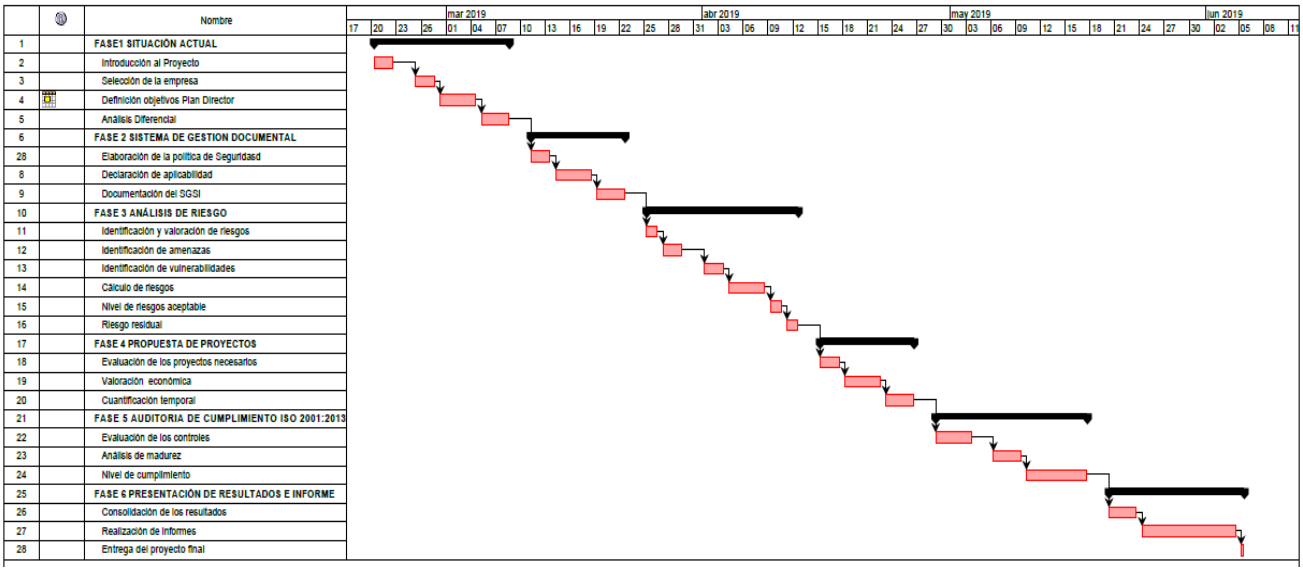


Ilustración 3 Diagrama de gantt

En la tabla siguiente aparece cada una de las actividades con su fecha de inicio y de fin, que coinciden con las recogidas en el diagrama de Gantt.

TAREA	Fecha Inicio	Fecha final
FASE1 SITUACIÓN ACTUAL	20/02/2019 8:00	08/03/2019 17:00
Introducción al Proyecto	20/02/2019 8:00	22/02/2019 17:00
Selección de la empresa	25/02/2019 8:00	27/02/2019 17:00
Definición objetivos Plan Director	28/02/2019 8:00	04/03/2019 17:00
Análisis Diferencial	05/03/2019 8:00	08/03/2019 17:00
FASE 2 SISTEMA DE GESTION DOCUMENTAL	11/03/2019 8:00	22/03/2019 17:00
Elaboración de la política de Seguridad	11/03/2019 8:00	13/03/2019 17:00
Declaración de aplicabilidad	14/03/2019 8:00	18/03/2019 17:00
Documentación del SGSI	19/03/2019 8:00	22/03/2019 17:00
FASE 3 ANÁLISIS DE RIESGO	25/03/2019 8:00	12/04/2019 17:00
Identificación y valoración de riesgos	25/03/2019 8:00	26/03/2019 17:00
Identificación de amenazas	27/03/2019 8:00	29/03/2019 17:00
Identificación de vulnerabilidades	01/04/2019 8:00	03/04/2019 17:00
Cálculo de riesgos	04/04/2019 8:00	08/04/2019 17:00
Nivel de riesgos aceptable	09/04/2019 8:00	10/04/2019 17:00
Riesgo residual	11/04/2019 8:00	12/04/2019 17:00
FASE 4 PROPUESTA DE PROYECTOS	15/04/2019 8:00	26/04/2019 17:00
Evaluación de los proyectos necesarios	15/04/2019 8:00	17/04/2019 17:00
Valoración económica	18/04/2019 8:00	22/04/2019 17:00
Cuantificación temporal	23/04/2019 8:00	26/04/2019 17:00
FASE 5 AUDITORIA DE CUMPLIMIENTO ISO 2001:2013	29/04/2019 8:00	17/05/2019 17:00
Evaluación de los controles	29/04/2019 8:00	03/05/2019 17:00

Análisis de madurez	06/05/2019 8:00	09/05/2019 17:00
Nivel de cumplimiento	10/05/2019 8:00	17/05/2019 17:00
FASE 6 PRESENTACIÓN DE RESULTADOS E INFORME	20/05/2019 8:00	05/06/2019 17:00
Consolidación de los resultados	20/05/2019 8:00	23/05/2019 17:00
Realización de informes	24/05/2019 8:00	04/06/2019 17:00
Entrega del proyecto final	05/06/2019 8:00	05/06/2019 17:00

Tabla 1 Fechas de ejecución previstas

1.10 ANÁLISIS DIFERENCIAL

Antes de iniciar el proyecto de implantación, tendremos que realizar un análisis diferencial de las medidas de seguridad y la normativa que tenga la Organización en relación a la Seguridad de la Información. Este análisis nos va a dar una orientación del grado de cumplimiento de la empresa con relación a los requisitos de la ISO/IEC 27001 e ISO/IEC 27002, y nos permitirá conocer de manera global el estado actual de la compañía en relación a dicha Seguridad de la Información.

1.10.1 ANÁLISIS DIFERENCIAL CON RESPECTO A LA ISO 27001:2013

	Requerimientos ISO 27001	Evaluación	Valor	Total
4	**Contexto de la organización**			1
4.1	Comprensión de la organización y de su contexto	2 - Repetible	2	2
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	2 - Repetible	2	2
4.3	Determinación del alcance del SGSI	0 - No existente	0	0
4.4	SGSI	0 - No existente	0	0
5	**Liderazgo**			1
5.1	Liderazgo y compromiso	1 - Inicial	1	1
5.2	Política	0 - No existente	0	0
5.3	Roles, responsabilidades y autoridades en la organización	2 - Repetible	2	2
6	**Planificación**			2
6.1	Acciones para tratar los riesgos y oportunidades	2 - Repetible	2	2
6.2	Objetivos de seguridad de la información y planificación para su consecución	2 - Repetible	2	2
7	**Soporte**			0,5
7.1	Recursos	0 - No existente	0	0
7.2	Competencia	1 - Inicial	1	1
7.3	Concienciación	1 - Inicial	1	1
7.4	Comunicación	0 - No existente	0	0
8	**Operación**			0,67
8.1	Planificación y control operacional	1 - Inicial	1	1
8.2	Apreciación de los riesgos de seguridad de la información	0 - No existente	0	0

8.3	Tratamiento de los riesgos de seguridad de la información	1 - Inicial	1	1
9	**Evaluación del desempeño**			1
9.1	Seguimiento, medición, análisis y evaluación	0 - No existente	0	0
9.2	Auditoría interna	3 - Definido	3	3
9.3	Revisión por la dirección	0 - No existente	0	0
10	**Mejora**			1
10.1	No conformidad y acciones correctivas	2 - Repetible	2	2
10.2	Mejora continua	0 - No existente	0	0

Tabla 2 Análisis Diferencial ISO 27001

1.10.1.1 DIAGRAMA DE RADAR DEL ANÁLISIS DIFERENCIAL CON RESPECTO A LA ISO 27001:2013

Representación gráfica del grado de cumplimiento de los controles de la ISO 27001:2013 por parte de la empresa

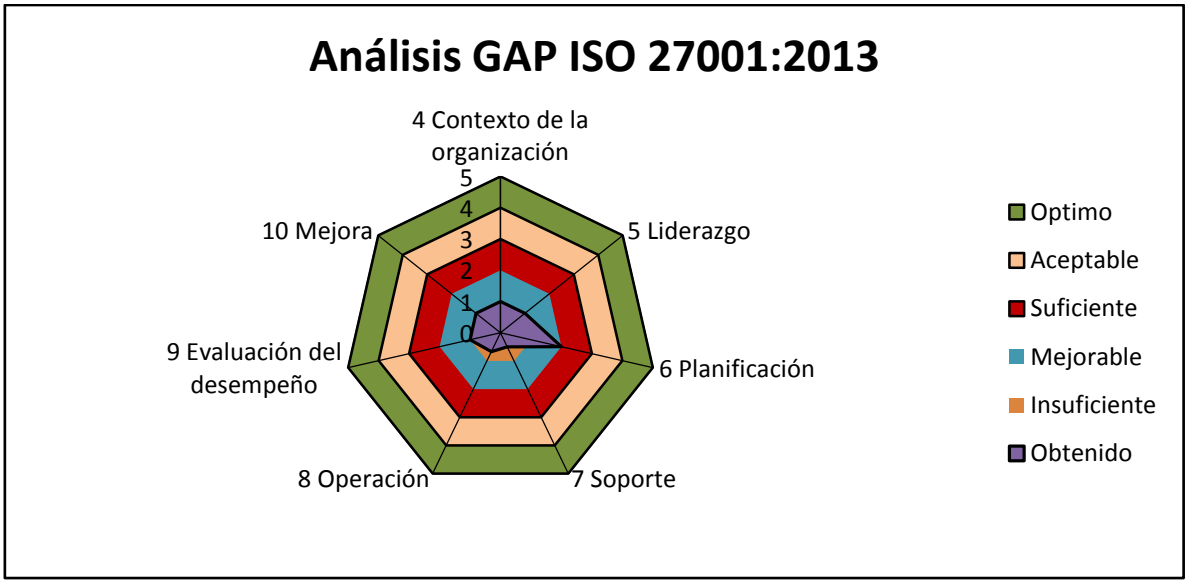


Ilustración 4 Representación gráfica análisis GAP

1.10.2 ANÁLISIS DIFERENCIAL CON RESPECTO A LA ISO 27002

La ISO 27002 no es una norma en sí, sino que es un código de buenas prácticas, y por lo tanto, no es certificable como lo pueda ser la ISO 27001.

Tal como he mencionado anteriormente, para el análisis diferencial nos hemos servido de la ISO 27002:2013, para lo cual, se ha revisado el grado de

cumplimientos que tiene la empresa con relación a cada uno de los 114 controles de los que consta dicha norma. La ISO 27002:2013 tiene 14 dominios de seguridad, 35 objetivos de control y 114 controles y fue concebida para servir de guía en la implantación de un Sistema de Gestión de Seguridad de la Información.

En esa primera fase del estudio, se revisa el grado de implantación de cada uno de los controles, pero como veremos más adelante cuando se haga el análisis de aplicabilidad, no todos los controles tiene que ser de aplicación a nuestra empresa, conforme se vaya haciendo el análisis, se irá viendo si le aplica o no.

CONTROL			Evaluación	Valor	Total
5 Politicas de seguridad de la información					2,5
5.1 Directrices de gestión de la seguridad de la información					2,5
	5.1.1	Políticas para la seguridad de la información	3 - Definido	3	
	5.1.2	Revisión de las políticas para la seguridad de la información	2 - Repetible	2	
6 Organización de la seguridad de la información					1,3
6.1 Organización interna					1,6
	6.1.1	Roles y responsabilidades en seguridad de la información	3 - Definido	3	
	6.1.2	Segregación de tareas	2 - Repetible	2	
	6.1.3	Contacto con las autoridades	2 - Repetible	2	
	6.1.4	Contacto con grupos de interés especial	1 - Inicial	1	
	6.1.5	Seguridad de la información en la gestión de proyectos	0 - No existente	0	
6.2 Dispositivos móviles y el teletrabajo					1
	6.2.1	Política de dispositivos móviles	1 - Inicial	1	
	6.2.2	Teletrabajo	1 - Inicial	1	
7 Seguridad relativa a los recursos humanos					1,16667
7.1 Antes del empleo					1,5
	7.1.1	Investigación de antecedentes	0 - No existente	0	
	7.1.2	Términos y condiciones del empleo	3 - Definido	3	
7.2 Durante el empleo					2
	7.2.1	Responsabilidades de gestión	3 - Definido	3	
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	1 - Inicial	1	
	7.2.3	Proceso disciplinario	2 - Repetible	2	
7.3 Finalización del empleo o cambio en el puesto de trabajo					0
	7.3.1	Responsabilidades ante la finalización o cambio	0 - No existente	0	
8 Gestión de activos					1,19444
8.1 Responsabilidad sobre los activos					2,25
	8.1.1	Inventario de activos	3 - Definido	3	
	8.1.2	Propietario de los activos	3 - Definido	3	
	8.1.3	Uso aceptable de los activos	2 - Repetible	2	
	8.1.4	Devolución de activos	1 - Inicial	1	
8.2 Clasificación de la información					0,66667
	8.2.1	Clasificación de la información	0 - No existente	0	
	8.2.2	Etiquetado de la información	0 - No existente	0	
	8.2.3	Manipulación de la información	2 - Repetible	2	
8.3 Manipulación de los soportes					0,66667
	8.3.1	Gestión de soportes extraíbles	0 - No existente	0	
	8.3.2	Eliminación de soportes	2 - Repetible	2	
	8.3.3	Soportes físicos en tránsito	0 - No existente	0	
9 Control de acceso					2,74167
9.1 Requisitos de negocio para el control de acceso					4
	9.1.1	Política de control de acceso	4 - Gestionado	4	
	9.1.2	Acceso a las redes y los servidores de red	4 - Gestionado	4	
9.2 Gestión de acceso de usuario					3,16667

		9.2.1	Registro y baja de usuario	4 - Gestionado	4	
		9.2.2	Provisión de acceso de usuario	4 - Gestionado	4	
		9.2.3	Gestión de privilegios de acceso	4 - Gestionado	4	
		9.2.4	Gestión de la información secreta de autenticación de los usuarios	0 - No existente	0	
		9.2.5	Revisión de los derechos de acceso de usuario	2 - Repetible	2	
		9.2.6	Retirada o reasignación de los derechos de acceso	5 - Optimizado	5	
	9.3 Responsabilidades del usuario					0
		9.3.1	Uso de la información secreta de autenticación	0 - No existente	0	
	9.4 Control de acceso a sistemas y aplicaciones					3,8
		9.4.1	Restricción del acceso no autorizado a los sistemas y aplicaciones	4 - Gestionado	4	
		9.4.2	Procedimientos seguros de inicio de sesión	4 - Gestionado	4	
		9.4.3	Sistema de gestión de contraseñas	4 - Gestionado	4	
		9.4.4	Uso de utilidades con privilegios del sistema	3 - Definido	3	
		9.4.5	Control de acceso al código fuente de los programas	4 - Gestionado	4	
10 Criptografía						2
	10.1 Controles criptográficos					2
		10.1.1	Política de uso de los controles criptográficos	2 - Repetible	2	
		10.1.2	Gestión de claves	2 - Repetible	2	
11 Seguridad física y entorno						2,97222
	11.1 Áreas seguras					3,16667
		11.1.1	Perímetro de seguridad física	3 - Definido	3	
		11.1.2	Controles físicos de entrada	4 - Gestionado	4	
		11.1.3	Seguridad de oficinas, despachos y recursos	3 - Definido	3	
		11.1.4	Protección contra las amenazas externas y ambientales	3 - Definido	3	
		11.1.5	El trabajo en áreas seguras	2 - Repetible	2	
		11.1.6	Áreas de carga y descarga	4 - Gestionado	4	
	11.2 Seguridad de los equipos					2,77777
		11.2.1	Emplazamiento y protección de equipos	3 - Definido	3	
		11.2.2	Instalaciones de suministro	3 - Definido	3	
		11.2.3	Seguridad del cableado	0 - No existente	0	
		11.2.4	Mantenimiento de equipos	3 - Definido	3	
		11.2.5	Retirada de material propiedad de la empresa	3 - Definido	3	
		11.2.6	Seguridad de los equipos fuera de las instalaciones	3 - Definido	3	
		11.2.7	Reutilización o eliminación segura de equipos	4 - Gestionado	4	
		11.2.8	Equipo de usuario desatendido	4 - Gestionado	4	
		11.2.9	Política de puestos de trabajo despejado y pantalla limpia	2 - Repetible	2	
12 Seguridad de operaciones						2,09524
	12.1 Procedimientos y responsabilidades operacionales					1,66667
		12.1.1	Documentación de procedimientos de operación	0 - No existente	0	
		12.1.2	Gestión de cambios	3 - Definido	3	
		12.1.3	Gestión de capacidades	2 - Repetible	2	
		12.1.4	Separación de recursos de desarrollo, prueba y operación	0 - No existente	0	
	12.2 Protección contra el software malicioso (malware)					2
		12.2.1	Controles contra el código malicioso	2 - Repetible	2	

12.3 Copias de seguridad					4
	12.3.1	Copias de seguridad de la información	4 - Gestionado	4	
12.4 Registros y supervisión					0
	12.4.1	Registro de eventos	0 - No existente	0	
	12.4.2	Protección de la información de registro	0 - No existente	0	
	12.4.3	Registros de administración y operación	0 - No existente	0	
	12.4.4	Sincronización de reloj	0 - No existente	0	
12.5 Control del software en explotación					3
	12.5.1	Instalación del software en explotación	3 - Definido	3	
12.6 Gestión de vulnerabilidades técnicas.					2
	12.6.1	Gestión de las vulnerabilidades técnicas	1 - Inicial	1	
	12.6.2	Restricción en la instalación del software	3 - Definido	3	
12.7 Consideraciones sobre la auditoría de sistemas de información					2
	12.7.1	Controles de auditoría de sistemas de información	2 - Repetible	2	
13 Seguridad de las comunicaciones					2,33333
13.1 Gestión de la seguridad de redes					2,66667
	13.1.1	Controles de red	2 - Repetible	2	
	13.1.2	Seguridad de los servidores de red	3 - Definido	3	
	13.1.3	Segregación en redes	3 - Definido	3	
13.2 Intercambio de información					2
	13.2.1	Políticas y procedimientos de intercambio de información	2 - Repetible	2	
	13.2.2	Acuerdos de intercambio de información	0 - No existente	0	
	13.2.3	Mensajería electrónica	3 - Definido	3	
	13.2.4	Acuerdos de confidencialidad o no revelación	3 - Definido	3	
14 Adquisición, desarrollo y mantenimiento de los sistemas de información					2,66667
14.1 Requisitos de seguridad en sistemas de información					1,66667
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	2 - Repetible	2	
	14.1.2	Asegurar los servicios de aplicaciones en redes públicas	2 - Repetible	2	
	14.1.3	Protección de las transacciones de servicios de aplicaciones	1 - Inicial	1	
14.2 Seguridad en el desarrollo y en los procesos de soporte					3,33333
	14.2.1	Políticas de desarrollo seguro	3 - Definido	3	
	14.2.2	Procedimiento de control de cambios en sistemas	4 - Gestionado	4	
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3 - Definido	3	
	14.2.4	Restricciones a los cambios en los paquetes de software	1 - Inicial	1	
	14.2.5	Principios de ingeniería de sistemas seguros	3 - Definido	3	
	14.2.6	Entornos de desarrollo seguro	4 - Gestionado	4	
	14.2.7	Externalización del desarrollo de software	4 - Gestionado	4	
	14.2.8	Pruebas funcionales de seguridad de sistemas	4 - Gestionado	4	
	14.2.9	Pruebas de aceptación de sistemas	4 - Gestionado	4	
14.3 Datos de prueba					3
	14.3.1	Protección de los datos de prueba	3 - Definido	3	
15 Relación con proveedores					3

15.1 Seguridad en las relaciones con proveedores					3
	15.1.1	Política de seguridad de la información en las relaciones con los proveedores	3 - Definido	3	
	15.1.2	Requisitos de seguridad en contratos con terceros	3 - Definido	3	
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	3 - Definido	3	
15.2 Gestión de la provisión de servicios del proveedor					3
	15.2.1	Control y revisión de la provisión de servicios del proveedor	3 - Definido	3	
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	3 - Definido	3	
16 Gestión de incidentes de seguridad de la información					2,42857
16.1 Gestión de incidentes de seguridad de la información y mejoras					2,42857
	16.1.1	Responsabilidades y procedimientos	1 - Inicial	1	
	16.1.2	Notificación de los eventos de seguridad de la información	3 - Definido	3	
	16.1.3	Notificación de puntos débiles de la seguridad	3 - Definido	3	
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	2 - Repetible	2	
	16.1.5	Respuesta a incidentes de seguridad de la información	2 - Repetible	2	
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	3 - Definido	3	
	16.1.7	Recopilación de evidencias	3 - Definido	3	
17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio					1,5
17.1 Continuidad de la seguridad de la información					3
	17.1.1	Planificación de la continuidad de la seguridad de la información	3 - Definido	3	
	17.1.2	Implementar la continuidad de la seguridad de la información	3 - Definido	3	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	3 - Definido	3	
17.2 Redundancias					0
	17.2.1	Disponibilidad de los recurso de tratamiento de la información	0 - No existente	0	
18 Cumplimiento					3,2
18.1 Cumplimiento de los legales y contractuales					3,4
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	4 - Gestionado	4	
	18.1.2	Derechos de propiedad intelectual (DPI)	4 - Gestionado	4	
	18.1.3	Protección de los registros de la organización	3 - Definido	3	
	18.1.4	Protección y privacidad de la información de carácter personal	4 - Gestionado	4	
	18.1.5	Regulación de los controles criptográficos	2 - Repetible	2	
18.2 Revisión de la seguridad de la información					3
	18.2.1	Revisión independiente de la seguridad de la información	3 - Definido	3	
	18.2.2	Cumplimiento de las políticas y normas de seguridad	3 - Definido	3	
	18.2.3	Comprobación del cumplimiento técnico	3 - Definido	3	

Tabla 3 Análisis Diferencial ISO 27002

En el siguiente cuadro se hace una breve reseña del significado de los valores que toma la columna “Evaluación” de la tabla anterior.

Este cuadro que se basa en el Modelo de Madurez de la Capacidad (CMM):

SIGNIFICADO	DESCRIPCIÓN
Inexistente	No existe ni se tiene conocimiento del proceso al que hace referencia el control.
Inicial	Los procedimientos a los que se refiere el control son llevados a cabo de forma individual, no existe un procedimiento oficial, y el éxito es debido al desempeño personal de cada uno. Estamos en una fase inicial.
Repetible	Los procesos similares se llevan en forma parecida por diferentes personas que hacen la misma tarea. El éxito depende del conocimiento y la experiencia de cada persona, no habiendo por parte de la empresa un entrenamiento formal.
Definido	Los procesos están implantados, documentados y comunicados mediante entrenamiento.
Gestionado	Los procesos a los que hace referencia el control, están completamente implantados de tal forma que se puede seguir su evolución y control, mediante indicadores numéricos y estadísticos.
Optimizado	Los procesos están bajo constante mejora, y mediante los resultados de las métricas de control, se puede ver la desviación con respecto a lo previsto. El sistema está completamente implantado.

Tabla 4 Madurez CMM

1.10.2.1 REPRESENTACIÓN GRÁFICA DEL ANÁLISIS DIFERENCIAL

Representación gráfica del grado de cumplimiento de los controles de la ISO 27002 por parte de la empresa

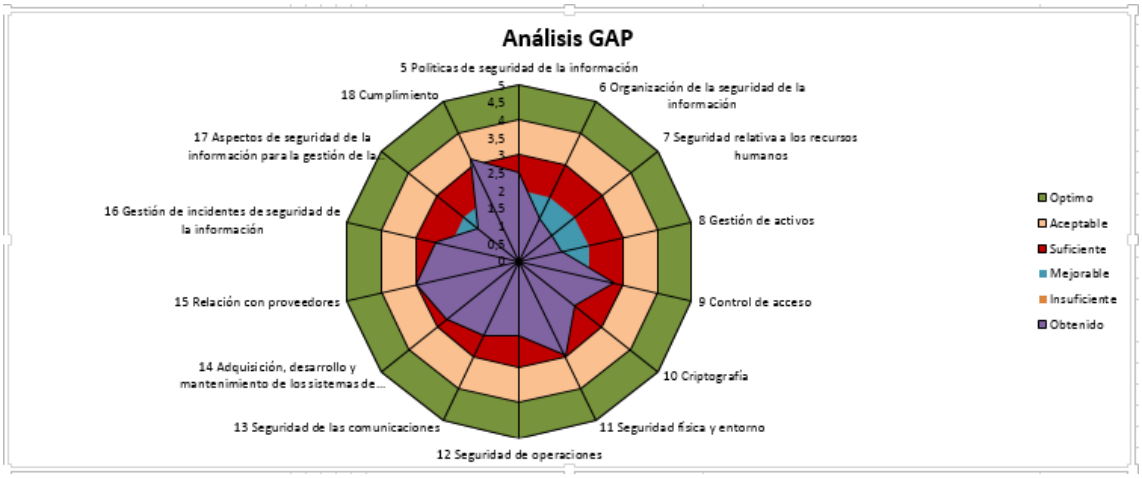


Ilustración 5 Representación gráfica análisis GAP

1.11 CONCLUSIONES:

La conclusión que se puede sacar del análisis diferencial, es que, a pesar de no haberse llevado a cabo una implantación de la seguridad de la información de acuerdo a estándares reconocidos, en líneas generales se encuentra en unos niveles relativamente aceptables de seguridad.

Como se puede apreciar en la gráfica anterior, la mayoría de los dominios (9) se encuentran en unos valores suficientes de seguridad, un total de 4 se encuentran en un nivel mejorable y un dominio (Cumplimiento) se encuentra en un nivel aceptable.

Hace falta mejorar los dominios, pero al menos no se parte de unas calificaciones "Insuficiente" de cumplimiento.

1.12 BREVE DESCRIPCIÓN DEL GRADO INICIAL DE CUMPLIMIENTO DE LOS DOMINIOS.

5 Políticas de seguridad de la información

Existe unas normas publicadas por parte de la dirección, que sin llegar a ser unos procedimientos, establece la manera en que se encuentra organizada la seguridad, tanto física como de la información. En esas normas se manifiesta la obligación que tienen los usuarios de usar los sistemas de forma adecuada y la prohibición de la utilización de los equipos para fines que no estén relacionados con la actividad laboral.

6 Organización de la seguridad de la información

Hay nombrado un Jefe de Seguridad, que es el encargado de coordinar todo lo relativo a la seguridad de la información y a la seguridad física.

No está implantado el uso de VPN por parte de los usuarios, sólo se utiliza en casos excepcionales para conectarse de forma remota. Para poder utilizar la VPN tiene que ser autorizado por la dirección.

Los dispositivos móviles no tienen una especial protección. Los teléfonos móviles tienen instalado un antivirus y unas aplicaciones estándar, pero el usuario puede instalar cualquier app sin que el sistema se lo impida.

7 Seguridad relativa a los recursos humanos

Durante la fase de contratación, no se hace una investigación previa de los candidatos. La contratación se lleva a cabo evaluando el curriculum y realizando una entrevista con un representante de RRHH y con el futuro jefe, quien por regla general elige a la persona que mejor le parece de entre una terna.

Tras la elección del candidato, se le suele hacer un contrato con un período de prueba de 6 meses.

Una vez ha pasado a formar parte de la plantillad, ya no se llevan a cabo ningún muestreo de seguridad. Lo que sí se ha enviado a todo el personal es un comunicado con la obligación de cumplir con el Reglamento de Protección de Datos, pero más que con la intención de hacer cumplir la ley y poner los medios para ello, parece que está hecho con el ánimo de salvaguardar los intereses de la empresa ante cualquier problema o denuncia.

8 Gestión de activos

Existe un inventario de los activos de la empresa, cada ordenador o equipo propiedad de la compañía dispone de un número de identificación que indica dónde se encuentra y bajo la responsabilidad de quién está.

Cuando se reutiliza un dispositivo, o se le entrega a un nuevo usuario, no se lleva a cabo un borrado seguro de la información que contiene. En algunos casos se hace un formateo y reconfiguración del mismo.

9 Control de acceso

Con relación al control de acceso, tanto a la información como a las instalaciones, existen ciertas medidas y reglas.

Cada usuario dispone de una tarjeta de proximidad con su nombre y fotografía, que usa para el acceso al edificio y a ciertas salas dentro de la compañía. Los permisos

de acceso los gestiona el departamento de seguridad pero con la información facilitada por el departamento de recursos humanos.
No se revisa de forma periódica si ha habido cambios en los roles de cada uno de los empleados que haga que ya no necesite algunos de los permisos facilitados.

Con relación al acceso a los sistemas de información, la identificación se lleva cabo mediante usuario y contraseña a través de un directorio activo. Cada 3 meses se obliga al cambio de la contraseña de acceso.

Los usuarios de los ordenadores portátiles tienen derechos de administrador, lo que hace que se pueda producir una situación de especial riesgo para la red de la empresa.

10 Criptografía

No hay una directriz clara sobre el uso de programas o hardware criptográfico. Algunos empleados usan "motu proprio" aplicaciones criptográficas para salvaguardar la confidencialidad de la información, pero no hay unos procedimientos ni unas instrucciones generales al respecto.

Con relación a las claves, pasa algo parecido. Si alguien cifra la información del ordenador, la empresa no puede acceder a la misma, ya que no dispone de las claves.

11 Seguridad física y entorno

Con relación a la seguridad física, se dispone de un sistema perimetral de seguridad equipado con cámaras de visión nocturna y barreras de infrarrojos a lo largo de todo el perímetro del edificio.

En el interior, se disponen de sensores de rotura de cristales, volumétricos y magnéticos de puerta, todos ellos conectados a una central de seguridad, cuyo control se encuentra en la planta baja.

Con relación a la seguridad de los cableados, no se tienen medidas especiales de protección.

El acceso a la zona de desarrollo está protegida por una puerta con control de acceso, que evita que el personal no autorizado acceda a la misma.

12 Seguridad de operaciones

Existe una separación entre los sistemas en producción, los de desarrollo y los de prueba, con el fin de evitar interferencias entre ellos.

Para evitar la instalación de softwares malicioso se dispone del antivirus Kaspersky, además de un firewall que evita conexiones no autorizadas.

Por parte del administrador se llevan a cabo de forma periódica copias de seguridad total, incremental y diferencial. Existe una instrucción donde se recoge cómo se deben de realizar las copias, el soporte en el que hay que hacerlas, cuánto tiempo hay que mantenerlas y dónde hay que guardarlas

13 Seguridad de las comunicaciones

El acceso a los servidores y a los sistemas de gestión de red se encuentra reservado al administrador de red y al de seguridad. La protección se hace mediante controles de accesos y claves.

A las personas que tienen acceso a información sensible de la empresa, se les hace firmar un acuerdo de confidencialidad y no revelación de información.

14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Antes de la implantación de un nuevo sistema, equipo o aplicativo, se llevan a cabo pruebas operativas y de seguridad, impidiendo que un sistema poco maduro pase a producción.

Por parte de la empresa, hay una instrucción que prohíbe la manipulación del software instalado, así como el uso de herramientas de hacking con el fin de obtener acceso a equipos o sistemas.

Los datos de prueba se eliminan una vez que han cumplido su finalidad.

15 Relación con proveedores

A los proveedores de servicio, se les hace firmar una cláusula de confidencialidad con el fin de salvaguardar la confidencialidad de nuestras instalaciones y sistemas.

Por regla general, antes de la contratación con un proveedor, se redacta una instrucción técnica que recoge los requisitos del servicio o del equipo que se va a adquirir, y además se firma un contrato tipo con las cláusulas que los servicios jurídicos han considerado adecuadas.

16 Gestión de incidentes de seguridad de la información

Existe una página donde se debe de reportar cualquier incidente de seguridad que se detecte. Además se establece que también se puede notificar cualquier incidente al correo electrónico del jefe de seguridad. La verdad es que parece ser

que nunca se ha utilizado, cada vez que ha ocurrido algún problema se ha informado verbalmente.

No hay un procedimiento establecido para la respuesta ante un incidente de seguridad de la información. Tan sólo existe para el caso de una intrusión, ya que en ese caso se comunica a la policía para que actúe.

17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Existe un estudio sobre continuidad del negocio en el que se recoge las medidas a tomar en caso de que ocurra una situación catastrófica que ponga en riesgo la continuidad de la empresa. Entre las situaciones planteadas está el incendio, inundación etc.

18 Cumplimiento

Por parte de la compañía se tiene identificada la legislación aplicable en materia de seguridad, de propiedad intelectual y protección de datos.

La empresa se ha adaptado al actual Reglamente de Protección de Datos de Carácter Personal, por lo que protege los datos de acuerdo a la normativa vigente.

2 SISTEMA DE GESTIÓN DOCUMENTAL

2.1 INTRODUCCIÓN

Como suele ocurrir con cualquier norma certificable, con la ISO/IEC 27001:2013 es necesario documentar todos los proceso, procedimientos, auditorías, instrucciones técnicas, hojas de resultados, etc, y en general cualquier evidencia que demuestre el cumplimento de la norma.

La información documentada necesaria para la certificación de nuestro sistema de seguridad de la información, según la ISO/IEC 27001:20013, es bastante amplia, estando formada por procedimientos, registros y evidencias que se recogen en el cuerpo de la norma ISO/IEC 27001:2013, aunque en este trabajo, para reducir el volumen de documentación, vamos a elaborar los siguientes documentos:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores.
- Procedimiento Revisión por la Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgos.
- Declaración de Aplicabilidad

2.2 ESQUEMA DOCUMENTAL

2.2.3 POLÍTICA DE SEGURIDAD:

La Política de Seguridad es un documento de alto nivel donde se recogen los principales objetivos del SGSI. Por regla general es un documento relativamente breve en extensión, ya que el desarrollo de cada uno de los puntos de la política, suele ser objeto de desarrollo aparte.

El documento debe de ser conocido por todos los afectados por el sistema de seguridad de la información, por lo que debe de realizarse la correspondiente difusión para general conocimiento

El objetivo último es el de marcar las directrices que la compañía va a seguir en lo relativo a la Seguridad de la Información.

La Política de Seguridad se encuentra en el **Anexo I. Política de Seguridad**

2.2.4 Procedimiento de Auditorías Internas.

El procedimiento de Auditorías Internas, es el documento que sirve de base para llevar a cabo la auditoría de primera parte que la compañía realiza para determinar el grado de cumplimiento de los requisitos de la ISO 27001 con vistas a detectar posibles incumplimientos.

El procedimiento incluye quién realizará la auditoría, los criterios a seguir en la auditoría, una planificación de las auditorías que se van a realizar a lo largo del período marcado etc.

Como resultado de la auditoría se generará el correspondiente informe con los resultados de la auditoría.

El Programa de Auditorías Internas se recoge en el **Anexo II. "Auditorías Internas"**

2.2.5 Gestión de Indicadores

La implantación de un Sistema de Gestión de la Información de acuerdo a la ISO/IEC 27001, conlleva el compromiso de cumplir con la citada norma.

Para saber en todo momento el grado de efectividad de los controles, es necesario llevar a cabo un muestreo de aquellos que le son de aplicación y que nos dará una idea del grado de cumplimiento actual.

La tabla del documento de gestión de indicadores recoge aquellos indicadores que se usarán para realizar la medición, además de la fórmula utilizada, valor nominal, valor real obtenido y frecuencia con que se realizará la medición.

La gestión de indicadores se encuentra en el **Anexo III. "Gestión de Indicadores".**

2.2.6 PROCEDIMIENTO REVISIÓN POR LA DIRECCIÓN.

En el apartado 9.3 de la norma ISO/IEC 27001:2013 se establece que

"La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de sus conveniencia, adecuación y eficacia continuas."

Con esta revisión por parte de la dirección, se consigue que ésta se involucre en el sistema de gestión de seguridad de la información y a la vez, se faciliten los recursos, se asignen los roles y se vea por parte de todos los interesados el compromiso que existe en la compañía por la seguridad de la información.

El procedimiento de Revisión por la Dirección se encuentra en el **Anexo IV. "Procedimiento de revisión por la Dirección".**

2.2.7 GESTIÓN DE ROLES Y RESPONSABILIDADES.

En el Sistema de Gestión de Seguridad de la Información se deben de especificar qué rol desempeña cada uno de los interesados. Esto es importante en cualquier sistema, pero lo es aún más cuando hablamos de seguridad ya que en algunos casos puede llevar consigo responsabilidad civil o incluso penal.

Los asuntos más importantes relativos a la Seguridad de la Información, deberán de ser tratado en el comité de seguridad. De dicho comité forma parte el Director General, lo que hace que las decisiones allí tomadas son conocidas y respaldadas por la dirección de la compañía.

Se debería de establecer los roles y responsabilidades en todas las políticas y procedimiento, mientras que las funciones y responsabilidades de seguridad para terceros se debería de recoger en los contratos.

El documento de Gestión de Roles y Responsabilidades se encuentra en el **Anexo V. "Gestión de Roles y Responsabilidades".**

2.2.8 METODOLOGÍA DE ANÁLISIS DE RIESGOS.

El análisis de riesgos es la piedra angular de toda la gestión de la seguridad de la información, ya que a partir de dicho análisis cuando conocemos a qué riesgos

estamos sometidos y por lo tanto qué medidas debemos de tomar para mitigarlos, eliminarlo o transmitirlo a un tercero.

El análisis de riesgos no se puede realizar de forma arbitraria y anárquica, sino que se tienen que seguir algún método fiable y ampliamente probado.

La metodología que vamos a utilizar es Magerit v3. .

Magerit es una metodología desarrollada por la Administración pública española, de libre uso. A partir de Magerit, han aparecido una serie de programas como PILAR que ayudan a realizar el análisis de riesgos de los sistemas de seguridad.

El documento de la Metodología de análisis de riesgos se encuentra en el **Anexo VI. "Metodología de Análisis de Riesgos".**

2.2.9 Declaración de Aplicabilidad.

La Declaración de aplicabilidad es un documento clave dentro del Sistema de Gestión de la Seguridad de la Información ya que en él se recogen los controles del Anexo A que son aplicables a nuestra empresa.

La tabla de la Declaración de Aplicabilidad está formada por los 114 controles del Anexo A y si son de aplicación o no.

El documento de declaración de aplicabilidad debe de ser a probado por el comité de seguridad y revisado por la alta dirección, ya que si se parte de un documento que no se ajuste a nuestra compañía, el resultado final del SGSI, no será el adecuado.

El documento de la Declaración de Aplicabilidad se encuentra en el **Anexo VII. "Declaración de Aplicabilidad".**

3 ANÁLISIS DE RIESGOS

3.1 INTRODUCCIÓN

Para poder proteger cualquier activo, lo primero que hay que determinar es su valor y las amenazas a las que se encuentra expuesto, ya que de lo contrario será imposible de preparar la defensa y protección del mismo.

En el presente apartado del trabajo, se va a realizar el análisis de riesgos de nuestro sistema de información y se van a establecer los procesos necesarios para su gestión, con la correspondiente mitigación, eliminación, transferencia o aceptación del riesgo.

El análisis de riesgos se va a realizar desde las cinco dimensiones de seguridad que establece la metodología Magerit, que son la Disponibilidad, la Autenticidad, la Integridad, la Confidencialidad y la Trazabilidad, así como la gestión de dichos riesgos para reducirlos a unos niveles aceptables.

Una vez hecho el análisis, podemos seguir cuatro posibles estrategias a la hora de gestionarlos, que son: evitarlo, reducirlo, transferirlo o asumirlo. En la mayoría de los casos la estrategia a seguir será la de reducir los riesgos, ya que evitarlo puede ser complicado o imposible, dado que podría suponer la no prestación del servicio o el dejar de usar el activo en cuestión, transferirlo podría ser una opción en algunos casos que no implique la cesión del conocimiento y el asumirlo tampoco parece sea una medida adecuada siempre y cuando los niveles de riesgo sean altos.

La gestión de los riesgos es un proceso continuo, que habitualmente se planifica para un periodo de un año, de tal forma que nos permita el seguimiento y la mejora continua del sistema de seguridad de la información.

El análisis de riesgo se basará en el repositorio de salvaguardas y procedimientos asociados a cada una de las medidas del Anexo A de la ISO/IEC 27001, siguiendo la metodología MAGERIT v3.

La gestión de riesgo se hará siguiendo la misma filosofía, es decir, describiendo cómo mejorar la eficacia de las salvaguardas y procedimientos.

3.2 INVENTARIO DE ACTIVOS:

El siguiente paso que hay que seguir en el proceso del análisis y la gestión de los riesgos, es el de realizar el inventario de los activos de la compañía que en mayor o menor grado están relacionados con la seguridad de la información.

Tal como se recoge en el punto 2.1 Activos esenciales del libro II- Catálogo de Elementos de la "Metodología de Análisis y Gestión de riesgos de los Sistemas de Información", en un sistema de información hay dos cosas esenciales, que son:

- la información que se maneja y
- los servicios que prestan.

Desde ese punto de vista, se puede determinar que los activos esenciales de la compañía son las actividades o servicios que hacen que la compañía pueda seguir desarrollando su actividad. A partir de estos activos o servicios esenciales, se determinan los secundarios que le dan soporte.

Los activos esenciales son los que marcan los requisitos de seguridad de los demás componentes del sistema.

Dado que Gespa es una empresa dedicada al desarrollo, tanto software como hardware, a la fabricación, la instalación, la puesta en servicio y el mantenimiento de sistema de control industrial, los activos esenciales serán:

- El servicio de Desarrollo
- El servicio de Instalación
- El servicio de Puesta en servicio
- El servicio de Mantenimiento.

A partir de estos servicios o activos esenciales se determinan los secundarios que le dan soporte como son:

Ámbito	Código	Activo	cantidad	propietario
[L] Instalaciones				
	L.01	CPD	1	Director I+D y producción
	L.02	Oficinas	1	Director General
[HW] Equipamiento hardware				
	HW.01	Pc portátiles	80	Director I+D y producción
	HW.02	Pc de sobremesa	35	Director I+D y producción

	HW.03	Servidor de proyectos	1	Director I+D y producción
	HW.04	Servidor de desarrollo	1	Director I+D y producción
	HW.05	Servidor de administración	1	Director I+D y producción
	HW.06	Servidor de impresión	1	Director I+D y producción
	HW.07	Routers	2	Director I+D y producción
	HW.08	Teléfonos móviles	93	Director I+D y producción
	HW.09	Teléfonos de sobremesa	103	Director I+D y producción
	HW.10	Switches	4	Director I+D y producción
	HW.11	Firewall	1	Director I+D y producción
	HW.12	Impresoras	5	Director I+D y producción
	HW.13	sistema de backup	1	Director I+D y producción
	HW.14	Punto de acceso wifi	1	Director I+D y producción
[SW] Aplicaciones				
	SW.01	Sistemas operativos	115	Director I+D y producción
	SW.02	Software antivirus	115	Director I+D y producción
	SW.03	Aplicaciones ofimáticas.	115	Director I+D y producción
	SW.04	Aplicativo ERP	115	Director I+D y producción
	SW.05	Software de gestión de proyectos	15	Director I+D y producción
	SW.06	Software de desarrollo	30	Director I+D y producción
	SW.07	Aplicación financiera	5	Director I+D y producción
[D] Datos				
	D.01	Datos de clientes	1	Director marketing
	D.02	Datos de proyectos	1	Director operaciones
	D.03	Datos de desarrollo	1	Director I+D y producción
	D.04	Datos de emails	1	Director RRHH
	D.05	Datos personales	1	Director RRHH
[COM] Red de comunicaciones				
	COM.01	Red LAN		Director I+D y producción
	COM.02	red inalámbrica		Director I+D y producción
	COM.03	Telefonía fija		Director I+D y producción
	COM.04	telefonía móvil		Director I+D y producción
	COM.05	Internet.		Director I+D y producción
[SS] Servicios subcontratados				
	SS.01	Correo electrónico	1	Director I+D y producción

[AUX] Equipamiento Auxiliar				
	AUX.01	Sistema de alimentación ininterrumpida	1	Director de instalaciones
	AUX.02	Sistema de alarmas	1	Director de instalaciones
	AUX.03	Sistema contraincendios	1	Director de instalaciones
	AUX.04	Sistema de climatización.	1	Director de instalaciones
[P] Personal				
	P.01	Director general	1	Director general
	P.02	Administrador del sistema	1	Director I+D y producción
	P.03	Usuarios	38	Director RRHH
	P.04	Jefe de Seguridad	1	Director general

Tabla 5 Inventario de activos

Con respecto a los riesgos, el **dueño riesgo** será el propietario del activo al que se encuentre asociado, a menos que las circunstancias aconsejen que otra persona es la más adecuada para gestionarlo, en tal caso, quedará constancia por escrito.

3.3 VALORACIÓN DE ACTIVOS:

En el presente apartado se va a hacer la valoración de los activos de la información de Gespa.

Existen muchas formas de hacer la valoración de los activos de una organización, entre las que se encuentra la valoración económica que sólo tiene en cuenta el valor económico del activo. Sin embargo, la valoración que nos interesa es la de las consecuencias que tendría para la seguridad de la información en caso de degradación del sistema, alteración, ataque etc. La valoración de los activos la vamos a plantear desde el punto de vista de la necesidad de protegerlo, debido a las consecuencias que tendría para la seguridad de la organización, no se está determinando por tanto el valor económico del activo en cuestión.

La valoración de un activo no es un dato aislado, sino que depende de otros activos con los que está relacionado y del que en cierto modo depende la seguridad del mismo.

De acuerdo con punto 3.1.1 del libro 1 de la metodología Magerit, “Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las

comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos."

Lo que se pone de manifiesto es una estructura de árbol, donde la seguridad de los activos que se encuentran en un punto más alto del árbol, dependen de la seguridad de los activos de los que dependen y se encuentran por debajo, es decir, que la seguridad de los activos superiores depende de los activos considerados hijos en la estructura.

De acuerdo con el punto IV.1 "Dependencias entre activos" del Manual de la Herramienta de Análisis de Riesgos PILAR 6.2, las reglas generales para establecer las dependencias son:

- La información esencial depende de los servicios esenciales
- Los servicios esenciales dependen del equipamiento (hw, sw, comunicaciones y soportes de información).
- Los equipos materiales dependen de las instalaciones
- Todos los activos dependen de los usuarios que pueden dañarlos con sus actividades.

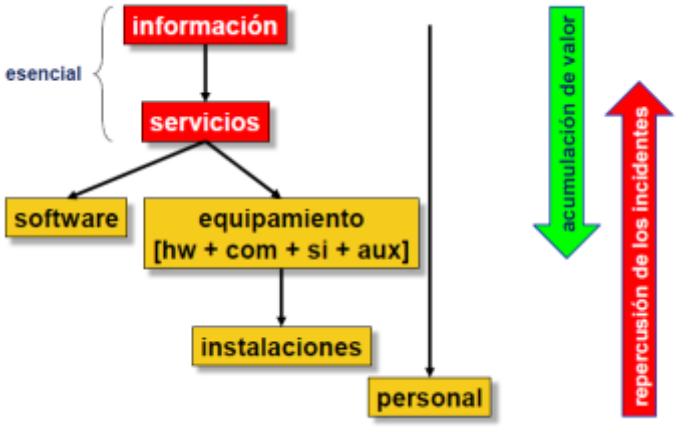


Ilustración 6 Dependencia general entre activos

A partir de la información de nuestros activos, podemos establecer el siguiente diagrama general de dependencias.

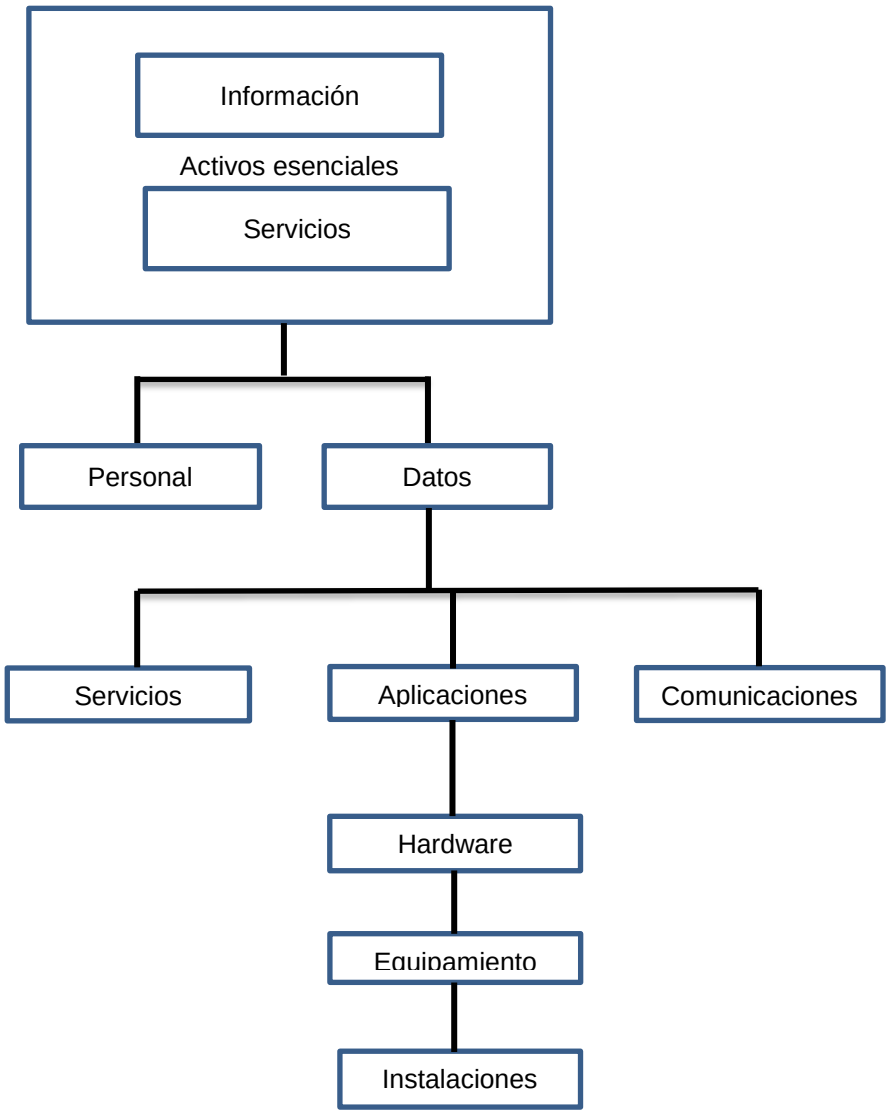


Ilustración 7 Representación gráfica Dependencia entre activos

Por lo tanto, para hacer una buena valoración hay que establecer la relación de dependencia entre los diferentes activos de la compañía. Es por ello, que en el siguiente cuadro no sólo se ha puesto la valoración del activo en base a los valores de la tabla simplificada, sino que también se ha añadido la dependencia entre los diferentes activos. Por ejemplo, el fallo en el funcionamiento de un ordenador puede suponer el no poder acceder a sus datos, o que las aplicaciones que está corriendo en él dejen de estar operativas, y por tanto, puede suponer un riesgo para su seguridad. Otro ejemplo puede ser el suministro de energía, ya que si falla, puede fallar el resto del sistema, y por lo tanto, verse afectada su seguridad.

Ejemplo de las dependencias son:

- El CPD depende del edificio, del sistema de alimentación ininterrumpida y del sistema de climatización, en caso de problemas de seguridad en uno de ellos, afecta a la seguridad del CPD.
- El correcto funcionamiento de los servidores, routers, firewall, switches etc. depende del buen funcionamiento de las instalaciones, del sistema de alimentación ininterrumpida, del sistema de climatización, del sistema contraincendios, y del administrador del sistema, ya que un fallo en el funcionamiento de esos sistemas o un error del administrador, ponen en peligro su seguridad, por lo que dependen de ellos.

Con las dependencias entre los activos se crea el árbol de dependencia que nos da una visión general de cómo influyen entre ellos.

Además de la dependencia entre los activos, hay que determinar, mediante un coeficiente, el grado de dependencia que existe entre ellos.

Tal como se establece en el apartado 2.2.2 del libro 3 de la metodología Magerit, para realizar el cálculo de dependencia, utilizaremos la siguiente fórmula basada en el cálculo de probabilidad de Bayer.

a + b = 1 - (1-a) x (1-b)

Vemos con un ejemplo cómo se calcularía el grado de dependencia entre activos.

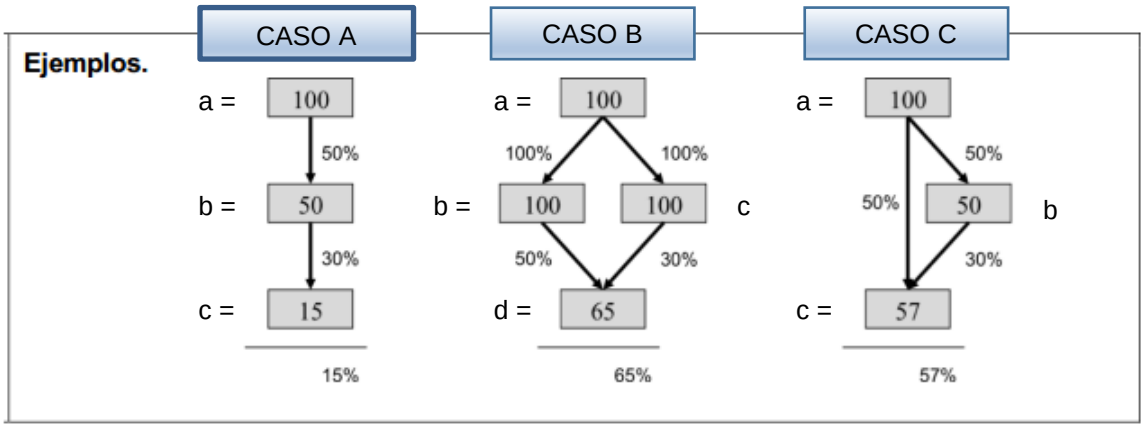


Ilustración 8 Ejemplo cálculo dependencia entre activos

CASO A

a = 100

b = 50 = a x 50%

c = 15 = b x 30%

CASO B

a = 100

b = 100= a x 100%

c = 100 = a x 100%

d= 1-(1- 0,5) x (1- 0,3)= 0, 65 = 65%

CASO C

c = 1 – (1-0,5) x (1 – (0,5 x 0,3)) = 0.575 = 57%

A partir de la dependencia entre activos, se calcula el **valor acumulado**, definiéndose el valor acumulado sobre el activo B, a la suma de los activos superiores del activo B ponderados por el grado de dependencia.

Normalmente el cálculo de las dependencias y el valor acumulado del riesgo, no se suele hacer manualmente, sino que para ello se utiliza la herramienta PILAR del CCN que realiza los cálculos de forma automática.

De acuerdo con lo recomendado en el apartado 2.1 del Libro 3 de la metodología Magerit, la escala que vamos a utilizar para hacer la valoración de los activos es:

- MB: Muy baja
- B: Baja
- M: Media
- A: Alta
- MA: Muy alta

Ambito	Código	Activo	Valor	Dependencia
[L] Instalaciones				
	L.01	CPD	**MA**	[L.02] Edificio [AUX.01] Sistema de alimentación ininterrumpida [AUX.02] Sistema de climatización.
	L.02	Edificio	**A**	
[HW] Equipamiento hardware				
	HW.01	Pc portátiles	**B**	[L.01]CPD [L.02]Edificio
	HW.02	Pc de sobremesa		[L.01]CPD
	HW.03	Servidor de proyectos	**A**	[L.01] CPD [AUX.01] Sistema de alimentación ininterrumpida [AUX.04] Sistema de climatización. [AUX.03]Sistema contraincendios [P.02]Administrador del sistema
	HW.04	Servidor de desarrollo	**A**	
	HW.05	Servidor de administración	**A**	
	HW.06	Servidor de impresión	**B**	
	HW.09	Routers	**A**	
	HW.10	Switches	**M**	
	HW.12	Firewall	**A**	
	HW.13	Sistema de backup	**A**	
	HW.08	Teléfonos de sobremesa	**B**	[L.01]CPD [L.02]Edificio [COM.05]Internet.
	HW.11	Impresoras	**B**	[L.02]Edificio [P.02]Administrador del sistema
	HW.07	Teléfonos móviles	**B**	[COM.04]telefonía móvil
	HW.15	Punto de acceso wifi	**M**	[L.02]Edificio
[SW] Aplicaciones				
	SW.01	Sistemas operativos	**B**	[HW.02]Pc de sobremesa [HW.01]Pc portátiles
	SW.02	Software antivirus	**B**	
	SW.03	Aplicaciones ofimáticas.	**B**	
	SW.04	Aplicativo ERP	**M**	[HW.05]Servidor de administración
	SW.05	Software de gestión de proyectos	**B**	[HW.03]Servidor de proyectos
	SW.06	Software de desarrollo	**M**	[HW.04]Servidor de desarrollo
	SW.07	Aplicación financiera	**A**	[HW.05]Servidor de administración
[D] Datos				
	D.01	Datos de clientes	**A**	
	D.02	Datos de proyectos	**M**	[SW.06]Software de gestión de proyectos
	D.03	Datos de desarrollo	**A**	[SW.07]Software de desarrollo
	D.04	Datos de emails	**A**	[SS.01]Correo electrónico
	D.05	Datos personales	**A**	[SW.08]Aplicación financiera

[COM] Red de comunicaciones				
	COM.01	Red LAN	**M**	[L.02]Edificio
	COM.02	red inalámbrica	**M**	[HW.15]Punto de acceso wifi
	COM.03	Telefonía fija	**B**	[COM.05]Internet.
	COM.04	telefonía móvil	**B**	
	COM.05	Internet.	**MA**	[HW.7]Routers
[SS] Servicios subcontratados				
	SS.01	Correo electrónico	**A**	[COM.05]Internet.
[AUX] Equipamiento Auxiliar				
	AUX.01	Sistema de alimentación ininterrumpida	**A**	[L.02]Edificio
	AUX.02	Sistema de alarmas	**M**	[L.02]Edificio
	AUX.03	Sistema contraincendios	**A**	[L.02]Edificio
	AUX.04	Sistema de climatización.	**A**	[L.02]Edificio
[P] Personal				
	P.01	Director general	**B**	
	P.02	Administrador del sistema	**A**	
	P.03	Usuarios	**B**	
	P.04	Jefe de Seguridad	**M**	

Tabla 6 Valoración de activos

3.4 DIMENSIONES DE SEGURIDAD:

La metodología seguida para la realización del Análisis y la posterior Gestión de Riesgos es la que se recoge en la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que es la metodología reconocida a nivel internacional como uno de los métodos formales para investigar los riesgos que soportan los Sistemas de Información, así como para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

En lo referente a los riesgos, podemos distinguir:

- riesgo **potencial**: es el riesgo al que se encuentra sometido el activo sin tener en cuenta ninguna medidas de seguridad o de salvaguarda,

- el riesgo **presente** o **actual** que es el riesgo al que se encuentra sometido el activo en el momento de hacer el análisis, teniendo en cuenta las medidas de seguridad actualmente desplegadas.
- el riesgo **planificado** es el que se va obteniendo conforme se vayan implantado las medidas de seguridad que se estimen oportunas.

Para la valoración de nuestros activos, vamos a utilizar la escala recomendada en el libro II de Magerit v3. Esta escala va de 0 a 10 donde 0 representa el mínimo y 10 el máximo del valor.

Partiendo de esta escala decimal, se puede obtener una tabla simplificada de menos nivel de detalle. La correlación entre ambas escalas puede ser la siguiente.

VALOR		CRITERIO
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	Alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos.

Tabla 7 Escala de valoración

Dado que la valoración de los sistemas de información se ha realizado conforme a lo recomendado por la metodología Magerit, se han tenido en cuenta las siguientes dimensiones:

- **Disponibilidad**: Es la disposición de los servicios a ser usados cuando sea necesario por lo que se debe de analizar las consecuencias que tendría el que una persona autorizada no pudiera usar el servicio cuando lo necesita. Es una valoración típica de los servicios.
- **Confidencialidad**: Es la cualidad por la que el sistema sólo permite que la información llegue a las personas autorizadas, por lo que se debe de analizar las consecuencias que tendría su revelación a personas no autorizadas o que no necesiten conocer la información, es decir, qué daño

causaría que lo conociera quien no debe. La confidencialidad es una propiedad de difícil recuperación. Es una valoración típica de datos.

- **Integridad**: Es el mantenimiento de la integridad y corrección de los datos, por lo que hay que analizar las consecuencias que tendría para la empresa el que los datos fueran manipulados por personal no autorizado, o que estuviesen dañados o corruptos. Es una valoración típica de datos.
- **Autenticidad**: Es la propiedad por la que una entidad o individuo es quien dice ser, por lo que habría que analizar las consecuencias que supone para la empresa el hecho de la persona o entidad no sea quien dice ser. Es una valoración típica de servicios.
- **Trazabilidad:** Es el aseguramiento de que se puede saber en todo momento quién hace qué y en qué momento, por lo que habría que analizar las consecuencias que supondría el no poder rastrear a posteriori quién ha accedido o modificado una cierta información.

De las dimensiones anteriores, se consideran dimensiones básicas la confidencialidad, integridad y la disponibilidad.

A la hora de proteger un activo, hay que determinar por qué hay que protegerlo, y tal como se establece en el apartado 3 del libro I de Magerit, *"la valoración se puede ver desde la perspectiva de la "necesidad de proteger", pues cuanto más valioso es un activo, mayor nivel de protección requerirnos en la dimensión (o dimensiones de seguridad que sean pertinentes".*
"El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a la necesidad de explotación y protección de lo esencial."

3.5 TABLA RESUMEN DE VALORACIÓN:

A partir de todo lo visto hasta el momento se puede genera una tabla, donde se reflejará la valoración del riesgo en función de las distintas dimensiones que le son de aplicación, ya que no todas le afectan de igual modo a los diferentes activos.

El criterio de valoración que he seguido teniendo en cuenta las distintas dimensiones ha sido:

3.5.1 CRITERIOS DE VALORACIÓN:

3.6 DISPONIBILIDAD

Extremo/Muy alto

- Porque la falta de disponibilidad de la información o del servicio provocaría:
  - ✓ un daño grave, de difícil o imposible recuperación
  - ✓ el incumplimiento grave de una norma o la legislación
  - ✓ un daño reputacional grave.

Alto/Medio

- Porque la falta de disponibilidad de la información o del servicio provocaría:
  - ✓ un daño importante, de difícil o imposible recuperación
  - ✓ el incumplimiento importante de una norma o la legislación
  - ✓ un daño reputacional importante

Bajo

- Porque la indisponibilidad de la información o del servicio causaría:
  - ✓ algún perjuicio
  - ✓ el incumplimiento leve de una norma
  - ✓ un daño reputacional apreciable con los ciudadanos o con otras organizaciones

Despreciable

- Cuando la información es prescindible por tiempo indefinido

3.7 INTEGRIDAD DE LA INFORMACIÓN O DEL SERVICIO

Extremo/Muy alto

- Porque su manipulación o modificación no autorizada causaría:
  - ✓ un grave daño, de difícil o imposible recuperación
  - ✓ pérdidas económicas elevadas o alteraciones financieras significativas
  - ✓ un daño reputacional grave con los ciudadanos o con otras organizaciones

Alto/Medio

- Porque su manipulación o modificación no autorizada de la información o del servicio que maneja causaría:
  - ✓ un daño importante aunque subsanable

- ✓ el incumplimiento material o formal de una norma
- ✓ pérdidas económicas importantes
- ✓ un daño reputacional importante con los ciudadanos o con otras organizaciones

Bajo

- Porque su manipulación o modificación no autorizada causaría:
  - ✓ algún perjuicio
  - ✓ un daño reputacional apreciable con los ciudadanos o con otras organizaciones

Despreciable

- Cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables

3.8 CONFIDENCIALIDAD DE LA INFORMACIÓN O DEL SERVICIO

Extremo/Muy alto

- Porque su revelación causaría:
  - ✓ un grave daño, de difícil o imposible recuperación
  - ✓ supondría el incumplimiento grave de una norma
  - ✓ pérdidas económicas elevadas o alteraciones financieras significativas
  - ✓ un daño reputacional grave con los ciudadanos o con otras organizaciones

Alto/Medio

- Porque su revelación:
  - ✓ causaría un daño importante aunque subsanable
  - ✓ supondría el incumplimiento material o formal de una norma
  - ✓ causaría pérdidas económicas importantes
  - ✓ causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

Bajo

- Porque la revelación de la información:
  - ✓ causaría algún perjuicio
  - ✓ supondría el incumplimiento leve de una norma
  - ✓ supondría pérdidas económicas apreciables
  - ✓ un daño reputacional apreciable con los ciudadanos o con otras organizaciones

Despreciable

- Información de carácter público, accesible por cualquier persona

3.9 AUTENTICIDAD

Extremo/Muy alto

- Porque la falsedad en su origen o en su destinatario causaría:
  - ✓ un grave daño, de difícil o imposible recuperación
  - ✓ pérdidas económicas elevadas o alteraciones financieras significativas
  - ✓ un daño reputacional grave con los ciudadanos o con otras organizaciones

Alto/Medio

- Porque la falsedad en su origen o en su destinatario causaría:
  - ✓ un daño importante aunque subsanable
  - ✓ pérdidas económicas importantes
  - ✓ un daño reputacional importante con los ciudadanos o con otras organizaciones

Bajo

- Porque la falsedad en su origen o en su destinatario causaría:
  - ✓ algún perjuicio
  - ✓ pérdidas económicas apreciables
  - ✓ un daño reputacional apreciable con los ciudadanos o con otras organizaciones

Despreciable

- Cuando el origen es irrelevante o ampliamente conocido por otros medios

3.10 TRAZABILIDAD

Extremo/Muy alto

- Porque la incapacidad para rastrear un acceso a la información o al servicio:
  - ✓ impediría o dificultaría notablemente la capacidad de subsanar un error grave
  - ✓ dificultaría notablemente la capacidad para perseguir delitos
  - ✓ facilitaría enormemente la comisión de delitos graves

Alto/Medio:

- Porque la incapacidad para rastrear un acceso a la información:
  - ✓ impediría o dificultaría notablemente la capacidad de subsanar un error importante
  - ✓ dificultaría notablemente la capacidad para perseguir delitos
  - ✓ facilitaría la comisión de delitos

Bajo

- Porque la incapacidad para rastrear un acceso a la información:

- ✓ dificultaría la capacidad de subsanar errores
- ✓ dificultaría la capacidad para perseguir delitos

Despreciable

- Cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
- Cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios

3.11 TABLA RESUMEN DE VALORACIÓN:

Ámbito	Código	Activo	Valor	[A]	[C]	[I]	[D]	[T]
[L] Instalaciones								
	L.01	CPD	MA	7	7		9	
	L.02	Edificio	A				9	
[HW] Equipamiento hardware								
	HW.01	Pc portátiles	B	7	8	5	4	8
	HW.02	Pc de sobremesa	B	7	6	5	4	8
	HW.03	Servidor de proyectos	A	9	8	8	9	8
	HW.04	Servidor de desarrollo	A	7	8	8	8	8
	HW.05	Servidor de administración	A	7	8	8	8	8
	HW.06	Servidor de impresión	B				7	3
	HW.07	Teléfonos móviles	B	3	9	8	5	5
	HW.08	Teléfonos de sobremesa	B		5		3	
	HW.09	Routers	A	8	7	9	9	7
	HW.10	Switches	M	5	6	7	8	6
	HW.11	Impresoras	B				5	
	HW.12	Firewall	A	5	9	9	7	8
	HW.13	Sistema de backup	A	8	9	9	9	7
	HW.14	Punto de acceso wifi	M				7	
[SW] Aplicaciones								
	SW.01	Sistemas operativos	B	7	5	8	8	6
	SW.02	Software antivirus	B	7	6	8	8	8
	SW.03	Aplicaciones ofimáticas.	M	7	8	8	8	7
	SW.04	Aplicativo ERP	A	7	9	9	7	8
	SW.05	Software de gestión de proyectos	M	7	8	8	6	7
	SW.06	Software de desarrollo	M	7	9	9	7	9

	SW.07	Aplicación financiera	**A**	7	9	9	7	9
[D] Datos								
	D.01	Datos de clientes	**A**	7	9	8	7	7
	D.02	Datos de proyectos	**M**	8	8	7	6	
	D.03	Datos de desarrollo	**A**	8	9	9	7	
	D.04	Datos de emails	**A**	6	9	8	6	
	D.05	Datos personales	**A**	6	9	8	6	
[COM] Red de comunicaciones								
	COM.01	Red LAN	**M**	8	8	8	9	8
	COM.02	red inalámbrica	**M**	8	8	8	4	7
	COM.03	Telefonía fija	**B**	4	7	3	5	
	COM.04	telefonía móvil	**B**	7	7	7	3	8
	COM.05	Internet.	**MA**	4	7	4	6	6
[SS] Servicios subcontratados								
	SS.01	Correo electrónico	**A**	8	8	6	8	6
[AUX] Equipamiento Auxiliar								
	AUX.01	Sistema de alimentación ininterrumpida	**A**				9	
	AUX.02	Sistema de alarmas	**M**				8	
	AUX.03	Sistema contraincendios	**A**				9	
	AUX.04	Sistema de climatización.	**A**				9	
[P] Personal								
	P.01	Director general	**MA**	8	9		9	
	P.02	Administrador del sistema	**A**	7	8		8	
	P.03	Usuarios	**M**	6	8		6	
	P.04	Jefe de Seguridad	**MA**	8	9		9	

Tabla 8 Tabla resumen de valoración

3.12 ANÁLISIS DE AMENAZAS

Según la norma UNE71504, una amenaza es la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Una amenaza es todo aquello que puede desencadenar un incidente en la compañía, produciendo daños materiales o pérdidas inmateriales en sus activos, es decir, produciendo una degradación de los activos, que se traduce en una pérdida de su valor.

No todos los activos son vulnerables a todas los tipos de amenazas existentes, sino que les afecta en función del tipo de activo que sea, por ejemplo el fuego en la instalación puede afectar a la disponibilidad de los equipos y sistemas hardware, pero no tiene por qué afectar a la integridad del software de desarrollo. La vulnerabilidad de un activo frente a una amenaza se mide en términos de la frecuencia de materialización de la amenaza y la degradación del activo en caso de que dicha amenaza llegue a materializarse.

Lo normal es que el riesgo no se elimina, sino que se gestiona, de tal forma, que mediante las respectivas salvaguardas se puede reducir el daño que podrían causar las amenazas.

Cada metodología tiene su propio catálogo de amenazas. En nuestro caso como estamos usando la metodología Magerit, usaremos el catálogo propuesto en dicho método.

En el libro Libro 2 “Catálogo de Elementos” (Punto 5)). Se clasifican las amenazas en los siguientes bloques:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

TIPO DE AMENAZA	AMENAZA
[N] Desastres naturales: sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta	[N.1] Fuego. [N.2] Daños por agua. [N.*] Otros desastres naturales que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.
[I] De origen industrial: sucesos que pueden ocurrir de forma accidental, derivados de	[I.1] Fuego.

TIPO DE AMENAZA	AMENAZA
la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada	[I.2] Daños por agua. [I.3] Contaminación mecánica. [I.4] Contaminación electromagnética. [I.5] Avería de origen físico o lógico. [I.6] Corte del suministro eléctrico. [I.7] Condiciones inadecuadas de temperatura y/o humedad. [I.8] Fallo de servicios de comunicaciones. [I.9] Interrupción de otros servicios y suministros esenciales. [I.10] Degradación de los soportes de almacenamiento de la información [I.11] Emanaciones electromagnéticas [I.*] Otros desastres industriales debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc.
[E] Errores y fallos no intencionados: fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados ([A]), muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.	[E.1] Errores de los usuarios. [E.2] Errores del administrador. [E.3] Errores de monitorización (log). [E.4] Errores de configuración. [E.7] Deficiencias en la organización. [E.8] Difusión de software dañino. [E.9] Errores de [re-]encaminamiento. [E.10] Errores de secuencia. [E.14] Escapes de información. [E.15] Alteración de la información. [E.16] Introducción de información incorrecta. [E.17] Degradación de la información. [E.18] Destrucción de la información. [E.19] Divulgación de información. [E.20] Vulnerabilidades de los programas (software). [E.21] Errores de mantenimiento / actualización de programas (software). [E.23] Errores de mantenimiento / actualización de equipos (hardware). [E.24] Caída del sistema por agotamiento de recursos. [E.25] Pérdidas de equipos [E.28] Indisponibilidad del personal.
[A] Ataques intencionados: fallos deliberados causados por las personas. La numeración tampoco es consecutiva en este caso, para coordinarla con los errores no intencionados ([E]), muchas veces de naturaleza similar a los ataques deliberados, difiriendo	[A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de la configuración. [A.5] Suplantación de la identidad del usuario. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto.

TIPO DE AMENAZA	AMENAZA
únicamente en el propósito del sujeto.	[A.8] Difusión de software dañino. [A.9] [Re-]encaminamiento de mensajes. [A.10] Alteración de secuencia. [A.11] Acceso no autorizado. [A.12] Análisis de tráfico. [A.13] Repudio. [A.14] Intercepción de información (escucha). [A.15] Modificación de la información. [A.16] Introducción de falsa información. [A.17] Corrupción de la información. [A.18] Destrucción de la información. [A.19] Divulgación de información. [A.22] Manipulación de programas. [A.24] Denegación de servicio. [A.25] Robo. [A.26] Ataque destructivo. [A.27] Ocupación enemiga. [A.28] Indisponibilidad del personal. [A.29] Extorsión. [A.30] Ingeniería social (picaresca)

Tabla 9 Agrupación de amenazas

Tabla con los valores de la escala de impacto

Impacto	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Tabla 10 valores de la escala de impacto

En la siguiente tabla se muestran los activos, junto con la frecuencia de ocurrencia de cada una de las amenazas y el impacto sobre las dimensiones de seguridad.

Tabla con la escala de la frecuencia de ocurrencia

Valor	Nivel	Descripción
100	Muy frecuente	A diario
10	Frecuente	Una vez al mes
1	Normal	Una vez al año
0,1	Poco frecuente	Cada varios años

Tabla 11 Frecuencia de ocurrencia

					Impacto				
Ambito	**Código**	**Activo**	**AMENAZA**	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones									
	L.01	CPD				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				75%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.11] Emanaciones electromagnéticas	0,1		50%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.26] Ataque destructivo	0,1				100%	
	L.02	Edificio						100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				50%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			Emanaciones electromagnéticas	0,1		50%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.26] Ataque destructivo	0,1				100%	
[HW] Equipamiento hardware									
	HW.01	Pc portátiles			75%	100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				75%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				50%	
			[I.4] Contaminación electromagnética	0,1				20%	
			[I.5] Avería de origen físico o lógico	1				100%	
			[I.6] Corte del suministro eléctrico	1				20%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				50%	
			[I.11] Emanaciones electromagnéticas	0,1		20%			
			[E.1] Errores de los usuarios	10		20%	20%	20%	
			[E.2] Errores del administrador del sistema / de la seguridad	10		50%	50%	50%	
			[E.8] Difusión de software dañino	1		100%	100%	100%	
			[E.15] Alteración de la información	10			50%		
			[E.18] Destrucción de la información	0,1				50%	
			[E.19] Fugas de información	1		50%			
			[E.20] Vulnerabilidades de los programas (software)	10		50%	20%	50%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			20%	50%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1			20%	50%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				50%	
			[E.25] Pérdida de equipos	1		100%		100%	
			[A.5] Suplantación de la identidad	1	75%	100%	100%		
			[A.6] Abuso de privilegios de acceso	1		100%	75%	75%	
			[A.7] Uso no previsto	1		75%	75%	75%	
			[A.8] Difusión de software dañino	10		100%	100%	100%	
			[A.11] Acceso no autorizado	1		100%	100%	100%	
			[A.15] Modificación de la información	10			75%		

			[A.18] Destrucción de la información	1			100%	
			[A.19] Revelación de información	1		100%		
			[A.22] Manipulación de programas	1		75%	75%	75%
			[A.23] Manipulación del hardware	1		75%		75%
			[A.24] Denegación de servicio	1				50%
			[A.25] Robo de equipos	1		100%		100%
			[A.26] Ataque destructivo	1				100%
	HW.02	Pc de sobremesa			100%	100%	100%	100%
			[N.1] Fuego	0,1				100%
			[N.2] Daños por agua	0,1				100%
			[N.*] Desastres naturales	0,1				100%
			[I.1] Fuego	0,1				100%
			[I.2] Daños por agua	0,1				20%
			[I.*] Desastres industriales	0,1				20%
			[I.3] Contaminación medioambiental	0,1				20%
			[I.4] Contaminación electromagnética	0,1				20%
			[I.5] Avería de origen físico o lógico	0,1				50%
			[I.6] Corte del suministro eléctrico	1				100%
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				20%
			[I.11] Emanaciones electromagnéticas	0,1		20%		
			[E.1] Errores de los usuarios	10		75%	75%	75%
			[E.2] Errores del administrador del sistema / de la seguridad	1		100%	100%	100%
			[E.8] Difusión de software dañino	1		100%	100%	100%
			[E.15] Alteración de la información	0,1			100%	
			[E.18] Destrucción de la información	0,1				75%
			[E.19] Fugas de información	0,1		100%		
			[E.20] Vulnerabilidades de los programas (software)	10		50%	50%	50%
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	20%
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				20%
			[E.24] Caída del sistema por agotamiento de recursos	0,1				20%
			[A.5] Suplantación de la identidad	0,1	100%	100%	100%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%
			[A.7] Uso no previsto	1		75%	75%	75%
			[A.8] Difusión de software dañino	1		100%	100%	100%
			[A.11] Acceso no autorizado	0,1		100%	100%	100%
			[A.15] Modificación de la información	10			20%	
			[A.18] Destrucción de la información	0,1				100%
			[A.19] Revelación de información	0,1		100%		
			[A.22] Manipulación de programas	0,1		75%	50%	75%
			[A.23] Manipulación del hardware	0,1		20%		20%
			[A.24] Denegación de servicio	0,1				20%
			[A.25] Robo de equipos	1		75%		100%
			[A.26] Ataque destructivo	0,1				100%
	HW.03	Servidor de proyectos			100%	100%	100%	100%
			[N.1] Fuego	0,1				100%
			[N.2] Daños por agua	0,1				100%
			[N.*] Desastres naturales	0,1				100%
			[I.1] Fuego	0,1				100%
			[I.2] Daños por agua	0,1				100%
			[I.*] Desastres industriales	0,1				100%
			[I.5] Avería de origen físico o lógico	0,1				75%
			[I.6] Corte del suministro eléctrico	1				50%
			[I.7] Condiciones inadecuadas de	1				75%

			temperatura o humedad						
			[E.1] Errores de los usuarios	10		50%	20%	20%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.3] Errores de monitorización (log)	1			50%		
			[E.4] Errores de configuración	1			100%		
			[E.8] Difusión de software dañino	1		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	10		75%	50%	50%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			75%	75%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				75%	
			[A.3] Manipulación de los registros de actividad (log)	0,1			75%		
			[A.4] Manipulación de los ficheros de configuración	0,1		100%	100%	100%	
			[A.5] Suplantación de la identidad	1	100%	100%	100%		
			[A.6] Abuso de privilegios de acceso	1		100%	100%	100%	
			[A.7] Uso no previsto	1		75%	75%	75%	
			[A.8] Difusión de software dañino	1		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.13] Repudio (negación de actuaciones)	1			100%		
			[A.15] Modificación de la información	10			50%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.04	Servidor de desarrollo			100%	100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	0,1				75%	
			[I.6] Corte del suministro eléctrico	0,1				50%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				75%	
			[E.1] Errores de los usuarios	10		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.3] Errores de monitorización (log)	1			50%		
			[E.4] Errores de configuración	1			100%		
			[E.8] Difusión de software dañino	1		100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	10		75%	75%	75%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			75%	75%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				75%	
			[A.3] Manipulación de los registros de actividad (log)	0,1			75%		
			[A.4] Manipulación de los ficheros de	0,1		100%	100%	100%	

			configuración						
			[A.5] Suplantación de la identidad	1	100%	100%	100%		
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.7] Uso no previsto	1		75%	75%	75%	
			[A.8] Difusión de software dañino	10		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.13] Repudio (negación de actuaciones)	1			100%		
			[A.15] Modificación de la información	10			50%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.05	Servidor de administración				100%	100%	100%	100%
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	0,1				75%	
			[I.6] Corte del suministro eléctrico	0,1				50%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				75%	
			[E.1] Errores de los usuarios	10		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.3] Errores de monitorización (log)	1			50%		
			[E.4] Errores de configuración	1			100%		
			[E.8] Difusión de software dañino	10		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	10		75%	75%	75%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	10			75%	75%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				75%	
			[A.3] Manipulación de los registros de actividad (log)	0,1			75%		
			[A.4] Manipulación de los ficheros de configuración	0,1		100%	100%	100%	
			[A.5] Suplantación de la identidad	1	100%	100%	100%		
			[A.6] Abuso de privilegios de acceso	1		100%	100%	100%	
			[A.7] Uso no previsto	1		75%	75%	75%	
			[A.8] Difusión de software dañino	10		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.13] Repudio (negación de actuaciones)	1			100%		
			[A.15] Modificación de la información	10			50%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.06	Servidor de impresión				50%	75%	75%	75%
			[I.5] Avería de origen físico o lógico	1				100%	
			[E.1] Errores de los usuarios	10		5%	5%	5%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		50%	5%	20%	
			[E.3] Errores de monitorización (log)	1			50%		
			[E.8] Difusión de software dañino	10		20%	20%	20%	

			[E.15] Alteración de la información	1			20%		
			[E.18] Destrucción de la información	1				50%	
			[E.20] Vulnerabilidades de los programas (software)	10		50%	20%	20%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1				50%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				50%	
			[A.3] Manipulación de los registros de actividad (log)	0,1			50%		
			[A.5] Suplantación de la identidad	0,1	50%	50%	50%		
			[A.6] Abuso de privilegios de acceso	0,1		20%	20%	20%	
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.8] Difusión de software dañino	10		75%	75%	75%	
			[A.11] Acceso no autorizado	0,1		50%	50%	50%	
			[A.13] Repudio (negación de actuaciones)	1			50%		
			[A.15] Modificación de la información	10			50%		
			[A.18] Destrucción de la información	0,1				50%	
			[A.19] Revelación de información	0,1		75%			
			[A.22] Manipulación de programas	0,1		75%	75%	75%	
			[A.24] Denegación de servicio	0,1				50%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.07	Teléfonos móviles				100%	100%	100%	
			[I.5] Avería de origen físico o lógico	1				100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.25] Pérdida de equipos	0,1		100%		100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.25] Robo de equipos	0,1		100%		100%	
	HW.08	Teléfonos de sobremesa						100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				50%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	1				100%	
	HW.09	Routers				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[I.6] Corte del suministro eléctrico	1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				100%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		50%	50%	50%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				75%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.11] Acceso no autorizado	1		100%	100%	100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.10	Switches				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	

			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	1				100%	
			[I.6] Corte del suministro eléctrico	1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				100%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		100%	100%	100%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				75%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.11] Acceso no autorizado	1		100%	100%	100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.11	Impresoras				75%	75%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				100%	
			[I.5] Avería de origen físico o lógico	1				100%	
			[I.6] Corte del suministro eléctrico	1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		50%	50%	50%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1				100%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				50%	
			[A.6] Abuso de privilegios de acceso	0,1		50%	50%	50%	
			[A.7] Uso no previsto	1		20%	20%	50%	
			[A.11] Acceso no autorizado	0,1		75%	75%	75%	
			[A.23] Manipulación del hardware	0,1		75%		75%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.12	Firewall			100%	100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[I.6] Corte del suministro eléctrico	1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				75%	
			[E.1] Errores de los usuarios	0,1		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1				100%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.5] Suplantación de la identidad	0,1	100%	100%	100%		

			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.13	Sistema de backup			100%	100%	100%	100%	
			[A.22] Manipulación de programas	0,1				100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	1				100%	
			[I.6] Corte del suministro eléctrico	1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				75%	
			[I.10] Degradación de los soportes de almacenamiento de la información	0,1				100%	
			[E.1] Errores de los usuarios	1		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	0,1		100%	100%	100%	
			[E.3] Errores de monitorización (log)	0,1			75%		
			[E.4] Errores de configuración	1			100%		
			[E.8] Difusión de software dañino	0,1		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	0,1		75%	75%	75%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	0,1			75%	75%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1				75%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.3] Manipulación de los registros de actividad (log)	1			100%		
			[A.4] Manipulación de los ficheros de configuración	1		100%	100%	100%	
			[A.5] Suplantación de la identidad	0,1	100%	100%	100%		
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.7] Uso no previsto	0,1		100%	100%	100%	
			[A.8] Difusión de software dañino	0,1		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.13] Repudio (negación de actuaciones)	0,1			100%		
			[A.15] Modificación de la información	0,1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	1		100%	100%	100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	HW.14	Punto de acceso wifi				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				100%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[I.6] Corte del suministro eléctrico	0,1				100%	
			[I.7] Condiciones inadecuadas de temperatura o humedad	1				50%	

			[E.2] Errores del administrador del sistema / de la seguridad	1		50%	50%	50%	
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				100%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
			[A.11] Acceso no autorizado	0,1		100%	100%	100%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
[SW] Aplicaciones									
	SW.01	Sistemas operativos				100%	100%	100%	
			[E.1] Errores de los usuarios	10		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.8] Difusión de software dañino	10		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	10		75%	75%	75%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.8] Difusión de software dañino	1		100%	100%	100%	
			[A.15] Modificación de la información	10			100%		
			[A.22] Manipulación de programas	1		50%	50%	50%	
	SW.02	Software antivirus				100%	100%	100%	
			[E.1] Errores de los usuarios	0,1		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.8] Difusión de software dañino	0,1		100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	1		75%	75%	75%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[A.7] Uso no previsto	0,1		50%	50%	50%	
			[A.8] Difusión de software dañino	0,1		100%	100%	100%	
			[A.15] Modificación de la información	1			100%		
			[A.18] Destrucción de la información	0,1				50%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		75%	75%	75%	
	SW.03	Aplicaciones ofimáticas.				100%	100%	100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[E.1] Errores de los usuarios	10		50%	50%	50%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.8] Difusión de software dañino	0,1		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	1		50%	75%	50%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.8] Difusión de software dañino	1		100%	100%	100%	
			[A.15] Modificación de la información	1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
	SW.04	Aplicativo ERP				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		

			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	1		100%			
			[E.28] Indisponibilidad del personal	1				50%	
			[A.15] Modificación de la información	1			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.28] Indisponibilidad del personal	1				20%	
			[A.30] Ingeniería social (picaresca)	0,1		20%	20%	20%	
	SW.05	Software de gestión de proyectos				100%	100%	100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[E.1] Errores de los usuarios	10		50%	50%	20%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	50%	
			[E.8] Difusión de software dañino	0,1		100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	1		50%	50%	50%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[A.7] Uso no previsto	1		20%	20%	20%	
			[A.8] Difusión de software dañino	0,1		100%	100%	100%	
			[A.15] Modificación de la información	1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
	SW.06	Software de desarrollo				100%	100%	100%	
			[I.5] Avería de origen físico o lógico	0,1				100%	
			[E.1] Errores de los usuarios	10		50%	50%	20%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	50%	
			[E.8] Difusión de software dañino	0,1		100%	100%	100%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.20] Vulnerabilidades de los programas (software)	1		50%	50%	50%	
			[E.21] Errores de mantenimiento / actualización de programas (software)	1			50%	50%	
			[A.7] Uso no previsto	0,1		20%	20%	20%	
			[A.8] Difusión de software dañino	0,1		100%	100%	100%	
			[A.15] Modificación de la información	1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.22] Manipulación de programas	0,1		50%	50%	50%	
	SW.07	Aplicación financiera			100%	100%	100%	100%	
			[I.9] Interrupción de otros servicios o suministros esenciales	1				50%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	0,1		100%			
			[A.5] Suplantación de la identidad	0,1	100%	100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				100%	
[D] Datos									
	D.01	Datos de clientes				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.19] Fugas de información	0,1		100%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	

			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				50%	
	D.02	Datos de proyectos				100%	100%	100%	
			[E.15] Alteración de la información	0,1			50%		
			[E.19] Fugas de información	0,1		50%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				50%	
	D.03	Datos de desarrollo				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.19] Fugas de información	1		100%			
			[A.11] Acceso no autorizado	1		100%	100%		
			[A.15] Modificación de la información	10			50%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				50%	
	D.04	Datos de emails				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.19] Fugas de información	0,1		100%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				50%	
	D.05	Datos personales				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.19] Fugas de información	0,1		100%			
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				50%	
[COM] Red de comunicaciones									
	COM.01	Red LAN				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				20%	
			[N.*] Desastres naturales	0,1				50%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				20%	
			[I.*] Desastres industriales	0,1				50%	
			[I.3] Contaminación medioambiental	0,1				5%	
			[I.4] Contaminación electromagnética	0,1				5%	
			[I.8] Fallo de servicios de comunicaciones	1				5%	
			[I.11] Emanaciones electromagnéticas	1		20%		5%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		20%	20%	20%	
			[E.9] Errores de [re-]encaminamiento	1		50%			
			[E.10] Errores de secuencia	1			50%		
			[E.15] Alteración de la información	0,1			100%		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				20%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.9] [Re-]encaminamiento de mensajes	1		100%			
			[A.10] Alteración de secuencia	0,1			100%		
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.12] Análisis de tráfico	0,1		100%			
			[A.14] Interceptación de información (escucha)	0,1		100%			

			[A.23] Manipulación del hardware	1		75%		75%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.25] Robo de equipos	0,1				50%	
			[A.26] Ataque destructivo	0,1				100%	
	COM.02	red inalámbrica				100%	100%	100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				50%	
			[N.*] Desastres naturales	0,1				50%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				50%	
			[I.*] Desastres industriales	0,1				50%	
			[I.3] Contaminación medioambiental	0,1				20%	
			[I.4] Contaminación electromagnética	0,1				20%	
			[I.8] Fallo de servicios de comunicaciones	1				100%	
			[I.11] Emanaciones electromagnéticas	1		20%			
			[E.2] Errores del administrador del sistema / de la seguridad	1		100%	100%	100%	
			[E.9] Errores de [re-]encaminamiento	0,1		100%			
			[E.10] Errores de secuencia	0,1			100%		
			[E.15] Alteración de la información	0,1			100%		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				50%	
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.9] [Re-]encaminamiento de mensajes	1		100%			
			[A.10] Alteración de secuencia	0,1			100%		
			[A.11] Acceso no autorizado	1		100%	100%		
			[A.12] Análisis de tráfico	1		100%			
			[A.14] Interceptación de información (escucha)	1		100%			
			[A.23] Manipulación del hardware	1		75%		75%	
			[A.24] Denegación de servicio	0,1				100%	
			[A.25] Robo de equipos	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	COM.03	Telefonía fija				100%	100%	100%	
			[I.8] Fallo de servicios de comunicaciones	1				100%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		50%	50%	50%	
			[E.19] Fugas de información	0,1		100%			
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%		
			[A.7] Uso no previsto	0,1		50%	50%	50%	
			[A.11] Acceso no autorizado	1		100%	100%		
			[A.12] Análisis de tráfico	0,1		100%			
			[A.14] Interceptación de información (escucha)	0,1		100%			
			[A.18] Destrucción de la información	0,1				50%	
			[A.19] Revelación de información	1		100%			
			[A.24] Denegación de servicio	0,1				100%	
	COM.04	telefonía móvil				100%	100%	100%	
			[I.8] Fallo de servicios de comunicaciones	1				100%	
			[E.19] Fugas de información	0,1		100%			
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%		
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.14] Interceptación de información (escucha)	0,1		100%			
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				100%	

	COM.05	Internet.				100%	100%	100%	
			[I.8] Fallo de servicios de comunicaciones	1				100%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		75%	75%	75%	
			[E.9] Errores de [re-]encaminamiento	1		100%			
			[E.10] Errores de secuencia	1			100%		
			[E.15] Alteración de la información	1			100%		
			[E.19] Fugas de información	0,1		100%			
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.6] Abuso de privilegios de acceso	0,1		50%	50%		
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.9] [Re-]encaminamiento de mensajes	0,1		100%			
			[A.10] Alteración de secuencia	0,1			100%		
			[A.11] Acceso no autorizado	1		100%	100%		
			[A.12] Análisis de tráfico	0,1		100%			
			[A.14] Interceptación de información (escucha)	1		100%			
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				100%	
[SS] Servicios subcontratados									
	SS.01	Correo electrónico			100%	100%	100%	100%	
			[I.9] Interrupción de otros servicios o suministros esenciales	1				75%	
			[E.15] Alteración de la información	1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	0,1		100%			
			[A.5] Suplantación de la identidad	0,1	100%	100%	100%		
			[A.15] Modificación de la información	10			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				100%	
			[I.8] Fallo de servicios de comunicaciones	1				100%	
			[E.2] Errores del administrador del sistema / de la seguridad	1		100%	100%	100%	
			[E.9] Errores de [re-]encaminamiento	1		100%			
			[E.10] Errores de secuencia	0,1			100%		
			[E.15] Alteración de la información	0,1			100%		
			[E.24] Caída del sistema por agotamiento de recursos	0,1				100%	
			[A.6] Abuso de privilegios de acceso	0,1		100%	100%		
			[A.7] Uso no previsto	1		50%	50%	50%	
			[A.9] [Re-]encaminamiento de mensajes	0,1		100%			
			[A.10] Alteración de secuencia	0,1			100%		
			[A.11] Acceso no autorizado	0,1		100%	100%		
			[A.12] Análisis de tráfico	0,1		100%			
			[A.14] Interceptación de información (escucha)	0,1		100%			
			[A.15] Modificación de la información	1			20%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.24] Denegación de servicio	0,1				100%	
[AUX] Equipamiento Auxiliar									
	AUX.01	Sistema de alimentación ininterrumpida						100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				50%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				50%	
			[I.*] Desastres industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				100%	

			[A.23] Manipulación del hardware	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	AUX.02	Sistema de alarmas						100%	
			[N.1] Fuego	0,1				100%	
			[N.2] Daños por agua	0,1				50%	
			[N.*] Desastres naturales	0,1				100%	
			[I.1] Fuego	0,1				100%	
			[I.2] Daños por agua	0,1				50%	
			[I.*] Desastres industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				50%	
			[A.23] Manipulación del hardware	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	AUX.03	Sistema contraincendios						100%	
			[N.1] Fuego	0,1				100%	
			[N.*] Desastres naturales	0,1				50%	
			[I.1] Fuego	0,1				100%	
			[I.*] Desastres industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				50%	
			[A.23] Manipulación del hardware	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
	AUX.04	Sistema de climatización.						100%	
			[N.1] Fuego	0,1				100%	
			[N.*] Desastres naturales	0,1				50%	
			[I.1] Fuego	0,1				100%	
			s industriales	0,1				100%	
			[I.3] Contaminación medioambiental	0,1				50%	
			[A.23] Manipulación del hardware	0,1				100%	
			[A.26] Ataque destructivo	0,1				100%	
[P] Personal									
	P.01	Director general				100%	100%	100%	
			[E.15] Alteración de la información	0,1			75%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	0,1		100%			
			[E.28] Indisponibilidad del personal	1				50%	
			[A.15] Modificación de la información	0,1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.28] Indisponibilidad del personal	1				50%	
			[A.29] Extorsión	0,1		75%	75%	75%	
			[A.30] Ingeniería social (picaresca)	0,1		20%	20%	20%	
	P.02	Administrador del sistema				100%	100%	100%	
			[E.15] Alteración de la información	0,1			100%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	0,1		100%			
			[E.28] Indisponibilidad del personal	1				50%	
			[A.15] Modificación de la información	0,1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.28] Indisponibilidad del personal	1				50%	
			[A.29] Extorsión	0,1		100%	100%	100%	
			[A.30] Ingeniería social (picaresca)	0,1		20%	20%	20%	
	P.03	Usuarios				100%	100%	100%	
			[E.15] Alteración de la información	0,1			75%		
			[E.18] Destrucción de la información	0,1				100%	
			[E.19] Fugas de información	0,1		100%			
			[E.28] Indisponibilidad del personal	1				50%	
			[A.15] Modificación de la información	0,1			100%		
			[A.18] Destrucción de la información	0,1				100%	
			[A.19] Revelación de información	0,1		100%			
			[A.28] Indisponibilidad del personal	1				50%	
			[A.29] Extorsión	0,1		75%	75%	75%	

		[A.30] Ingeniería social (picaresca)	0,1		20%	20%	20%	
	P.04	Jefe de Seguridad			100%	100%	100%	
		[E.15] Alteración de la información	0,1			100%		
		[E.18] Destrucción de la información	0,1				100%	
		[E.19] Fugas de información	0,1		100%			
		[E.28] Indisponibilidad del personal	1				50%	
		[A.15] Modificación de la información	0,1			100%		
		[A.18] Destrucción de la información	0,1				100%	
		[A.19] Revelación de información	0,1		100%			
		[A.28] Indisponibilidad del personal	1				50%	
		[A.29] Extorsión	0,1		75%	75%	75%	
		[A.30] Ingeniería social (picaresca)	0,1		20%	20%	20%	

Tabla 12 Tabla de activos y dimensiones de la seguridad

3.13 IMPACTO POTENCIAL

Una vez que se ha hecho la valoración de los activos y el análisis de las amenazas, podemos calcular el impacto potencial que supone para la empresa el que se materialice una amenaza.

En el cálculo del impacto potencial no se tiene en cuenta ninguna salvaguarda, por lo que los valores obtenidos se verán modificados cuando se le aplique las contramedidas pertinentes.

El impacto potencial se calcula con la siguiente fórmula:

Impacto potencial = valor del activo x impacto

			valoración					impacto					impacto potencial				
Ámbito	**Código**	**Activo**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones																	
	L.01	CPD	7	7		9			100%	100%	100%		7,0	7,0		9,0	
	L.02	Edificio				9					100%					9,0	
[HW] Equipamiento hardware																	
	HW.01	Pc portátiles	7	8	5	4	8	75%	100%	100%	100%		5,3	8,0	5,0	4,0	0,0
	HW.02	Pc de sobremesa	7	6	5	4	8	100%	100%	100%	100%		7,0	6,0	5,0	4,0	0,0
	HW.03	Servidor de proyectos	9	8	8	9	8	100%	100%	100%	100%		9,0	8,0	8,0	9,0	0,0
	HW.04	Servidor de desarrollo	7	8	8	8	8	100%	100%	100%	100%		7,0	8,0	8,0	8,0	0,0
	HW.05	Servidor de administración	7	8	8	8	8	100%	100%	100%	100%		7,0	8,0	8,0	8,0	0,0
	HW.06	Servidor de impresión				7	3	50%	75%	75%	75%		0,0	0,0	0,0	5,3	0,0
	HW.07	Routers	8	7	9	9	7		100%	100%	100%		0,0	7,0	9,0	9,0	0,0
	HW.10	Switches	5	6	7	8	6				100%		0,0	0,0	0,0	8,0	0,0

	HW.11	Firewall	5	9	9	7	8		100%	100%	100%		0,0	9,0	9,0	7,0	0,0
	HW.13	Sistema de backup	8	9	9	9	7		100%	100%	100%		0,0	9,0	9,0	9,0	0,0
	HW.09	Teléfonos de sobremesa		5		3			75%	75%	100%		0,0	3,8	0,0	3,0	0,0
	HW.12	Impresoras				5		100%	100%	100%	100%		0,0	0,0	0,0	5,0	0,0
	HW.08	Teléfonos móviles	3	9	8	5	5	100%	100%	100%	100%		3,0	9,0	8,0	5,0	0,0
	HW.15	Punto de acceso wifi				7			100%	100%	100%		0,0	0,0	0,0	7,0	0,0
[SW] Aplicaciones																	
	SW.01	Sistemas operativos	7	5	8	8	6		100%	100%	100%		0,0	5,0	8,0	8,0	0,0
	SW.02	Software antivirus	7	6	8	8	8		100%	100%	100%		0,0	6,0	8,0	8,0	0,0
	SW.03	Aplicaciones ofimáticas.	7	8	8	8	7		100%	100%	100%		0,0	8,0	8,0	8,0	0,0
	SW.04	Aplicativo ERP	7	9	9	7	8		100%	100%	100%		0,0	9,0	9,0	7,0	0,0
	SW.05	Software de gestión de proyectos	7	8	8	6	7		100%	100%	100%		0,0	8,0	8,0	6,0	0,0
	SW.06	Software de desarrollo	7	9	9	7	9		100%	100%	100%		0,0	9,0	9,0	7,0	0,0
	SW.07	Aplicación financiera	7	9	9	7	9	100%	100%	100%	100%		7,0	9,0	9,0	7,0	0,0
[D] Datos																	
	D.01	Datos de clientes	7	9	8	7	7		100%	100%	100%		0,0	9,0	8,0	7,0	0,0
	D.02	Datos de proyectos	8	8	7	6			100%	100%	100%		0,0	8,0	7,0	6,0	0,0
	D.03	Datos de desarrollo	8	9	9	7			100%	100%	100%		0,0	9,0	9,0	7,0	0,0
	D.04	Datos de emails	6	9	8	6			100%	100%	100%		0,0	9,0	8,0	6,0	0,0
	D.05	Datos personales	6	9	8	6			100%	100%	100%		0,0	9,0	8,0	6,0	0,0
[COM] Red de comunicaciones																	
	COM.01	Red LAN	8	8	8	9	8		100%	100%	100%		0,0	8,0	8,0	9,0	0,0
	COM.02	red inalámbrica	8	8	8	4	7		100%	100%	100%		0,0	8,0	8,0	4,0	0,0
	COM.03	Telefonía fija	4	7	3	5			100%	100%	100%		0,0	7,0	3,0	5,0	0,0
	COM.04	telefonía móvil	7	7	7	3	8		100%	100%	100%		0,0	7,0	7,0	3,0	0,0
	COM.05	Internet.	4	7	4	6	6		100%	100%	100%		0,0	7,0	4,0	6,0	0,0
[SS] Servicios subcontratados																	
	SS.01	Correo electrónico	8	8	6	8	6	100%	100%	100%	100%		8,0	8,0	6,0	8,0	6,0
[AUX] Equipamiento Auxiliar																	
	AUX.01	Sistema de alimentación ininterrumpida				9					100%		0,0	0,0	0,0	9,0	0,0
	AUX.02	Sistema de alarmas				8					100%		0,0	0,0	0,0	8,0	0,0
	AUX.03	Sistema contraincendios				9					100%		0,0	0,0	0,0	9,0	0,0
	AUX.04	Sistema de climatización.				9					100%		0,0	0,0	0,0	9,0	0,0
[P] Personal																	
	P.01	Director general	8	9		9			100%	100%	100%		0,0	9,0	0,0	9,0	0,0
	P.02	Administrador del sistema	7	8		8			100%	100%	100%		0,0	8,0	0,0	8,0	0,0
	P.03	Usuarios	6	8		6			100%	100%	100%		0,0	8,0	0,0	6,0	0,0
	P.04	Jefe de Seguridad	8	9		9			100%	100%	100%		0,0	9,0	0,0	9,0	0,0

Tabla 13 Tabla de impacto potencial

3.14 NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Tal como se ha comentado anteriormente, normalmente los riesgos no se eliminan, sino que se gestionan, es decir, se tratará de que los riesgos estén por debajo de un cierto nivel, al que llamaremos nivel de riesgo aceptable.

A los riesgos que estén por encima del nivel de riesgo aceptable se les deberá de aplicar las salvaguardas correspondientes para intentar conseguir que queden por debajo de ese nivel.

Una vez aplicadas las salvaguardas, al riesgo que quede es lo que se llama riesgo residual. Se intentará que todos los riesgos residuales estén por debajo del nivel de riesgo aceptable.

El nivel de riesgo de los activos se realiza mediante la siguiente fórmula:

Nivel de Riesgo = Impacto Potencial x Frecuencia

Como se puede deducir, el riesgo será mayor cuanto mayor sea la frecuencia de ocurrencia y el impacto potencial que tenga sobre el activo.

En la tabla siguiente se ve que el valor máximo del riesgo es 90, por lo que vamos a tomar ese valor como nuestro máximo valor de riesgo, y a partir de ahí se determina la siguiente escala de riesgos:

NIVEL DE RIESGO	RANGO DE VALORES
Alto	75 =< Riesgo
Medio – alto	50<= Riesgo <75
Medio – bajo	25 =< Riesgo <50
Bajo	Riesgo <25

Tabla 14 Tabla niveles de riesgo

Según el criterio anterior, la matriz de riesgos sería la siguiente:

frecuencia									
	100	100	200	300	400	500	600	700	800	900
	10	10	20	30	40	50	60	70	80	90
	9	9	18	27	36	45	54	63	72	81
	8	8	16	24	32	40	48	56	64	72
	7	7	14	21	28	35	42	49	56	63
	6	6	12	18	24	30	36	42	48	54
	5	5	10	15	20	25	30	35	40	45
	4	4	8	12	16	20	24	28	32	36
	3	3	6	9	12	15	18	21	24	27
	2	2	4	6	8	10	12	14	16	18
	1	1	2	3	4	5	6	7	8	9
	0,1	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
		1	2	3	4	5	6	7	8	9
Impacto										

La empresa se ha marcado como objetivo el reducir los niveles de riesgos por debajo de un valor 50, es decir que el nivel de riesgo aceptable será 50.

				impacto potencial						Riesgo				
Ambito	**Código**	**Activo**	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones														
	L.01	CPD	**0,1**	7,0	7,0		9,0			0,7	0,7	0,0	0,9	0,0
	L.02	Edificio	**0,1**				9,0			0,0	0,0	0,0	0,9	0,0
[HW] Equipamiento hardware														
	HW.01	Pc portátiles	**10**	5,3	8,0	5,0	4,0	0,0		52,5	80,0	50,0	40,0	0,0
	HW.02	Pc de sobremesa	**10**	7,0	6,0	5,0	4,0	0,0		70,0	60,0	50,0	40,0	0,0
	HW.03	Servidor de proyectos	**10**	9,0	8,0	8,0	9,0	0,0		90,0	80,0	80,0	90,0	0,0
	HW.04	Servidor de desarrollo	**10**	7,0	8,0	8,0	8,0	0,0		70,0	80,0	80,0	80,0	0,0
	HW.05	Servidor de administración	**10**	7,0	8,0	8,0	8,0	0,0		70,0	80,0	80,0	80,0	0,0
	HW.06	Servidor de impresión	**10**	0,0	0,0	0,0	5,3	0,0		0,0	0,0	0,0	52,5	0,0
	HW.07	Routers	**1**	0,0	7,0	9,0	9,0	0,0		0,0	7,0	9,0	9,0	0,0
	HW.10	Switches	**1**	0,0	0,0	0,0	8,0	0,0		0,0	0,0	0,0	8,0	0,0
	HW.11	Firewall	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	HW.13	Sistema de backup	**1**	0,0	9,0	9,0	9,0	0,0		0,0	9,0	9,0	9,0	0,0
	HW.09	Teléfonos de sobremesa	**1**	0,0	3,8	0,0	3,0	0,0		0,0	3,8	0,0	3,0	0,0
	HW.12	Impresoras	**1**	0,0	0,0	0,0	5,0	0,0		0,0	0,0	0,0	5,0	0,0
	HW.08	Teléfonos móviles	**1**	3,0	9,0	8,0	5,0	0,0		3,0	9,0	8,0	5,0	0,0

	HW.15	Punto de acceso wifi	**1**	0,0	0,0	0,0	7,0	0,0		0,0	0,0	0,0	7,0	0,0
[SW] Aplicaciones															
	SW.01	Sistemas operativos	**10**	0,0	5,0	8,0	8,0	0,0		0,0	50,0	80,0	80,0	0,0
	SW.02	Software antivirus	**1**	0,0	6,0	8,0	8,0	0,0		0,0	6,0	8,0	8,0	0,0
	SW.03	Aplicaciones ofimáticas.	**10**	0,0	8,0	8,0	8,0	0,0		0,0	80,0	80,0	80,0	0,0
	SW.04	Aplicativo ERP	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	SW.05	Software de gestión de proyectos	**10**	0,0	8,0	8,0	6,0	0,0		0,0	80,0	80,0	60,0	0,0
	SW.06	Software de desarrollo	**10**	0,0	9,0	9,0	7,0	0,0		0,0	90,0	90,0	70,0	0,0
	SW.07	Aplicación financiera	**10**	7,0	9,0	9,0	7,0	0,0		70,0	90,0	90,0	70,0	0,0
[D] Datos															
	D.01	Datos de clientes	**10**	0,0	9,0	8,0	7,0	0,0		0,0	90,0	80,0	70,0	0,0
	D.02	Datos de proyectos	**10**	0,0	8,0	7,0	6,0	0,0		0,0	80,0	70,0	60,0	0,0
	D.03	Datos de desarrollo	**10**	0,0	9,0	9,0	7,0	0,0		0,0	90,0	90,0	70,0	0,0
	D.04	Datos de emails	**10**	0,0	9,0	8,0	6,0	0,0		0,0	90,0	80,0	60,0	0,0
	D.05	Datos personales	**10**	0,0	9,0	8,0	6,0	0,0		0,0	90,0	80,0	60,0	0,0
[COM] Red de comunicaciones															
	COM.01	Red LAN	**1**	0,0	8,0	8,0	9,0	0,0		0,0	8,0	8,0	9,0	0,0
	COM.02	red inalámbrica	**1**	0,0	8,0	8,0	4,0	0,0		0,0	8,0	8,0	4,0	0,0
	COM.03	Telefonía fija	**1**	0,0	7,0	3,0	5,0	0,0		0,0	7,0	3,0	5,0	0,0
	COM.04	telefonía móvil	**1**	0,0	7,0	7,0	3,0	0,0		0,0	7,0	7,0	3,0	0,0
	COM.05	Internet.	**1**	0,0	7,0	4,0	6,0	0,0		0,0	7,0	4,0	6,0	0,0
[SS] Servicios subcontratados															
	SS.01	Correo electrónico	**1**	8,0	8,0	6,0	8,0	6,0		8,0	8,0	6,0	8,0	6,0
[AUX] Equipamiento Auxiliar															
	AUX.01	Sistema de alimentación ininterrumpida	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
	AUX.02	Sistema de alarmas	**0,1**	0,0	0,0	0,0	8,0	0,0		0,0	0,0	0,0	0,8	0,0
	AUX.03	Sistema contraincendios	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
	AUX.04	Sistema de climatización.	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
[P] Personal															
	P.01	Director general	**1**	0,0	9,0	0,0	9,0	0,0		0,0	9,0	0,0	9,0	0,0
	P.02	Administrador del sistema	**1**	0,0	8,0	0,0	8,0	0,0		0,0	8,0	0,0	8,0	0,0
	P.03	Usuarios	**1**	0,0	8,0	0,0	6,0	0,0		0,0	8,0	0,0	6,0	0,0
	P.04	Jefe de Seguridad	**1**	0,0	9,0	0,0	9,0	0,0		0,0	9,0	0,0	9,0	0,0

Tabla 15 Tabla de riesgos

3.15 RESULTADOS

Como resultado de los estudios anteriores, se puede obtener la relación de activos de la empresa que se encuentran sometidos a un mayor nivel de riesgo, y por tanto, son en los que hay que centrar los esfuerzos para reducirlo.

La siguiente tabla recoge los activos con un nivel de riesgo medio-alto y alto, que son sobre los que hay que aplicar las salvaguardas para reducir su valor por debajo del nivel 50.

Activos con un nivel alto de riesgo.

Ambito	Código	Activo
[HW] Equipamiento hardware		
	HW.01	Pc portátiles
	HW.03	Servidor de proyectos
	HW.04	Servidor de desarrollo
	HW.05	Servidor de administración
[SW] Aplicaciones		
	SW.01	Sistemas operativos
	SW.03	Aplicaciones ofimáticas.
	SW.05	Software de gestión de proyectos
	SW.06	Software de desarrollo
	SW.07	Aplicación financiera
[D] Datos		
	D.01	Datos de clientes
	D.02	Datos de proyectos
	D.03	Datos de desarrollo
	D.04	Datos de emails
	D.05	Datos personales

Tabla 16 Tabla de activos con nivel alto de riesgo

Activos con un nivel medio-alto de riesgo

Ambito	Código	Activo
[HW] Equipamiento hardware		
	HW.02	Pc de sobremesa
	HW.06	Servidor de impresión

Tabla 17 Tabla con activos con nivel medio-alto de riesgo

4 PROPUESTA DE PROYECTOS

4.1 INTRODUCCIÓN

Una vez realizado todo el análisis de las amenazas a las que se encuentra sometida nuestra empresa, visto el impacto potencial, y determinado el nivel de riesgo aceptable, es el momento de decidir el **plan de acción**, donde se establezcan los proyectos o acciones a llevar a cabo para intentar reducir los niveles de riesgos a los que nos encontramos sometidos, pero sobre todo, intentar que los riesgos que se encuentran en un nivel alto o medio-alto pasen a tener un valor medio-bajo o bajo.

Las acciones o proyectos que se llevarán a cabo, no sólo entran dentro del ámbito de las medidas técnicas o tecnológicas, sino en que la mayoría de los casos son acciones procedimentales, organizativas o de comportamientos.

De forma general se admite que el eslabón más débil de la cadena de seguridad suele ser el usuario, por lo que a él deben de ir encaminadas la mayor parte de las acciones o proyectos.

Además de los proyectos que son necesarios emprender para reducir los niveles de riesgo, lo normal es que el equipo auditor, como expertos en la materia, aconsejen alguna medida o acción encaminadas a mejorar la seguridad de nuestros sistemas, sobre todo, teniendo en cuenta las tendencias en el mundo de la seguridad / inseguridad de la información.

Del estudio anterior se desprende que hay que mejorar en sectores como el equipamiento hardware, las aplicaciones y los datos, por lo que serán en esa dirección donde se encaminen los esfuerzos de mejora.

A pesar de que la empresa no tiene la certificación ISO 27001, se encuentra en unos niveles aceptables de seguridad, aunque, tal como se pudo ver cuando se realizó el análisis diferencial, hay que mejorar y/o implementar algunos de los 114 controles recogidos en la ISO 27002.

Una vez realizado el plan de acción con todos los proyectos identificados, es posible que sea aconsejable dividir el plan de acción en más de una fase, de esta forma, se podría dosificar el esfuerzo y los recursos asignados, así como que los diferentes interesados se vayan adaptando de forma paulatina a la nueva situación, además, se puede analizar el efecto que la aplicación de la acción realizada tiene sobre la seguridad de la información. Si se consigue que todos los empleados se

convenzan de que la seguridad es importante para la continuidad del negocio y se involucren en ella, los resultados serán mucho mejores.

Según el estudio realizado, los activos con un nivel alto o medio-alto de riego corresponden al grupo de [HW] Equipamiento hardware, [SW] Aplicaciones y [D] Datos, será por tanto en estos activos sobre los que habrá que actuar para reducir su nivel de riesgo.

4.2 ACCIONES Y PROYECTOS

En el siguiente cuadro se recoge la relación de los diferentes proyectos o acciones propuestos para mejorar la seguridad de la compañía:

PROYECTO	DESCRIPCIÓN
PRT01	Elaboración de la política de seguridad
PRT02	Revisión de los procedimientos operativos
PRT03	Plan de formación de empleados
PRT04	Implantación de un sistema de cifrado global
PRT05	Implantación de un sistema antimalware
PRT06	Procedimiento de uso de dispositivos móviles
PRT07	Procedimiento de copias de seguridad
PRT08	Elaboración del Inventario, clasificación y etiquetado de activos
PRT09	Elaboración de plantilla para contratos base con terceros
PRT10	Seguridad relativa a los recursos humanos
PRT11	Análisis de vulnerabilidades

Tabla 18 Relación de proyectos

4.2.1 PRT01: ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD:

- **Descripción:** En el análisis diferencial realizado de la empresa Gespa, se ha detectado que no existe una política de seguridad que cumpla con lo previsto en la ISO 27002, tan solo hay unas instrucciones que recogen algunas de las obligaciones que tienen los usuarios con respecto al sistema de información,

por lo tanto, lo primero que hay que hacer, junto con el inventario de activos, es la elaboración de la política de seguridad de la empresa.

Tal como se establece en la ISO 27002, la política de seguridad es un documento al más alto nivel aprobado por la dirección, donde se establecen el enfoque de la organización para gestionar sus objetivos de seguridad de la información, por lo tanto, se debe de considerar tanto los requisitos de seguridad como los objetivos y principios.

Al ser un documento al más alto nivel, la política de seguridad debe de ser aprobada por la alta dirección y debe de ser publicada para general conocimiento de los interesados.

Al no ser la política de seguridad un documento estático, debido sobre todo a los posibles cambios de la empresa, se deberá de establecer cada cuánto tiempo o ante qué circunstancias tiene que revisarse la política.

La política de seguridad deberá de contener declaraciones relativas a:

- Asignación de responsabilidades
- La definición de seguridad de la información, de sus objetivos y principios.
- Los procesos para el tratamiento desviaciones y excepciones

Si se estima oportuno, se pueden incluir algunas referencias o descripciones destinadas al usuario final o a políticas temáticas concretas como son por ejemplo:

- Al uso de dispositivos móviles,
- Uso adecuado de activos.
- Transferencia de información,
- Restricciones de uso de software etc.

Se usará como guía para la elaboración de la política de seguridad, lo establecido en el apartado 5 “Políticas de seguridad de la información” de la la ISO 27002.

A la finalización del proyecto se debe de obtener un documento que sea aprobado por la dirección y que recoja las líneas maestras de la seguridad de la información teniendo en cuenta los requisitos del negocio, la legislación actual aplicable y las normas pertinentes.

- **Tipo de activos involucrados**: **Los activos afectados son:**
  - [L] Instalaciones
  - [HW] Equipamiento hardware
  - [SW] Aplicaciones
  - [D] Datos
  - [COM] Red de comunicaciones

- [SS] Servicios subcontratados
- [AUX] Equipamiento Auxiliar
- [P] Personal

- **Dominios y/o Controles afectados**:

5.1.1 Políticas para la seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información

- Duración estimada: **1 mes**
- Coste estimado:
- Coste H/H personal propio: **120 h**
- Adquisiciones y Subcontrataciones:
- Coste total**: 5.000 €**
- Plazo previsto para consecución de objetivos: La política de seguridad debe de estar realizado en un periodo de un mes pero su implantación es a largo plazo.

4.2.2 PRT02: REVISIÓN DE LOS PROCEDIMIENTOS OPERATIVOS:

- **Descripción:** La seguridad de la información, no sólo se ve comprometida por actos ilícitos cometidos tanto por elementos externos a la compañía como por empleados desleales, sino que en muchas ocasiones se puede ver afectada por una mala operación, es decir, por errores cometidos en la operación o manejo de los activos.

En nuestro caso de estudio, se puede apreciar que uno de los factores que afectan directamente a la seguridad de la información, son los errores cometidos por los usuarios y administradores en el desempeño normal de sus funciones.

Los errores normalmente son cometidos por una falta de formación del usuario, por procedimientos mal desarrollados, o por un incumplimiento de los mismos por parte de los usuarios.

Con el fin de mitigar el riesgo producido por estos errores, se va a llevar a cabo una revisión de los procedimientos e instrucciones técnicas de la compañía en cada una de las áreas de operación que sean susceptibles de afectar a la seguridad de la información.

Las fases del proyecto serán:

- Identificación de las actividades con más errores.
- Revisión de los procedimientos.

- Revisión de las Instrucciones técnicas
- Publicación de las instrucciones técnicas y procedimientos modificados
- Seguimiento de los resultados.

- **Tipo de activos involucrados**: **Los activos afectados son:**
  - [SS] Servicios subcontratados
  - [P] Personal

- **Dominios y/o Controles**:

7.2.2 Concienciación, educación y capacitación en seguridad de la información.
12.1.1 Documentación de procedimientos de operación

- **Amenazas:**

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador.
- [E.4] Errores de configuración
- [E.21] Errores de mantenimiento / actualización de programas (software).
- [E.23] Errores de mantenimiento / actualización de equipos (hardware).
-

- Duración prevista: **4 meses**
- Coste económico previsto:
- Coste H/H personal propio: **80 h.**
- Adquisiciones y Subcontrataciones:
- Coste total estimado: **2.800 €**
- Plazo previsto para consecución de objetivos: El proyecto está previsto que se lleve a cabo a largo plazo, debiendo hacerse anualmente una evaluación de los procedimientos.

4.3 PRT03: PLAN DE FORMACIÓN DE EMPLEADOS:

- **Descripción:** Como se ha puesto de manifiesto con el análisis de riesgos realizado, uno de los motivos que hace que el nivel de riesgos aumente, son los posibles errores de los usuarios a la hora de llevar a cabo su trabajos.

La mitigación de este riesgo se puede intentar conseguir, además de con medidas procedimentales, con la formación e información tanto de los empleados de Gespa como de las subcontratas y/o personal subcontratado que trabaje para ella.

Este proyecto tiene como finalidad el hacer un estudio del actual nivel de formación de los empleados según su rol en la empresa, de tal forma que se evalúe la necesidad de cursos formativos relativos a su puesto de trabajo.

La formación irá encaminada al uso de las herramientas tanto software como hardware que utilice el empleado, así como de los procedimientos e instrucciones técnicas que afecten al proceso que esté ejecutando.

Además de la formación puramente operativa, se impartirá formación sobre la seguridad de la información.

Las fases de proyecto serán:

- Identificación de los puestos con necesidades formativas.
- Hacer un plan de formación anual.
- Preparación de los cursos formativos.
- Impartición de los cursos

Dependiendo del tipo de curso a impartir, podrían necesitarse tanto recursos propios como externos.

Los cursos sobre concienciación en seguridad de la información los impartirá el Jefe de Seguridad, mientras que para los de procedimientos lo hará el jefe del departamento correspondiente o persona que en cada momento se considere la más adecuada por su nivel de formación y dotes docentes.
En la medida de lo posible, los cursos de formación los impartirá personal de la propia compañía experto en la materia, procediéndose a la contratación o apoyo externo en caso necesario.

Para la duración prevista de este proyecto se ha tenido en cuenta el tiempo necesario para la determinación de los cursos, la preparación de los mismos, la impartición y que los profesores estarán preparando los cursos a tiempo parcial.

Para los cálculos se ha estimado un par de cursos de 2 días de duración de 10 alumnos cada uno.

- **Tipo de activos involucrados**: Los activos afectados son:
  - [SS] Servicios subcontratados
  - [P] Personal
- **Dominios y/o Controles**:

7.2.2 Concienciación, educación y capacitación en seguridad de la información

- **Amenazas**:

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador.
- [E.4] Errores de configuración
- [E.21] Errores de mantenimiento / actualización de programas (software).
- [E.23] Errores de mantenimiento / actualización de equipos (hardware).
-
- Duración prevista: **6 meses**
- Coste económico previsto:
- Total H/H personal propio profesor: **200 h**.
- Total H/H personal propio alumnos: **400 h.**
- Adquisiciones y Subcontrataciones:
- Coste total estimado: **18.000 €**
- Plazo previsto para consecución de objetivos: El proyecto está previsto que se lleve a cabo a largo plazo, debiendo hacerse anualmente una evaluación de las necesidades formativas.

4.4 PRT04: IMPLANTACIÓN DE UN SISTEMA DE CIFRA GLOBAL:

- **Descripción**: Una vez realizado el estudio, tanto de cumplimiento normativo como de los controles de la ISO 27002, podemos apreciar que no existe en la compañía un sistema de cifrado de información adecuado ni para cumplir con la legislación vigente ni para garantizar que la información, en caso de verse comprometida por ataques, tanto en tránsito como en almacenamiento, o por pérdida de dispositivos removibles, se vea comprometida su confidencialidad.

La finalidad última del proyecto es la de dotar al sistema de unas medidas de seguridad que garantice la integridad, confidencialidad, trazabilidad y autenticidad de la información. Las características principales que va a aportar al sistema son:

- Utilización de cifrado único, mediante un sistema de claves compartidas y administrada de forma centralizada.
- Cifrado de dispositivos removibles, creando una partición cifrada y otra sin cifrar, de tal forma que a la parte cifrada sólo se puede acceder cuando se está utilizando los ordenadores y sistemas de la compañía, mientras que la otra partición se puede usar en cualquier lugar. Esto hace que sea más difícil la infección del sistema Gespa o que algún empleado transporte o utilice la información en medios no seguros.
- Cifrado de los datos que se encuentran en los servidores de la compañía.
- Posibilidad de cifrado de discos completos

- En caso de pérdida o robo, la posibilidad de desactivar dispositivos remotamente.
- Generación y administración de las claves de los usuarios.

Las Fases del proyecto serían:

- Nombramiento del responsable del proyecto.
- Investigación de productos existentes en el mercado, en estos momentos se está pensando en una solución tipo Enpoint Encryption.
- Planificación y cálculo de coste reales en base a los productos del mercado
- Contratación de los servicios y producto.
- Instalación del sistema en un entorno de pruebas
- Pruebas de funcionamiento operativas.
- Instalación en equipos en producción.
- Pruebas del sistema
- Cursos de formación.

- **Tipo de activos involucrados**: Los activos afectados son**:**
  - [SW] Aplicaciones
  - [D] Datos
  - [COM] Red de comunicaciones

- **Dominios y/o Controles**:

8.1.3 Uso aceptable de los activos
8.3.1 Gestión de soportes extraíbles
9.1.1 Política de control de acceso
9.1.2 Acceso a las redes y los servidores de red
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves
13.1.1 Controles de red
13.1.2 Seguridad de los servidores de red
18.1.3 Protección de los registros de la organización
18.1.4 Protección y privacidad de la información de carácter personal
18.1.5 Regulación de los controles criptográficos

- Duración prevista: La duración estimada es de 2 meses
- Coste económico estimado:
- Coste H/H personal propio:
- Adquisiciones y Subcontrataciones: **5.000 €**
- Coste total: **5.000 €**
- Plazo previsto para consecución de objetivos: el plazo previsto para la consecución de los objetivos es corto. Se estima que en dos meses el sistema puede estar implementado.

4.5 PRT05: IMPLANTACIÓN DE UN SISTEMA ANTIMALWARE:

- Descripción: Actualmente, la compañía dispone de un sistema antivirus tradicional, instalado en los distintos equipos de la empresa. Pero está cada vez más demostrado que ese tipo de software no surte los efectos deseados para la protección integral de la información y de los sistemas, debido a que cada vez se usan unos métodos más sofisticados de ataques.

En nuestro análisis de riesgos, se ve que una de las amenazas que pueden influir más en la seguridad, es la distribución de software dañino, por lo que con este proyecto se pretende dotar a Gespa de los medios adecuados para reducir el nivel de riesgo al que se encuentra sometido por dicha amenaza.

La solución barajada consiste en una aplicación tipo Endpoint Protection que no sólo dispone de un sistema antivirus, sino previene de los ataque de día cero (ZeroDay) y la detección perimetral.

Uno de los objetivos del proyecto es el determinar qué producto de los existentes en el mercado se adapta mejor a nuestras necesidades y a nuestro modelo de negocio, teniendo en cuenta nuestra actividad productiva y el número de equipos y empleados.

Idealmente el sistema debería de permitir la protección del propio equipo individual, la protección perimetral para detección de amenazas antes de que el malware llegue a alcanzar el equipo o sistema objetivo, posibilidad de inspeccionar tráfico cifrado, detección de comportamientos anómalos etc.

El sistema que se decida instalar debe de ser capaz de protegernos de los ataques provenientes de cualquiera de los activos que forman nuestro sistema, es decir, móviles, portátiles, ordenadores de sobre mesa, correo electrónico, navegación por internet etc.

Las fases del proyecto serán las siguientes:

- Investigación las soluciones existentes en el mercado
- Estudio comparativo de las soluciones existentes.
- Adquisición de la solución elegida.
- Preparación de un entorno de instalación y pruebas.
- Instalación y prueba de la solución en la maqueta de pruebas.
- Preparación del plan de transición al sistema de producción.
- Instalación de la solución en el sistema en producción.
- Pruebas del sistema.
- Aceptación.

- **Tipo de activos involucrados**: Los activos afectados son**:**

- [HW] Equipamiento hardware
- [SW] Aplicaciones
- [D] Datos
- [COM] Red de comunicaciones

- **Dominios y/o Controles**:

9.4.1 Restricción del acceso no autorizado a los sistemas y aplicaciones
12.2.1 Controles contra el código malicioso
12.6.1 Gestión de las vulnerabilidades técnicas
13.1.2 Seguridad de los servidores de red

- Duración estimada: **4 meses**, de los cuales 1 es para la decisión y contratación del producto más idóneo y 3 meses para la implantación de la solución.

- Coste económico previsto:
- Coste H/H personal propio:
- Adquisiciones y Subcontrataciones: **2.500 €**
- Coste total: **2.500 €**
- Plazo previsto para consecución de objetivos: El proyecto debe de conseguir los objetivos a corto plazo, aunque la explotación es a largo plazo.

4.6 PRT06: PROCEDIMIENTO DE USO DE DISPOSITIVOS MÓVILES:

- Descripción: En la actualidad, cada vez está más extendido el uso de dispositivos móviles, ya sean teléfonos móviles, tablets u ordenadores portátiles, que hacen que los problemas de seguridad aumenten para las empresas, debido en muchos casos al uso indebido del mismo, o a su pérdida o robo.

Teniendo en cuenta que a través de los dispositivos móviles tenemos acceso a los datos y aplicaciones de la compañía, se hace necesario que se establezca un procedimiento de uso de esos dispositivos móviles, sobre todo, a la hora establecer los límites de uso y las actuaciones en caso de pérdida o robo.

Debido a las especiales características de utilización de los dispositivos móviles, se hace necesario la creación de un procedimiento de uso de los mismos, donde se recojan aspectos como:

- Registro de los dispositivos móviles propiedad de la empresa, donde se recojan las principales características identificativas del mismo y la persona a la que está asignado
- Prohibición de instalación de software o cambio de configuración por parte de los usuarios.

- No almacenar información que no sea estrictamente necesaria para el desempeño profesional.
- La información confidencial, debe de almacenarse de forma cifrada.
- Forma de actuación en caso de pérdida o robo del dispositivo, así como las precauciones que hay que tener cuando se trabaje fuera de la oficina.
- Se aplicarán las partes correspondientes a la política de uso de dispositivos en el puesto de trabajos, sobre todo lo relativo a bloqueo de equipos, uso de contraseñas etc.

Con lo anterior se pretende minimizar los riesgos inherentes al uso de dispositivos fuera de la oficina.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [HW01] Ordenadores portátiles
  - [HW08] Teléfonos móviles
  - [SS.01] Correo electrónico
  - [SW] Aplicaciones
  - [D] Datos
  - [COM] Red de comunicaciones

- Dominios y/o Controles:

  - 8.1.1Inventario de activos
  - 8.1.2 Propietario de los activos
  - 6.2.1 Política de dispositivos móviles
  - 6.2.2 Teletrabajo

- Duración prevista: **1 mes**
- Coste económico previsto:
- Coste H/H personal propio: 4**0 h**
- Adquisiciones y Subcontrataciones:
- Coste total: **1.400 €**
- Plazo previsto para consecución de objetivos: El procedimiento debe de estar listo a corto plazo, pero la aplicación de procedimiento es a largo plazo, ya que será de obligado cumplimiento hasta que sea modificado o derogado.

4.7 PRT07: PROCEDIMIENTO DE COPIAS DE SEGURIDAD:

- Descripción: A pesar de todas las medidas adoptadas para garantizar la integridad y disponibilidad de la información, podemos encontrarnos con que se materialice alguno de los riesgos previstos, y por lo tanto, se

produzca la pérdida de toda o parte de la información almacenada en nuestros sistemas.

Si tal situación se produjese, debemos de tener disponible una copia de seguridad reciente que nos permita recuperar la información almacenada, ya que en caso contrario, se podría llegar a poner en peligro la continuidad del negocio, y por lo tanto de la empresa.

En la empresa existen unas instrucciones, en base a las cuales se realizan actualmente las copias de seguridad, pero dado la gran importancia que para la compañía tienen la información, estas copias de seguridad no se pueden realizar de una forma arbitraria y al criterio de la persona que en cada momento pueda estar a cargo de realizarla. Es por ello, que se hace necesario procedimentar este proceso tan importante.

De forma general, las copias de seguridad que se suelen hacer son las completas, diferencial (se copian los datos modificados desde la última copia completa), o incremental (se copian los datos modificados desde la última copia realizada).

Con el procedimiento de copias de seguridad se intenta marcar las pautas a seguir para la realización de las copias de la información de la compañía. El procedimiento será realizado por el administrador de seguridad y revisado por el Jefe de Seguridad. En este procedimiento se deben de recoger aspectos como:

- Sistema de backup utilizado.
- Soporte de almacenamiento de las copias de seguridad.
- Lugar de almacenamiento.
- Tipo de copia de seguridad (total, diferencial o incremental).
- Responsable de realizar las copias.
- Si las copias se cifran o se guardan en claro.
- Cada cuanto tiempo se realizan cada una de las copias de seguridad.
- El procedimiento se debe de revisar anualmente.
- Tipo de información o datos que hay que copiar.
- El procedimiento debe de recoger la forma en que se recuperan los datos y quién puede hacer la recuperación de los mismos.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [SW] Aplicaciones
  - [D] Datos

- Dominios y/o Controles:

12.3.1 Copias de seguridad de la información

- Duración estimada: **1 semana**
- Coste económico previsto:
- Coste H/H personal propio: **24 h**
- Adquisiciones y Subcontrataciones:
- Coste total estimado: **800 €**
- Plazo previsto para consecución de objetivos: El procedimiento se debe de realizar a corto plazo, así como la implementación del mismo, que no debe de tardar más de 1 mes en estar implementado.

4.8 PRT08: ELABORACIÓN DEL INVENTARIO, CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS:

- Descripción: En el estudio realizado, se ha visto la carencia que tiene la empresa en lo relativo a la gestión de activos, ya que se han detectado deficiencias en el inventario, etiquetado y clasificación.

Para solucionar esta deficiencia y cumplir con control previsto en la ISO 27002, se pretende llevarla a cabo con este proyecto.

El inventario y clasificación de activos se puede considerar como la configuración de los activos implicados en la seguridad de la información, y por lo tanto es ahí donde se deben de recoger toda la información técnica relevante y la identificativa de cada uno de los componentes del sistema de información, es decir el conjunto de características funcionales y físicas de los activos.

Los elementos a inventariar, son el conjunto de equipo físico, soporte electrónico, software, material procesado, servicios o cualquiera de sus partes que intervienen o afectan a la seguridad de la información y que se elige para ser gestionado específicamente dentro de un proceso global.

Tomando como base la configuración de los activos, el presente proyecto tiene como finalidad:

- Elaborar la plantilla que nos sirva para la introducción de los datos de cada uno de los activos, dependiendo de que sea hardware, software, datos o servicios.
- Elaboración del listado de los activos.
- Identificación del propietario del activo.
- Control de cambios donde se controles los cambios habidos en el sistema.
- Auditorías previstas para comprobar el inventario y el correcto etiquetado de los activos.
- Elaboración de los criterios de etiquetado de los elementos, en función de sus características técnicas, lógicas, funcionales o de ubicación.
- Identificación del responsable de mantener actualizado el inventario.

A la finalización del proyecto, los activos deben de encontrarse inventariados, clasificados y etiquetados.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [L] Instalaciones
  - [HW] Equipamiento hardware
  - [SW] Aplicaciones
  - [D] Datos
  - [COM] Red de comunicaciones
  - [SS] Servicios subcontratados
  - [AUX] Equipamiento Auxiliar

- Dominios y/o Controles:
  - 8.1.1 Inventario de activos
  - 8.1.2 Propietario de los activos
  - 8.2.1 Clasificación de la información
  - 8.2.2 Etiquetado de la información
  - 8.2.3 Manipulación de la información
  - 8.3.1 Gestión de soportes extraíbles

- Duración prevista: **1 mes**
- Coste estimado:
- Coste H/H personal propio: **160 h.**
- Adquisiciones y Subcontrataciones:
- Coste total estimado: **4.000 €**
- Plazo previsto para consecución de objetivos: Los objetivos de este proyecto son a corto plazo, ya que es básico para la seguridad de la información tener perfectamente inventariado y clasificado todo los activos.

4.9 PRT09: ELABORACIÓN DE PLANTILLA PARA LOS CONTRATOS BASE CON TERCEROS:

- Descripción: A la hora de acometer los trabajos necesarios para el desempeño de nuestra actividad, no siempre se puede realizar con recursos propios, por lo que en ciertos momentos, debido a falta de personal, por la falta de cualificación o porque sólo los puede prestar un tercero, es necesario contratar algunos de los servicios a empresas o personal ajeno a nuestra organización. En estos casos no solo hay que garantizar que la empresa en cuestión cumple con los requisitos mínimos necesarios para garantizar la seguridad de la información a la que tiene acceso o que ponemos a su disposición para realizar el trabajo, sino que se tiene que quedar plasmado en un documento formal con validez legal, donde se recoja el compromiso y obligación de confidencialidad y reserva con respecto a la información y al sistema de seguridad al que tiene acceso por razones contractuales.

El presente proyecto tiene como objetivo el preparar unas cláusulas con los requisitos generales que sean de aplicación a las distintas empresas subcontratistas y que formarán parte del clausulado general de todos los contratos.

Se debe de recoger:

- Obligación de confidencialidad.
- Obligación de devolver la información puesta a su disposición, una vez terminada la relación contractual.
- Garantizar la integridad, confidencialidad y trazabilidad de la información
- Establecer la prohibición de transferir la información a un tercero sin nuestro permiso expreso por escrito.
- Obligación de cumplir con las obligaciones legales en lo relativo a la protección y manejo de información y datos personales.
- Establecer procedimientos para la medición del cumplimiento de estos requisitos.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [SS] Servicios subcontratados

- Dominios y/o Controles:

15.1.1 Política de seguridad de la información en las relaciones con los proveedores
15.1.2 Requisitos de seguridad en contratos con terceros
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

- Duración estimada: **1 semana**

- Coste estimado:
- Coste H/H personal propio: **16 h**
- Adquisiciones y Subcontrataciones:
- Coste total estimado: 650 €
- Plazo previsto para consecución de objetivos: Este proyecto tiene como objetivo el aplicar las cláusulas a largo plazo.

4.10 PRT010: SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS:

- Descripción:

En todos los estudios relativos a seguridad se concluye que el eslabón más débil en la cadena suelen ser los recursos humanos, por sus errores y actividades ilícitas.

Dado que en los contratos firmados entre la empresa y los nuevos empleados no se dispone de las cláusulas relativas a los compromisos de confidencialidad y del cumplimiento normativo en lo relativo a la seguridad de la información, se hace necesario la creación de un documento con las clausulas tipo que se incluirán en los contratos que se lleven a cabo para la incorporación de personal, independientemente de la modalidad de contrato (temporal, fijo, en prácticas etc.) y del personal subcontratado.

En el documento se debe de recoger cómo se va a llevar a cabo la verificación de los datos aportado por el candidato así como los antecedentes penales, sobre todo si la persona va a tener acceso a información y/o sistemas confidenciales. Cualquier tipo de investigación o comprobación se deberá de llevar a cabo bajo el más estricto cumplimiento de la legislación vigente.

En el contrato se deben de recoger las cláusulas de confidencialidad, las responsabilidades legales con respecto al manejo de información confidencial, protección de datos personales, conducta ética, medidas disciplinarias en caso de incumplimiento de sus obligaciones etc.

En el contrato tiene que quedar claro por ambas partes cuáles son las responsabilidades que se adquieren con la firma del contrato y el acceso a la información.

El documento también debe de recoger la forma de garantizar el cumplimiento de las obligaciones en materia de seguridad una vez el personal ha sido contratado, incluyendo por ejemplo la comprobación de que se les proporciona las directrices adecuadas, continúan teniendo el perfil profesional adecuado, están motivados, etc.

Además se debe incluir la forma de proporcionar la formación, concienciación y capacitación en seguridad a los empleados, así como las medidas disciplinarias que se encuentran en vigor para el supuesto de que provoque alguna brecha de seguridad al sistema.

Por último debe incluirse en el contrato el compromiso de mantener confidencialidad después de finalización de las relaciones contractuales.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [P] Personal

- Dominios y/o Controles afectados:

7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones del empleo
7.2.1 Responsabilidades de gestión
7.2.2 Concienciación, educación y capacitación en seguridad de la información
7.2.3 Proceso disciplinario

- Duración estimada: **1 mes**

- Coste estimado:
- Coste H/H personal propio: **120 h.**
- Adquisiciones y Subcontrataciones:
- Coste total: **5.000 h**
- Plazo previsto para consecución de objetivos:

4.11 PRT011: ANÁLISIS DE VULNERABILIDADES:

- **Descripción**:

Aparte de las medidas de protección, tanto técnicas como procedimentales previstas en la compañía para garantizar la seguridad de la información contra posibles ataque tanto internos como externos que pongan en peligro la integridad, disponibilidad y confidencialidad de la información, es necesario verificar mediante herramientas especializadas, la robustez de nuestro sistema. Es lo que se ha dado en llamar hacking ético.

Dado que en la empresa no disponemos de los medios ni de los especialistas adecuados para llevar a cabo este análisis de vulnerabilidades (hacking ético), es necesario contratar estos servicios a través de un proveedor externo.

El proyecto consiste:

- Búsqueda de posibles empresas que den ese servicio.
- Petición de ofertas.
- Contratación del servicio.
- Realización de las pruebas de vulnerabilidad.
- Corrección de las vulnerabilidades detectadas.
- Planificar las revisiones periódicas.

- Tipo de activos involucrados: **Los activos afectados son:**
  - [HW] Equipamiento hardware
  - [SW] Aplicaciones
  - [D] Datos
  - [COM] Red de comunicaciones
  - [SS] Servicios subcontratados

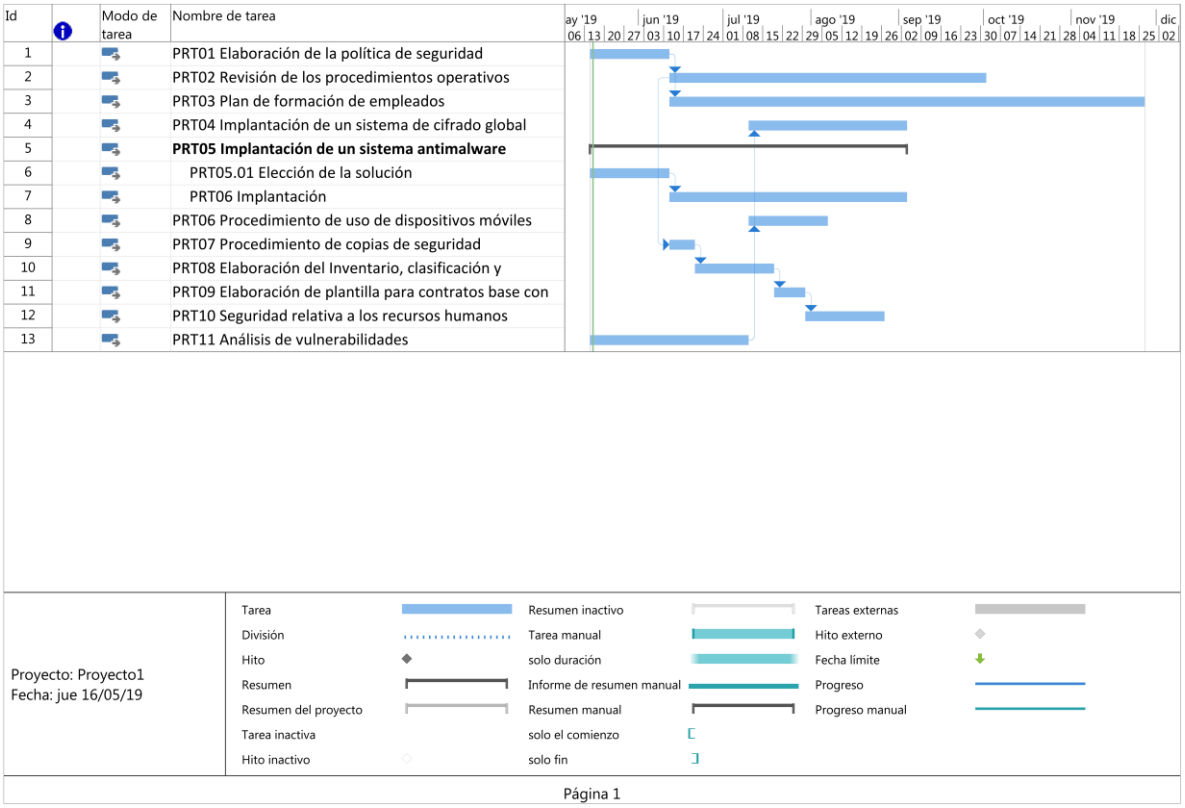
- Dominios y/o Controles afectados:

12.6.1 Gestión de las vulnerabilidades técnicas
12.6.2 Restricción en la instalación del software
13.2.3 Mensajería electrónica

- Duración estimada: **2 mes**

- Coste estimado:
- Coste H/H personal propio:
- Adquisiciones y Subcontrataciones: **2.000 €**
- Coste total: **2.000 h**
- Plazo previsto para consecución de objetivos: Los resultados están previsto obtenerlos a corto plazo.

4.12 DIAGRAMA DE GANTT DE LOS PROYECTOS:



4.13 RESULTADOS:

Tras la propuesta de proyectos para mejorar de la seguridad de la información de la empresa y para el cumplimiento con los diferentes dominios de la norma ISO 27002, es necesario hacer una análisis de cómo quedará la nueva situación tras la ejecución de los proyecto.

El objetivo último de los proyectos ha sido el de mejorar la seguridad de la información y el cumplir con la ISO 27002, por lo que se han planteado como actividades que se tienen que ejecutar, abarcando todos los ámbitos de la

seguridad de la empresa. Para ello hemos comenzado con la definición de la política de seguridad, como paso previo imprescindible para acometer cualquier trabajo posterior en este sentido. Hemos hecho el inventario de activos, ya que si no sabemos con claridad qué forma nuestro sistema, difícilmente podremos protegerlo. También se han abordado los aspectos legales y normativos de la contratación de personal y de servicios, la implantación de un sistema de cifrado global, etc.

Además de los proyectos necesarios para subsanar deficiencias encontradas en el sistema de seguridad, se ha acometido uno de formación del personal, como algo imprescindible para el buen funcionamiento de cualquier sistema, ya sea de seguridad o no.

Una vez se hayan acometido los diferentes proyectos, la situación cambia considerablemente. Al objeto de ver la evolución sufrida, se presenta un nuevo análisis diferencial y un nuevo análisis de riesgos. Si a pesar de los proyectos acometidos, fuesen necesarios nuevos proyectos, se plantearían para una segunda fase.

4.14 NUEVO CUADRO DE IMPACTO POTENCIAL TRAS EJECUTAR LOS PROYECTOS:

Una vez implementadas las acciones (proyectos) previstas, se estima que el nuevo cuadro del impacto potencial sería el de la *tabla 18*. Como se puede apreciar, los niveles de riesgo han bajado considerablemente, ya que se han reducido considerablemente la frecuencia de ocurrencia de alguno de los riesgos que hacían que los niveles estuvieran por encima del nivel de riesgo aceptable.

				impacto potencial						impacto potencial				
Ambito	**Código**	**Activo**	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones														
	L.01	CPD	**0,1**	7,0	7,0		9,0			0,7	0,7	0,0	0,9	0,0
	L.02	Edificio	**0,1**				9,0			0,0	0,0	0,0	0,9	0,0
[HW] Equipamiento hardware														
	HW.01	Pc portátiles	**1**	5,3	8,0	5,0	4,0	0,0		5,3	8,0	5,0	4,0	0,0
	HW.02	Pc de sobremesa	**1**	7,0	6,0	5,0	4,0	0,0		7,0	6,0	5,0	4,0	0,0
	HW.03	Servidor de proyectos	**1**	9,0	8,0	8,0	9,0	0,0		9,0	8,0	8,0	9,0	0,0
	HW.04	Servidor de desarrollo	**1**	7,0	8,0	8,0	8,0	0,0		7,0	8,0	8,0	8,0	0,0

	HW.05	Servidor de administración	**1**	7,0	8,0	8,0	8,0	0,0		7,0	8,0	8,0	8,0	0,0
	HW.06	Servidor de impresión	**1**	0,0	0,0	0,0	5,3	0,0		0,0	0,0	0,0	5,3	0,0
	HW.07	Routers	**1**	0,0	7,0	9,0	9,0	0,0		0,0	7,0	9,0	9,0	0,0
	HW.10	Switches	**1**	0,0	0,0	0,0	8,0	0,0		0,0	0,0	0,0	8,0	0,0
	HW.11	Firewall	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	HW.13	Sistema de backup	**1**	0,0	9,0	9,0	9,0	0,0		0,0	9,0	9,0	9,0	0,0
	HW.09	Teléfonos de sobremesa	**1**	0,0	3,8	0,0	3,0	0,0		0,0	3,8	0,0	3,0	0,0
	HW.12	Impresoras	**1**	0,0	0,0	0,0	5,0	0,0		0,0	0,0	0,0	5,0	0,0
	HW.08	Teléfonos móviles	**1**	3,0	9,0	8,0	5,0	0,0		3,0	9,0	8,0	5,0	0,0
	HW.15	Punto de acceso wifi	**1**	0,0	0,0	0,0	7,0	0,0		0,0	0,0	0,0	7,0	0,0
[SW] Aplicaciones														
	SW.01	Sistemas operativos	**1**	0,0	5,0	8,0	8,0	0,0		0,0	5,0	8,0	8,0	0,0
	SW.02	Software antivirus	**1**	0,0	6,0	8,0	8,0	0,0		0,0	6,0	8,0	8,0	0,0
	SW.03	Aplicaciones ofimáticas.	**1**	0,0	8,0	8,0	8,0	0,0		0,0	8,0	8,0	8,0	0,0
	SW.04	Aplicativo ERP	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	SW.05	Software de gestión de proyectos	**1**	0,0	8,0	8,0	6,0	0,0		0,0	8,0	8,0	6,0	0,0
	SW.06	Software de desarrollo	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	SW.07	Aplicación financiera	**1**	7,0	9,0	9,0	7,0	0,0		7,0	9,0	9,0	7,0	0,0
[D] Datos														
	D.01	Datos de clientes	**1**	0,0	9,0	8,0	7,0	0,0		0,0	9,0	8,0	7,0	0,0
	D.02	Datos de proyectos	**1**	0,0	8,0	7,0	6,0	0,0		0,0	8,0	7,0	6,0	0,0
	D.03	Datos de desarrollo	**1**	0,0	9,0	9,0	7,0	0,0		0,0	9,0	9,0	7,0	0,0
	D.04	Datos de emails	**1**	0,0	9,0	8,0	6,0	0,0		0,0	9,0	8,0	6,0	0,0
	D.05	Datos personales	**1**	0,0	9,0	8,0	6,0	0,0		0,0	9,0	8,0	6,0	0,0
[COM] Red de comunicaciones														
	COM.01	Red LAN	**1**	0,0	8,0	8,0	9,0	0,0		0,0	8,0	8,0	9,0	0,0
	COM.02	red inalámbrica	**1**	0,0	8,0	8,0	4,0	0,0		0,0	8,0	8,0	4,0	0,0
	COM.03	Telefonía fija	**1**	0,0	7,0	3,0	5,0	0,0		0,0	7,0	3,0	5,0	0,0
	COM.04	telefonía móvil	**1**	0,0	7,0	7,0	3,0	0,0		0,0	7,0	7,0	3,0	0,0
	COM.05	Internet.	**1**	0,0	7,0	4,0	6,0	0,0		0,0	7,0	4,0	6,0	0,0
[SS] Servicios subcontratados														
	SS.01	Correo electrónico	**1**	8,0	8,0	6,0	8,0	6,0		8,0	8,0	6,0	8,0	6,0
[AUX] Equipamiento Auxiliar														
	AUX.01	Sistema de alimentación ininterrumpida	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
	AUX.02	Sistema de alarmas	**0,1**	0,0	0,0	0,0	8,0	0,0		0,0	0,0	0,0	0,8	0,0
	AUX.03	Sistema contraincendios	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
	AUX.04	Sistema de climatización.	**0,1**	0,0	0,0	0,0	9,0	0,0		0,0	0,0	0,0	0,9	0,0
[P] Personal														
	P.01	Director general	**1**	0,0	9,0	0,0	9,0	0,0		0,0	9,0	0,0	9,0	0,0

	P.02	Administrador del sistema	**1**	0,0	8,0	0,0	8,0	0,0		0,0	8,0	0,0	8,0	0,0
	P.03	Usuarios	**1**	0,0	8,0	0,0	6,0	0,0		0,0	8,0	0,0	6,0	0,0
	P.04	Jefe de Seguridad	**1**	0,0	9,0	0,0	9,0	0,0		0,0	9,0	0,0	9,0	0,0

Tabla 19 Tabla de impacto potencial después de ejecutar los proyectos

4.15 NUEVO DIAGRAMA DE RADAR:

Diagrama de radar previsto una vez implementados los proyectos

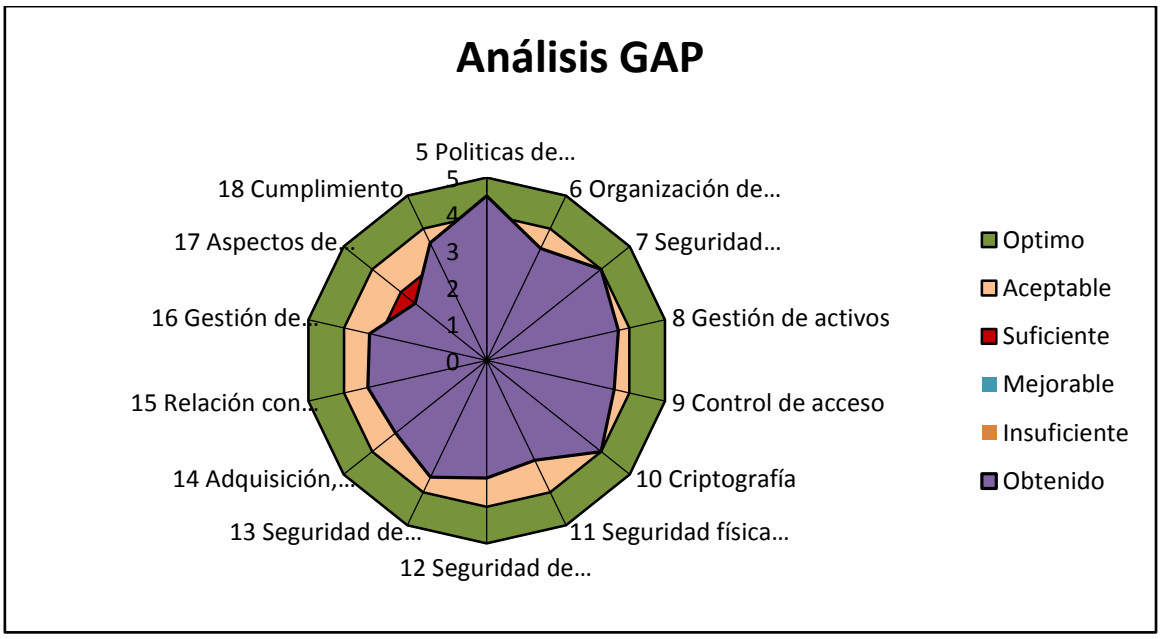


Ilustración 9 Representación gráfica análisis GAP una vez ejecutados los proyectos

Diagrama de radar antes de implementar los proyectos.

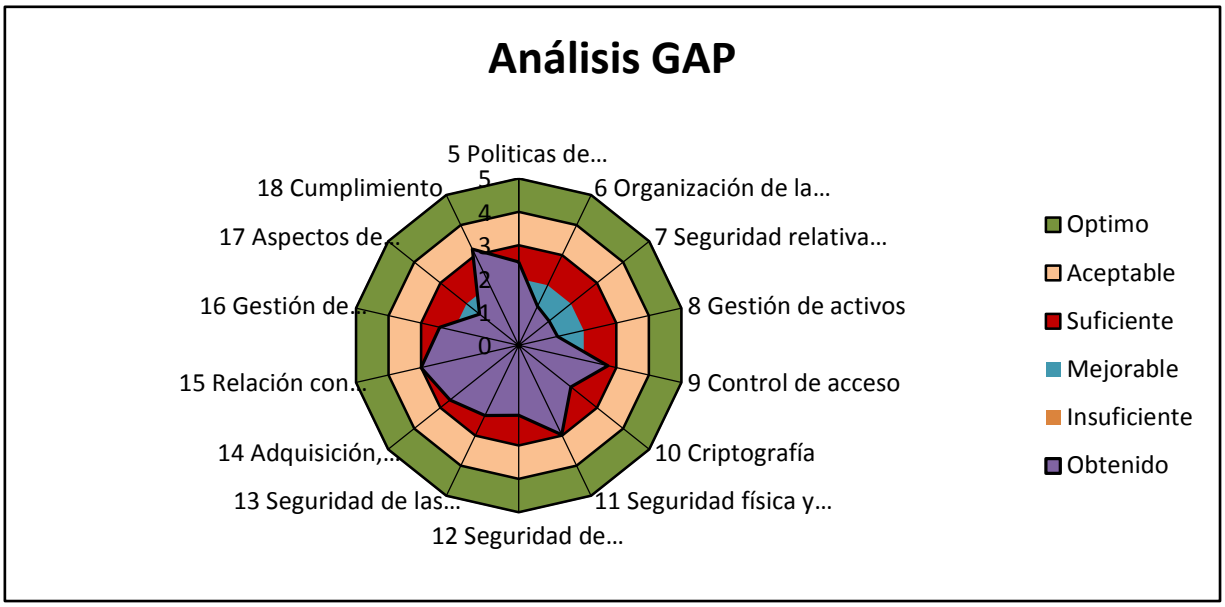


Ilustración 10 Representación gráfica análisis GAP antes de ejecutar los proyectos.

5 AUDITORÍA DE CUMPLIMIENTO

5.1 INTRODUCCIÓN:

En este momento ya hemos realizado una radiografía bastante detallada de la situación de la empresa con relación a la seguridad de la información, se ha hecho un estudio de los riesgos y amenazas a los que nos encontramos expuestos, así como las acciones o proyectos ejecutados para intentar corregir en la medida de lo posible los problemas de seguridad que se han ido encontrando.

Llegados a este punto es necesario realizar una auditoría para ver el grado de cumplimiento con las buenas prácticas en materia de seguridad.

Esta auditoría nos servirá para realizar nuevas acciones en caso de que se detecten algún incumplimiento importante, y a la vez nos servirá como punto de partida para nuevas auditorías.

5.2 METODOLOGÍA

Como se ha manifestado anteriormente, el objetivo de la auditoría es el de determinar el grado de cumplimiento de la compañía con respecto a las buenas prácticas en materia de seguridad. Para ver el grado de cumplimiento de los 114 controles y 14 dominios recogidos en la ISO 27002, se determinará su nivel de madurez en base a los niveles definidos por CMM y que se recogen en la tabla siguiente.

Efectividad	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el 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 en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de caca individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen 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 comunes y se optimizan los procesos.

Tabla 20 Criterios para la evaluación de los niveles de madurez

Este tipo de evaluación nos proporciona una visión rápida del grado cumplimiento de la empresa en materia de seguridad de la información, teniendo como gran ventaja, el que se puede adjuntar a los informes a la dirección, dado que es un resumen muy visual de la situación, sin entrar en detalles técnicos.

Una vez realizada la auditoría de cumplimiento en base al CMM, estaremos en disposición de sacar conclusiones e identificar los puntos fuertes y debilidades que nos podrían llevar a plantear nuevos proyectos.

5.3 ALCANCE

Para la evaluación de la madurez, se ha analizado tanto el cumplimiento con respecto a los apartados de la ISO 27001:2013 como con respecto a los dominios de la ISO 27002.

Los apartados de la ISO 27001:2013 analizados son:

- 4 Contexto de la organización
- 5 Liderazgo
- 6 Planificación
- 7 Soporte

- 8 Operación
- 9 Evaluación del desempeño
- 10 Mejora

Los dominios que vamos a analizar para realizar la evaluación de la madurez son los siguientes:

- 5 Políticas de seguridad de la información
- 6 Organización de la seguridad de la información
- 7 Seguridad relativa a los recursos humanos
- 8 Gestión de activos
- 9 Control de acceso
- 10 Criptografía
- 11 Seguridad física y entorno
- 12 Seguridad de operaciones
- 13 Seguridad de las comunicaciones
- 14 Adquisición, desarrollo y mantenimiento de los sistemas de información
- 15 Relación con proveedores
- 16 Gestión de incidentes de seguridad de la información
- 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- 18 Cumplimiento

5.4 EVALUACIÓN CON RESPECTO A LA ISO 27001:2013

Requerimientos ISO 27001		Evaluación	Valor	Total
4	**Contexto de la organización**			4
4.1	Comprensión de la organización y de su contexto	4 - Gestionado	4	4
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	4 - Gestionado	4	4
4.3	Determinación del alcance del SGSI	4 - Gestionado	4	4
4.4	SGSI	4 - Gestionado	4	4
5	**Liderazgo**			4,33
5.1	Liderazgo y compromiso	4 - Gestionado	4	4
5.2	Política	5 - Optimizado	5	5
5.3	Roles, responsabilidades y autoridades en la organización	4 - Gestionado	4	4
6	**Planificación**			2,33
6.1	Acciones para tratar los riesgos y oportunidades	4 - Gestionado	4	4
6.2	Objetivos de seguridad de la información y planificación para su consecución	3 - Definido	3	3
7	**Soporte**			3,5
7.1	Recursos	4 - Gestionado	4	4

7.2	Competencia	3 - Definido	3	3
7.3	Concienciación	4 - Gestionado	4	4
7.4	Comunicación	3 - Definido	3	3
8	**Operación**			3,67
8.1	Planificación y control operacional	3 - Definido	3	3
8.2	Apreciación de los riesgos de seguridad de la información	4 - Gestionado	4	4
8.3	Tratamiento de los riesgos de seguridad de la información	4 - Gestionado	4	4
9	**Evaluación del desempeño**			4,33
9.1	Seguimiento, medición, análisis y evaluación	4 - Gestionado	4	4
9.2	Auditoría interna	4 - Gestionado	4	4
9.3	Revisión por la dirección	5 - Optimizado	5	5
10	**Mejora**			3,5
10.1	No conformidad y acciones correctivas	4 - Gestionado	4	4
10.2	Mejora continua	3 - Definido	3	3

Tabla 21 Análisis Diferencial ISO 27001

5.4.1 Diagrama de radar actual del cumplimiento de la ISO 27001:2013

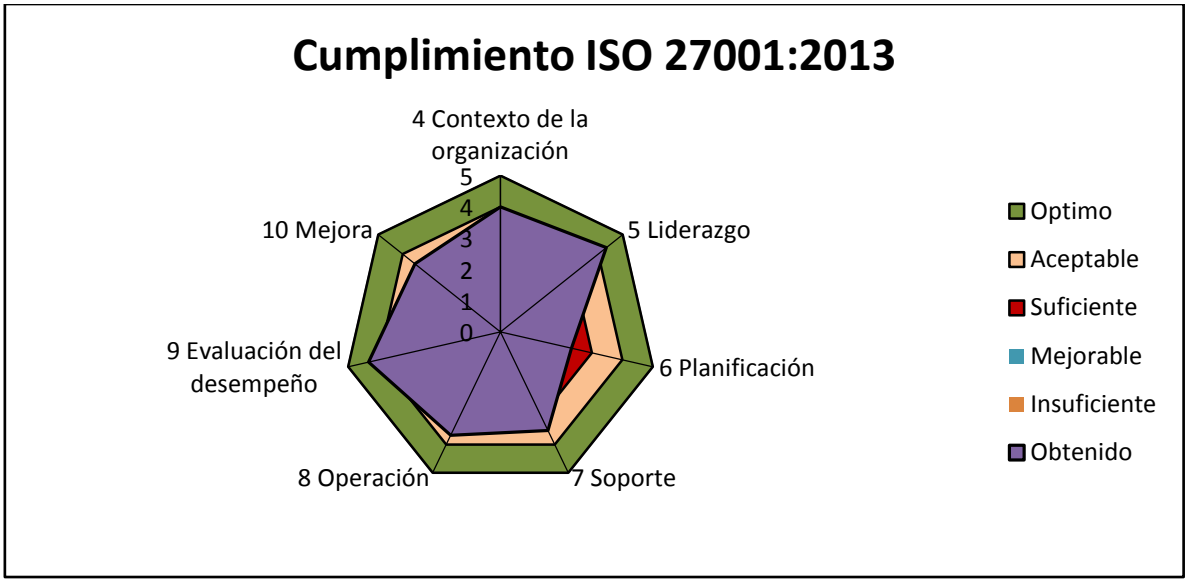


Ilustración 11 Representación gráfica cumplimiento final ISO 27001

Para facilitar la comparación, a continuación se pone el diagrama de radar inicial.

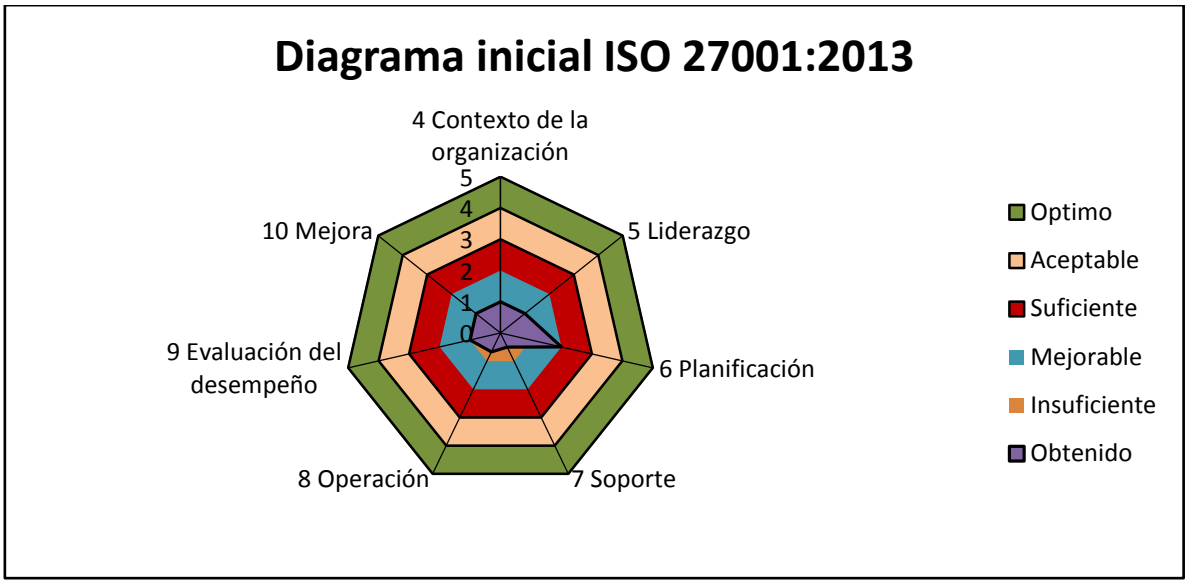


Ilustración 12 Representación gráfica cumplimiento inicial ISO 27001

5.5 EVALUACIÓN DE LA MADUREZ

Tal como se ha dicho en el punto anterior, en este apartado del proyecto se va a evaluar la madurez de la seguridad de la información de la empresa con respecto a los 114 controles de la ISO/IEC 27002:2013.

Para que la evaluación sea efectiva, además de conocer la norma, es necesario disponer de un profundo conocimiento de la organización, ya que en caso contrario, los resultados obtenidos no recogerían la realidad de la situación.

En este momento, después de haber hecho una descripción contextual de la empresa, después de haber realizado el análisis de riesgos y de las posibles amenazas a las que nos encontramos expuestos, después de haber realizado los proyectos para corregir las deficiencias, creo que estamos en una óptima situación para realizar la evaluación de la madurez.

En las siguientes tablas se van a recoger los valores correspondientes a la situación actual, posteriormente se compararán con los obtenidos al principio del proyecto, de esta forma se podrá comparar la evolución que ha sufrido la seguridad con las medidas organizativas, documentales y técnicas llevadas a cabo.

En cada uno de los dominios se incluirá los objetivos de control y los controles correspondientes con su nivel de madurez.

5 Políticas de seguridad de la información

Objetivo:

- Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo a los requisitos del negocio la legislación y normativa aplicable

CONTROL				Evaluación	CMM	Valor	Total
5 Políticas de seguridad de la información							98 %
	5.1 Directrices de gestión de la seguridad de la información						98 %
		5.1.1	Políticas para la seguridad de la información	4 - Gestionado	L4	95 %	
		5.1.2	Revisión de las políticas para la seguridad de la información	5 - Optimizado	L5	100 %	

6 Organización de la seguridad de la información

Objetivo 1:

- Establecer un marco de gestión para iniciar y controlar la implantación y la operación de la seguridad de la información dentro de la organización

Objetivo 2:

- Garantizar la seguridad del teletrabajo y en el uso de los dispositivos móviles.

CONTROL				Evaluación	CMM	Valor	Total
6 Organización de la seguridad de la información							**83 %**
	6.1 Organización interna						68 %
		6.1.1	Roles y responsabilidades en seguridad de la información	4 - Gestionado	L4	95 %	
		6.1.2	Segregación de tareas	4 - Gestionado	L4	95 %	
		6.1.3	Contacto con las autoridades	2 - Repetible	L2	50 %	
		6.1.4	Contacto con grupos de interés especial	2 - Repetible	L2	50 %	
		6.1.5	Seguridad de la información en la gestión de proyectos	2 - Repetible	L2	50 %	
	6.2 Dispositivos móviles y el teletrabajo						98 %
		6.2.1	Política de dispositivos móviles	5 - Optimizado	L5	100 %	
		6.2.2	Teletrabajo	4 - Gestionado	L4	95 %	

7 Seguridad relativa a los recursos humanos

Objetivo 1:

- Garantizar que tanto los empleados como los subcontratistas entienden sus responsabilidades y tienen la capacitación técnica y personal adecuada al puesto para el que han sido elegidos.

Objetivo 2:

- Asegurar de que todas las partes interesadas, en lo relativo a la seguridad de la información, conocen y cumplen con sus responsabilidades

Objetivo 3:

- Proteger los intereses de la empresa ante el cambio o finalización de un contrato, relaciones laborales o comerciales de empleados y subcontratistas.

CONTROL			Evaluación	CMM	Valor	Total
7 Seguridad relativa a los recursos humanos						**95 %**
7.1 Antes del empleo						95 %
	7.1.1	Investigación de antecedentes	3 - Definido	L3	90 %	
	7.1.2	Términos y condiciones del empleo	5 - Optimizado	L5	100 %	
7.2 Durante el empleo						95 %
	7.2.1	Responsabilidades de gestión	4 - Gestionado	L4	95 %	
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	4 - Gestionado	L4	95 %	
	7.2.3	Proceso disciplinario	4 - Gestionado	L4	95 %	
7.3 Finalización del empleo o cambio en el puesto de trabajo						95 %
	7.3.1	Responsabilidades ante la finalización o cambio	4 - Gestionado	L4	95 %	

8 Gestión de activos

Objetivo 1:

- Identificar los activos de la empresa y definir las responsabilidades para una adecuada protección.

Objetivo 2:

- Asegurar que se aplica a la información un nivel de protección de acuerdo con su nivel de clasificación y/o importancia.

Objetivo 3:

- Evitar la divulgación, modificación, eliminación o destrucción de la información almacenada en los diferentes soportes.

CONTROL				Evaluación	CMM	Valor	Total
8 Gestión de activos							**90 %**
	8.1 Responsabilidad sobre los activos						94 %
		8.1.1	Inventario de activos	4 - Gestionado	L4	95 %	
		8.1.2	Propietario de los activos	4 - Gestionado	L4	95 %	
		8.1.3	Uso aceptable de los activos	3 - Definido	L3	90 %	
		8.1.4	Devolución de activos	4 - Gestionado	L4	95 %	
	8.2 Clasificación de la información						80 %
		8.2.1	Clasificación de la información	2 - Repetible	L2	50 %	
		8.2.2	Etiquetado de la información	4 - Gestionado	L4	95 %	
		8.2.3	Manipulación de la información	4 - Gestionado	L4	95 %	
	8.3 Manipulación de los soportes						95 %
		8.3.1	Gestión de soportes extraíbles	4 - Gestionado	L4	95 %	
		8.3.2	Eliminación de soportes	4 - Gestionado	L4	95 %	
		8.3.3	Soportes físicos en tránsito	4 - Gestionado	L4	95 %	

9 Control de acceso

Objetivo 1:

- Controlar el acceso tanto a la información como a los recursos para su almacenamiento, tratamiento o transporte.

Objetivo 2:

- Garantizar el acceso a los usuarios autorizados e impedir que el personal no autorizado no accede ni a la información ni a los medidos de almacenamiento o transporte.

Objetivo 3:

- Hacer que los usuarios se hagan responsables de custodiar la información de autenticación en los sistemas información.

Objetivo 4:

- Mediante el control de acceso a los sistemas y aplicaciones, impedir que personal no autorizado acceda a los mismos.

CONTROL			Evaluación	CMM	Valor	Total
9 Control de acceso						**91 %**
9.1 Requisitos de negocio para el control de acceso						95 %
	9.1.1	Política de control de acceso	4 - Gestionado	L4	95 %	
	9.1.2	Acceso a las redes y los servidores de red	4 - Gestionado	L4	95 %	
9.2 Gestión de acceso de usuario						87 %
	9.2.1	Registro y baja de usuario	4 - Gestionado	L4	95 %	
	9.2.2	Provisión de acceso de usuario	4 - Gestionado	L4	95 %	
	9.2.3	Gestión de privilegios de acceso	4 - Gestionado	L4	95 %	
	9.2.4	Gestión de la información secreta de autenticación de los usuarios	2 - Repetible	L2	50 %	
	9.2.5	Revisión de los derechos de acceso de usuario	3 - Definido	L3	90 %	
	9.2.6	Retirada o reasignación de los derechos de acceso	4 - Gestionado	L4	95 %	
9.3 Responsabilidades del usuario						90 %
	9.3.1	Uso de la información secreta de autenticación	3 - Definido	L3	90 %	
9.4 Control de acceso a sistemas y aplicaciones						94 %
	9.4.1	Restricción del acceso no autorizado a los sistemas y aplicaciones	4 - Gestionado	L4	95 %	
	9.4.2	Procedimientos seguros de inicio de sesión	4 - Gestionado	L4	95 %	
	9.4.3	Sistema de gestión de contraseñas	4 - Gestionado	L4	95 %	
	9.4.4	Uso de utilidades con privilegios del sistema	3 - Definido	L3	90 %	
	9.4.5	Control de acceso al código fuente de los programas	4 - Gestionado	L4	95 %	

10 Criptografía

Objetivo1:

- El objetivo de los controles criptográficos es el garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

CONTROL			Evaluación	CMM	Valor	Total
10 Criptografía						**95 %**
10.1 Controles criptográficos						95 %
	10.1.1	Política de uso de los controles criptográficos	4 - Gestionado	L4	95 %	
	10.1.2	Gestión de claves	4 - Gestionado	L4	95 %	

11 Seguridad física y entorno

Objetivo 1:

- Mediante las áreas de seguridad intenta prevenir el acceso físico no autorizado tanto a la información como a los sistemas de tratamiento o almacenamiento, con el fin de evitar daños o interferencias.

Objetivo 2:

- Mediante seguridad de los equipos se intenta evitar la pérdida, daño, robo, manipulación o interceptación de las operaciones de la compañía.

CONTROL			Evaluación	CMM	Valor	Total
11 Seguridad física y entorno						**83 %**
11.1 Áreas seguras						85 %
	11.1.1	Perímetro de seguridad física	3 - Definido	L3	90 %	
	11.1.2	Controles físicos de entrada	4 - Gestionado	L4	95 %	
	11.1.3	Seguridad de oficinas, despachos y recursos	3 - Definido	L3	90 %	
	11.1.4	Protección contra las amenazas externas y ambientales	3 - Definido	L3	90 %	
	11.1.5	El trabajo en áreas seguras	2 - Repetible	L2	50 %	
	11.1.6	Áreas de carga y descarga	4 - Gestionado	L4	95 %	
11.2 Seguridad de los equipos						81 %
	11.2.1	Emplazamiento y protección de equipos	3 - Definido	L3	90 %	
	11.2.2	Instalaciones de suministro	3 - Definido	L3	90 %	
	11.2.3	Seguridad del cableado	2 - Repetible	L2	50 %	
	11.2.4	Mantenimiento de equipos	3 - Definido	L3	90 %	
	11.2.5	Retirada de material propiedad de la empresa	3 - Definido	L3	90 %	
	11.2.6	Seguridad de los equipos fuera de las instalaciones	3 - Definido	L3	90 %	
	11.2.7	Reutilización o eliminación segura de equipos	4 - Gestionado	L4	95 %	
	11.2.8	Equipo de usuario desatendido	4 - Gestionado	L4	95 %	
	11.2.9	Política de puestos de trabajo despejado y pantalla limpia	3 - Definido	L3	90 %	

12 Seguridad de operaciones

Objetivo 1:

- El objetivo de los procedimientos y responsabilidades operacionales es el de asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

Objetivo 2:

- El objetivo de la protección contra software malicioso es de asegurar que la información y los recursos de tratamiento de información están protegidos contra el malware.

Objetivo 3:

- Evitar mediante las copias de seguridad la pérdida de datos.

Objetivo 4:

- El objetivo de los registros y supervisión es de registrar los eventos y generar evidencias.

Objetivo 5:

- Asegurar la integridad del software en explotación mediante el control del mismo.

Objetivo 6:

- El objetivo de la gestión de la vulnerabilidad técnica es el de reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

Objetivo 7:

- El intentar que las auditorías impacten lo menos posible en los sistemas que se encuentran en explotación y que están operativos.

CONTROL			Evaluación	CMM	Valor	Total
12 Seguridad de operaciones						**93 %**
12.1 Procedimientos y responsabilidades operacionales						108 %
	12.1.1	Documentación de procedimientos de operación	3 - Definido	L3	90 %	
	12.1.2	Gestión de cambios	3 - Definido	L3	90 %	
	12.1.3	Gestión de capacidades	2 - Repetible	L2	50 %	
	12.1.4	Separación de recursos de desarrollo, prueba y operación	4 - Gestionado	L4	95 %	
12.2 Protección contra el software malicioso (malware)						95 %
	12.2.1	Controles contra el código malicioso	4 - Gestionado	L4	95 %	
12.3 Copias de seguridad						95 %
	12.3.1	Copias de seguridad de la información	4 - Gestionado	L4	95 %	
12.4 Registros y supervisión						93 %
	12.4.1	Registro de eventos	3 - Definido	L3	90 %	
	12.4.2	Protección de la información de registro	4 - Gestionado	L4	95 %	
	12.4.3	Registros de administración y operación	4 - Gestionado	L4	95 %	
	12.4.4	Sincronización de reloj	3 - Definido	L3	90 %	
12.5 Control del software en explotación						95 %
	12.5.1	Instalación del software en explotación	4 - Gestionado	L4	95 %	
12.6 Gestión de vulnerabilidades técnicas.						70 %
	12.6.1	Gestión de las vulnerabilidades técnicas	2 - Repetible	L2	50 %	
	12.6.2	Restricción en la instalación del software	3 - Definido	L3	90 %	
12.7 Consideraciones sobre la auditoría de sistemas de información						95 %
	12.7.1	Controles de auditoría de sistemas de información	4 - Gestionado	L4	95 %	

13 Seguridad de las comunicaciones

Objetivo 1:

- El asegurar la protección de las redes y los recursos de tratamiento de la información.

Objetivo 2:

- El mantener la seguridad de la información que se transfiere o transmite tanto dentro de la empresa como fuera de ella, ya sea a personal propio o externo.

CONTROL			Evaluación	CMM	Valor	Total
13 Seguridad de las comunicaciones						**93 %**
	13.1 Gestión de la seguridad de redes					92 %
	13.1.1	Controles de red	3 - Definido	L3	90 %	
	13.1.2	Seguridad de los servidores de red	4 - Gestionado	L4	95 %	
	13.1.3	Segregación en redes	3 - Definido	L3	90 %	
	13.2 Intercambio de información					94 %
	13.2.1	Políticas y procedimientos de intercambio de información	4 - Gestionado	L4	95 %	
	13.2.2	Acuerdos de intercambio de información	4 - Gestionado	L4	95 %	
	13.2.3	Mensajería electrónica	3 - Definido	L3	90 %	
	13.2.4	Acuerdos de confidencialidad o no revelación	4 - Gestionado	L4	95 %	

14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo 1:

- Mediante los requisitos de seguridad en sistemas de información se pretende garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida, incluidos los servicios proporcionados a través de redes públicas.

Objetivo 2:

- Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.

Objetivo 3:

- Garantizar la protección de los datos que se usan en la fase de pruebas de los activos.

CONTROL			Evaluación	CMM	Valor	Total
14 Adquisición, desarrollo y mantenimiento de los sistemas de información						**91 %**
14.1 Requisitos de seguridad en sistemas de información						90 %
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	3 - Definido	L3	90 %	
	14.1.2	Asegurar los servicios de aplicaciones en redes públicas	3 - Definido	L3	90 %	
	14.1.3	Protección de las transacciones de servicios de aplicaciones	3 - Definido	L3	90 %	
14.2 Seguridad en el desarrollo y en los procesos de soporte						93 %
	14.2.1	Políticas de desarrollo seguro	3 - Definido	L3	90 %	
	14.2.2	Procedimiento de control de cambios en sistemas	3 - Definido	L3	90 %	
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3 - Definido	L3	90 %	
	14.2.4	Restricciones a los cambios en los paquetes de software	4 - Gestionado	L4	95 %	
	14.2.5	Principios de ingeniería de sistemas seguros	3 - Definido	L3	90 %	
	14.2.6	Entornos de desarrollo seguro	4 - Gestionado	L4	95 %	
	14.2.7	Externalización del desarrollo de software	4 - Gestionado	L4	95 %	
	14.2.8	Pruebas funcionales de seguridad de sistemas	4 - Gestionado	L4	95 %	
	14.2.9	Pruebas de aceptación de sistemas	4 - Gestionado	L4	95 %	
14.3 Datos de prueba						90 %
	14.3.1	Protección de los datos de prueba	3 - Definido	L3	90 %	

15 Relación con proveedores

Objetivo 1:

- Garantizar la protección de los activos que se ponen a disposición de los proveedores.

Objetivo 2:

- Garantizar los niveles de servicios acordados con los proveedores según las SLA (Acuerdo de los niveles de servicio).

CONTROL			Evaluación	CMM	Valor	Total
15 Relación con proveedores						**92 %**
15.1 Seguridad en las relaciones con proveedores						93 %
	15.1.1	Política de seguridad de la información en las relaciones con los proveedores	4 - Gestionado	L4	95 %	
	15.1.2	Requisitos de seguridad en contratos con terceros	4 - Gestionado	L4	95 %	
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	3 - Definido	L3	90 %	
15.2 Gestión de la provisión de servicios del proveedor						90 %
	15.2.1	Control y revisión de la provisión de servicios del proveedor	3 - Definido	L3	90 %	
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	3 - Definido	L3	90 %	

16 Gestión de incidentes de seguridad de la información

Objetivo 1:

- Garantizar, mediante la gestión de incidentes de seguridad, que se le da un enfoque coherente y eficaz a la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

CONTROL			Evaluación	CMM	Valor	Total
16 Gestión de incidentes de seguridad de la información						**91 %**
16.1 Gestión de incidentes de seguridad de la información y mejoras						91 %
	16.1.1	responsabilidades y procedimientos	4 - Gestionado	L4	95 %	
	16.1.2	Notificación de los eventos de seguridad de la información	4 - Gestionado	L4	95 %	
	16.1.3	Notificación de puntos débiles de la seguridad	3 - Definido	L3	90 %	
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	3 - Definido	L3	90 %	
	16.1.5	Respuesta a incidentes de seguridad de la información	3 - Definido	L3	90 %	
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	3 - Definido	L3	90 %	
	16.1.7	Recopilación de evidencias	3 - Definido	L3	90 %	

17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Objetivo 1:

- Asegurar que la continuidad de la seguridad de la información forma parte de los sistemas de gestión de continuidad del negocio de la compañía.

Objetivo 2:

- Asegurar mediante las redundancias, la disponibilidad de los recursos de tratamiento de la información.

CONTROL				Evaluación	CMM	Valor	Total
17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio							**70 %**
	17.1 Continuidad de la seguridad de la información						90 %
		17.1.1	Planificación de la continuidad de la seguridad de la información	3 - Definido	L3	90 %	
		17.1.2	Implementar la continuidad de la seguridad de la información	3 - Definido	L3	90 %	
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	3 - Definido	L3	90 %	
	17.2 Redundancias						50 %
		17.2.1	Disponibilidad de los recurso de tratamiento de la información	2 - Repetible	L2	50 %	

18 Cumplimiento

Objetivo 1:

- Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

Objetivo 2:

- Garantizar, mediante las revisiones de la seguridad de la información, que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

18 Cumplimiento							**93 %**
	18.1 Cumplimiento de los legales y contractuales						94 %
		18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	4 - Gestionado	L4	95 %	
		18.1.2	Derechos de propiedad intelectual (DPI)	4 - Gestionado	L4	95 %	
		18.1.3	Protección de los registros de la organización	3 - Definido	L3	90 %	
		18.1.4	Protección y privacidad de la información de carácter personal	4 - Gestionado	L4	95 %	
		18.1.5	Regulación de los controles criptográficos	4 - Gestionado	L4	95 %	
	18.2 Revisión de la seguridad de la información						92 %
		18.2.1	Revisión independiente de la seguridad de la información	3 - Definido	L3	90 %	
		18.2.2	Cumplimiento de las políticas y normas de seguridad	4 - Gestionado	L4	95 %	
		18.2.3	Comprobación del cumplimiento técnico	3 - Definido	L3	90 %	

5.6 TABLA COMPARATIVA

En la siguiente tabla se presentan los resultados de la evaluación inicial junto con los resultados de la evaluación de cumplimiento realizada tras la ejecución de los proyectos.

			SITUACIÓN INICIAL				SITUACIÓN ACTUAL			
CONTROL			Evaluación	CMM	Valor	Total	Evaluación	CMM	Valor	Total
5 Políticas de seguridad de la información						70 %				98 %
5.1 Directrices de gestión de la seguridad de la información						70 %				98 %
	5.1.1	Políticas para la seguridad de la información	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	5.1.2	Revisión de las políticas para la seguridad de la información	2 - Repetible	L2	50 %		5 - Optimizado	L5	100 %	
6 Organización de la seguridad de la información						**25 %**				**83 %**
6.1 Organización interna						40 %				68 %
	6.1.1	Roles y responsabilidades en seguridad de la información	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	6.1.2	Segregación de tareas	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
	6.1.3	Contacto con las autoridades	2 - Repetible	L2	50 %		2 - Repetible	L2	50 %	
	6.1.4	Contacto con grupos de interés especial	1 - Inicial	L1	10 %		2 - Repetible	L2	50 %	
	6.1.5	Seguridad de la información en la gestión de proyectos	0 - No existente	L0	0 %		2 - Repetible	L2	50 %	
6.2 Dispositivos móviles y el teletrabajo						10 %				98 %
	6.2.1	Política de dispositivos móviles	1 - Inicial	L1	10 %		5 - Optimizado	L5	100 %	
	6.2.2	Teletrabajo	1 - Inicial	L1	10 %		4 - Gestionado	L4	95 %	
7 Seguridad relativa a los recursos humanos						**32 %**				**95 %**
7.1 Antes del empleo						45 %				95 %
	7.1.1	Investigación de antecedentes	0 - No existente	L0	0 %		3 - Definido	L3	90 %	
	7.1.2	Términos y condiciones del empleo	3 - Definido	L3	90 %		5 - Optimizado	L5	100 %	
7.2 Durante el empleo						50 %				95 %
	7.2.1	Responsabilidades de gestión	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	1 - Inicial	L1	10 %		4 - Gestionado	L4	95 %	
	7.2.3	Proceso disciplinario	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
7.3 Finalización del empleo o cambio en el puesto de trabajo						0 %				95 %
	7.3.1	Responsabilidades ante la finalización o cambio	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
8 Gestión de activos						**31 %**				**90 %**

8.1 Responsabilidad sobre los activos					60 %					94 %
	8.1.1	Inventario de activos	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	8.1.2	Propietario de los activos	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	8.1.3	Uso aceptable de los activos	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
	8.1.4	Devolución de activos	1 - Inicial	L1	10 %		4 - Gestionado	L4	95 %	
8.2 Clasificación de la información					17 %					80 %
	8.2.1	Clasificación de la información	0 - No existente	L0	0 %		2 - Repetible	L2	50 %	
	8.2.2	Etiquetado de la información	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
	8.2.3	Manipulación de la información	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
8.3 Manipulación de los soportes					17 %					95 %
	8.3.1	Gestión de soportes extraíbles	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
	8.3.2	Eliminación de soportes	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
	8.3.3	Soportes físicos en tránsito	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
9 Control de acceso					**65 %**					**91 %**
9.1 Requisitos de negocio para el control de acceso					95 %					95 %
	9.1.1	Política de control de acceso	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.1.2	Acceso a las redes y los servidores de red	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
9.2 Gestión de acceso de usuario					73 %					87 %
	9.2.1	Registro y baja de usuario	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.2.2	Provisión de acceso de usuario	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.2.3	Gestión de privilegios de acceso	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.2.4	Gestión de la información secreta de autenticación de los usuarios	0 - No existente	L0	0 %		2 - Repetible	L2	50 %	
	9.2.5	Revisión de los derechos de acceso de usuario	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
	9.2.6	Retirada o reasignación de los derechos de acceso	5 - Optimizado	L5	100 %		4 - Gestionado	L4	95 %	
9.3 Responsabilidades del usuario					0 %					90 %
	9.3.1	Uso de la información secreta de autenticación	0 - No existente	L0	0 %		3 - Definido	L3	90 %	
9.4 Control de acceso a sistemas y aplicaciones					94 %					94 %
	9.4.1	Restricción del acceso no autorizado a los sistemas y aplicaciones	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.4.2	Procedimientos seguros de inicio de sesión	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	

	9.4.3	Sistema de gestión de contraseñas	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	9.4.4	Uso de utilidades con privilegios del sistema	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	9.4.5	Control de acceso al código fuente de los programas	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
10 Criptografía						**50 %**				**95 %**
	10.1 Controles criptográficos					50 %				95 %
	10.1.1	Política de uso de los controles criptográficos	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
	10.1.2	Gestión de claves	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
11 Seguridad física y entorno						**81 %**				**83 %**
	11.1 Áreas seguras					85 %				85 %
	11.1.1	Perímetro de seguridad física	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.1.2	Controles físicos de entrada	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	11.1.3	Seguridad de oficinas, despachos y recursos	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.1.4	Protección contra las amenazas externas y ambientales	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.1.5	El trabajo en áreas seguras	2 - Repetible	L2	50 %		2 - Repetible	L2	50 %	
	11.1.6	Áreas de carga y descarga	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	11.2 Seguridad de los equipos					77 %				81 %
	11.2.1	Emplazamiento y protección de equipos	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.2.2	Instalaciones de suministro	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.2.3	Seguridad del cableado	0 - No existente	L0	0 %		2 - Repetible	L2	50 %	
	11.2.4	Mantenimiento de equipos	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.2.5	Retirada de material propiedad de la empresa	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.2.6	Seguridad de los equipos fuera de las instalaciones	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	11.2.7	Reutilización o eliminación segura de equipos	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	11.2.8	Equipo de usuario desatendido	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
	11.2.9	Política de puestos de trabajo despejado y pantalla limpia	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
12 Seguridad de operaciones						**55 %**				**93 %**
	12.1 Procedimientos y responsabilidades operacionales					47 %				108 %
	12.1.1	Documentación de procedimientos de operación	0 - No existente	L0	0 %		3 - Definido	L3	90 %	
	12.1.2	Gestión de cambios	3 - Definido	L3	90 %		3 - Definido	L3	90 %	

	12.1.3	Gestión de capacidades	2 - Repetible	L2	50 %		2 - Repetible	L2	50 %	
	12.1.4	Separación de recursos de desarrollo, prueba y operación	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
12.2 Protección contra el software malicioso (malware)						50 %				95 %
	12.2.1	Controles contra el código malicioso	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
12.3 Copias de seguridad						95 %				95 %
	12.3.1	Copias de seguridad de la información	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
12.4 Registros y supervisión						0 %				93 %
	12.4.1	Registro de eventos	0 - No existente	L0	0 %		3 - Definido	L3	90 %	
	12.4.2	Protección de la información de registro	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
	12.4.3	Registros de administración y operación	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
	12.4.4	Sincronización de reloj	0 - No existente	L0	0 %		3 - Definido	L3	90 %	
12.5 Control del software en explotación						90 %				95 %
	12.5.1	Instalación del software en explotación	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
12.6 Gestión de vulnerabilidades técnicas.						50 %				70 %
	12.6.1	Gestión de las vulnerabilidades técnicas	1 - Inicial	L1	10 %		2 - Repetible	L2	50 %	
	12.6.2	Restricción en la instalación del software	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
12.7 Consideraciones sobre la auditoría de sistemas de información						50 %				95 %
	12.7.1	Controles de auditoría de sistemas de información	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
13 Seguridad de las comunicaciones						**67 %**				**93 %**
13.1 Gestión de la seguridad de redes						77 %				92 %
	13.1.1	Controles de red	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
	13.1.2	Seguridad de los servidores de red	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
	13.1.3	Segregación en redes	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
13.2 Intercambio de información						58 %				94 %
	13.2.1	Políticas y procedimientos de intercambio de información	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %	
	13.2.2	Acuerdos de intercambio de información	0 - No existente	L0	0 %		4 - Gestionado	L4	95 %	
	13.2.3	Mensajería electrónica	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	13.2.4	Acuerdos de confidencialidad o no revelación	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	

14 Adquisición, desarrollo y mantenimiento de los sistemas de información					**70 %**				**91 %**
14.1 Requisitos de seguridad en sistemas de información					37 %				90 %
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
14.1.3	Protección de las transacciones de servicios de aplicaciones	1 - Inicial	L1	10 %		3 - Definido	L3	90 %	
14.2 Seguridad en el desarrollo y en los procesos de soporte					84 %				93 %
14.2.1	Políticas de desarrollo seguro	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
14.2.2	Procedimiento de control de cambios en sistemas	4 - Gestionado	L4	95 %		3 - Definido	L3	90 %	
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
14.2.4	Restricciones a los cambios en los paquetes de software	1 - Inicial	L1	10 %		4 - Gestionado	L4	95 %	
14.2.5	Principios de ingeniería de sistemas seguros	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
14.2.6	Entornos de desarrollo seguro	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
14.2.7	Externalización del desarrollo de software	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
14.2.8	Pruebas funcionales de seguridad de sistemas	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
14.2.9	Pruebas de aceptación de sistemas	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %	
14.3 Datos de prueba					90 %				90 %
14.3.1	Protección de los datos de prueba	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
15 Relación con proveedores					**90 %**				**92 %**
15.1 Seguridad en las relaciones con proveedores					90 %				93 %
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
15.1.2	Requisitos de seguridad en contratos con terceros	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
15.2 Gestión de la provisión de servicios del proveedor					90 %				90 %

		15.2.1	Control y revisión de la provisión de servicios del proveedor	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
		15.2.2	Gestión de cambios en la provisión del servicio del proveedor	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
16 Gestión de incidentes de seguridad de la información							**67 %**				**91 %**
	16.1 Gestión de incidentes de seguridad de la información y mejoras						67 %				91 %
		16.1.1	responsabilidades y procedimientos	1 - Inicial	L1	10 %		4 - Gestionado	L4	95 %	
		16.1.2	Notificación de los eventos de seguridad de la información	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %	
		16.1.3	Notificación de puntos débiles de la seguridad	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
		16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
		16.1.5	Respuesta a incidentes de seguridad de la información	2 - Repetible	L2	50 %		3 - Definido	L3	90 %	
		16.1.6	Aprendizaje de los incidentes de seguridad de la información	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
		16.1.7	Recopilación de evidencias	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio							**45 %**				**70 %**
	17.1 Continuidad de la seguridad de la información						90 %				90 %
		17.1.1	Planificación de la continuidad de la seguridad de la información	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
		17.1.2	Implementar la continuidad de la seguridad de la información	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	3 - Definido	L3	90 %		3 - Definido	L3	90 %	
	17.2 Redundancias						0 %				50 %
		17.2.1	Disponibilidad de los recurso de tratamiento de la información	0 - No existente	L0	0 %		2 - Repetible	L2	50 %	
18 Cumplimiento							**88 %**				**93 %**
	18.1 Cumplimiento de los legales y contractuales						85 %				94 %

		18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %		
		18.1.2	Derechos de propiedad intelectual (DPI)	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %		
		18.1.3	Protección de los registros de la organización	3 - Definido	L3	90 %		3 - Definido	L3	90 %		
		18.1.4	Protección y privacidad de la información de carácter personal	4 - Gestionado	L4	95 %		4 - Gestionado	L4	95 %		
		18.1.5	Regulación de los controles criptográficos	2 - Repetible	L2	50 %		4 - Gestionado	L4	95 %		
	18.2 Revisión de la seguridad de la información						90 %					92 %
		18.2.1	Revisión independiente de la seguridad de la información	3 - Definido	L3	90 %		3 - Definido	L3	90 %		
		18.2.2	Cumplimiento de las políticas y normas de seguridad	3 - Definido	L3	90 %		4 - Gestionado	L4	95 %		
		18.2.3	Comprobación del cumplimiento técnico	3 - Definido	L3	90 %		3 - Definido	L3	90 %		

Tabla 22 Tabla comparativa de la madurez inicial y final

5.7 REPRESENTACIÓN GRÁFICA DE LOS RESULTADOS

En el siguiente gráfico se representa la madurez de los controles ISO una vez realizada la auditoría de cumplimiento. Con este tipo de representaciones gráficas se facilita la percepción de la situación de la compañía con relación al cumplimiento de la ISO 27002.

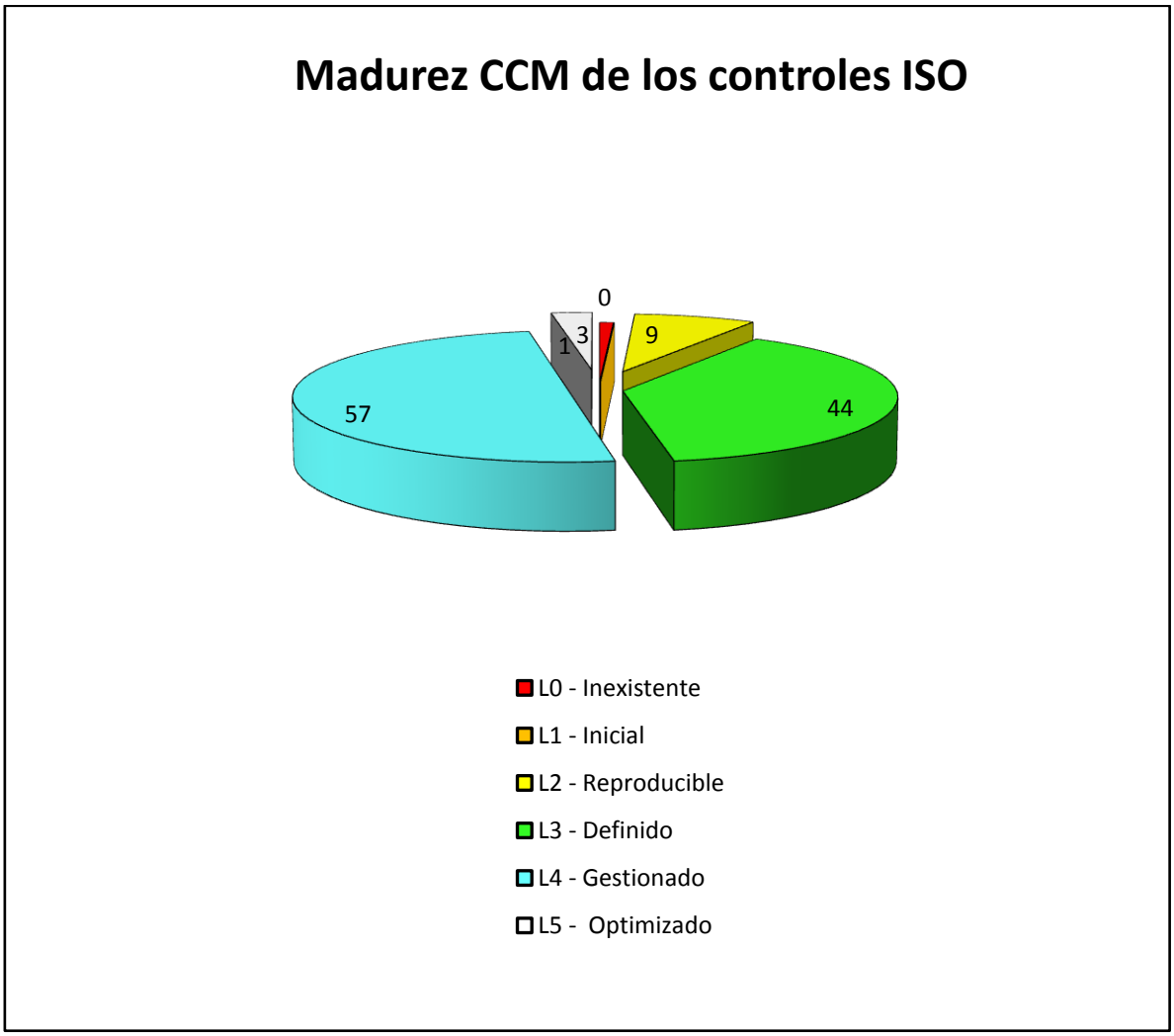


Ilustración 13 Representación gráfica de la madurez de los controles ISO.

En el siguiente diagrama de radar se hace una representación el grado de cumplimiento de cada uno de los dominios de la ISO 27002.

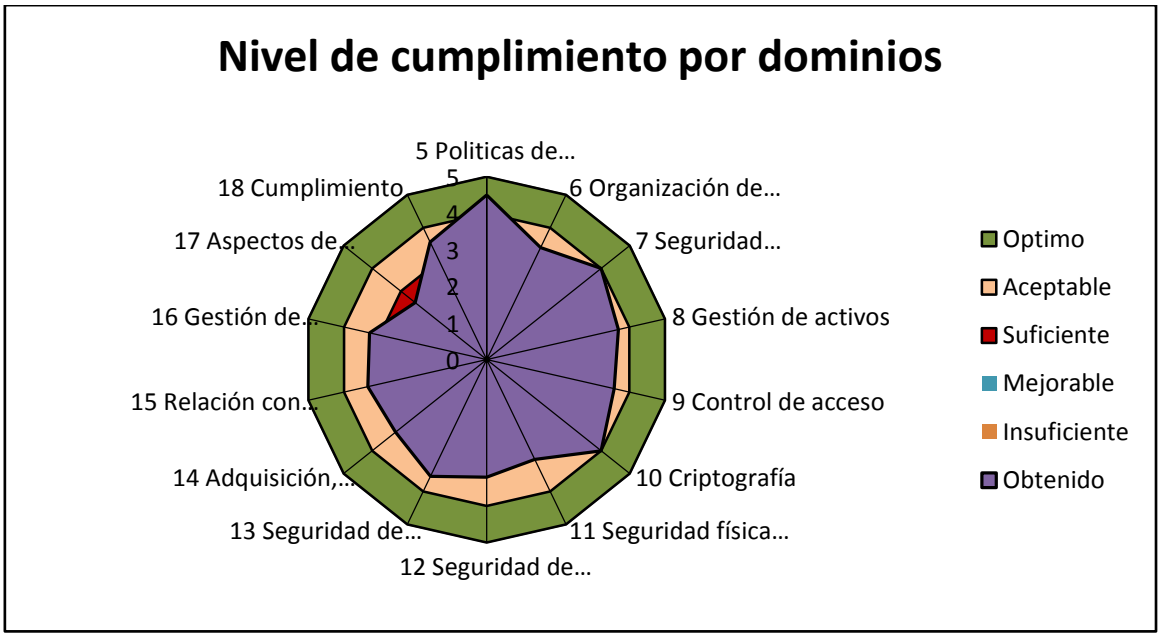


Ilustración 14 Representación gráfica de la madurez de los dominios de la ISO 27002.

5.8 RESULTADOS

Tal como se puede apreciar en la tabla 19 y en la ilustración 11 todos los dominios se encuentran en unos valores aceptables, encontrándose como valor más bajo el dominio 17 "Aspectos de seguridad de la información para la gestión de la continuidad del negocio" que está a un 70% de cumplimiento, debido sobre todo a que no existe un sistema redundante.

5.8.3 INFORME DE AUDITORÍA

I. Identificación de la sociedad auditada

Razón Social: Gespa S.L.
NIF: B-285382893L
Dirección: Calle Rio Loira, 28 - Madrid

II. Identificación del alcance de la auditoría

Alcance:

Todos los procesos o sistemas que participan en el manejo, almacenamiento o transmisión de la información, de acuerdo con la declaración de aplicabilidad.

Datos identificativos del equipo auditor:

Auditor Jefe (aj): Juan Fernández Redondo
Auditor 1 (a1): Laura González Martínez

Datos identificativos de la auditoría:

Norma: ISO 27002:2013
Tipo de auditoría: Auditoría de cumplimiento
Fecha: 5 de mayo de 2019
Centro: Instalaciones de Madrid
Áreas auditadas: Todas

III. Objetivos y criterios de la auditoría

Objetivos de la auditoría:

El objetivo de la auditoría es el de evaluar el nivel de madurez de la seguridad de la información de la empresa Gespa de acuerdo con la ISO 27002:2013

Criterios de la auditoría:

Documentación de aplicación:

- Norma ISO 27002:2013
- Política de seguridad
- Procedimientos de la compañía
- Instrucciones técnicas

IV. Reunión de apertura

Participantes:

Director General: Ángel Rodríguez Castro
Jefe de seguridad: José González Herrera
Director de Operaciones: César Gómez López
Director de I+D y Producción: Julián Sevilla Lorenzo
Auditor Jefe (aj): Juan Fernández Redondo
Auditor 1 (a1): Laura González Martínez

Temas tratados:

Por parte del Auditor Jefe se hace una exposición de los resultados de la situación inicial de la empresa con respecto al grado de cumplimiento de la norma ISO 27001 y la ISO 27002.

Se comunica el alcance de la auditoría, así como el plan previsto.

Los directores de operaciones y de I+D y Producción comunican las personas de sus departamentos que intervendrán en la auditoría.

El director general pide la máxima colaboración, ya que tiene mucho interés en que la empresa cumpla con los requisitos de seguridad establecidos en la política de seguridad.

V. Resultado de la auditorías

Nº de NO conformidades Mayores: 0
Nº de NO conformidades menores: 8
Nº de Oportunidades de mejora:

VI. Hallazgos de la auditoria

En este apartado se van a exponer los resultados de la auditoría. El resultado obtenido puede ser una no conformidad mayor si se detecta un incumplimiento grave, no conformidad menor si el incumplimiento es leve, observaciones y fortalezas.

En el informe se enumeran las no conformidades menores (m) que se han detectado en el transcurso de la auditoría, indicándose la descripción de la misma.

Identificador:	NC 01	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	6. Organización de la seguridad de la información		
Controles afectados:	6.1.3 Contacto con las autoridades 6.1.4 Contacto con grupos de interés especial		
Descripción	No está definido y documentado el contacto con las autoridades ni con grupos de interés especial. El contacto no se lleva a cabo de forma procedimentada.		
Acción:	Generar un documento donde se recojan las principales autoridades y grupos de especial interés con los que hay que mantener un contacto de forma rutinaria. Recoger en el documento los objetivos e interés del contacto.		
Responsable:	Jefe de seguridad		

Identificador:	NC 02	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	6. Organización de la seguridad de la información		
Controles afectados:	6.1.5 Seguridad de la información en la gestión de proyectos		
Descripción	En el procedimiento de gestión de proyectos no se contempla la manera de garantizar la seguridad de la información generada y/o utilizada en los proyectos.		
Acción:	Modificar el procedimiento de gestión de proyectos para incluir un apartado sobre la seguridad de la información.		
Responsable:	Director de operaciones		

Identificador:	NC 03	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	8 Gestión de activos		
Controles afectados:	8.2.1 Clasificación de la información		
Descripción	Existen activos que no han sido clasificados en función de su importancia con relación a la seguridad, y aunque están protegidos, no disponen del distintivo del nivel de clasificación.		
Acción:	Revisar los activos para comprobar que disponen de la clasificación adecuada.		
Responsable:	Propietario del activo		

Identificador:	NC 04	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	9 Control de acceso		
Controles afectados:	9.2.4 Gestión de la información secreta de autenticación de los usuarios		
Descripción	No se hace un análisis de la fortaleza de la clave de cada usuario, ni se comprueba que cuando se cambie la clave, no se repite la misma que hay actualmente.		
Acción:	Establecer los mecanismos técnicos y procedimentales para que las claves de usuario tenga una fortaleza mínima, y que cuando se cambien, que la nueva password sea distinta a la actual.		
Responsable:	Administrador del sistema		

Identificador:	NC 05	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	11 Seguridad física y entorno		
Controles afectados:	11.2.3 Seguridad del cableado		
Descripción	Existe cableado de comunicaciones en la misma bandeja que cableado de energía. El cableado no se encuentra etiquetado.		
Acción:	Separar los cableados en función de su utilización y etiquetarlo, tanto en los extremos como cada cierta distancia.		
Responsable:	Director de I+D y producción		

Identificador:	NC 06	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	12 Seguridad de operaciones		
Controles afectados:	12.1.3 Gestión de capacidades		
Descripción	No hay evidencia de que se haya hecho un análisis de las capacidades mínimas necesarias para el mantenimiento de la actividad.		
Acción:	Hacer un estudio de las capacidades necesaria en cada departamento y establecer un procedimiento de borrado de datos obsoletos y de recuperación de recursos infrautilizados.		
Responsable:	Director de I+D y producción		

Identificador:	NC 07	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	12 Seguridad de operaciones		
Controles afectados:	12.6.1 Gestión de las vulnerabilidades técnicas		
Descripción	No se han identificado los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas.		
Acción:	Identificar los recursos de información que se utilizarán para identificar las vulnerabilidades y actualizarlos según se modifica el inventario.		
Responsable:	Director de I+D y producción		

Identificador:	NC 08	Fecha:	05/05/2019
Hallazgo:	No conformidad menor		
Dominio:	17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio		
Controles afectados:	17.2.1 Disponibilidad de los recurso de tratamiento de la información		
Descripción	No se dispone de recursos de tratamiento de la información redundantes.		
Acción:	Identificar claramente cuáles son los recursos que necesitan ser redundados para garantizar la disponibilidad.		
Responsable:	Director de I+D y producción		

VII. COMENTARIOS Y OPORTUNIDADES DE MEJORA

VIII. ASPECTOS POSITIVOS Y PUNTOS FUERTES

Como punto fuerte hay que destacar la gran concienciación que existe en todos los empleados con respecto a la seguridad de la información. Existe una voluntad de conseguir los máximos niveles de seguridad en la compañía.

IX. Reunión de cierre

Participantes:

Director General: Ángel Rodríguez Castro
Jefe de seguridad: José González Herrera
Director de Operaciones: César Gómez López
Director de I+D y Producción: Julián Sevilla Lorenzo
Auditor Jefe (aj): Juan Fernández Redondo
Auditor 1 (a1): Laura González Martínez

Comentarios:

El auditor jefe hace una exposición de cómo ha ido la auditoría y de los resultados de la misma.

6 ANEXOS

6.1 ANEXO I "POLÍTICA DE SEGURIDAD"

6.2 ANEXO II "AUDITORÍA INTERNA"

6.3 ANEXO III "GESTIÓN DE INDICADORES"

6.4 ANEXO IV "PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN".

6.5 ANEXO V "ROLES Y RESPONSABILIDADES".

6.6 ANEXO VI "METODOLOGÍA DE ANÁLISIS DE RIESGOS".

6.7 ANEXO VII "DECLARACIÓN DE APLICABILIDAD".

7 BIBLIOGRAFÍA Y ENLACES UTILIZADOS

- Norma ISO/IEC 27000:2013
- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27002
- Norma ISO 17799:2005
- MAGERIT – versión 3.0: Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones
  - Libro I – Método.
  - Libro II - Catálogo de Elementos.
  - Libro III - Guía de Técnicas.
  - Material docente de la asignatura "Sistema de Gestión de la Seguridad de la Información". *Autores: Daniel Cruz Allende Silvia Garre Gui*
- Implantación de SGSI en la empresa. *Autor: Equipo de Inteco*
- Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica. *Autores: Gustavo Pallas y María Eugenia Corti*.
- Gestión de riesgos: una guía de aproximación para el empresario. *Autor: Equipo de Inteco*
- La norma ISO 27001. Aspectos clave de su diseño e implantación. Autor: Isotools.(**https://www.isotools.org/pdfs-pro/iso27001-sistema-gestion-seguridad-informacion.pdf**).
- **https://es.wikipedia.org/wiki/ISO/IEC_27000-series**
- **http://kemal.bhsearch.com/wp-content/uploads/2012/11/ISMS_Implementation_-ISO-27003.pdf**
- **https://es.wikipedia.org/wiki/ISO/IEC_27003**
- **https://www.pgm-ssi.com/2013/12/iso27001-origen/**
- **https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf**

–