Máster MISTIC - Plan de Implementación de la ISO/IEC27001:2013

Empresa Web Consulting S.A

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Alumno: Iñaki Gorriti Aranguren

Consultor: Antonio José Segovia Henares

Segundo semestre del curso 2014/15

Resumen

El proyecto indicado en este documento se trata del Trabajo Final de Máster del Máster interuniversitario "Seguridad de las tecnologías de la información y de las comunicaciones". Este máster esta impartido por la Universitat Oberta de Catalunya (UOC), Universitat Autónoma de Barcelona (UAB), la Universitat Rovira i Virgili (URV) y la participación de la Universitat de les Illes Balears (UIB). El objetivo del mismo es la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa ficticia llamada Web Consulting S.A.

Un SGSI es un conjunto de políticas de administración de la información enmarcadas dentro de la norma ISO/IEC 27001:2013. Además disponemos de una serie de recomendaciones asociadas en la norma ISO/IEC 27002:2013 que nos permitirá poder acometer la implantación del SGSI de una forma más eficaz. La aplicación de este sistema trata de preservar la confidencialidad, integridad, y disponibilidad de la información así como los sistemas que traten la información dentro de la organización.

Summary

The project in this document is the final work of the interuniversitary master in "Information Technology security and communications". This Master is taught by Universitat Oberta de Catalunya (UOC), Universitat Autónoma de Barcelona (UAB), la Universitat Rovira i Virgili (URV) and the participation of Universitat de les Illes Balears (UIB). The Object of the project is the implementation of a Management System for Information Security (ISMS) into Web Consulting S.A fictional enterprise.

An ISMS is a set of information management policies within ISO/IEC 27001:2013. We also have a number of recommendations related to the ISO/IEC 27002:2013 that will allow us to undertake the implementation of ISMS more effectively. The application of this system is to preserve the confidentiality, integrity and availability of information and systems that use this information within the organization.

Tabla de contenido

Tabla de ilustraciones

Situación Actual: contextualización, objetivos y análisis diferencial

1. Introducción ISO 27001:2013

Para la realización del Plan Director de seguridad de la empresa nos basaremos en la normativa ISO 27001 publicada en 2005 posteriormente corregido y ampliada en 2013. El origen de la misma está basada en la BS 7799-2:2002 y se trata de la normativa para certificar los sistemas de gestión de la seguridad de la información.

Para poder lograr y alcanzar la finalidad del proyecto realizaremos unas primeras entregas delimitando el alcance del proyecto y escogiendo la empresa que queremos auditar en base a esta normativa. Para ello procederemos en un punto posterior tras un análisis de la empresa a enumerar los distintos objetivos y controles que queremos que se vean reflejados en la empresa auditada.

Además de la ISO 27001 disponemos de una guía de buenas prácticas que puede ayudarnos a obtener dicho reconocimiento denominándose esta guía como ISO 27002. Dentro de esta última podremos encontrar los distintos puntos de control necesarias para la 27001, claro ejemplo de ello el que sea un anexo de la normativa.

2. Definición de objetivos del Plan Director de Seguridad

Hemos seleccionado a la empresa **Web Consulting S.A** para poder realizar el Plan Director de Seguridad de la misma. Actualmente no tienen una regulación ni control claro y están en proceso de normalización y posible expansión. Por esto mismo requieren ganar la confianza de los nuevos clientes mediante el logro de la correcta implantación de la normativa en sus sistemas de gestión de la seguridad.

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información dirigido a reducir los riesgos a los que la empresa está expuesta hasta llegar a unos niveles aceptables de riesgos a partir de un análisis inicial de la situación.

En la norma 27001:2013 en el punto 6.2 podemos observar los objetivos del plan director de seguridad de la información. En el caso de **Web Consulting S.A** la empresa quiere poder realizar los siguientes objetivos:

- Asegurar la confidencialidad, seguridad y correcto uso de los sistemas de la empresa además de la información de la misma.
- Demostrar a actuales y futuros clientes que se protege de forma adecuada la información y tecnologías empleadas en la empresa aumentando así el valor comercial de la propia empresa y los servicios ofertados por la misma.
- Garantizar el compromiso de la dirección de la empresa con la seguridad de la información. Establecer los canales adecuados para poder garantizar la seguridad de la información en todos los procesos productivos de la empresa.

- Identificar los riesgos que puedan afectar al negocio de la empresa minimizando las amenazas que puedan impactar sobre las mismas y provocando a su vez una disminución de los riesgos asociados a todos los activos.
- Mejorar y crear nuevos controles para garantizar el cumplimiento de los niveles de riesgo que acepta la dirección de la empresa.
- Establecer la forma de poder controlar y cuantificar el estado actual y futuro de los sistemas de la seguridad de la información mediante el uso de autorías internas. Provocando de esta forma una mejora continua y detección de nuevas amenazas contra los activos.
- Normalización de la gestión documental electrónica mediante la correcta categorización de la misma clasificándola, gestionando el impacto sobre la empresa y el desarrollo de sus correctas funciones comerciales.
- Asegurar cumplimiento normativo en el tratamiento de la información propia de la empresa y de clientes que están siendo gestionados a través de ella.
- Aumentar la concienciación sobre la seguridad de la información para asegurar la continuidad del negocio. Formación a los empleados de la empresa especializada en la seguridad de la información mejorando la motivación y satisfacción del personal al involucrarlos en procesos empresariales.
- Mejorar en las inversiones realizadas por la empresa en la gestión de los sistemas de seguridad de la información. Una vez descubiertos los puntos débiles se reforzarán mediante la implantación de nuevos sistemas, evolución de los mismos o mejora de procedimientos en la seguridad de la información.
- Mejorar las oportunidades en el mercado tras atraer la atención de posibles clientes o inversores al establecer una buena base basada en la seguridad de los sistemas de la información. Una mejor imagen tras una mayor implicación por parte de la dirección y todos los departamentos integrantes de la empresa.
- Establecer mejoras de categorización TIER del CPD de la empresa para poder atraer una mayor cota de mercado hacia los servicios ofrecidos por la empresa.

3. Alcance del plan director de seguridad

El alcance del proyecto abarca a la totalidad de las instalaciones de Web Consulting S.A y todos aquellos procesos empresariales que sean necesarios para la consecución de sus objetivos empresariales. Teniendo en cuenta este punto podemos decir que afectará a todo el sistema además de la información que pueda procesarse en la empresa, siendo esta de la propia empresa o de terceros que estén utilizando sus servicios. Es decir, se incluye la gestión de la seguridad de la información tanto de los soportes físicos como lógicos de la información. Incluyendo además la seguridad de las propias instalaciones en lo referente al acceso o uso de la información de la empresa, accediendo a la misma remotamente o localmente.

4. Introducción y objetivos de la empresa

Web Consulting S.A es una empresa fundada en 2003 por un grupo de emprendedores que con el paso del tiempo han podido consolidar su empresa como una de las prestadoras Web y de consultoría mejor posicionadas de Cantabria. Gracias a las ayudas proporcionadas por la comunidad autónoma y distintos medios para emprendedores, obtuvieron un buen abanico de clientes iniciales que posteriormente le abrieron las puertas a distintas empresas del sector como Real Club Marítimo o el Parque tecnológico y científico de Cantabria. En este último se cuenta con la publicación Web de múltiples empresas que han depositado la confianza en Web Consulting S.A usando sus servicios de hosting, seo y community manager.

Inicialmente iba a ser una empresa de consultoría de SEO la cual se asentaba en un espacio de coworking. En estos espacios las empresas comparten un mismo espacio de oficina y reuniones e infraestructuras tecnológicas. Gracias a esto pudo rentabilizar los gastos y hacer networking profesional con otras empresas del sector que compartían espacio. Tras un análisis posterior vio la posibilidad de absorber varias de estas empresas en estado de spin off para poder ofrecer nuevos servicios de IT. Tras la absorción y reorganización interna, la empresa aumentó, con lo que en 2007 tuvieron que buscar una nueva ubicación y finalmente alquilaron una zona de oficinas del Parque tecnológico y científico de Cantabria. Tras más de siete años dando servicios a clientes de Cantabria han podido evolucionar de forma conservadora afianzándose económicamente. Viendo la evolución y posibilidades de las redes han descubierto la necesidad de aumentar su rango de captación de clientes con lo que han decidido iniciar un proceso de partnership con otras empresas (nacionales y extranjeras) e incluso expansión a nivel nacional.

Para poder aumentar la confianza de sus clientes tecnológicos y la posible expansión que hemos citado, la empresa ha pensado en obtener la ISO 27001:2013. Es por esto que realizará distintas acciones para poder obtenerla además de mejorar su calidad y seguridad en la empresa.

5. Actividad económica

Actualmente Web Consulting S.A realiza multitud de labores relacionadas con los entornos Web que podríamos desglosar de la siguiente forma.

- **Hosting**: alberga en los servidores de sus oficinas los entornos web públicos de múltiples clientes gestionadas según las distintas modalidades que ofrece la empresa. Estas modalidades pueden ser un simple hospedaje en un entorno compartido hasta entornos propios gestionados por técnicos especialistas.
- **Subcontratación / Consultoría Web**: Además de hospedar las páginas Web Consulting S.A realiza consultoría de entornos Web empresariales que estén en los propios clientes. Se les dan instrucciones y configuraciones para sus futuras implantaciones además de poder revisar o gestionar sus entornos mediante conexiones remotas a los clientes.
- **Diseño e implantación de entornos Web**: Dentro de los distintos servicios web ofrecidos podemos ver la posibilidad de rediseñar tanto Webs públicas como intranets empresariales. Este servicio denominado UX (User Experience) realiza un estudio de las interacciones persona computador para poder maximizar las funcionalidades de dichos entornos.
- **Community Manager**: Con la llegada de las redes sociales empresariales se requiere de un nuevo enfoque de marketing en el que se requiere que la necesidad de venta de la empresa converja con las necesidades de los clientes. Para ello se utiliza el servicio de community management en el que expertos en marketing y campañas online ayudan a las empresas a mejorar sus cotas de mercado online.
- **SEO**: Este servicio está incluido en consultoría e implantaciones en la propia oficina de Web Consulting S.A. En el caso de realizar labores en otras oficinas, se puede contratar este servicio de optimización de las páginas Web de las empresas para conseguir mejorar su posicionamiento en buscadores Web.

6. Infraestructura de red

La compañía tiene la siguiente arquitectura de red para poder proveer los servicios que tiene a disposición del público además de los servicios internos necesarios para el correcto funcionamiento de la empresa.

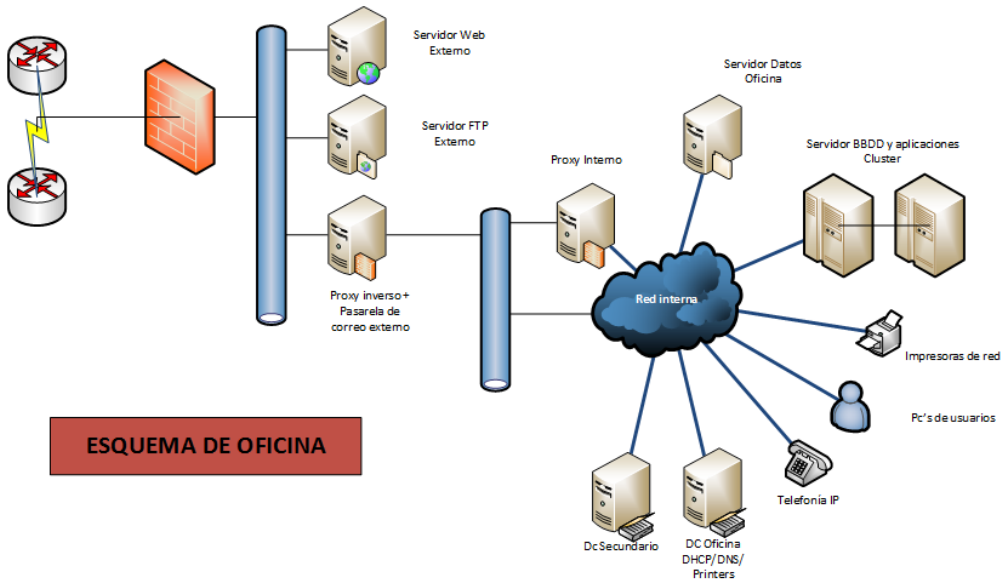

Ilustración 1 Infraestructura de red

Explicaremos en el entorno de izquierda a derecha.

Se conectan a Internet a través de un proveedor de servicios de Internet que además les ha ofertado los servicios de telefonía VoIP del que disponen en la empresa. Para ello tienen configurados dos router en modo activo-pasivo a modo de contingencia. En caso de caída de uno de los nodos podrán conectarse a través del otro nodo.

Antes de llegar a la red DMZ (zona desmilitarizada) podemos encontrarnos con un Firewall que está gestionado por los técnicos de la propia empresa.

Una vez llegamos a la DMZ vemos que se dispone de varios servicios:

- **Servidor Web Externo:** Tienen un servidor Web en el que publican las distintas páginas web de clientes.
- **Servidor FTP externo:** para el envío de documentación pesada a clientes se dispone de un servidor Web sencillo en el que publican documentación para que posteriormente sea eliminada. Tan solo es un intercambiador.
- **Proxy inverso + pasarela de correo:** un servidor que tiene doble funcionalidad. Por un lado tenemos la opción de proxy inverso que permite a algunos usuarios catalogados como VIP el acceso a la Intranet de forma controlada a través de una VPN. Por otro lado tenemos la pasarela de correo externa que utiliza la empresa para sus comunicaciones internas y externas. Se trata de un servicio importante ya que actualmente se trata de una vía de trabajo importante para ellos ya sea en la contratación o en la resolución de consultas técnicas.

En la zona interna podemos observar que se dispone de bastante material para poder proveer servicios internos y acceder desde la DMZ para algunas BBDD o acceso a máquinas para usuarios VIP.

- **Proxy interno:** el proxy interno ayuda en múltiples aspecto como pueda ser una navegación web controlada, mejora del rendimiento de los router al no hacer tantas peticiones externas, posibilidad de establecer vínculos de confianza con otras empresas, antivirus de navegación e incluso auditoría de acceso Web.
- **Servidor datos de oficina:** en este servidor se almacena de forma jerarquizada la información de los usuarios, recursos departamentales, información de clientes y diverso material sensible de la empresa.
- **Dc (dns/dhcp/impresoras):** Se trata del controlador de dominio principal que dispone de servicios de dns (domain name server), dhcp (Dynamic Host Configuration Protocol), servicio de impresión y la gestión de permisos en directorio activo.
- **Dc secundario:** se trata de un servidor secundario que en caso de fallo del principal podríamos utilizarlo para la validación de los usuarios y los demás servicios.
- **Servidor BBDD y aplicaciones (clúster):** para el acceso a las bases de datos de los distintos CMS (content management system) o aplicaciones internas que tienen en la empresa han optado por un servicio clusterizado de base de datos. De esta forma no solo consiguen mejorar el rendimiento del servicio sino que además obtienen una alta disponibilidad del mismo.
- **Ordenador de usuarios:** Los usuarios disponen de ordenador personal para poder realizar sus trabajos habituales. Algunos de ellos, la rama comercial y gerencia, disponen de ordenadores portátiles pero el resto tienen puestos fijos.
- **Impresoras:** las impresoras disponen de acceso de red con lo que directamente han sido publicadas en los controladores de dominio para poder proveer de servicio de impresión a todo aquel que tenga permisos para ello.
- **Teléfonos VoIP:** con el tiempo vieron la necesidad de mejorar el sistema de telefonía y el propio proveedor de servicios les ofreció un servicio completo de telefonía ip. Los teléfonos son cedidos por el propio ISP y la administración y reparación también.

7. Distribución de la empresa

La empresa dispone de una sede única en el Parque tecnológico y científico de Cantabria con un tamaño aproximado de 400m2 útiles de forma diáfana, excepto la sala de ordenadores que se encuentra distribuido de la siguiente forma:

- **Sala de reuniones**: se dispone de un pequeño despacho de reuniones para los clientes externos o reuniones de coordinación internas. Dispone de cañón para presentación y polycom (teléfono para reuniones) para poder hacer conferencias con el exterior.
- **Despacho de dirección**: se trata de un despacho compartido entre el director de la empresa y el subdirector de la misma.
- **Entorno de CPD**: despacho donde tienen configurado todo su sistema informático. Dos armarios, uno de comunicaciones y otro donde se encuentran los distintos servidores.
- **Entorno de oficina**: el resto del área está a disposición tanto de técnicos como comerciales. Se trata de mesas alargadas con paneles para separación. Máquina de café en la propia sala.
- **Espacio de aseos**: espacio para un baño separado para hombres y mujeres.
- **Cuadro eléctrico CPD**
- **Cuadro eléctrico general**
- **3 extintores:** extintores de diferentes tipos dependiendo del tipo de fuego que puede llegar a producirse.
- **Cámaras de seguridad:** A pesar de ser una empresa modesta se dispone de cámaras de seguridad en la entrada, cpd y zona general de oficina.

8. Organigrama

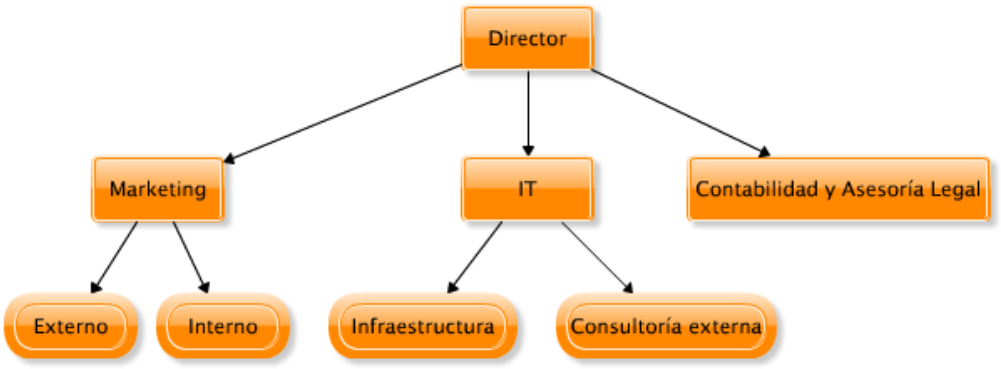

Ilustración 2 Organigrama

Al ser una empresa pequeña dispone de un organigrama sencillo que podemos ilustrarlo como se muestra en la figura anterior.

El director es el coordinador de todas las áreas de la empresa las cuales cuentan con un coordinador y personal específico de dicho departamento.

En Marketing se ven dos áreas que serían ***externo*** donde se englobarían los clientes de la empresa que requieren los servicios de networking, seo o reputación online. En la parte de ***interno*** podemos incluir al personal que se encarga del marketing de la propia empresa.

Dentro del departamento de IT podemos ver el grupo de ***infraestructura*** que se encarga de gestionar el entorno de CPD propio y de los clientes, es decir, es el equipo técnico de la empresa. Además podemos ver el grupo ***consultoría externa*** que son técnicos que se desplazan a otras empresas para asesoría o realización de proyectos puntuales en sus instalaciones.

El departamento de contabilidad y asesoría legal realmente lo compone una sola persona que es el subdirector que en caso de no estar el director se encarga de sus funciones. En momento puntuales de más trabajo pueden llegar a subcontratar la parte de contabilidad debido al impacto que tiene en la coordinación de proyectos.

9. Análisis diferencial del estado actual

Este análisis se realiza con respecto a la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, lo cual nos permitirá conocer de forma global el estado de la empresa con respecto a los sistemas de gestión de la seguridad actuales.

Para poder revisar los distintos controles que están englobados dentro de la ISO/IEC 27002:2013 podemos revisar el siguiente:

http://iso27000.es/download/ControlesISO27002-2013.pdf

Para poder cuantificar el estado de los diferentes controles realizaremos una estimación del estado de los mismos tal como se marca en el enunciado del TFM. Para ello emplearemos el Modelo de Madurez de la Capacidad o CMM.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCION
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver
10%	L1	Inicial	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 cada 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	Gestionable 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 1 Modelo de Madurez de la capacidad

Una vez definidos el distinto estado de madurez procedemos al análisis de los controles de la ISO/IEC 27002:2013.

NOMBRE DE LOS CONTROLES	CUMPLIDOS
5. POLITICAS DE SEGURIDAD.	
5.1 Directrices de la Dirección en seguridad de la información.	
5.1.1 Conjunto de políticas para la seguridad de la información.	L2
5.1.2 Revisión de las políticas para la seguridad de la información.	L1
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	
6.1 Organización interna.	
6.1.1 Asignación de responsabilidades para la segur. de la información.	L2
6.1.2 Segregación de tareas.	L1
6.1.3 Contacto con las autoridades.	L2
6.1.4 Contacto con grupos de interés especial.	L3
6.1.5 Seguridad de la información en la gestión de proyectos.	L1
6.2 Dispositivos para movilidad y teletrabajo.	
6.2.1 Política de uso de dispositivos para movilidad.	L1
6.2.2 Teletrabajo.	L2
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	L5
7.1.2 Términos y condiciones de contratación.	L5
7.2 Durante la contratación.	
7.2.1 Responsabilidades de gestión.	L5
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	L2
7.2.3 Proceso disciplinario.	L2
7.3 Cese o cambio de puesto de trabajo.	
7.3.1 Cese o cambio de puesto de trabajo.	L5
8. GESTION DE ACTIVOS.	
8.1 Responsabilidad sobre los activos.	
8.1.1 Inventario de activos.	L4
8.1.2 Propiedad de los activos.	L5
8.1.3 Uso aceptable de los activos.	L5
8.1.4 Devolución de activos.	L2
8.2 Clasificación de la información.	
8.2.1 Directrices de clasificación.	L2
8.2.2 Etiquetado y manipulado de la información.	L4
8.2.3 Manipulación de activos.	L5
8.3 Manejo de los soportes de almacenamiento.	
8.3.1 Gestión de soportes extraíbles.	L3
8.3.2 Eliminación de soportes.	L5
8.3.3 Soportes físicos en tránsito.	L5
9. CONTROL DE ACCESOS.	
9.1 Requisitos de negocio para el control de accesos.	
9.1.1 Política de control de accesos.	L2
9.1.2 Control de acceso a las redes y servicios asociados.	L3
9.2 Gestión de acceso de usuario.	
9.2.1 Gestión de altas/bajas en el registro de usuarios.	L5
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	L4

NOMBRE DE LOS CONTROLES	CUMPLIDOS
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	L4
9.2.4 Gestión de información confidencial de autenticación de usuarios.	L2
9.2.5 Revisión de los derechos de acceso de los usuarios.	L3
9.2.6 Retirada o adaptación de los derechos de acceso	L5
9.3 Responsabilidades del usuario.	
9.3.1 Uso de información confidencial para la autenticación.	L5
9.4 Control de acceso a sistemas y aplicaciones.	
9.4.1 Restricción del acceso a la información.	L2
9.4.2 Procedimientos seguros de inicio de sesión.	L5
9.4.3 Gestión de contraseñas de usuario.	L5
9.4.4 Uso de herramientas de administración de sistemas.	L2
9.4.5 Control de acceso al código fuente de los programas.	L5
10. CIFRADO.	
10.1 Controles criptográficos.	
10.1.1 Política de uso de los controles criptográficos.	L5
10.1.2 Gestión de claves.	L4
11. SEGURIDAD FISICA Y AMBIENTAL.	
11.1 Áreas seguras.	
11.1.1 Perímetro de seguridad física.	L5
11.1.2 Controles físicos de entrada.	L5
11.1.3 Seguridad de oficinas, despachos y recursos.	L5
11.1.4 Protección contra las amenazas externas y ambientales.	L5
11.1.5 El trabajo en áreas seguras.	L5
11.1.6 Áreas de acceso público, carga y descarga.	L5
11.2 Seguridad de los equipos.	
11.2.1 Emplazamiento y protección de equipos.	L5
11.2.2 Instalaciones de suministro.	L5
11.2.3 Seguridad del cableado.	L2
11.2.4 Mantenimiento de los equipos.	L5
11.2.5 Salida de activos fuera de las dependencias de la empresa.	L2
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	L5
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	L5
11.2.8 Equipo informático de usuario desatendido.	L5
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	L2
12. SEGURIDAD EN LA OPERATIVA.	
12.1 Responsabilidades y procedimientos de operación.	
12.1.1 Documentación de procedimientos de operación.	L5
12.1.2 Gestión de cambios.	L2
12.1.3 Gestión de capacidades.	L2
12.1.4 Separación de entornos de desarrollo, prueba y producción.	L5
12.2 Protección contra código malicioso.	
12.2.1 Controles contra el código malicioso.	L5
12.3 Copias de seguridad.	
12.3.1 Copias de seguridad de la información.	L1

NOMBRE DE LOS CONTROLES	CUMPLIDOS
12.4 Registro de actividad y supervisión.	
12.4.1 Registro y gestión de eventos de actividad.	L5
12.4.2 Protección de los registros de información.	L5
12.4.3 Registros de actividad del administrador y operador del sistema.	L2
12.4.4 Sincronización de relojes.	L5
12.5 Control del software en explotación.	
12.5.1 Instalación del software en sistemas en producción.	L2
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Gestión de las vulnerabilidades técnicas.	L2
12.6.2 Restricciones en la instalación de software.	L2
12.7 Consideraciones de las auditorias de los sistemas de información.	
12.7.1 Controles de auditoria de los sistemas de información.	L4
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	
13.1.1 Controles de red.	L5
13.1.2 Mecanismos de seguridad asociados a servicios en red.	L5
13.1.3 Segregación de redes.	L5
13.2 Intercambio de información con partes externas.	
13.2.1 Políticas y procedimientos de intercambio de información.	L2
13.2.2 Acuerdos de intercambio.	L0
13.2.3 Mensajería electrónica.	L0
13.2.4 Acuerdos de confidencialidad y secreto.	L5
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
14.1 Requisitos de seguridad de los sistemas de información.	
14.1.1 Análisis y especificación de los requisitos de seguridad.	L4
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	L5
14.1.3 Protección de las transacciones por redes telemáticas.	L5
14.2 Seguridad en los procesos de desarrollo y soporte.	
14.2.1 Política de desarrollo seguro de software.	L1
14.2.2 Procedimientos de control de cambios en los sistemas.	L2
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L5
14.2.4 Restricciones a los cambios en los paquetes de software.	L2
14.2.5 Uso de principios de ingeniería en protección de sistemas.	L5
14.2.6 Seguridad en entornos de desarrollo.	L2
14.2.7 Externalización del desarrollo de software.	L5
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	L5
14.2.9 Pruebas de aceptación.	L5
14.3 Datos de prueba.	
14.3.1 Protección de los datos utilizados en pruebas.	L5
15. RELACIONES CON SUMINISTRADORES.	
15.1 Seguridad de la información en las relaciones con suministradores.	
15.1.1 Política de seguridad de la información para suministradores.	L5

NOMBRE DE LOS CONTROLES	CUMPLIDOS
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	L5
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	L5
15.2 Gestión de la prestación del servicio por suministradores.	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	L5
15.2.2 Gestión de cambios en los servicios prestados por terceros.	L5
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION.	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	
16.1.1 Responsabilidades y procedimientos.	L3
16.1.2 Notificación de los eventos de seguridad de la información.	L5
16.1.3 Notificación de puntos débiles de la seguridad.	L2
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	L2
16.1.5 Respuesta a los incidentes de seguridad.	L3
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	L3
16.1.7 Recopilación de evidencias.	L5
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO	
17.1 Continuidad de la seguridad de la información.	
17.1.1 Planificación de la continuidad de la seguridad de la información.	L2
17.1.2 Implantación de la continuidad de la seguridad de la información.	L2
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L2
17.2 Redundancias.	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	L2
18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	
18.1.1 Identificación de la legislación aplicable.	L5
18.1.2 Derechos de propiedad intelectual (DPI).	L5
18.1.3 Protección de los registros de la organización.	L3
18.1.4 Protección de datos y privacidad de la información personal.	L3
18.1.5 Regulación de los controles criptográficos.	L5
18.2 Revisiones de la seguridad de la información.	
18.2.1 Revisión independiente de la seguridad de la información.	L2
18.2.2 Cumplimiento de las políticas y normas de seguridad.	L2
18.2.3 Comprobación del cumplimiento.	L2

Tabla 2 Análisis diferencial - Cumplimiento controles 27002:2013

En la siguiente tabla podemos ver una relación de los cumplimientos que hemos podido ver de los distintos controles de la ISO 27002:2013.

NOMBRE DE LOS CONTROLES	CUMPLE	NO CUMPLE
5. POLITICAS DE SEGURIDAD.	35%	65%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	36%	64%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	97%	3%
8. GESTION DE ACTIVOS.	87%	13%
9. CONTROL DE ACCESOS.	84.5%	15.5%
10. CIFRADO.	97.5%	2.5%
11. SEGURIDAD FISICA Y AMBIENTAL.	91.6%	8.3%
12. SEGURIDAD EN LA OPERATIVA.	61%	39%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	68,7%	31.3%
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	81.4%	18.6%
15. RELACIONES CON SUMINISTRADORES.	100%	0%
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION.	81%	19%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO	50%	50%
18. CUMPLIMIENTO.	73%	37%

Tabla 3 Análisis diferencial - Controles 27002:2013 Incumplimientos

Si lo indicamos en una gráfica podemos ver la siguiente gráfica que nos muestra la variación en el cumplimiento de la norma ISO/IEC 27002:2013

Ilustración 3 Análisis 27002:2013

Procederemos a realizar la misma revisión en relación a la norma ISO/IEC 27001:2013

NOMBRE DE CONTROLES	CUMPLIDO
4.CONTEXTO DE LA ORGANIZACIÓN	
4.1 Comprensión de la organización y de su contexto	**L1**
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	**L1**
4.3 Determinación del alcance del SGSI	**L1**
4.4 SGSI	**L1**
5. LIDERAZGO	
5.1 Liderazgo y compromiso	**L1**
5.2 Política	**L1**
5.3 Roles, responsabilidades y autoridades en la organización	**L1**
6. PLANIFICACIÓN	
6.1 Acciones para hacer frente a los riesgos y oportunidades	
6.1.1 General	**L0**
6.1.2 Valoración de los riesgos de seguridad de la información	**L0**
6.1.3 Tratamiento de los riesgos de seguridad de la información	**L1**
6.2 Objetivos de seguridad de la información y planificación para conseguirlos	**L1**
7. SOPORTE	
7.1 Recursos	**L1**
7.2 Competencia	**L1**
7.3 Concienciación	**L1**
7.4 Comunicación	**L1**
7.5 Información documentada	
7.5.1 General	**L1**
7.5.2 Creando y actualizando	**L1**
7.5.3 Control de la información documentada	**L1**
8. OPERACIÓN	
8.1 Planificación y control	**L1**
8.2 Valoración de los riesgos de la seguridad de la información	**L1**
8.3 Tratamiento de los riesgos de la seguridad de la información	**L1**
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 Seguimiento, medición, análisis y evaluación	**L1**
9.2 Auditoría interna	**L1**
9.3 Revisión por la dirección	**L0**
10. MEJORA	
10.1 No conformidad y acciones correctivas	**L0**
10.2 Mejora continua	**L0**

Si revisamos el estado actual con respecto a la norma ISOI/IEC 27001:2013 podemos ver la una evolución gráfica que indica la situación de la empresa con respecto a la norma. Como podemos apreciar los valores son muy bajos debido a que la empresa actualmente carece de un sistema de seguridad de la información implantado y la gestión del mismo actualmente está en un estado de inmadurez. Al igual que en podemos observar que disponen de correctas medidas técnicas en muchas áreas y controles que nos dan buenas perspectiva de cara a la ISO/IEC 27002:2013, en el caso de la ISO/IEC 27001:2013 podemos apreciar que la Dirección y personal tienen un gran desconocimiento de la seguridad de la información de la empresa.

Ilustración 4 Análisis 27001:2013

Sistema de gestión documental

1. Introducción al esquema documental

Las políticas de sistemas de gestión se apoyan en documentación para poder cumplir con la normativa con lo que requeriremos para nuestro Sistema de gestión de Seguridad de la información una serie de documentos que son los que desarrollaremos en esta fase.

Tal como se muestra en la ISO/IEC 270001 se requiere de los siguientes documentos (enunciado de la fase 2):

- **Política de Seguridad**: Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.
- **Procedimiento de Auditorías Internas**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.
- **Gestión de Indicadores**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.
- **Procedimiento Revisión por Dirección**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.
- **Metodología de Análisis de Riesgos**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.
- **Declaración de Aplicabilidad**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

2. Política de Seguridad

La política de seguridad tal como se indicaba previamente se trata de una normativa interna que debe de conocer el personal afectado por el alcance del Sistema de gestión de la Seguridad de la información.

En el caso de **Web Consulting S.A** indicaremos las directrices de seguridad del uso de los recursos de la Organización además de comportamiento en caso de incidentes de seguridad.

- La entrada y salida de los empleados en la empresa seguirán las pautas de seguridad que han sido remitidas por el personal de RRHH y seguridad física. En este caso concreto sería el departamento de Contabilidad y asesoría legal.
- Todo el personal con independencia del cargo tiene que cumplir una política de *mesas vacías* donde no se dejará información de ningún tipo visible a simple vista.
- Para poder acceder a los recursos telemáticos es necesario la aprobación del responsable del departamento y la posterior aprobación por parte del responsable de seguridad.
- El acceso a la información se concede de forma nominal en todos los casos con lo que no debe en ningún momento generarse accesos genéricos o departamentales. El compartir las claves de acceso corresponderá con la oportuna amonestación de RRHH por violación de la seguridad (aunque no lleguen a ocurrir eventos de riesgo al uso).
- Todo el personal recibirá formación adecuada y documentación para el correcto cumplimiento de la normativa de seguridad de la información. Dicho material puede comprender múltiple información como una muestra de normas de la LOPD para gestión de documentación, esta política de seguridad y las normativas internas del departamento correspondiente. Además incluiremos información de seguridad física como pueda ser vías de evacuación y asignaciones de personal como referencia en casos de emergencia.
- El personal dispondrá en todo momento de información publicada en la intranet donde podrá consultar información sobre el resto de personas que trabajan en la empresa para comprobar accesos a información si fuese necesario. Además de ello se tendrá acceso a diversa documentación de circuitos operativos de seguridad en la empresa. Dentro de este sistema se publicarán diversos informes formativos que deberán de ser leídos por todos los miembros del personal y confirmado su realización.
- En caso de tener cualquier tipo de problemas relacionado con los sistemas de seguridad de la información, el personal deberá de notificar a su responsable o en su defecto al responsable de la seguridad aquellos problemas o infracciones que haya podido observar.
- El personal tendrá a su disposición un buzón de sugerencias para poder comunicar las distintas mejoras o defectos encontrados que puedan encontrar en el actual sistema de gestión. Se quiere conseguir una gestión activa y dinámica con la ayuda del personal.

3. Procedimiento de auditoría interna

En este documento se trata de normalizar el proceso a seguir para la realización de una auditoría de tipo interna de la empresa **Web Consulting S.A.**

Para poder realizar una auditoría interna se requiere de un **plan de auditoría.** En este plan se definen los elementos o departamentos que van a ser auditados. Para proceder con esta labor primeramente debemos de generar un equipo auditor que llevaran a cabo la misma.

Las auditorías internas se realizan con una periodicidad anual por distintos integrantes de la empresa que deben de cumplir una serie de requisitos. Además queda abierta la posibilidad de realización **auditorías excepcionales** donde se indicaría al departamento o grupo afectado el motivo y alcance de la auditoría.

Las auditorías anuales planificadas tienen como objetivo poder contrastar el correcto cumplimiento de todos los indicadores que se han establecido y generar documentación con todos aquellos elementos que puedan sobrepasar los umbrales establecidos por la dirección de la empresa. Tal como se establece las auditorías requieren la total cooperación por parte del personal para poder desempeñar correctamente su labor y en caso de encontrar problemas se realizarán partes a los responsables directos que serán quienes gestiones dichos comportamientos anómalos. Las fechas se auditoría se concretarán con los responsables de cada área a auditar. En el caso de necesitar acceso a entornos de producción por parte del equipo auditor se acompañará siempre a los miembros del grupo por un responsable de IT para que no afecte a la continuidad del negocio.

Los **auditores deben de cumplir** los siguientes requisitos:

- Deben de ser independientes con lo que no podrían haber participado en el trabajo que están auditando.
- Deben de estar cualificados en la materia, es decir, deben de estar formados en el sistema de auditoría además de tener experiencia en el campo de la seguridad de información.

En la generación de dicho **grupo auditor** que normalmente suele estar formado por un jefe auditor y los distintos consultores tecnológicos que asesoran al auditor. En el caso de ser una auditoría de gran envergadura puede haber una mayor cantidad de auditores. Los consultores previamente mencionados también deben de ser independientes y cualificados ya que se serán consultados como expertos.

Una vez hemos definido a un grupo de auditoría que cumple los puntos que indicamos previamente se debe de realizar una primera reunión con el responsable de departamento / elementos a auditar o personal asignado para ello. En esta primera reunión se comunicaría el alcance del proyecto y el programa de auditoría que se quiere aplicar. Una vez finalizado pasaríamos a la fase de revisión de documentación aplicable además de verificar el cumplimiento de todo aquello registrado en dicha documentación. Finalmente se establecerá una reunión final donde se indicará al departamento o responsable las desviaciones que se han encontrado en la misma para poder registrarlo.

Los **informes de auditoría** deberán recoger diversa información como:

- Fecha de auditoría
- Equipo auditor
- Identificación de la compañía
- Objetivos de la auditoría
- El alcance y la norma de referencia
- Conformidad del SGSI con la norma
- No conformidades detectadas en el proceso

En este proceso además se pueden incluir las observaciones del responsable para poder mejorar el proceso de auditoría (tener en cuenta que se trata de un proceso cíclico y el material o elementos pueden cambiar con el tiempo). Finalmente se obtendrá un informa de auditoría y será entregado al Responsable de Seguridad. Esta información servirá para poder ser contrastada con pasadas auditorías y poder comprobar la evolución y mejora del sistema de gestión de seguridad de la información.

Cuando ha finalizado el proceso de auditoría se remitirán los informes al comité de seguridad donde estarán miembros de la dirección de la empresa y responsable de todas las áreas. De este modo se podrá evaluar de forma efectiva el resultado de las auditorías y generar si hiciesen falta proyectos de evolución para reducir los problemas encontrados. En caso de no conformidad se establecerán nuevas citas con el grupo auditor para poder tratarlas.

4. Gestión de indicadores

Para poder medicar la eficacia de los controles de seguridad implantados es necesario el uso de distintos indicadores

http://www.iso27000.es/iso27002_5.html

CONTROL	OBJETIVO	FRECUENCIA	FORMULA / TOLERANCIA	RESPONSABLE
5.1 Política de Seguridad	Verificar que el documento es revisado por Dirección	Anual	Mínimo 1 revisión	Responsable IT Backup: Subdirector
6.1 Organización interna.	90% aceptación roles del personal. 90% implantación de SGSI departamental	Anual	80% es tolerable	Responsable IT Backup: Subdirector
6.2 Dispositivos para movilidad y teletrabajo.	5 incidencias graves anuales	Anual	6-9 incidencias	Responsable IT Backup: Subdirector
7.1 Antes de la contratación.	100% comprobación de empleados y contratas.	Anual	90%	Subdirector
7.2 Durante la contratación.	70% de feedback de empleado y contratas. (respuestas a concienciación seguridad)	Anual	60%	Subdirector
7.3 Cese o cambio de puesto de trabajo.	0% de usuarios que cesan actividad en la empresa por motivos ajenos a la misma	Anual	10% (inicio de jornadas de reflexión)	Subdirector
8.1 Responsabilidad sobre los activos.	100% de activos con planes de mitigación de riesgos	Semestral	90%	Responsable IT Backup: Subdirector
8.2 Clasificación de la información.	100% activos categorizados	Anual	90%	Responsable IT Backup: Subdirector
8.3 Manejo de los soportes de almacenamiento.	100% Backups encriptados	Semestral	95%	Responsable IT Backup: Subdirector
9.1 Requisitos de negocio para el control de accesos.	100% de identificación de propietarios de información	Anual	95%	Responsable IT Backup: Subdirector
9.2 Gestión de acceso de usuario.	1 hora tiempo medio para gestión de acceso a usuarios	Anual	2 horas es asumible por carga de trabajo	Responsable IT Backup: Subdirector
9.3 Responsabilidades del usuario.	100% aceptación responsabilidades de personal. Documento de aceptación.	Anual	95%	Responsable IT Backup: Subdirector
9.4 Control de acceso a sistemas y aplicaciones.	100% Backups encriptados	Anual	95%	Responsable IT Backup: Subdirector
10.1 Controles criptográficos.	% de sistemas que contienen datos sensibles y están encriptados. Se busca el 90%	Anual	80%	Responsable IT Backup: Subdirector
11.1 Áreas seguras.	Realización de inspección técnica de las áreas seguras.	Semestral	2 incidencias leves.	Responsable IT Backup: Subdirector

CONTROL	OBJETIVO	FRECUENCIA	FORMULA / TOLERANCIA	RESPONSABLE
11.2 Seguridad de los equipos.	0% de incidentes de seguridad con personal interno	Anual	5%	Seguridad de edificio Responsable de departamento (del personal afectado)
12.1 Responsabilidades y procedimientos de operación.	100% aplicación de parches de seguridad a sistemas	Semestral	95%	Responsable IT Backup: Adjunto IT
12.2 Protección contra código malicioso.	0 incidencias de seguridad por software malicioso	Semestral	3 incidencias	Responsable IT Backup: Adjunto IT
12.3 Copias de seguridad.	100% Backup OK	Mensual	95%	Responsable IT Backup: Adjunto IT
12.4 Registro de actividad y supervisión.	100% de sistemas monitorizados	Trimestral	90%	Responsable IT Backup: Adjunto IT
12.5 Control del software en explotación.	100% Incidencias resultas por instalación de software según procedimiento.	Mensual	90%	Responsable IT Backup: Adjunto IT
12.6 Gestión de la vulnerabilidad técnica.	100% vulnerabilidades técnicas resueltas	Trimestral	95% aplicando planes de contención	Responsable IT Backup: Subdirector
12.7 Consideraciones de las auditorias de los sistemas de información.	100% recomendaciones de auditoría atendidas	Semestral	90% si se trata de problemas de presupuesto o evolución ya definidos en proyectos futuros	Responsable IT Backup: Subdirector
13.1 Gestión de la seguridad en las redes.	0 incidencias graves	Semestral	2 incidencias graves	Responsable IT Backup: Subdirector
13.2 Intercambio de información con partes externas.	0 incidencias relativas a intercambio de información con terceras partes	Anual	1 incidencia de grados medio	Responsable IT Responsible Marketing Backup: Subdirector
14.1 Requisitos de seguridad de los sistemas de información.	100% de aplicaciones y sistemas catalogados	Trimestral	95%	Responsable IT Responsible Marketing Backup: Subdirector
14.2 Seguridad en los procesos de desarrollo y soporte.	0 incidencias graves relativas a informe plan de mantenimiento de sistemas / aplicaciones	Mensual	2 incidencias de grado medio	Responsable IT Responsible Marketing Backup: Subdirector
14.3 Datos de prueba.	100% sistemas revisados según plan de seguridad	Trimestral	95%	Responsable IT Responsible Marketing Backup: Subdirector
15.1 Seguridad de la información en las relaciones con suministradores.	0 incidencias de seguridad de traspasos de información a suministradores	Mensual	2 incidencias de grados medio. Tras la primera se procede a buscar nuevos. 1 grave implica compensaciones.	Responsable IT Responsible Marketing Backup: Subdirector
15.2 Gestión de la prestación del servicio por suministradores.	100% cumplimiento de SLA	Mensual	90%	Responsable IT Responsible Marketing Backup: Subdirector
16.1 Gestión de incidentes de seguridad de la información y mejoras.	0 incidencias graves de seguridad	Trimestral	4 incidencias leves	

CONTROL	OBJETIVO	FRECUENCIA	FORMULA / TOLERANCIA	RESPONSABLE
17.1 Continuidad de la seguridad de la información.	100% de elementos incluidos en plan de continuidad de negocio	Semestral	90%	Responsable IT Responsible Marketing Backup: Subdirector
17.2 Redundancias.	100% de servicios redundados	Trimestral	90%	Responsable IT Responsible Marketing Backup: Subdirector
18.1 Cumplimiento de los requisitos legales y contractuales.	100% de recomendaciones atendidas	Mensual	95%	Subdirector Backup: Asesoría externa
18.2 Revisiones de la seguridad de la información.	0% hallazgos en auditorías internas relativas a seguridad de la información	Trimestral	15%	Responsable IT Responsible Marketing Backup: Subdirector

Tabla 4 Gestión de indicadores - Indicadores y controles

5. Procedimiento revisión por Dirección

De forma periódica debe de revisarse las distintas cuestiones asociadas con el Sistema de Gestión de la Seguridad de la información (SGSI). Para ello es necesario que la Dirección sea parte integrante de la revisión ya que afectan al funcionamiento de la empresa y es necesario e imprescindible que formen parte de la toma de decisiones.

Anualmente en **Web Consulting S.A** se revisará dicho SGSI con el fin de comprobar que se han alcanzado los objetivos marcados en el proceso. En dicho proceso de revisión se obtendrán como resultado decisiones para aplicar cambios en base a la información percibida de la auditoría interna y distintos registros del SGSI.

Las entradas y puntos para la reunión de seguimiento serían:

- Resultados de mediciones realizadas, auditorías y revisiones del SGSI
- Propuestas de mejora obtenidas por personal o por responsables de departamento
- Elementos no tratados adecuadamente en el SGSI
- Retroalimentación de clientes
- Acciones correctivas o preventivas a tener en cuenta
- Conformidad del servicio prestado
- Evaluación de formaciones de la empresa (peticiones departamentales)
- Cumplimiento contratos de servicio con clientes y proveedores
- Política de seguridad de la empresa
- Objetivos de seguridad

Dichas entradas deben de ser revisadas por Dirección para en base al actual estado del negocio, impacto en clientes y planes de proyección de futuro puedan establecer distintos elementos de salida que activen planes de mejora del SGSI y por tanto de los servicios ofrecidos a clientes. Tras la reunión se realiza un resumen de reunión y acta de la misma.

6. Gestión de roles y responsabilidades

El SGSI requiere de un equipo que se encargue de gestionar el propio sistema. Para ello se plantean distintos roles y responsabilidades, es decir que las funciones han de quedar muy bien definidas y se han de atribuir las mismas a personas concretas. Dentro de estas atribuciones pueden ser de tipo parcial o completa, de modo que una persona tenga asociada un único rol en la empresa o pueda asumir varios dependiendo de cuándo sean necesarios dichos roles. Dentro de estos roles y responsabilidades podemos encontrar los siguientes

1. Comité de dirección

Este grupo está constituido por:

- Director general / Presidente de la compañía
- Subdirector (responsable del departamento de contabilidad y asesoría legal)
- Responsable de departamento IT
- Responsable del departamento Marketing

Tienen las siguientes funciones:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
- Nombrar a los miembros de un Comité de Seguridad de la Información y darles soporte, dotarlo de los recursos necesarios y establecer sus directrices de trabajo.
- Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.
- Determinar el umbral de riesgo aceptable en materia de seguridad.
- Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el Plan de seguridad de la información, que recoge los principales proyectos e iniciativas en la materia.
- Realizar el seguimiento del cuadro de mando de la seguridad de la información.

Estas funciones han sido obtenidas a la asignatura de Sistemas de Gestión de la Seguridad de información, concretamente del apartado 3.1

2. Comité de seguridad

En este comité es requisito poder contar con altos cargos de la compañía además de contar con responsables de departamentos donde la seguridad de la información pueda cobrar un gran papel. En el caso de **Web Consulting S.A** lo formarían:

- Director general / Presidente de la compañía
- Subdirector (responsable del departamento de contabilidad y asesoría legal)
- Responsable de departamento IT
- Responsable del departamento Marketing

Si bien es cierto que se puede ver que el personal es el mismo en ambos comités es debido al tamaño de la propia empresa. Se trata de una empresa de tamaño medio que no dispone de sedes o múltiples departamentos donde puedan producirse una mayor segregación de personal (mayor granularidad de responsabilidades).

Las funciones de dicho comité serían:

- Implantar las directrices del Comité de Dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).
- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.
- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

Estas funciones han sido obtenidas a la asignatura de Sistemas de Gestión de la Seguridad de información, concretamente del apartado 3.2

3. Responsable de seguridad de la información

Para poder centralizar la gestión de la seguridad de la información se debe de escoger a un único responsable que pueda coordinar los esfuerzos de los distintos órganos que hemos establecido en el SGSI. En el caso de **Web Consulting S.A** el responsable de IT será quien se convierta en el responsable de seguridad de la información. Más aún si tenemos en cuenta que se encargaría tanto de la seguridad física como de la lógica.

Las funciones de dicho responsable serían:

- Implantar las directrices del Comité de Seguridad de la Información de la compañía.
- Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información.
- Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el área de Organización/RR. HH., en el cual se recogerá quién asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.
- Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.

- Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.
- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección. Elevar el mapa de riesgos y el Plan de seguridad de la información al CSI.
- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando. Una vez aprobado dicho plan y el presupuesto por el CSI, el RSI deberá gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.
- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.
- Velar por el cumplimiento legal (LOPD, RD 3/2010 Esquema Nacional de Seguridad, Basilea, SOX...), coordinando las actuaciones necesarias con las unidades responsables.
- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al CSI si corresponde.
- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.
- Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al CSI si corresponde.
- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El RSI debe analizar y mantener actualizado dicho cuadro de mando, presentándolo al CSI con la periodicidad que se establezca.

Estas funciones han sido obtenidas a la asignatura de Sistemas de Gestión de la Seguridad de información, concretamente del apartado 3.3. Como podemos ver es una gran cantidad de funciones que tiene que asumir pero una gran parte de ellas consiste en gestionar que otros grupos operativos puedan proceder a realizar dichos trabajos, un ejemplo de ello podría ser la formación del personal en materia de seguridad. Los distintos responsables tendrán que encargarse de sus departamentos pero sería el RSI quien coordinaría a los mismos.

4. Responsables de departamento IT

Actualmente tal como se ha organizado el organigrama para la empresa y el estado de la distribución de las funciones podemos ver que en el punto 3.4.3 de sistemas de gestión de la

seguridad se le atribuirían más funciones pero estas mismas se pueden asumir dentro del rol de RSI que ya está asumiendo el responsable de IT de la empresa.

5. Responsable de departamento RRHH (contabilidad y asesoría legal)

El responsable de RRHH en **Web Consulting S.A** tiene varias funciones como hemos podido ver en la introducción de la empresa. En el caso de la esta empresa sería el propio Subdirector y asumiría las siguientes funciones por pertenencia al grupo de RRHH en la gestión de personal:

- Informar a las unidades gestoras de recursos de información sobre cambios / movimientos de personal para poder realizar una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría y/o funciones, cambios organizativos, etc.
- Trabajar conjuntamente con el RSI en el desarrollo de la política de seguridad de la información en los temas referentes al personal.
- Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo.

Estas funciones se han extraído del punto 3.4.5 de sistemas de gestión de la seguridad de la información. En el caso de la empresa podemos comprobar que parte de dichas funciones ya las tenía previamente asumidas pero no estaban contempladas en ningún documento con lo que lo reflejamos en este punto.

6. Personal en general

En este grupo se engloba todo aquel profesional que no esté incluida en las categorías de responsables o dirección de la empresa. En este punto podemos encontrar las siguientes funciones aplicables a todos ellos:

- Mantener la confidencialidad de la información.
- Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados.
- Respetar las normas y procedimientos vigentes en materia de seguridad de la información, y velar por que terceras partes en prestación de servicios también la respeten.
- Utilizar adecuadamente las credenciales de acceso a los sistemas de información.
- Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación.
- Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.

Estas funciones se han extraído del punto 3.4.2 de sistemas de gestión de la seguridad de la información.

7. Metodología de análisis de riesgos

La metodología aplicada en **Web Consulting S.A** es MAGERIT en su tercera versión. Esta metodología se trata de una forma de análisis de riesgos muy utiliza en España. Está separada una serie de fases diferenciadas tal y como siguen:

Fase 1 Toma de datos. Procesos de la información.

Esta primera fase debe de definirse el alcance que se ha de estudiar o analizar, punto muy importante ya que es lo que hará que el proyecto pueda ser más o menos costoso.

Se compone de:

- Definición de alcance
- Estudio de los procesos de la organización de la empresa
- Establecer el nivel de granularidad en el análisis. El nivel de detalle al que se quiere llegar en este proceso.

Fase 2 Dimensionamiento. Establecimiento de parámetros

Consiste en el establecimiento de parámetros que se emplearan en todo el proceso de análisis de riesgos. Es decir que vamos a identificar dichos parámetros de medición que serían:

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

El **valor de los activos** se toma en base a los siguientes valores:

1. Valor de reposición: el valor que tiene para la organización.
2. Valor de configuración: el tiempo que se necesita desde que se obtiene un activo hasta que se pone a punto para ser un activo.
3. El uso del activo: el valor que pierde la organización por la pérdida del mismo.
4. Pérdida de oportunidad: valor que pierde potencialmente la organización al no disponer de dicho activo un tiempo.

Es decir que tal y como hemos podido comprobar un elemento para distintas empresas puede tener valor distintos en función del uso que se le dé a dicho elemento. Un ejemplo de cuantificación de los elementos a cuantificar podría ser la siguiente tabla:

Valoración	Rango	Valor
Muy alta	valor > 200.000 €	300.000 €
Alta	100.000€ < valor > 200.000 €	150.000 €
Media	50.000€ < valor > 100.000€	75.000 €
baja	10.000€ < valor > 50.000€	30.000 €
Muy Baja	valor < 10.000 €	10.000 €

Tabla 5 Riesgos - Cuantificación elementos

La v**ulnerabilidad** se toma en MAGERIT como la frecuencia de ocurrencia de una amenaza, es decir con qué frecuencia se enfrentará la organización con dicha amenaza. Para calcularlo podríamos representarlo de la siguiente forma:

Vulnerabilidad = Frecuencia estimada / días del año

Un ejemplo de clasificación de la vulnerabilidad podría ser el siguiente cuadro teniendo en cuenta que el año tiene un total de 52 semanas:

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada 2 semanas	26/365 = 0,07123
Frecuencia media	1 vez cada 2 meses	6/365 = 0,016438
Frecuencia baja	1 vez cada 6 meses	2/365=0,005479
Frecuencia muy baja	1 vez al año	1/365=0,002739

Tabla 6 Riesgos - vulnerabilidades

Los valores que se van estimando no pueden modificados a la largo de la auditoría ya que pueden desvirtuar los resultados finales.

Dentro de la metodología MAGERIT se entiendo como **impacto** se entiende como el porcentaje del valor del activo que se pierde en caso de que suceda una incidencia con el mismo. Para poder calcularlo se debe de realizar una estimación de rango de impactos para lo que debemos definir un determinado rango como por ejemplo.

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

Tabla 7 Riesgos - impacto

La **Efectividad del control de la seguridad** tiene como objetivo poder cuantificar la influencia de las medidas de seguridad antes los riesgos que se detectan, es decir, en como mitigan el impacto que tienen en los elementos de la empresa. De modo que podemos indicar que se trataría de comprobar la variación del impacto / vulnerabilidad para lo que podemos guiarnos por la siguiente tabla.

Variación Impacto / vulnerabilidad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Tabla 8 Riesgos - impacto / vulnerabilidad

La información de esta FASE2 se ha podido obtener de la documentación de la asignatura SGSI concretamente del tema análisis de riesgos.

Fase 3 Análisis de activos

En esta tercera fase se identificarán los distintos activos que poseen la empresa y qué es necesario para poder desempeñar su negocio. En este caso tendríamos que identificar los siguientes elementos.

- Activos físicos: serían todos los activos hardware que se utilizan en la organización.
- Activos lógicos: serían los desarrollos, licencias y elementos software.
- Activos de personal: el propio personal desde el punto de vista de los roles y responsabilidades.
- Activos de entorno infraestructura: en este caso hablaríamos del entorno donde se ubica la empresa y que permite el desempeño de las funciones normales de la misma. En el caso de nuestra empresa este activo se encuentra subcontratado.
- Activos intangibles: en este punto se tiene en cuenta el conocimiento y el propio valor de la marca de la empresa en el mercado.

Fase 4 Análisis de amenazas

Una amenaza es aquella situación que puede llegar a darse en una empresa y que desembocarían en un problema de seguridad para la misma.

En MAGERIT se realiza la siguiente **clasificación de amenazas**:

Accidentes → Son aquellas situaciones no provocadas. Dentro de esta categoría de accidentes existen diferentes tipos, como son: accidentes físicos (inundación, incendio, terremoto, explosión, etc.), averías, interrupciones de los servicios esenciales (cortes en el suministro eléctrico, en las telecomunicaciones, etc.) y accidentes mecánicos o electromagnéticos (choque, caída, radiación, etc.)

Errores → Son aquellas situaciones que son cometidas de forma involuntaria entre las cuales podemos citar las siguientes: errores en la utilización de los sistemas, errores en el diseño conceptual de las aplicaciones, errores en el desarrollo de las aplicaciones, errores de actualización, errores en la monitorización, errores de compatibilidad entre aplicaciones o errores inesperados (virus, troyanos, etc.)

Amenazas intencionales presenciales → Son las provocadas por el propio personal de la organización de forma voluntaria las cuales podemos citar las siguientes: acceso físico no autorizado, acceso lógico no autorizado, interceptación pasiva de la información, indisponibilidad de recursos, ya sean humanos (bajas, vacaciones, abandono, enfermedad, etc.) o técnicos (bloqueo de sistema, etc.) y filtración de datos a terceras organizaciones, ya sean datos personales (LOPD) o técnicos.

Amenazas intencionales remotas →Amenazas provocadas por terceras personas, es decir, por personas ajenas a nuestra organización y que consiguen dañarla. Entre las cuales podemos citar las siguientes: acceso lógico no autorizado, suplantación del origen, gusanos o denegaciones de servicio.

Fase 5 Establecimiento de vulnerabilidades

Dentro de MAGERIT no es necesario enumerar o listar las vulnerabilidades pero si que es importante tenerlas en cuenta con el fin de estimar y calcular la frecuencia de la ocurrencia de una terminada amenaza.

Fase 6 Establecimiento de impactos

Los impactos se definen como las consecuencias que provoca en la organización una amenaza que aprovechando una vulnerabilidad afecte a un activo de la empresa.

Es decir que podríamos indicar que sería:

Impacto potencial = Valor del activo (según la dimensión del mismo) X Valor del impacto

Fase 7 Análisis de riesgo intrínseco

Hasta llegar a este punto hemos sido capaces de evaluar los riesgos actuales a los que esta sometida la empresa. En este punto realizaremos el cálculo de los valores reales de los riesgos a los que la empresa está sometida. Para ello procederemos la siguiente:

Riesgo = Valor de activo X vulnerabilidad X Impacto

En este punto habiendo obtenido el valor del riesgo deberá de decidir la empresa el rango de riesgo aceptable para la misma. De esta forma podemos ver un rango como el que vemos a continuación:

Nivel aceptable de riesgo	Valor
Alto	75%
Medio	50%
Bajo	25%

Tabla 9 Riesgos - nivel aceptable de riesgo

Fase 8 Influencia de salvaguardas

Una vez hemos identificado el punto en el que se encuentra le empresa y lo que la misma está dispuesta a asumir como riesgos aceptable tenemos que proceder a cuantificar la influencia de las salvaguardas o controles de seguridad de la información sobre la empresa. En este punto estaríamos entrando en la **gestión de riesgos** donde seleccionaríamos la mejor solución de seguridad que permita reducirlos. Existen dos tipos:

- Preventivas →aquellas que reducen las vulnerabilidades (firewall)
- Correctivas →aquellas que reducen el impacto de las amenazas (Backups)

Fase 9 Análisis de riesgo efectivo

Es el resultado de realizar el estudio de cómo reducir los riesgos en cada una de las medidas de protección. Es decir que procederemos a calcular el riesgo definitivo que tendría la organización para una de las amenazas identificadas. Quedando de la siguiente forma:

Riesgo intrínseco

Valor activo X vulnerabilidad x Impacto

Riesgo efectivo

Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto) = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto.

Fase 10 Evaluación de riesgos

En esta última fase la organización tiene que realizar una toma de decisiones sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permitirían reducir los riesgos.

Se deberá de disminuir todos los riesgos por debajo del umbral de riesgos que es el punto en que una organización considera que los riesgos a los que se encuentra expuesta no son aceptables. Para gestionar los riesgos en una empresa pueden tomarse tres decisiones:

- Reducirlos
- Transferirlos
- Aceptarlos

Para ello debe de gestionarse un plan de acción que debería de contener la siguiente información:

- Establecer prioridades → asignar prioridad a los riesgos que deben de reducirse en primer lugar.
- Planteamiento del análisis de coste / beneficio → para cada medida comprobar si el coste de la misma supera el beneficio.
- Selección de controles definitivos
- Asignación de responsabilidades → asignar responsable para la implantación de los controles.
- Implantación de controles

8. Declaración de aplicabilidad

Este documento es el ***Statement Of Applicability*** de un SGSI donde podemos relacionar los distintos controles de seguridad de la ISO 27002 con la aplicación dentro de la empresa. De forma que una organización debe seleccionar aquellos que debe de implantar y mantener en su sistema. El resultado de la elección de controles forma parte del Plan de Tratamiento de riesgos dando como salida el resultante documento.

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
5. POLITICAS DE SEGURIDAD.		
5.1 Directrices de la Dirección en seguridad de la información.		
5.1.1 Conjunto de políticas para la seguridad de la información.	SI	Requerido para certificación y revisión de políticas de seguridad de empresa. (auditorías internas)
5.1.2 Revisión de las políticas para la seguridad de la información.	SI	Requerido para certificación y revisión de políticas de seguridad de empresa. (auditorías internas)
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.		
6.1 Organización interna.		
6.1.1 Asignación de responsabilidades para la seguridad de la información.	SI	Necesario para definición de roles
6.1.2 Segregación de tareas.	SI	Necesario para definición de roles y tareas
6.1.3 Contacto con las autoridades.	SI	Requerido para norma y establecer procedimientos internos.
6.1.4 Contacto con grupos de interés especial.	SI	Requerido para norma y establecer procedimientos internos. Adecuación a normativa especial local.
6.1.5 Seguridad de la información en la gestión de proyectos.	SI	Requerido para norma.
6.2 Dispositivos para movilidad y teletrabajo.		
6.2.1 Política de uso de dispositivos para movilidad.	SI	Requerido para norma y gestionar accesos a información. Auditoría interna.
6.2.2 Teletrabajo.	SI	Requerido para norma y gestionar accesos a información. Auditoría interna.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		
7.1 Antes de la contratación.		
7.1.1 Investigación de antecedentes.	SI	Requerido para norma y mejor en procesos selectivos internos (establecer procedimientos).
7.1.2 Términos y condiciones de contratación.	SI	Requerido para norma y mejor en procesos selectivos internos (establecer procedimientos). Mejora para posible regulación por convenio propio
7.2 Durante la contratación.		
7.2.1 Responsabilidades de gestión.	SI	Requerido por norma y mejora de procedimientos.
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	SI	Requerido por norma y mejora de formación del personal en seguridad. Planificación de formaciones.
7.2.3 Proceso disciplinario.	SI	Requerido por norma y procedimientos internos para personal.
7.3 Cese o cambio de puesto de trabajo.		

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
7.3.1 Cese o cambio de puesto de trabajo.	SI	Requerido por norma. Generación de procedimientos de gestión de personal en alta/baja/cambio.
8. GESTION DE ACTIVOS.		
8.1 Responsabilidad sobre los activos.		
8.1.1 Inventario de activos.	SI	Requerido por norma. Correcta gestión de activos.
8.1.2 Propiedad de los activos.	SI	Requerida por norma. Establecer responsabilidades.
8.1.3 Uso aceptable de los activos.	SI	Requerida por norma. Procedimiento de uso de bienes y activos de la empresa.
8.1.4 Devolución de activos.	SI	Requerida por norma. Procedimiento de uso de bienes y activos de la empresa.
8.2 Clasificación de la información.		
8.2.1 Directrices de clasificación.	SI	Requerida por norma. Documento de clasificación de información.
8.2.2 Etiquetado y manipulado de la información.	SI	Requerida por norma. Documento de clasificación de información.
8.2.3 Manipulación de activos.	SI	Requerida por norma. Documento de clasificación de información.
8.3 Manejo de los soportes de almacenamiento.		
8.3.1 Gestión de soportes extraíbles.	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa.
8.3.2 Eliminación de soportes.	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa.
8.3.3 Soportes físicos en tránsito.	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa.
9. CONTROL DE ACCESOS.		
9.1 Requisitos de negocio para el control de accesos.		
9.1.1 Política de control de accesos.	SI	Requerida por norma. Gestión de acceso de personal.
9.1.2 Control de acceso a las redes y servicios asociados.	SI	Requerida por norma. Gestión de acceso de personal.
9.2 Gestión de acceso de usuario.		
9.2.1 Gestión de altas/bajas en el registro de usuarios.	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.2.4 Gestión de información confidencial de autenticación de usuarios.	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso	SI	Requerida por norma. Procedimiento de gestión de usuarios.
9.3 Responsabilidades del usuario.		
9.3.1 Uso de información confidencial para la autenticación.	SI	Requerida por norma. Asignación de roles y procedimiento de gestión de usuarios.
9.4 Control de acceso a sistemas y aplicaciones.		
9.4.1 Restricción del acceso a la información.	SI	Requerida por norma. Clasificación de la información.

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
9.4.2 Procedimientos seguros de inicio de sesión.	SI	Requerida por norma. Clasificación de la información.
9.4.3 Gestión de contraseñas de usuario.	SI	Requerida por norma. Clasificación de la información.
9.4.4 Uso de herramientas de administración de sistemas.	SI	Requerida por norma. Clasificación de la información.
9.4.5 Control de acceso al código fuente de los programas.	SI	Requerida por norma. Clasificación de la información.
10. CIFRADO.		
10.1 Controles criptográficos.		
10.1.1 Política de uso de los controles criptográficos.	SI	Requerida por norma. Gestión de la información, seguridad.
10.1.2 Gestión de claves.	SI	Requerida por norma. Gestión de la información, seguridad.
11. SEGURIDAD FISICA Y AMBIENTAL.		
11.1 Áreas seguras.		
11.1.1 Perímetro de seguridad física.	SI	Requerida por norma. Gestión de accesos.
11.1.2 Controles físicos de entrada.	SI	Requerida por norma. Gestión de accesos.
11.1.3 Seguridad de oficinas, despachos y recursos.	SI	Requerida por norma. Gestión de accesos.
11.1.4 Protección contra las amenazas externas y ambientales.	SI	Requerida por norma. Gestión de accesos.
11.1.5 El trabajo en áreas seguras.	SI	Requerida por norma. Gestión de accesos.
11.1.6 Áreas de acceso público, carga y descarga.	SI	Requerida por norma. Gestión de accesos.
11.2 Seguridad de los equipos.		
11.2.1 Emplazamiento y protección de equipos.	SI	Requerida por norma. Gestión de activos, bienes. Seguridad de bienes.
11.2.2 Instalaciones de suministro.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.3 Seguridad del cableado.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.4 Mantenimiento de los equipos.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.5 Salida de activos fuera de las dependencias de la empresa.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Requerida por norma. Gestión de activos, bienes.
11.2.8 Equipo informático de usuario desatendido.	SI	Requerida por norma. Gestión de activos, bienes. Gestión de accesos.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	SI	Requerida por norma. Gestión de activos, bienes. Gestión de accesos.
12. SEGURIDAD EN LA OPERATIVA.		
12.1 Responsabilidades y procedimientos de operación.		
12.1.1 Documentación de procedimientos de operación.	SI	Requerido por norma. Procedimientos y operativas de personal.
12.1.2 Gestión de cambios.	SI	Requerido por norma. Procedimientos y operativas de personal. Gestión de material comprar / retirada.
12.1.3 Gestión de capacidades.	SI	Requerido por norma. Procedimientos y operativas de personal. Mapa de conocimiento de personal.

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
12.1.4 Separación de entornos de desarrollo, prueba y producción.	SI	Requerido por norma. Procedimientos y operativas de personal. Seguridad en operativo de sistemas informáticos.
12.2 Protección contra código malicioso.		
12.2.1 Controles contra el código malicioso.	SI	Requerido por norma. Seguridad lógica.
12.3 Copias de seguridad.		
12.3.1 Copias de seguridad de la información.	SI	Requerido por norma. Plan de continuidad de negocio.
12.4 Registro de actividad y supervisión.		
12.4.1 Registro y gestión de eventos de actividad.	SI	Requerid por norma. Gestión de acceso a información.
12.4.2 Protección de los registros de información.	SI	Requerid por norma. Gestión de acceso a información.
12.4.3 Registros de actividad del administrador y operador del sistema.	SI	Requerid por norma. Gestión de acceso a información.
12.4.4 Sincronización de relojes.	SI	Requerid por norma. Gestión de acceso a información.
12.5 Control del software en explotación.		
12.5.1 Instalación del software en sistemas en producción.	SI	Requerido por norma. Seguridad lógica.
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Requerido por norma. Seguridad lógica.
12.6.2 Restricciones en la instalación de software.	SI	Requerido por norma. Seguridad lógica.
12.7 Consideraciones de las auditorias de los sistemas de información.		
12.7.1 Controles de auditoria de los sistemas de información.	SI	Requerido por normal. Evolución del sistema de gestión de la seguridad.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.		
13.1 Gestión de la seguridad en las redes.		
13.1.1 Controles de red.	SI	Requerido por norma. Seguridad lógica.
13.1.2 Mecanismos de seguridad asociados a servicios en red.	SI	Requerido por norma. Seguridad lógica.
13.1.3 Segregación de redes.	SI	Requerido por norma. Seguridad lógica.
13.2 Intercambio de información con partes externas.		
13.2.1 Políticas y procedimientos de intercambio de información.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
13.2.2 Acuerdos de intercambio.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
13.2.3 Mensajería electrónica.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
13.2.4 Acuerdos de confidencialidad y secreto.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION		
14.1 Requisitos de seguridad de los sistemas de información.		
14.1.1 Análisis y especificación de los requisitos de seguridad.	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información.
14.1.3 Protección de las transacciones por redes telemáticas.	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información.
14.2 Seguridad en los procesos de desarrollo y soporte.		
14.2.1 Política de desarrollo seguro de software.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
14.2.2 Procedimientos de control de cambios en los sistemas.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.4 Restricciones a los cambios en los paquetes de software.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.5 Uso de principios de ingeniería en protección de sistemas.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.6 Seguridad en entornos de desarrollo.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.7 Externalización del desarrollo de software.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Procedimiento de aceptación de ofertas.
14.2.9 Pruebas de aceptación.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Procedimiento de aceptación de ofertas.
14.3 Datos de prueba.		
14.3.1 Protección de los datos utilizados en pruebas.	SI	Requerido por norma. Procedimiento de protección de datos y uso de los mismos.
15. RELACIONES CON SUMINISTRADORES.		
15.1 Seguridad de la información en las relaciones con suministradores.		
15.1.1 Política de seguridad de la información para suministradores.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
15.2 Gestión de la prestación del servicio por suministradores.		
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
15.2.2 Gestión de cambios en los servicios prestados por terceros.	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos.
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION.		
16.1 Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1 Responsabilidades y procedimientos.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades.
16.1.2 Notificación de los eventos de seguridad de la información.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Procedimiento de contingencia.
16.1.3 Notificación de puntos débiles de la seguridad.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades.

NOMBRE DE LOS CONTROLES	APLICA	JUSTIFICACION
16.1.5 Respuesta a los incidentes de seguridad.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Procedimiento de contingencia.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades.
16.1.7 Recopilación de evidencias.	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Procedimiento de protección de datos.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO		
17.1 Continuidad de la seguridad de la información.		
17.1.1 Planificación de la continuidad de la seguridad de la información.	SI	Requerido por norma. Seguridad lógica, política de seguridad.
17.1.2 Implantación de la continuidad de la seguridad de la información.	SI	Requerido por norma. Seguridad lógica, política de seguridad.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Requerido por norma. Seguridad lógica, política de seguridad.
17.2 Redundancias.		
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	SI	Requerido por normal. Continuidad del negocio.
18. CUMPLIMIENTO.		
18.1 Cumplimiento de los requisitos legales y contractuales.		
18.1.1 Identificación de la legislación aplicable.	SI	Requerido por norma. Protección de datos y LSSIE.
18.1.2 Derechos de propiedad intelectual (DPI).	SI	Requerido por norma. Protección de datos y LSSIE.
18.1.3 Protección de los registros de la organización.	SI	Requerido por norma. Protección de datos y LSSIE.
18.1.4 Protección de datos y privacidad de la información personal.	SI	Requerido por norma. Protección de datos y LSSIE.
18.1.5 Regulación de los controles criptográficos.	SI	Requerido por norma. Protección de datos y LSSIE.
18.2 Revisiones de la seguridad de la información.		
18.2.1 Revisión independiente de la seguridad de la información.	SI	Requerido por norma. Protección de datos y LSSIE.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	SI	Requerido por norma. Protección de datos y LSSIE.
18.2.3 Comprobación del cumplimiento.	SI	Requerido por norma. Protección de datos y LSSIE.

Tabla 10 Declaración de aplicabilidad

Análisis de riesgos

1. Introducción

Un análisis de riesgos corresponde al proceso de identificación de los mismos, junto con su importancia o impacto e identificando los activos que requieren medidas de protección para tratar de reducir los riesgos sobre ellos. Tal como hemos definido en fases previas nos basaremos en la metodología de MAGERIT para el análisis de los riesgos.

En este punto lo que trataremos de realizar será la identificación de todos los elementos que queremos proteger de la empresa clasificándolos en el proceso. Una vez identificados tendremos que averiguar los riesgos o peligros que pueden afectarles además de la frecuencia y criticidad que tendrán en relación con los elementos identificados. La idea es posteriormente identificar cómo podremos protegernos de esos riesgos para mitigarlos o que no lleguen a producirse.

2. Inventario de activos

Tal como indicábamos en el punto anterior primeramente debemos de inventariar todos los activos de la empresa que queramos analizar. Para ello podemos agruparlos tal como indica la metodología MAGERIT. Esta información de agrupaciones la podemos obtener de MAGERIT Libro2 – Catalogo de elementos:

- Instalaciones [INS]
- Hardware [HW]
- Aplicación [SW]
- Datos [DA]
- Red [COM]
- Servicios [SER]
- Equipamiento Auxiliar [EA]
- Personal [PE]

Como puede verse le hemos añadido unas etiquetas que nos ayudarán a identificar los elementos y grupos en puntos posteriores. En base a estas agrupaciones realizaremos la siguiente relación inventariada que haremos de forma diferenciada para mayor comodidad.

Como instalaciones entendemos los entornos donde se desempeñan actividades de la empresa en la propia empresa.

AMBITO	ACTIVO
Instalaciones [INS]	Zona de CPD
	Zona de oficinas
	Zona de recepción

Tabla 11 Activos - Instalaciones

Dentro del apartado Hardware podemos identificar elementos de varios tipos que catalogaré en 3 grupos que serían:

- Hardware HW.1 → Elementos dentro de la LAN de la empresa
- Hardware HW.2 → Elementos de la DMZ o red externa.
- Hardware HW.3 → Elementos empleados en la LAN para usuarios

AMBITO	ACTIVO
Hardware [HW.1]	Servidor de datos de oficina
	Servidor proxy interno
	DC oficina principal / DHCP / DNS / Printers
	DC secundario
	Servidores de BBDD (dos)
	Switch gestionado

Tabla 12 Activos - Hardware Interno Servidores

AMBITO	ACTIVO
Hardware [HW.2]	Servidor Web Externo
	Firewall
	Dos router balanceados
	Servidor FTP externo
	Proxy Inverso

Tabla 13 Activos – Hardware DMZ / Externo

AMBITO	ACTIVO
Hardware [HW.3]	Puestos de trabajo
	Portátiles de trabajo
	Impresoras
	Teléfonos móviles de empresa
	Teléfonos fijos de empresa
	Cámara vigilancia

Tabla 14 Activos – Hardware usuarios

En el ámbito de las aplicaciones las separaremos en tres entornos:

- Aplicaciones [SW.1] → Aplicaciones expuestas al exterior
- Aplicaciones [SW.2] → Aplicaciones internas administradores
- Aplicaciones [SW.3] → Aplicaciones internas usuarios en general

AMBITO	ACTIVO
Aplicaciones [SW.1]	Datos de las BBDD internas
	Datos de soporte y licencias
	Proxy inverso (Correo electrónico y acceso a aplicaciones in ternas)

Tabla 15 Inventario - Activos Aplicaciones expuestas exterior

AMBITO	ACTIVO
Aplicaciones [SW.2]	SQL server 2013
	Aplicación gestión de backups
	Aplicaciones internas (gestión y administración)
	Antivirus corporativo
	Servidor de ficheros
	Servidor de DNS
	Servidor de DHCP
	Windows server 2012 (software y licencias de servidores internos)
	Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido

Tabla 16 Inventario - Activos Aplicaciones internas administradas

AMBITO	ACTIVO
Aplicaciones [SW.3]	Office 2013
	Windows 7 Professional
	Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)

Tabla 17 Activos Inventario - Aplicaciones internas usuarios

Dentro del apartado de Datos podemos encontrar todos englobados en un único grupo ya que la información está expuesta al exterior solo para usuarios internos tras varios procesos de autenticación en el acceso.

AMBITO	ACTIVO
Datos [DA]	Datos en las BBDD internas
	Datos de soporte y licencias
	Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)
	Logs de servidores y clientes
	Backups de servidores y clientes
	Datos departamentales (servidor de datos)

Tabla 18 Inventario - Activos Datos

En este apartado se encontrarían los servicios y elementos que proporcionan acceso y servicio de red a la empresa de forma externa. Es decir, hablamos de los servicios y elementos que proveen de acceso a la red.

AMBITO	ACTIVO
Red [COM]	Línea telefónica
	Servicio de VoIP externo
	Servicio de acceso datos
	Red inalámbrica

Tabla 19 Inventario – Activos de Red

En el apartado de servicios hablamos de elementos necesarios para poder organizar todo el sistema informático correctamente.

AMBITO	ACTIVO
Servicios [SER]	Acceso remoto
	Aplicaciones de control de intrusiones
	Aplicaciones internas de gestión
	Correo electrónico
	Servicio de ficheros FTP
	Acceso a entorno Web Interno
	Acceso a entorno Web externo
	Monitorización de servidores y servicios

Tabla 20 Inventario - Activos Servicios

El Equipamiento auxiliar hace referencia a aquellos materiales informáticos complementarios, consumibles o elementos necesarios para el funcionamiento de todo el sistema. Englobamos tanto la parte de hardware como la parte de usuarios.

AMBITO	ACTIVO
Equipamiento Auxiliar [EA]	Armario central de llaves (llavero)
	Fotocopiadoras (acceso por pin)
	Ficheros de documentos (requiere llave)
	Armario ignífugo (copias de seguridad + llave necesaria para acceso)
	Consumibles varios (cds, tóner, etc.)
	Sistemas de alimentación continua (UPS / SAI)
	Corriente eléctrica
	Elemento de aire acondicionado
	Teléfonos móviles
	Teléfonos fijos

Tabla 21 Inventario - Activos Equipamiento Auxiliar

Cuando hacemos referencia hablamos del personal de la empresa con lo que podemos definirlo como un único grupo. Cuando hablamos de marketing recordar que la empresa también tiene servicios de reputación online lo cual requiere del uso de aplicaciones especiales, etc...

AMBITO	ACTIVO
Personal [PE]	Director general
	Subdirector (contabilidad y asesoría legal)
	Responsable TIC
	Responsable Marketing
	Personal TIC
	Personal Marketing

Tabla 22 Inventario - Activos Personal

3. Valoración de los activos

En este punto trataremos de determinar el valor que tiene cada uno de los activos. Previo a este punto hemos realizado un inventario de los activos de la empresa y con la metodología MAGERIT podemos analizar el inventario para realizar una estimación cuantitativa. Para ellos no basamos en el libro 3 (punto 2.1) donde podemos encontrar información que hace referencia a este proceso.

Para poder realizar una valoración de los activos podemos hacer una valoración sencilla por medio de tablas que nos permitirán identificar la importancia relativa de los diferentes activos que puedan sufrir algún tipo de amenaza. Para esto podemos definir una escala para calificar el valor de los activos, magnitud de impacto y riesgo:

- MB: Muy bajo
- B: Bajo
- M: Medio
- A: Alto
- MA: Muy alto

Tal como se nos indica en MAGERIT podemos ver varias estimaciones que serían las siguientes.

Estimación del impacto

Impacto		**Degradación**		
		1%	10%	100%
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 23 Valoración - estimación impacto

Aquello que tengan valoraciones de tipo MA debería de ser objeto de atención inmediata

Estimación del riesgo

Se modelas impacto, probabilidad y riesgo por medio de escalas similares de tipo cualitativas:

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M:posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Tabla 24 Valoración - estimación riesgo

De modo que si lo combinamos todo obtendríamos la siguiente tabla para calcular el riesgo en base al impacto y probabilidad:

Riesgo		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 25 Valoración - Impacto / Riesgo / Posibilidad

En vez de realizar en análisis en este punto lo haremos en la tabla resumen donde podremos ver todas las relaciones entre inventario y sus correspondientes riesgos. Además tenemos que tener en cuenta que se genera una dependencia entre distintos activos las cuales trataremos a añadirlas posteriormente a modo de tabla. Un ejemplo claro sería la dependencia directa que tendría la aplicación de correo electrónico con el propio servidor de correo. Viendo además una relación también con el Firewall y el acceso a la red externa.

4. Dimensiones de seguridad

Una vez se han analizado los distintos activos se debe de realizar una valoración ACIDA de los mismos. Esta valoración permite que podamos medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio:

- [A] Autenticación
- [C] Confidencialidad
- [I] Integridad de los datos
- [D] Disponibilidad
- [A] Auditoría

Tal como indicamos en puntos previos si nos fijamos en el libro 2 de MAGERIT podemos encontrar en el punto 4 una relación de los criterios de valoración de los activos. Para ello emplearemos un sistema cualitativo que nos ayudará a poder categorizar correctamente los distintos activos. Para ello seguiremos el siguiente baremo:

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	Muy bajo	Irrelevante a efectos prácticos

Tabla 26 - Dimensiones seguridad Valoración

De esta forma podemos cuantificar la importancia de los distintos elementos en base a una numeración la cual la hará o poco relevante (valor 0) o de extrema importancia (valor 10).

La tabla resumen se nutrirá de la información que podemos encontrar en este punto. En el punto 4.1 del libro 2 de Magerit se nos muestra una escala estándar de valores y criterios de un grupo de acciones que son las siguientes y en las que nos basaremos:

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones

3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1pi1	pudiera causar molestias a un individuo

Tabla 27 Dimensiones seguridad - información de carácter personal

[lpo] Obligaciones legales		
9	9.lpo	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lpo	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lpo	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lpo1	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lpo1	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Tabla 28 Dimensiones seguridad - Obligaciones legales

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si 1	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si 1	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si 1	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si 1	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Tabla 29 Dimensiones seguridad - Seguridad

[da] Interrupción del servicio		
9	9.da1	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones

7	7.da1	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da1	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da1	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da1	Pudiera causar la interrupción de actividades propias de la Organización

Tabla 30 Dimensiones seguridad - Interrupción del servicio

[lpo] Obligaciones legales		
9	9.po1	alteración seria del orden público
6	6.po1	probablemente cause manifestaciones, o presiones significativas
3	3.po1	causa de protestas puntuales
1	1.po1	pudiera causar protestas puntuales

Tabla 31 Dimensiones seguridad - Obligaciones legales

[olm] Operaciones		
10	10.olm1	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm1	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm1	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm1	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm 1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Tabla 32 Dimensiones seguridad - Operaciones

[adm] Administración y gestión		
9	9.adm1	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm1	probablemente impediría la operación efectiva de la Organización
5	5.adm1	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm1	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm1	pudiera impedir la operación efectiva de una parte de la Organización

Tabla 33 Dimensiones seguridad - Administración y gestión

[lg] Pérdida de confianza (reputación)		
9	9.lg.1	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.2	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.1	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.2	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.1	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.2	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg1	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg1	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg1	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.lg1	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Tabla 34 Dimensiones seguridad - Pérdida de confianza

[crm] Persecución de delitos		
8	8.crm 1	Impida la investigación de delitos graves o facilite su comisión
4	4.crm1	Dificulte la investigación o facilite la comisión de delitos

Tabla 35 Dimensiones de seguridad - Persecución de delitos

[rto] Tiempo de recuperación de servicio		
7	7.rto1	RTO < 4 horas
4	4.rto 1	4 horas < RTO < 1 día
1	1.rto 1	1 día < RTO < 5 días
0	0.rto1	5 días < RTO

Tabla 36 Dimensiones de seguridad - Tiempo de recuperación de servicio

[lbl.nat] Información clasificada (nacional)		
10	10.lbl 1	Secreto
9	9.lbl 1	Reservado
8	8.lbl 1	Confidencial
7	7.lbl 1	Confidencial
6	6.lbl 1	Difusión limitada
5	5.lbl 1	Difusión limitada
4	4.lbl 1	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl 1	Sin clasificar
1	1.lbl 1	Sin clasificar

Tabla 37 Dimensiones de seguridad - Información clasificada

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue1	TRES SECRET UE
9	9.ue 1	SECRET UE
8	8.ue 1	CONFIDENTIEL UE
7	7.ue 1	CONFIDENTIEL UE
6	6.ue1	RESTREINT UE
5	5.ue1	RESTREINT UE
4	4.ue1	RESTREINT UE
3	3.ue1	RESTREINT UE

Tabla 38 Dimensiones de seguridad - Información clasificada (UE)

5. Tabla resumen de valoración

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
Instalaciones [INS]	Zona de CPD	INS.1	---	Alto	5.lpo	9.si1	9.si1	9.da1	7.si1
	Zona de oficinas	INS.2	---	Alto	5.lpo	5.lpo	3.da	3.da	3.si
	Zona de recepción	INS.3	---	Bajo	5.lpo	5.lpo	1.da	1.da	1.si
Hardware [HW.1]	Servidor de datos de oficina	HW.1.1	Ins.1 Ea.7 sw.2.4 sw.2.8 ea.6	Alto	7.si	7.da1	7.da1	3.da1	4.crm
	Servidor proxy interno	HW.1.2	Ins.1 Ea.7 sw.2.4 Sw.2.9 ea.6	Bajo	3.si	3.si	3.si	3.da1	4.crm
	DC oficina principal / DHCP / DNS / Printers	HW.1.3	Ins.1 Ea.7 sw.2.4 sw.2.8 ea.6	Bajo	7.si	1.adm	5.adm	3.da1	4.crm
	DC secundario	HW.1.4	Ins.1 Ea.7 sw.2.4 sw.2.8 ea.6	Bajo	7.si	1.adm	5.adm	3.da1	4.crm
	Servidores de BBDD (dos)	HW.1.5	Ins.1 Ea.7 sw.2.4 sw.2.8 ea.6	Alto	9.si	5.adm	5.adm	9.da1	4.crm
	Switch gestionado	HW.1.6	Ins.1 Ea.7 hw.2.1 ea.6	Bajo	x	x	x	3.da1	x
Hardware [HW.2]	Servidor Web Externo	HW.2.1	Ins.1 Ea.7 hw.2.1 sw.2.4 Sw.2.9 com.1 ea.6	Alto	7.si	7.da1	7.da1	9.da1	8.crm
	Firewall	HW.2.2	Ins.1 Ea.7 com.3 ea.6	Muy Alto	9.da1	9.da1	9.da1	9.da1	9.da1
	Dos router balanceados	HW.2.3	Ins.1 Ea.7 hw.2.1 com.1 com.3	Medio	5.da1	9.da1	5.da1	9.da1	5.da1
	Servidor FTP externo	HW.2.4	Ins.1 Ea.7 hw.2.1 hw.2.1 sw.2.4 Sw.2.9 ea.6	Bajo	$3.si_1$	$3.si_1$	3.si	3.da1	4.crm
	Proxy Inverso	HW.2.5	Ins.1 Sw.2.9 Ea.7 sw.2.4 ea.6	Bajo	7.si	3.si	1.si	3.da1	4.crm

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
Hardware [HW.3]	Puestos de trabajo	HW.3.1	Ea.7 Ins.2 hw.2.1 sw.2.4 Sw.3.1 Sw.3.2 com.3 ea.6	Medio	7.si	7.si	3.olm	3.da1	4.crm
	Portátiles de trabajo	HW.3.2	Ea.7 com.3 hw.2.1 sw.2.4 Sw.3.1 Sw.3.2 ea.6	Medio	7.si	7.si	3.olm	3.da1	4.crm
	Impresoras	HW.3.3	Ea.7 Ins.2 hw.2.1 ea.6	Bajo	3.si	x	1.olm	1.da1	x
	Teléfonos móviles de empresa	HW.3.4	Ea.7 sw.2.4 ea.6	Bajo	3.olm	3.olm	3.olm	1.da1	3.si
	Teléfonos fijos de empresa	HW.3.5	Ea.7 Ins.2 hw.2.1 com.1 com.3 ea.6	Bajo	3.olm	3.olm	3.olm	1.da1	3.si
	Cámara vigilancia	HW.3.6	Ea.7 Ins.2 Ins.1 Ins.3 hw.2.1 com.3 ea.6	Medio	3.olm	3.olm	3.olm	4.crm	3.si
Aplicaciones [SW.1]	Datos de las BBDD internas	SW.1.1	Sw.2.1 hw.1.5 hw1.3 hw.1.4	Muy Alto	10.si	9.lpo	10.si	9.da1	10.si
	Datos de soporte y licencias	SW.1.2	Hw.1.1 sw.1.1 hw.1.5 hw1.3 hw.1.4	Bajo	x	x	x	1.olm	x
	Proxy inverso (Correo electrónico y acceso a aplicaciones internas)	SW.1.3	hw.1.1 com.3 hw.2.5 hw1.3 hw.1.4	Bajo	$3.si_1$	7.lpo	$3.si_1$	1.da	4.crm
Aplicaciones [SW.2]	SQL server 2013	SW.2.1	Sw.2.8 hw.1.5 hw1.3 hw.1.4	Bajo	$7.si_1$	$3.si_1$	$7.si_1$	$7.si_1$	$7.si_1$
	Aplicación gestión de backups	SW.2.2	Sw.2.8 hw.1.5 hw1.3 hw.1.4	Bajo	$3.si_1$	$3.si_1$	$3.si_1$	5.olm	$7.si_1$
	Aplicaciones internas (gestión y administración)	SW.2.3	hw.1.1 hw.2.1 hw1.3 hw.1.4	Alto	5.si	7.lpo	5.si	5.olm	4.crm

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
	Antivirus corporativo	SW.2.4	hw.2.1 Sw.2.8 Sw.3.2 com.3	Bajo	$3.si_1$	$3.si_1$	$3.si_1$	$5_{.olm}$	4.crm
	Servidor de ficheros	SW.2.5	hw.1.1 Sw.2.8 hw1.3 hw.1.4	Bajo	$3.si_1$	$7_{.lpo}$	$3.si_1$	$5_{.olm}$	4.crm
	Servidor de DNS	SW.2.6	Sw.2.8 hw1.3	Bajo	$3_{.si}$	$3_{.si}$	$3_{.si}$	$7_{.si}$	$3_{.si}$
	Servidor de DHCP	SW.2.7	Sw.2.8 hw1.3	Bajo	$3_{.si}$	$3_{.si}$	$3_{.si}$	$7_{.si}$	$3_{.si}$
	Windows server 2012 (software y licencias de servidores internos)	SW.2.8	hw.1.1 com.3	Medio	$7_{.si}$	$7_{.si}$	$7_{.si}$	$3_{.si}$	8.crm
	Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido	SW.2.9	com.3	Medio	$7_{.si}$	$7_{.si}$	$7_{.si}$	$3_{.si}$	8.crm
	Documentación electrónica	SW.2.10	Hw.1.1	Alto	$7_{.si}$	$7_{.lpo}$	$7_{.si}$	$5_{.olm}$	8.crm
Aplicaciones [SW.3]	Office 2013	SW.3.1	Hw.3.1 Hw.3.2	Bajo	$3_{.si1}$	$3_{.si1}$	$3_{.si1}$	$1_{.da1}$	x
	Windows 7 Professional	SW.3.2	Hw3.1 Hw.3.2 hw1.3 hw.1.4	Medio	$3_{.si1}$	$3_{.si1}$	$7_{.si1}$	$3_{.da1}$	$3_{.si}$
	Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	SW.3.3	hw.1.1 Hw.3.1 com.3 hw.3.2	Medio	$3_{.si1}$	$7_{.si1}$	$7_{.si1}$	$3_{.da1}$	$3_{.si}$
Datos [DA]	Datos en las BBDD internas	DA.1	hw1.5	Muy alto	$10_{.si}$	$9_{.lpo}$	$10_{.si}$	$9_{.da1}$	$10_{.si}$
	Datos de soporte y licencias	DA.2	Hw.1.5	Bajo	x	$3_{.lpo}$	x	$1_{.da1}$	x

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
	Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	DA.3	Hw.3.1 hw.3.2 hw1.1	Alto	7.olm	7.lpo	7.olm	3.da1	7.si
	Logs de servidores y clientes	DA.4	Hw.1.1 hw1.3 hw.1.4	Medio	3.si1	3.si1	4.crm1	8.crm1	4.crm1
	Backups de servidores y clientes	DA.5	Hw1.1	Alto	7.olm	7.lpo	7.olm	3.da1	7.si
	Datos departamentales (servidor de datos)	DA.6	Hw1.1 hw1.3 hw.1.4	Alto	7.olm	7.lpo	7.olm	3.da1	7.si
Red [COM]	Línea telefónica	COM.1	---	Bajo	x	x	x	3.da1	x
	Servicio de VoIP externo	COM.2	Ea.7 com.3 hw1.3 hw.1.4	Bajo	x	x	x	3.da1	x
	Servicio de acceso datos	COM.3	Ea.7	Muy Alto	9.da1	9.si1	9.da1	9.da1	9.da1
	Red inalámbrica	COM.4	Ea.7 com.3 hw1.3 hw.1.4	Bajo	3.si	x	x	x	8.crm 1
Servicios [SER]	Acceso remoto	SER.1	hw.2.2 com.3	Bajo	x	3.si1	x	1.da1	x
	Aplicaciones de control de intrusiones	SER.2	hw.2.2 com.3 hw1.3 hw.1.4	Medio	x	x	x	x	8.crm 1
	Aplicaciones internas de gestión	SER.3	com.3 hw.1.3 hw1.1 hw1.3 hw.1.4	Medio	x	7.olm 1	x	7.olm 1	x
	Correo electrónico	SER.4	hw.2.2 com.3 hw1.1 hw1.3 hw.1.4	Bajo	7.si	7.si	7.si	7.si	7.si
	Servicio de ficheros FTP	SER.5	hw.2.2 com.3 hw.1.1 hw1.3 hw.1.4	Bajo	7.si	7.lpo	7.si	5.olm	3.si

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
	Acceso a entorno Web Interno	SER.6	hw.2.2 com.3 hw.1.1 hw1.3 hw.1.4	Bajo	7.si	3.lpo	3.si	5.olm	3.olm
	Acceso a entorno Web externo	SER.7	hw.2.2 com.3 hw.2.1	Muy alto	10.sa	10.sa	9.da1	9.da1	9.da1
	Monitorización de servidores y servicios	SER.8	hw.X (todos) sw.X(todos)	Bajo	x	x	x	1.da1	x
	Navegación	SER.9	hw.1.2 com.3 hw2.2 hw1.3 hw.1.4	Bajo	3.si	3.si	x	1.po1	x
Equipamiento Auxiliar [EA]	Armario central de llaves (llavero)	EA.1	Ins.2 ea.7 ea.6	Medio	3.si	3.si	7.si	9.olm	7.si
	Fotocopiadoras (acceso por pin)	EA.2	Ins.2 Ins.3 ea.7	Bajo	3.si	3.si	1.lpo	1.da	1.lpo
	Ficheros de documentos (requiere llave)	EA.3	Ins.3	Bajo	3.si	1.lpo	1.lpo	3.da	3.olm
	Armario ignífugo (copias de seguridad + llave necesaria para acceso)	EA.4	Ins.1	Medio	3.si	7.si	7.lpo	7.olm	7.lpo
	Consumibles varios (cds, toners, etc)	EA.5	Ins.3	Bajo	x	x	x	3.da	x
	Sistemas de alimentación continua (UPS / SAI)	EA.6	Ins.1 ea.7	Alto	7.olm	7.olm	7.olm	7.da1	x
	Corriente eléctrica	EA.7	---	Muy alto	x	x	x	9.da1	x
	Elemento de aire acondicionado	EA.8	Ins.1 Ins.2 Ins.3 ea.7	Bajo	x	x	x	1.da	x
	Teléfonos móviles	EA.9	Com.1	Bajo	3.si	3.si	3.si	1.da	3.da
	Teléfonos fijos	EA.10	ea.7 com.3 com.1	Bajo	3.si	3.si	3.si	1.da	3.da

					ASPECTOS CRITICOS				
AMBITO	ACTIVO	NUMERO	DEPENDENCIA	VALOR	A	C	I	D	A
Personal [PE]	Director general	PE.1	---	Muy alto	9.si1	x	x	x	3.si1
	Subdirector (contabilidad y asesoría legal)	PE.2	---	Medio	9.si1	x	x	x	3.si1
	Responsable TIC	PE.3	---	Muy alto	9.si1	x	x	x	9.si1
	Responsable Marketing	PE.4	---	Bajo	3.si1	x	x	x	3.si1
	Personal TIC	PE.5	---	Muy alto	9.si1	x	x	x	9.si1
	Personal Marketing	PE.6	---	Bajo	3.si1	x	x	x	3.si1

Tabla 39 Dimensiones de seguridad - Tabla Resumen Valoración

6. Análisis de amenazas

Una vez hemos realizado el inventariado de los activos e identificados los riesgos sobre los mismos podemos proceder a analizar las amenazas que puedan afectarles.

Para poder identificar las amenazas utilizaremos la metodología MAGERIT para lo que haremos referencia al libro dos "Catálogo de Elementos" concretamente al punto 5. En este punto podremos ver una gran cantidad de amenazas ya definidas que pueden afectar a distintos tipos de elementos quedando en las siguientes familias:

- Desastres naturales: pueden ocurrir sin intervención humana.
- Amenazas de origen industrial: pueden ocurrir como accidentes.
- Errores y fallos no intencionados: fallos no intencionados por las personas.
- Ataques intencionados: ataques malintencionados por personas.

Desastres naturales

[N.1] Fuego [N.1] Fuego	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. Ver: EBIOS: 01- INCENDIO	

Tabla 40 Amenazas - Desastres naturales - fuego

[N.2] Daños por agua [N.2] Daños por agua	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

Tabla 41 Amenazas - Desastres naturales - Agua

[N.*] Desastres naturales [N.*] Desastres naturales	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras,... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Ver:** EBIOS: 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN	

Tabla 42 Amenazas - Desastres naturales - General

Amenazas de origen industrial

[I.1] Fuego [I.1] Fuego	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	

Tabla 43 Amenazas - Origen industrial- fuego

[I.2] Daños por agua [I.2] Daños por agua	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

Tabla 44 Amenazas - Origen industrial- Agua

[I.*] Desastres industriales [I.*] Desastres industriales	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 04 - SINIESTRO MAYOR	

Tabla 45 Amenazas - Origen industrial- General

[I.3] Contaminación mecánica [I.3] Contaminación mecánica	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 03 – CONTAMINACIÓN	

Tabla 46 Amenazas - Origen industrial- contaminación mecánica

[I.4] Contaminación electromagnética [I.4] Contaminación electromagnética	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

Tabla 47 Amenazas - Origen industrial - contaminación electromagnética

[I.5] Avería de origen físico o lógico [I.5] Avería de origen físico o lógico	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

Tabla 48 Amenazas - Origen industrial - Avería de origen físico

[I.6] Corte del suministro eléctrico [I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

Tabla 49 Amenazas - Origen industrial - corte de suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad [I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN	

Tabla 50 Amenazas - Origen industrial - condiciones inadecuadas

[I.8] Fallo de servicios de comunicaciones [I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	

Tabla 51 Amenazas - Origen industrial – Fallo de comunicaciones

[I.9] Interrupción de otros servicios y suministros esenciales [I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [EA] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: no disponible	

Tabla 52 Amenazas - Origen industrial - interrupción de servicios esenciales

[I.10] Degradación de los soportes de almacenamiento de la información [I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [DA] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: como consecuencia del paso del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

Tabla 53Amenazas - Origen industrial - Degradación de los soportes de almacenamiento

[I.11] Emanaciones electromagnéticas [I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés "Transient Electromagnetic Pulse Standard"). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS	

Tabla 54 Amenazas - Origen industrial - Emanaciones electromagnéticas

Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.1] Errores de los usuarios	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones • [DA] Datos	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

Tabla 55 Amenazas - Errores y fallos no intencionados – usuarios

[E.2] Errores del administrador [E.2] Errores del administrador	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones • [DA] Datos • [SER] Servicios	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	

Tabla 56 Amenazas - Errores y fallos no intencionados – administrador

[E.3] Errores de monitorización (log) [E.3] Errores de monitorización (log)	
Tipos de activos: • [DA] Datos	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: no disponible	

Tabla 57 Amenazas - Errores y fallos no intencionados – monitorización

[E.4] Errores de configuración [E.4] Errores de configuración	
Tipos de activos: • [DA] Datos	**Dimensiones:** 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

Tabla 58 Amenazas - Errores y fallos no intencionados - configuración

[E.7] Deficiencias en la organización Obsoleta. [E.7] Deficiencias en la organización	
Tipos de activos: • [PE] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible	

Tabla 59 Amenazas - Errores y fallos no intencionados - organización obsoleta

[E.8] Difusión de software dañino [E.8] Difusión de software dañino	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

Tabla 60 Amenazas - Errores y fallos no intencionados - difusión de software dañino

[E.9] Errores de [re-]encaminamiento [E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software • [SER] Servicios • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. Ver: EBIOS: no disponible	

Tabla 61 Amenazas - Errores y fallos no intencionados - error de encaminamiento

[E.10] Errores de secuencia [E.10] Errores de secuencia	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software • [SER] Servicios • [COM] redes de comunicaciones	Dimensiones: 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos. Ver: EBIOS: no disponible	

Tabla 62 Amenazas - Errores y fallos no intencionados - errores de secuencia

[E.15] Alteración accidental de la información [E.15] Alteración accidental de la información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Ver: EBIOS: no disponible	

Tabla 63 Amenazas - Errores y fallos no intencionados - alteración accidental de la información

[E.18] Destrucción de información [E.18] Destrucción de información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones • [DA] Datos • [SER] Servicios	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

Tabla 64 Amenazas - Errores y fallos no intencionados - destrucción de información

[E.19] Fugas de información [E.19] Fugas de información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. Ver: EBIOS: no disponible	

Tabla 65 Amenazas - Errores y fallos no intencionados - fugas de información

[E.20] Vulnerabilidades de los programas (software) [E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software	Dimensiones: 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Ver: EBIOS: no disponible	

Tabla 66 Amenazas - Errores y fallos no intencionados - vulnerabilidades

[E.21] Errores de mantenimiento / actualización de programas (software) [E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software	Dimensiones: 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. Ver: EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

Tabla 67 Amenazas - Errores y fallos no intencionados - errores de mantenimiento de software

[E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. Ver: EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

Tabla 68 Amenazas - Errores y fallos no intencionados - errores de mantenimiento de equipos

[E.24] Caída del sistema por agotamiento de recursos [E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [COM] Redes • [SER] Servicios	Dimensiones: 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

Tabla 69 Amenazas - Errores y fallos no intencionados - caída del sistema

[E.25] Pérdida de equipos [E.25] Robo	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Ver: EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

Tabla 70 Amenazas - Errores y fallos no intencionados - pérdida de equipos

[E.28] Indisponibilidad del personal [E.28] Indisponibilidad del personal	
Tipos de activos: • [PER] Personal	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... Ver: EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

Tabla 71 Amenazas - Errores y fallos no intencionados - indisponibilidad del personal

Ataques intencionados

[A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: • [DA] Datos	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: Ver: EBIOS: no disponible	

Tabla 72 Amenazas - Ataques intencionados - manipulación de los registros de actividad

[A.4] Manipulación de la configuración [A.4] Manipulación de la configuración	
Tipos de activos: • [DA] Datos	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

Tabla 73 Amenazas - Ataques intencionados - Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario [A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Ver: EBIOS: 40 - USURPACIÓN DE DERECHO	

Tabla 74Amenazas - Ataques intencionados - suplantación de identidad del usuario

[A.6] Abuso de privilegios de acceso [A.6] Abuso de privilegios de acceso	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Ver: EBIOS: 39 - ABUSO DE DERECHO	

Tabla 75 Amenazas - Ataques intencionados - Abuso de privilegios de acceso

[A.7] Uso no previsto [A.7] Uso no previsto	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. Ver: EBIOS: no disponible	

Tabla 76 Amenazas - Ataques intencionados - uso no previsto

[A.8] Difusión de software dañino [A.8] Difusión de software dañino	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software	Dimensiones: 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Ver: EBIOS: no disponible	

Tabla 77 Amenazas - Ataques intencionados - difusión de software dañino

[A.9] [Re-]encaminamiento de mensajes [A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software • [SER] Servicios • [COM] Redes	Dimensiones: 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. Ver: EBIOS: no disponible	

Tabla 78 Amenazas - Ataques intencionados - encaminamiento de mensajes

[A.10] Alteración de secuencia [A.10] Alteración de secuencia	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software • [SER] Servicios • [COM] Redes	Dimensiones: 1. [I] integridad
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. Ver: EBIOS: 36 - ALTERACIÓN DE DATOS	

Tabla 79 Amenazas - Ataques intencionados - alteración de secuencia

[A.11] Acceso no autorizado [A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

Tabla 80 Amenazas - Ataques intencionados - acceso no autorizado

[A.12] Análisis de tráfico [A.12] Análisis de tráfico	
Tipos de activos: • [COM] Redes	Dimensiones: 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. Ver: EBIOS: no disponible	

Tabla 81 Amenazas - Ataques intencionados - análisis de tráfico

[A.13] Repudio [A.13] Repudio	
Tipos de activos: • [SER] servicios • [DA] Datos	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. Ver: EBIOS: 41 - NEGACIÓN DE ACCIONES	

Tabla 82 Amenazas - Ataques intencionados - repudio

[A.14] Interceptación de información (escucha) [A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. Ver: EBIOS: 19 - ESCUCHA PASIVA	

Tabla 83 Amenazas - Ataques intencionados - intercepción de información

[A.15] Modificación deliberada de la información [A.15] Modificación deliberada de la información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

Tabla 84 Amenazas - Ataques intencionados - Modificación deliberada de la información

[A.18] Destrucción de información [A.18] Destrucción de información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios	Dimensiones: 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

Tabla 85 Amenazas - Ataques intencionados - Destrucción de información

[A.19] Divulgación de información [A.19] Revelación de información	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [COM] Redes • [INS] instalaciones • [DA] Datos • [SER] Servicios • [PER] personal interno	Dimensiones: 1. [C] confidencialidad
Descripción: revelación de información. Ver: EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

Tabla 86 Amenazas - Ataques intencionados - Divulgación de información

[A.22] Manipulación de programas [A.22] Manipulación de programas	
Tipos de activos: • [SW.1][SW.2] [SW.3] Software	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Ver: EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

Tabla 87 Amenazas - Ataques intencionados - manipulación de programas

[A.23] Manipulación de los equipos [A.22] Manipulación de los equipos	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SW.1][SW.2] [SW.3] Software • [EA] equipamiento auxiliar	Dimensiones: 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Ver: EBIOS: 25 - SABOTAJE DEL HARDWARE	

Tabla 88 Amenazas - Ataques intencionados - manipulación de equipos

[A.24] Denegación de servicio [A.24] Denegación de servicio	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SER] Servicios • [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

Tabla 89 Amenazas - Ataques intencionados - denegación de servicio

[A.25] Robo [A.25] Robo	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SER] Servicios • [COM] redes de comunicaciones • [EA] equipamiento auxiliar	**Dimensiones:** 3. [D] disponibilidad 4. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

Tabla 90 Amenazas - Ataques intencionados – robo

[A.26] Ataque destructivo [A.26] Ataque destructivo	
Tipos de activos: • [HW.1][HW.2][HW.3] equipos informáticos (hardware) • [SER] Servicios • [INS] Instalaciones • [EA] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. Ver: EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES	

Tabla 91 Amenazas - Ataques intencionados - ataque destructivo

[A.27] Ocupación enemiga [A.27] Ocupación enemiga	
Tipos de activos: [INS] Instalaciones	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. Ver: EBIOS: no disponible	

Tabla 92 Amenazas - Ataques intencionados - ocupación enemiga

[A.28] Indisponibilidad del personal [A.28] Indisponibilidad del personal	
Tipos de activos: • [PER] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ... Ver: EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

Tabla 93 Amenazas - Ataques intencionados - indisponibilidad del personal

[A.29] Extorsión [A.29] Extorsión	
Tipos de activos: • [PER] personal interno	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. Ver: EBIOS: no disponible	

Tabla 94 Amenazas - Ataques intencionados - extorsión

[A.30] Ingeniería social (picaresca) [A.30] Ingeniería social (picaresca)	
Tipos de activos: [PER] personal interno	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Ver: EBIOS: no disponible	

Tabla 95 Amenazas - Ataques intencionados - ingeniería social

Tal como hemos podido comprobar existen multitud de amenazas posibles para los activos de la empresa para lo que debemos de realizar una asociación de qué elementos son vulnerables a todos ellos. Como hemos podido comprobar hemos hecho parte de esa labor en cada uno de esos elementos pero ahora debemos de analizar el impacto según ACIDT que correspondería con:

- A: Autenticación
- C: Confidencialidad
- I: Integridad
- D: Disponibilidad
- T: Trazabilidad

De estos puntos llegar a hacer un análisis de todos los elementos identificador como inventario de riesgos asociados a sus amenazas para lo cual realizaremos las siguientes tablas y obtener en posteriores puntos el impacto de los riesgos sobre los activos.

En la documentación de la asignatura "sistemas de gestión de la seguridad informática" podemos ver en el documento "Análisis de riesgos" en la página 21 como se puede clasificar las vulnerabilidades:

Vulnerabilidad	Rango	Valor
Frecuencia Extrema	1 vez al día	1
Frecuencia Alta	1 vez cada 2 semanas	26/365=0.07
Frecuencia Media	1 vez cada 2 meses	6/365=0.016
Frecuencia Baja	1 vez cada 6 meses	2/365=0.005
Frecuencia Muy baja	1 vez al año	1/365=0.002

Tabla 96 Amenazas - vulnerabilidad por rango

En la página 22 del mismo documento podremos además la valoración en base al impacto que tiene en el activo.

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

Tabla 97 Amenazas - valor / impacto

A partir de la información que hemos indicado vamos a proceder a hacer un análisis de las amenazas que pueden afectar a los distintos activos de la organización. Para ello lo vamos a agrupar tal como lo hemos hecho previamente para facilitar su comprensión y poder postreramente realizar un análisis del impacto.

Personas

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Personal [PE]	Identificativo							
Director general	PE.1	A	0,07		20%	100%	20%	
Subdirector (contabilidad y asesoría legal)	PE.2							
Responsable TIC	PE.3							
Responsable Marketing	PE.4							
Personal TIC	PE.5							
Personal Marketing	PE.6							
Amenazas								
Deficiencia en la organización	E.7	M	0,016			50%		
Indisponibilidad del personal	E.28	A	0,07			100%		
Divulgación de información	E.19	M	0,016		20%			
Extorsión	A.29	MB	0,002		20%	20%	20%	
Ingeniería Social	A.30	MB	0,002		20%	20%	20%	

Tabla 98 Amenazas - Resumen Personas

Equipamiento auxiliar

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Equipamiento Auxiliar [EA]	Identificativo							
Armario central de llaves (llavero)	EA.1	M	0,016		75	100	75	
Fotocopiadoras (acceso por pin)	EA.2							
Ficheros de documentos (requiere llave)	EA.3							
Armario ignífugo (copias de seguridad + llave necesaria para acceso)	EA.4							
Consumibles varios (cds, tóner, etc.)	EA.5							
Sistemas de alimentación continua (UPS / SAI)	EA.6							
Corriente eléctrica	EA.7							
Elemento de aire acondicionado	EA.8							
Teléfonos móviles	EA.9							
Teléfonos fijos	EA.10							
Amenazas								
Fuego	N.1	MB	0,002			5%		
Daños por agua	N.2	MB	0,002			5%		
Fuego	I.1	MB	0,002			5%		
Daños por agua	I.2	MB	0,002			5%		
Contaminación mecánica	I.3	MB	0,002			5%		
Contaminación electromagnética	I.4	MB	0,002			5%		
Avería de origen físico o lógico	I.5	B	0,005			20%		
Corte del suministro eléctrico	I.6	B	0,005			20%		
Condiciones inadecuadas de Cº	I.7	B	0,005			20%		
Interrupción de suministro esencial	I.9	B	0,005			20%		
Emanaciones electromagnéticas	I.11	MB	0,002			20%		
Errores de los usuarios	E.1	M	0,016		50%	50%	50%	
Errores de los administradores	E.2	B	0,005		75%	75%	75%	
Alteración accidental de la información	E.15	B	0,005				75%	
Destrucción de información	E.18	M	0,016			100%		
Fugas de información	E.19	B	0,005			50%		
Errores de mantenimiento	E.23	B	0,005			50%	50%	
Perdida de equipos	E.25	B	0,005		50%	50%		
Acceso no autorizado	A.11	B	0,005		50%		50%	
Manipulación de los equipos	A.23	M	0,016		75%	75%		
Robo	A.25	M	0,016		75%	100%		
ataque destructivo	A.26	MB	0,002			100%		

Tabla 99 Amenazas - Resumen Equipamiento auxiliar

Servicios

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Servicios [SER]	Identificativo							
Acceso remoto	SER.1	B	0,005	100%	100%	100%	100%	100%
Aplicaciones de control de intrusiones	SER.2							
Aplicaciones internas de gestión	SER.3							
Correo electrónico	SER.4							
Servicio de ficheros FTP	SER.5							
Acceso a entorno Web Interno	SER.6							
Acceso a entorno Web externo	SER.7							
Monitorización de servidores y servicios	SER.8							
Navegación	SER.9							
Amenazas								
Errores de administrador	E.2	B	0,005		75%	100%	75%	
Errores de encaminamiento	E.9	B	0,005			50%		
Errores de secuencia	E.10	B	0,005				50%	
Alteración accidental de información	E.15	B	0,005				100%	
Destrucción de información	E.18	B	0,005			100%		
Fugas de información	E.19	B	0,005			50%		
Caída del sistema por agotamiento de recursos	E.24	MB	0,002			100%		
Suplantación de identidad	A.5	B	0,005	100%	75%		50%	
Abuso de privilegios	A.6	B	0,005		100%	75%	100%	
uso no previsto	A.7	MB	0,002		50%	50%	50%	
Re-encaminamiento de mensajes	A.9	B	0,005		50%			

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		Posibilidad	Valor	A	C	D	I	T
Alteración de secuencia	A.10	B	0,005				50%	
Acceso no autorizado	A.11	B	0,005		75%		75%	
Repudio	A.13	B	0,005					100%
Modificación deliberada de la información	A.15	MB	0,002				100%	
Destrucción de la información	A.18	B	0,005			100%		
Divulgación de información	A.19	B	0,005			50%		
Denegación de servicio	A.24	B	0,005			100%		
Robo	A.25	MB	0,002		100%	75%		
Ataque destructivo	A.26	MB	0,002			100%		

Tabla 100 Amenazas - Resumen Servicios

Red

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		Posibilidad	Valor	A	C	D	I	T
Red [COM]	Identificativo							
Línea telefónica	COM.1	M	0,016	100%	100%	100%	100%	
Servicio de VoIP externo	COM.2							
Servicio de acceso datos	COM.3							
Red inalámbrica	COM.4							
Amenazas								
Fallo de servicios de comunicación	I.8	B	0,005			100%		
Errores de encamaciones	E.9	B	0,005		100%			
Errores de secuencia	E.10	B	0,005				100%	
Caída de sistema por agotamiento de recursos	E.24	B	0,005			100%		
suplantación de identidad	A.5	B	0,005	100%	100%	50%		
abuso de privilegios	A.6	M	0,016		75%	50%	50%	
uso no previsto	A.7	MB	0,002		50%	50%	50%	
re encaminamiento de mensajes	A.9	MB	0,002		75%			
alteración de secuencia	A.10	MB	0,002				75%	
acceso no autorizado	A.11	MB	0,002		75%		50%	
análisis de trafico	A.12	M	0,016		100%			
interceptación de información	A.14	MB	0,002		100%			
modificación deliberada de la información	A.15	MB	0,002				100%	
destrucción de la información	A.18	MB	0,002			75%		
divulgación de información	A.19	MB	0,002		100%			
denegación de servicio	A.24	MB	0,002			75%		

Tabla 101 Amenazas - Resumen Red

Datos

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Datos [DA]	Identificativo							
Datos en las BBDD internas	DA.1	M	0,016	100%	100%	100%	100%	100%
Datos de soporte y licencias	DA.2							
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	DA.3							
Logs de servidores y clientes	DA.4							
Backups de servidores y clientes	DA.5							
Datos departamentales (servidor de datos)	DA.6							
Amenazas								
Errores de los usuarios	E.1	M	0,016		50%	75%	75%	
Errores de los administradores	E.2	B	0,005		75%	75%	75%	
Errores de monitorización	E.3	M	0,016					20%
Errores de configuración	E.4	B	0,005				50%	
Deficiencia en la organización	E.7	B	0,005			100%		
Alteración accidental de la información	E.15	B	0,005				75%	
Destrucción de la información	E.18	B	0,005			100%		
Fugas de la información	E.19	MB	0,002		100%			
Manipulación de los registros	A.4	MB	0,002					100%
Manipulación de la configuración	A.3	MB	0,002	75%	50%	75%		
Suplantación de la identidad de un usuario	A.5	B	0,005	100%	75%	50%		
Abuso de los privilegios	A.6	B	0,005		100%	50%	50%	
uso no previsto	A.7	MB	0,002		20%	20%	20%	
Repudio	A.13	MB	0,002					75%
Modificación deliberada de la informacion0	A.15	MB	0,002				100%	
Destrucción de la información	A.18	MB	0,002			100%		
Divulgación de la información	A.19	MB	0,002		100%			

Tabla 102 Amenazas - Resumen Datos

Software

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Aplicaciones [SW.1][SW.2][SW.3]	Identificativo							
Datos de las BBDD internas	SW.1.1	M	0,016	100%	100%	100%	100%	
Datos de soporte y licencias	SW.1.2							
Proxy inverso (Correo electrónico y acceso a aplicaciones internas)	SW.1.3							
SQL server 2013	SW.2.1							
Aplicación gestión de Backups	SW.2.2							
Aplicaciones internas (gestión y administración)	SW.2.3							
Antivirus corporativo	SW.2.4							
Servidor de ficheros	SW.2.5							
Servidor de DNS	SW.2.6							
Servidor de DHCP	SW.2.7							
Windows server 2012 (software y licencias de servidores internos)	SW.2.8							
Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido	SW.2.9							
Documentación electrónica	SW.2.10							
Office 2013	SW.3.1							
Windows 7 Professional	SW.3.2							
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	SW.3.3							
Amenazas								
Avería de origen físico o lógico	I.5	B	0,005			75%		
Emanaciones electromagnéticas	I.11	MB	0,002		100%			
Errores de usuarios	E.1	M	0,016		50%	75%	75%	
Errores de administradores	E.2	B	0,005		75%	75%	75%	

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		Posibilidad	Valor	A	C	D	I	T
Difusión de software dañino	E.8	MB	0,002		75%	75%	75%	
Errores de secuencia	E.10	MB	0,002		50%			
Alteración accedente de la información	E.15	M	0,016				100%	
Destrucción de la información	E.18	M	0,016			100%		
Fugas de la información	E.19	M	0,016		100%			
vulnerabilidades de los programas	E.20	B	0,005		75%	20%	75%	
Errores de mantenimiento de programas	E.21	B	0,005			75%	75%	
Errores de mantenimiento equipos	E.23	B	0,005			75%		
Perdida de equipos	E.25	MB	0,002		100%	100%		
suplantación de identidad de usuario	A.5	B	0,005	100%	50%	75%		
Abuso de los privilegios de acceso	A.6	B	0,005		100%	20%	20%	
uso no previsto	A.7	MB	0,002		20%	20%	20%	
Difusión de software dañino	A.8	MB	0,002		100%	100%	100%	
Re echamiento de mensajes	A.9	MB	0,002		50%			
Alteración de secuencia	A.10	MB	0,002				50%	
Acceso no autorizado	A.11	B	0,005		100%		50%	
Modificación deliberada de la información	A.15	B	0,005				100%	
Destrucción de la in formación	A.18	B	0,005			100%		
Divulgación de la información	A.19	B	0,005		75%			
Manipulación de la información	A.22	B	0,005		50%	50%	75%	
Manipulación de los equipos	A.23	MB	0,002		50%	50%		

Tabla 103 Amenazas - Resumen Software

Hardware

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		**Posibilidad**	**Valor**	**A**	**C**	**D**	**I**	**T**
Hardware [HW.1][HW.2][HW.3]	Identificativo							
Servidor de datos de oficina	HW.1.1	B	0,005	75%	100%	100%	100%	
Servidor proxy interno	HW.1.2							
DC oficina principal / DHCP / DNS / Printers	HW.1.3							
DC secundario	HW.1.4							
Servidores de BBDD (dos)	HW.1.5							
Switch gestionado	HW.1.6							
Servidor Web Externo	HW.2.1							
Firewall	HW.2.2							
Dos router balanceados	HW.2.3							
Servidor FTP externo	HW.2.4							
Proxy Inverso	HW.2.5							
Puestos de trabajo	HW.3.1							
Portátiles de trabajo	HW.3.2							
Impresoras	HW.3.3							
Teléfonos móviles de empresa	HW.3.4							
Teléfonos fijos de empresa	HW.3.5							
Cámara vigilancia	HW.3.6							
Amenazas								
Fuego	N.1	MB	0,002			100%		
Agua	N.2	MB	0,002			100%		
Fuego	I.1	MB	0,002			100%		
Agua	I.2	MB	0,002			100%		
Contaminación mecánica	I.3	MB	0,002			100%		
Contaminación electromagnética	I.4	MB	0,002			100%		
avería de origen físico o lógico	I.5	B	0,005			100%		
corte de suministro	I.6	MB	0,002			100%		
condiciones inadecuadas de temperatura y humedad	I.7	B	0,005			100%		
emanaciones electromagnéticas	I.11	MB	0,002			100%		
Errores de los usuarios	E.1	B	0,005		50%	75%	50%	
errores de los administradores	E.2	MB	0,002		50%	50%	50%	
alteración accidental de la información	E.15	B	0,005				50%	
destrucción de la información	E.18	MB	0,002			100%		

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		Posibilidad	Valor	A	C	D	I	T
fugas de la información	E.19	MB	0,002		100%			
Errores de mantenimiento	E.23	MB	0,002			75%	75%	
Caída de sistema por agotamiento de los recursos	E.24	MB	0,002			100%		
Perdida de equipos	E.25	B	0,005		100%	100%		
Suplantación de la identidad de un usuario	A.5	B	0,005	75%	50%	50%		
Abuso de privilegios	A.6	B	0,005		50%	20%	50%	
uso no previsto	A.7	B	0,005		20%	20%	20%	
Acceso no autorizado	A.11	B	0,005		50%	50%		
modificación deliberada de la información	A.15	B	0,005				100%	
destrucción de la información	A.18	MB	0,002			75%		
divulgación de la información	A.19	MB	0,002		75%			
Manipulación de equipos	A.23	B	0,005		75%	75%	75%	
Denegación de servicio	A.24	MB	0,002			100%		
Robo	A.25	B	0,005		100%	100%		
ataque destructivo	A.26	MB	0,002			100%		

Tabla 104 Amenazas - Resumen Hardware

Instalaciones

		FRECUENCIA		ASPECTOS CRITICOS				
NOMBRE ACTIVO		Posibilidad	Valor	A	C	D	I	T
Instalaciones [INS]	Identificativo							
Zona de CPD	INS.1	M	0,016	50%	75%	100%	50%	
Zona de oficinas	INS.2							
Zona de recepción	INS.3							
Amenazas								
Fuego	N.1	MB	0,002			100%		
Agua	N.2	MB	0,002			100%		
Fuego	I.1	MB	0,002			100%		
Agua	I.2	MB	0,002			100%		
Contaminación mecánica	I.3	MB	0,002			100%		
contaminación electromagnética	I.4	MB	0,002			100%		
avería de origen físico o lógico	I.5	B	0,005			100%		
Corte de suministro eléctrico	I.6	MB	0,002			100%		
condiciones inadecuada de temperatura o humedad	I.7	MB	0,002			100%		
Emanaciones electromagnéticas	I.11	MB	0,002			100%		
Errores de los usuarios	E.1	B	0,005		50%	50%	50%	
Errores de los administradores	E.2	B	0,005		50%	50%	50%	
Alteración accidental de la información	E.15	B	0,005				50%	
Destrucción de la información	E.18	B	0,005		50%			
Fugas de información	E.19	B	0,005		75%			
Suplantación de la identidad de usuario	A.5	B	0,005	50%	50%	50%		
Abuso de privilegios	A.6	M	0,016		50%	20%	20%	
uso no previsto	A.7	M	0,016		20%	20%	20%	
acceso no autorizado	A.11	B	0,005		50%		50%	
modificación deliberada de la información	A.15	B	0,005				20%	
Destrucción de la información	A.18	B	0,005			50%		
Divulgación de la información	A.19	B	0,005		75%			
Ataque destructivo	A.26	MB	0,002			50%		
Ocupación enemiga	A.27	MB	0,002		20%	50%		

Tabla 105 Amenazas - Resumen Instalaciones

7. Impacto potencial

Una vez hemos realizado las anteriores tablas ahora poder obtener el impacto potencial que puede suponer para la empresa la materialización de las amenazas sobre los activos que hemos indicado.

El impacto potencial se calcula de la siguiente forma:

Impacto potencial = valor del activo X valor del impacto

De modo que mediante la conjunción de las tablas y el uso de la fórmula para poder obtener el impacto potencial obtenemos la siguiente tabla:

			ASPECTOS CRITICOS					%IMPACTO					%IMPACTO POTENCIAL				
NOMBRE ACTIVO		VALOR	A	C	I	D	A	A	C	D	I	T	A	C	D	I	T
Zona de CPD	INS.1	Alto	5.lpo	9.si1	9.si1	9.da1	7.si1	50%	75%	100%	50%		2,50	6,75	9,00	4,50	
Zona de oficinas	INS.2	Alto	5.lpo	5.lpo	3.da	3.da	3.si						2,50	3,75	3,00	1,50	
Zona de recepción	INS.3	Bajo	5.lpo	5.lpo	1.da	1.da	1.si						2,50	3,75	1,00	0,50	
Servidor de datos de oficina	HW.1.1	Alto	7.si	7.da1	7.da1	3.da1	4.crm	75%	100%	100%	100%		5,25	7,00	3,00	7,00	
Servidor proxy interno	HW.1.2	Bajo	3.si	3.si	3.si	3.da1	4.crm						2,25	3,00	3,00	3,00	
DC oficina principal / DHCP / DNS / Printers	HW.1.3	Bajo	7.si	1.adm	5.adm	3.da1	4.crm						5,25	1,00	3,00	5,00	
DC secundario	HW.1.4	Bajo	7.si	1.adm	5.adm	3.da1	4.crm						5,25	1,00	3,00	5,00	
Servidores de BBDD (dos)	HW.1.5	Alto	9.si	5.adm	5.adm	9.da1	4.crm						6,75	5,00	9,00	5,00	
Switch gestionado	HW.1.6	Bajo	x	x	x	3.da1	x						x	x	x	x	
Servidor Web Externo	HW.2.1	Alto	7.si	7.da1	7.da1	9.da1	8.crm						5,25	7,00	9,00	7,00	
Firewall	HW.2.2	Muy Alto	9.da1	9.da1	9.da1	9.da1	9.da1						6,75	9,00	9,00	9,00	
Dos router balanceados	HW.2.3	Medio	5.da1	9.da1	5.da1	9.da1	5.da1						3,75	9,00	9,00	5,00	
Servidor FTP externo	HW.2.4	Bajo	3.si1	3.si1	3.si	3.da1	4.crm						2,25	3,00	3,00	3,00	
Proxy Inverso	HW.2.5	Bajo	7.si	3.si	1.si	3.da1	4.crm						5,25	3,00	3,00	1,00	
Puestos de trabajo	HW.3.1	Medio	7.si	7.si	3.olm	3.da1	4.crm						5,25	7,00	3,00	3,00	
Portátiles de trabajo	HW.3.2	Medio	7.si	7.si	3.olm	3.da1	4.crm						5,25	7,00	3,00	3,00	
Impresoras	HW.3.3	Bajo	3.si	x	1.olm	1.da1	x						2,25		1,00	1,00	
Teléfonos móviles de empresa	HW.3.4	Bajo	3.olm	3.olm	3.olm	1.da1	3.si						2,25	3,00	1,00	3,00	
Teléfonos fijos de empresa	HW.3.5	Bajo	3.olm	3.olm	3.olm	1.da1	3.si						2,25	3,00	1,00	3,00	

			ASPECTOS CRITICOS					%IMPACTO					%IMPACTO POTENCIAL				
NOMBRE ACTIVO		VALOR	A	C	I	D	A	A	C	D	I	T	A	C	D	I	T
Cámara vigilancia	HW.3.6	Medio	3.olm	3.olm	3.olm	4.crm	3.si						2,25	3,00	4,00	3,00	
Datos de las BBDD internas	SW.1.1	Muy Alto	10.si	9.lpo	10.si	9.da1	10.si						10,00	9,00	9,00	10	
Datos de soporte y licencias	SW.1.2	Bajo	x	x	x	1.olm	x								1,00		
Proxy inverso (Correo electrónico y acceso a aplicaciones internas)	SW.1.3	Bajo	3.si1	7.lpo	3.si1	1.da	4.crm						3,00	7,00	1,00	3	
SQL server 2013	SW.2.1	Bajo	7.si1	3.si1	7.si1	7.si1	7.si1						7,00	3,00	7,00	7	
Aplicación gestión de Backups	SW.2.2	Bajo	3.si1	3.si1	3.si1	5.olm	7.si1						3,00	3,00	5,00	3	
Aplicaciones internas (gestión y administración)	SW.2.3	Alto	5.si	7.lpo	5.si	5.olm	4.crm						5,00	7,00	5,00	5	
Antivirus corporativo	SW.2.4	Bajo	3.si1	3.si1	3.si1	5.olm	4.crm						3,00	3,00		3	
Servidor de ficheros	SW.2.5	Bajo	3.si1	7.lpo	3.si1	5.olm	4.crm						3,00	7,00	5,00	3	
Servidor de DNS	SW.2.6	Bajo	3.si	3.si	3.si	7.si	3.si						3,00	3,00	7,00	3	
Servidor de DHCP	SW.2.7	Bajo	3.si	3.si	3.si	7.si	3.si	100 %	100%	100%	100%		3,00	3,00	7,00		
Windows server 2012 (software y licencias de servidores internos)	SW.2.8	Medio	7.si	7.si	7.si	3.si	8.crm						7,00	7,00	3,00	7	
Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido	SW.2.9	Medio	7.si	7.si	7.si	3.si	8.crm						7,00	7,00	3,00	7	
Documentación electrónica	SW.2.10	Alto	7.si	7.lpo	7.si	5.olm	8.crm						7,00	7,00	5,00	7	
Office 2013	SW.3.1	Bajo	3.si1	3.si1	3.si1	1.da1	x						3,00	3,00	1,00	3	
Windows 7 Professional	SW.3.2	Medio	3.si1	3.si1	7.si1	3.da1	3.si						3,00	3,00	3,00	7	
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	SW.3.3	Medio	3.si1	7.si1	7.si1	3.da1	3.si						3,00	7,00	3,00	7	
Datos en las BBDD internas	DA.1	Muy alto	10.si	9.lpo	10.si	9.da1	10.si	100 %	100%	100%	100%	10	10,00	9,00	9,00	10,00	10,00

			ASPECTOS CRITICOS					%IMPACTO					%IMPACTO POTENCIAL				
NOMBRE ACTIVO		VALOR	A	C	I	D	A	A	C	D	I	T	A	C	D	I	T
												0%					
Datos de soporte y licencias	DA.2	Bajo	x	3.lpo	x	1.da1	x							3,00	1,00		
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	DA.3	Alto	7.olm	7.lpo	7.olm	3.da1	7.si						7,00	7,00	3,00	7,00	7,00
Logs de servidores y clientes	DA.4	Medio	3.si1	3.si1	4.crm1	8.crm1	4.crm1						3,00	3,00	8,00	4,00	4,00
Backups de servidores y clientes	DA.5	Alto	7.olm	7.lpo	7.olm	3.da1	7.si						7,00	7,00	3,00	7,00	7,00
Datos departamentales (servidor de datos)	DA.6	Alto	7.olm	7.lpo	7.olm	3.da1	7.si							7,00	3,00	7,00	
Línea telefónica	COM.1	Bajo	x	x	x	3.da1	x	100%	100%	100%	100%				3,00		
Servicio de VoIP externo	COM.2	Bajo	x	x	x	3.da1	x								3,00		
Servicio de acceso datos	COM.3	Muy Alto	9.da1	9.si1	9.da1	9.da1	9.da1						9,00	9,00	9,00	9,00	
Red inalámbrica	COM.4	Bajo	3.si	x	x	x	8.crm1						3,00				
Acceso remoto	SER.1	Bajo	x	3.si1	x	1.da1	x	100%	100%	100%	100%	100%		3,00			
Aplicaciones de control de intrusiones	SER.2	Medio	x	x	x	x	8.crm1										8,00
Aplicaciones internas de gestión	SER.3	Medio	x	7.olm1	x	7.olm1	x							7,00			
Correo electrónico	SER.4	Bajo	7.si	7.si	7.si	7.si	7.si						7,00	7,00	7,00	7,00	7,00
Servicio de ficheros FTP	SER.5	Bajo	7.si	7.lpo	7.si	5.olm	3.si						7,00	7,00	7,00	7,00	3,00
Acceso a entorno Web Interno	SER.6	Bajo	7.si	3.lpo	3.si	5.olm	3.olm						7,00	3,00	7,00	3,00	3,00
Acceso a entorno Web externo	SER.7	Muy alto	10.sa	10.sa	9.da1	9.da1	9.da1						10,00	10,00	10,00	9,00	9,00
Monitorización de servidores y servicios	SER.8	Bajo	x	x	x	1.da1	x										
Navegación	SER.9	Bajo	3.si	3.si	x	1.po1	x						3,00	3,00	3,00		
Armario central de llaves (llavero)	EA.1	Medio	3.si	3.si	7.si	9.olm	7.si							2,25	9,00	5,25	
Fotocopiadoras (acceso por pin)	EA.2	Bajo	3.si	3.si	1.lpo	1.da	1.lpo		75%	100%	75%			2,25	1,00	0,75	

			ASPECTOS CRITICOS					%IMPACTO					%IMPACTO POTENCIAL				
NOMBRE ACTIVO		VALOR	A	C	I	D	A	A	C	D	I	T	A	C	D	I	T
Ficheros de documentos (requiere llave)	EA.3	Bajo	3.si	1.lpo	1.lpo	3.da	3.olm							0,00	3,00	0,75	
Armario ignífugo (copias de seguridad + llave necesaria para acceso)	EA.4	Medio	3.si	7.si	7.lpo	7.olm	7.lpo							0,75	7,00	5,25	
Consumibles varios (cds, toners, etc)	EA.5	Bajo	x	x	x	3.da	x								3,00		
Sistemas de alimentación continua (UPS / SAI)	EA.6	Alto	7.olm	7.olm	7.olm	7.da1	x							5,25	7,00	5,25	
Corriente eléctrica	EA.7	Muy alto	x	x	x	9.da1	x								9,00		
Elemento de aire acondicionado	EA.8	Bajo	x	x	x	1.da	x								1,00		
Teléfonos móviles	EA.9	Bajo	3.si	3.si	3.si	1.da	3.da							2,25	1,00	2,25	
Teléfonos fijos	EA.10	Bajo	3.si	3.si	3.si	1.da	3.da							2,25	1,00	2,25	
Director general	PE.1	Muy alto	9.si1	x	x	x	3.si1										
Subdirector (contabilidad y asesoría legal)	PE.2	Medio	9.si1	x	x	x	3.si1										
Responsable TIC	PE.3	Muy alto	9.si1	x	x	x	9.si1		20%	100%	20%						
Responsable Marketing	PE.4	Bajo	3.si1	x	x	x	3.si1										
Personal TIC	PE.5	Muy alto	9.si1	x	x	x	9.si1										
Personal Marketing	PE.6	Bajo	3.si1	x	x	x	3.si1										

Tabla 106 Impacto potencial ACDIT

8. Nivel de riesgo aceptable y riesgo residual

Una vez hemos definido los puntos anteriores debemos de designar una límite a partir del cual podamos decidir si asumir o no un riesgo para determinado activo. De este modo podemos aplicar controles que reduzcan los riesgos sobre los mismos.

Para poder establecer el riesgo utilizaremos la siguiente fórmula:

Riesgo = impacto potencial X Frecuencia

Habiendo obtenido previamente el impacto potencial utilizando la frecuencia podemos entonces obtener los riesgos de los distintos activos. Si recordamos anteriormente habíamos indicado un valor para la frecuencia en base al número de días del año y el número de veces que se puede producir cierta situación. En nuestro caso ***WebConsulting*** ha indicado que como máximo asume valores medios con lo que cualquier elemento valorado como ***ALTA*** debería de ser atendido que en nuestro caso serían valores superiores a 0.07.

Obteniendo la siguiente tabla:

				FRECUENCIA	%IMPACTO POTENCIAL					RIESGO				
NOMBRE ACTIVO		VALOR	Posibilidad	Valor	A	C	D	I	T	A	C	D	I	T
Zona de CPD	INS.1	Alto	M	0,016	2,50	6,75	9,00	4,50		0,04	0,11	0,14	0,07	0,00
Zona de oficinas	INS.2	Alto		0,016	2,50	3,75	3,00	1,50		0,04	0,06	0,05	0,02	0,00
Zona de recepción	INS.3	Bajo		0,016	2,50	3,75	1,00	0,50		0,04	0,06	0,02	0,01	0,00
Servidor de datos de oficina	HW.1.1	Alto	B	0,005	5,25	7,00	3,00	7,00		0,03	0,04	0,02	0,04	0,00
Servidor proxy interno	HW.1.2	Bajo		0,005	2,25	3,00	3,00	3,00		0,01	0,02	0,02	0,02	0,00
DC oficina principal / DHCP / DNS / Printers	HW.1.3	Bajo		0,005	5,25	1,00	3,00	5,00		0,03	0,01	0,02	0,03	0,00
DC secundario	HW.1.4	Bajo		0,005	5,25	1,00	3,00	5,00		0,03	0,01	0,02	0,03	0,00
Servidores de BBDD (dos)	HW.1.5	Alto		0,005	6,75	5,00	9,00	5,00		0,03	0,03	0,05	0,03	0,00
Switch gestionado	HW.1.6	Bajo		0,005						0,00	0,00	0,00	0,00	0,00
Servidor Web Externo	HW.2.1	Alto		0,005	5,25	7,00	9,00	7,00		0,03	0,04	0,05	0,04	0,00
Firewall	HW.2.2	Muy Alto		0,005	6,75	9,00	9,00	9,00		0,03	0,05	0,05	0,05	0,00
Dos router balanceados	HW.2.3	Medio		0,005	3,75	9,00	9,00	5,00		0,02	0,05	0,05	0,03	0,00

				FRECUENCIA	%IMPACTO POTENCIAL					RIESGO				
NOMBRE ACTIVO		VALOR	Posibilidad	Valor	A	C	D	I	T	A	C	D	I	T
Servidor FTP externo	HW.2.4	Bajo		0,005	2,25	3,00	3,00	3,00		0,01	0,02	0,02	0,02	0,00
Proxy Inverso	HW.2.5	Bajo		0,005	5,25	3,00	3,00	1,00		0,03	0,02	0,02	0,01	0,00
Puestos de trabajo	HW.3.1	Medio		0,005	5,25	7,00	3,00	3,00		0,03	0,04	0,02	0,02	0,00
Portátiles de trabajo	HW.3.2	Medio		0,005	5,25	7,00	3,00	3,00		0,03	0,04	0,02	0,02	0,00
Impresoras	HW.3.3	Bajo		0,005	2,25		1,00	1,00		0,01	0,00	0,01	0,01	0,00
Teléfonos móviles de empresa	HW.3.4	Bajo		0,005	2,25	3,00	1,00	3,00		0,01	0,02	0,01	0,02	0,00
Teléfonos fijos de empresa	HW.3.5	Bajo		0,005	2,25	3,00	1,00	3,00		0,01	0,02	0,01	0,02	0,00
Cámara vigilancia	HW.3.6	Medio		0,005	2,25	3,00	4,00	3,00		0,01	0,02	0,02	0,02	0,00
Datos de las BBDD internas	SW.1.1	Muy Alto		0,016	10,00	9,00	9,00	10		0,16	0,14	0,14	0,16	0,00
Datos de soporte y licencias	SW.1.2	Bajo		0,016			1,00			0,00	0,00	0,02	0,00	0,00
Proxy inverso (Correo electrónico y acceso a aplicaciones internas)	SW.1.3	Bajo		0,016	3,00	7,00	1,00	3		0,05	0,11	0,02	0,05	0,00
SQL server 2013	SW.2.1	Bajo		0,016	7,00	3,00	7,00	7		0,11	0,05	0,11	0,11	0,00
Aplicación gestión de backups	SW.2.2	Bajo		0,016	3,00	3,00	5,00	3		0,05	0,05	0,08	0,05	0,00
Aplicaciones internas (gestión y administración)	SW.2.3	Alto	M	0,016	5,00	7,00	5,00	5		0,08	0,11	0,08	0,08	0,00
Antivirus corporativo	SW.2.4	Bajo		0,016	3,00	3,00		3		0,05	0,05	0,00	0,05	0,00
Servidor de ficheros	SW.2.5	Bajo		0,016	3,00	7,00	5,00	3		0,05	0,11	0,08	0,05	0,00
Servidor de DNS	SW.2.6	Bajo		0,016	3,00	3,00	7,00	3		0,05	0,05	0,11	0,05	0,00
Servidor de DHCP	SW.2.7	Bajo		0,016	3,00	3,00	7,00			0,05	0,05	0,11	0,00	0,00
Windows server 2012 (software y licencias de	SW.2.8	Medio		0,016	7,00	7,00	3,00	7		0,11	0,11	0,05	0,11	0,00

				FRECUENCIA	%IMPACTO POTENCIAL					RIESGO				
NOMBRE ACTIVO		VALOR	Posibilidad	Valor	A	C	D	I	T	A	C	D	I	T
servidores internos)														
Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido	SW.2.9	Medio		0,016	7,00	7,00	3,00	7		0,11	0,11	0,05	0,11	0,00
Documentación electrónica	SW.2.10	Alto		0,016	7,00	7,00	5,00	7		0,11	0,11	0,08	0,11	0,00
Office 2013	SW.3.1	Bajo		0,016	3,00	3,00	1,00	3		0,05	0,05	0,02	0,05	0,00
Windows 7 Professional	SW.3.2	Medio		0,016	3,00	3,00	3,00	7		0,05	0,05	0,05	0,11	0,00
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	SW.3.3	Medio		0,016	3,00	7,00	3,00	7		0,05	0,11	0,05	0,11	0,00
Datos en las BBDD internas	DA.1	Muy alto		0,016	10,00	9,00	9,00	10,00	10,00	0,16	0,14	0,14	0,16	0,16
Datos de soporte y licencias	DA.2	Bajo		0,016		3,00	1,00			0,00	0,05	0,02	0,00	0,00
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	DA.3	Alto	M	0,016	7,00	7,00	3,00	7,00	7,00	0,11	0,11	0,05	0,11	0,11
Logs de servidores y clientes	DA.4	Medio		0,016	3,00	3,00	8,00	4,00	4,00	0,05	0,05	0,13	0,06	0,06
Backups de servidores y clientes	DA.5	Alto		0,016	7,00	7,00	3,00	7,00	7,00	0,11	0,11	0,05	0,11	0,11
Datos departamentales (servidor de datos)	DA.6	Alto		0,016		7,00	3,00	7,00		0,00	0,11	0,05	0,11	0,00

				FRECUENCIA	%IMPACTO POTENCIAL					RIESGO				
NOMBRE ACTIVO		VALOR	Posibilidad	Valor	A	C	D	I	T	A	C	D	I	T
Línea telefónica	COM.1	Bajo	M	0,016			3,00			0,00	0,00	0,05	0,00	0,00
Servicio de VoIP externo	COM.2	Bajo		0,016			3,00			0,00	0,00	0,05	0,00	0,00
Servicio de acceso datos	COM.3	Muy Alto		0,016	9,00	9,00	9,00	9,00		0,14	0,14	0,14	0,14	0,00
Red inalámbrica	COM.4	Bajo		0,016	3,00					0,05	0,00	0,00	0,00	0,00
Acceso remoto	SER.1	Bajo	B	0,005		3,00				0,00	0,02	0,00	0,00	0,00
Aplicaciones de control de intrusiones	SER.2	Medio		0,005					8,00	0,00	0,00	0,00	0,00	0,04
Aplicaciones internas de gestión	SER.3	Medio		0,005		7,00				0,00	0,04	0,00	0,00	0,00
Correo electrónico	SER.4	Bajo		0,005	7,00	7,00	7,00	7,00	7,00	0,04	0,04	0,04	0,04	0,04
Servicio de ficheros FTP	SER.5	Bajo		0,005	7,00	7,00	7,00	7,00	3,00	0,04	0,04	0,04	0,04	0,02
Acceso a entorno Web Interno	SER.6	Bajo		0,005	7,00	3,00	7,00	3,00	3,00	0,04	0,02	0,04	0,02	0,02
Acceso a entorno Web externo	SER.7	Muy alto		0,005	10,00	10,00	10,00	9,00	9,00	0,05	0,05	0,05	0,05	0,05
Monitorización de servidores y servicios	SER.8	Bajo		0,005						0,00	0,00	0,00	0,00	0,00
Navegación	SER.9	Bajo		0,005	3,00	3,00	3,00			0,02	0,02	0,02	0,00	0,00
Armario central de llaves (llavero)	EA.1	Medio	M	0,016		2,25	9,00	5,25		0,00	0,04	0,14	0,08	0,00
Fotocopiadoras (acceso por pin)	EA.2	Bajo		0,016		2,25	1,00	0,75		0,00	0,04	0,02	0,01	0,00
Ficheros de documentos (requiere llave)	EA.3	Bajo		0,016		0,00	3,00	0,75		0,00	0,00	0,05	0,01	0,00

				FRECUENCIA	%IMPACTO POTENCIAL					RIESGO				
NOMBRE ACTIVO		VALOR	Posibilidad	Valor	A	C	D	I	T	A	C	D	I	T
Armario ignífugo (copias de seguridad + llave necesaria para acceso)	EA.4	Medio		0,016		0,75	7,00	5,25		0,00	0,01	0,11	0,08	0,00
Consumibles varios (cds, toners, etc)	EA.5	Bajo		0,016			3,00			0,00	0,00	0,05	0,00	0,00
Sistemas de alimentación continua (UPS / SAI)	EA.6	Alto		0,016		5,25	7,00	5,25		0,00	0,08	0,11	0,08	0,00
Corriente eléctrica	EA.7	Muy alto		0,016			9,00			0,00	0,00	0,14	0,00	0,00
Elemento de aire acondicionado	EA.8	Bajo		0,016			1,00			0,00	0,00	0,02	0,00	0,00
Teléfonos móviles	EA.9	Bajo		0,016		2,25	1,00	2,25		0,00	0,04	0,02	0,04	0,00
Teléfonos fijos	EA.10	Bajo		0,016		2,25	1,00	2,25		0,00	0,04	0,02	0,04	0,00
Director general	PE.1	Muy alto	A	0,07						0,00	0,00	0,00	0,00	0,00
Subdirector (contabilidad y asesoría legal)	PE.2	Medio		0,07						0,00	0,00	0,00	0,00	0,00
Responsable TIC	PE.3	Muy alto		0,07						0,00	0,00	0,00	0,00	0,00
Responsable Marketing	PE.4	Bajo		0,07						0,00	0,00	0,00	0,00	0,00
Personal TIC	PE.5	Muy alto		0,07						0,00	0,00	0,00	0,00	0,00
Personal Marketing	PE.6	Bajo		0,07						0,00	0,00	0,00	0,00	0,00

Tabla 107 nivel de riesgo aceptable y riesgo residual

9. Resultados

Tal como hemos podido ver tener elementos que deben de tomarse en consideración en base a las decisiones que ha tomado WebConsulting y tratar de paliar los riesgos sobre ciertos elementos que inciden directamente en sus activos del negocio.

En la tabla previa la empresa tiene una gran dependencia de ciertas máquinas y operativas que deben de revisar para poder reducir los riesgos. Ya sea mediante la contratación de nuevos elementos, generación de proyectos o mediante procedimentación estricta.

			RIESGO				
NOMBRE ACTIVO		VALOR	A	C	D	I	T
Zona de CPD	INS.1	Alto	0,04	0,11	0,14	0,07	0,00
Datos de las BBDD internas	SW.1.1	Muy Alto	0,16	0,14	0,14	0,16	0,00
Proxy inverso (Correo electrónico y acceso a aplicaciones internas)	SW.1.3	Bajo	0,05	0,11	0,02	0,05	0,00
SQL server 2013	SW.2.1	Bajo	0,11	0,05	0,11	0,11	0,00
Aplicación gestión de Backups	SW.2.2	Bajo	0,05	0,05	0,08	0,05	0,00
Aplicaciones internas (gestión y administración)	SW.2.3	Alto	0,08	0,11	0,08	0,08	0,00
Servidor de ficheros	SW.2.5	Bajo	0,05	0,11	0,08	0,05	0,00
Windows server 2012 (software y licencias de servidores internos)	SW.2.8	Medio	0,11	0,11	0,05	0,11	0,00
Debian 7.8 (servidores Web, proxy inverso y FTP) + software libre incluido	SW.2.9	Medio	0,11	0,11	0,05	0,11	0,00
Documentación electrónica	SW.2.10	Alto	0,11	0,11	0,08	0,11	0,00
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	SW.3.3	Medio	0,05	0,11	0,05	0,11	0,00
Datos en las BBDD internas	DA.1	Muy alto	0,16	0,14	0,14	0,16	0,16
Clientes de aplicaciones internas (incluyendo acceso Web si requiere licencia propia)	DA.3	Alto	0,11	0,11	0,05	0,11	0,11
Backups de servidores y clientes	DA.5	Alto	0,11	0,11	0,05	0,11	0,11
Datos departamentales (servidor de datos)	DA.6	Alto	0,00	0,11	0,05	0,11	0,00
Servicio de acceso datos	COM.3	Muy Alto	0,14	0,14	0,14	0,14	0,00
Armario central de llaves (llavero)	EA.1	Medio	0,00	0,04	0,14	0,08	0,00
Armario ignífugo (copias de seguridad + llave necesaria para acceso)	EA.4	Medio	0,00	0,01	0,11	0,08	0,00
Sistemas de alimentación continua (UPS / SAI)	EA.6	Alto	0,00	0,08	0,11	0,08	0,00
Corriente eléctrica	EA.7	Muy alto	0,00	0,00	0,14	0,00	0,00

Tabla 108 Resumen de riesgo por activos

Debiendo enfocarse principalmente en:

- Datos de las BBDD internas (Software y los datos)
- Servicio de acceso a datos
- Documentación electrónica
- Corriente eléctrica
- Gestión de los Backups

Propuestas de proyectos

1. Introducción

En esta fase vamos a realizar la presentación de proyectos que tendrán un impacto en el riesgo asociado de los distintos elementos que hemos indicado en la fase previa. La idea es disminuir dicho riesgo asociado en base a la urgencia de los mismos

2. Propuestas de proyectos

Proyecto 1: Mejora en mantenimiento eléctrico del CPD

Responsable: Departamento de Sistemas
Prioridad de proyecto: Alta
Objetivo:

- Mejorar el flujo eléctrico del CPD para garantizar un mayor porcentaje de disponibilidad de los sistemas que dependen del fluido eléctrico.
- Mejora del apagado ordenado del entorno informático en caso de pérdida del fluido eléctrico de forma completa.

Descripción:

Se ha podido comprobar que actualmente hay una dependencia muy grande del Core de negocio de la empresa con respecto a la disponibilidad del entorno de CPD y los servicios de la información configurados en el mismo. Por esto mismo se quiere realizar un estudio en dos partes.

Parte 1

- Revisión de sistema eléctrico actual
- Adquisición de material si fuese necesario para poder admitir una segunda toma de tensión eléctrica.
- Duplicar las regletas del entorno para poder separar las fuentes de alimentación con dos PDUs.

Parte 2

- Cálculo de potencia requerida por los servidores para mantenerlos activos durante 10 minutos
- Consultar posibilidades con el resto de empresas del edificio para obtener un generador para todas las empresas. Comprobar existencia del mismo y precio de contratación de conexión
- Adquisición de sistema de energía ininterrumpido e instalación del mismo si falla el paso previo.
- Configuración del sistema de energía y generación de documentación ante incidentes.

Motivación:

Mejora de los resultados obtenido en el análisis de riesgos de la fase 3

Controles:

Estadísticas mensuales de disponibilidad de elementos
Pruebas anuales de simulacro de caída de líneas principales
Documentación y mejora de la misma tras simulacros

Tiempo: 3 *meses*

Coste: Fase 1 (Potencia eléctrica) / Pago mensual + Fase 2 (Material contingencia)
Fase 1 → Incremento factura eléctrica actual *2
Fase 2→ 2000 € (instalación incluida)

Proyecto 2: Mejora de acceso de datos de Internet

Responsable: Responsable de sistemas

Prioridad del proyecto: Alta

Objetivo:

- Mejora disponibilidad de servicios publicados en la red al comprobar que existe redundancia de HW pero no de línea de Backups o secundaria para mantener el servicio.

Descripción:

Tras una análisis del entorno de red se ha visto que la infraestructura HW es buena y está redundada pero se confirma que no está correctamente dimensionado el entorno de acceso a Internet. Es por esto que se va a proceder a la adquisición de una segunda línea de datos a través de otro proveedor de Internet distinto al actual. De esta forma se conseguiría una redundancia de acceso a la red externa disminuyendo posibles problemas de los ISP. Se ha decidido que este punto es importante ya que el Core del negocio de la empresa se basa en los servicios informáticos a través de su propia infraestructura Web.

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Disponibilidad de los elementos
- Pruebas semestrales de caída de línea

Tiempo: 2 mes

Coste: 1500 € incluyendo mano de obra y material

Proyecto 3: Plan de contingencia de datos - Backups y Restores

Responsable: Responsable de sistemas
Prioridad del proyecto: Alta
Objetivo:

- Mejora de contingencia de datos de los servidores
- Reducción en los tiempos de restauración de datos en caso de necesidad

Descripción:

Los servidores actualmente disponen de información de alta importancia para la empresa, ya sea en formato BBDD o documentación electrónica. Además por requerimientos legales se necesita mantener la información de algunos servidores incluyendo logs durante largos periodos de tiempo. Por ello se ha optado por la realización de un plan en dos fases que será el siguiente.

Fase 1 - centralización de copias

- Centralización de copias de seguridad de configuración de distintos servidores
- Centralización de Logs de distintos elementos (configuración de copias)
    - Especial auditorías y lopd

Fase 2 - librería de cintas

- Adquisición de librería de cinta con dos drive
- Adquisición de cintas necesarias para un año (52 cintas para copias semanales, 1 anual y 12 mensuales)
- Configuración de la librería de cintas y software de gestión para su uso
- Distribución de clientes en los servidores objetivo de las copias y configuración de los recursos que requieran Backups.
- Pruebas y puesta en marcha.
- Documentación para el departamento de sistemas de ciclo de Backups

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Restauración de la información de forma semanal
- Informe de Backups y Restores éxito / fallo

Tiempo: 4 meses

Coste: 3000€ el hardware / 600 € consumibles (mano de obra incluido en el proceso)

Proyecto 4: Plan de clasificación de la información y tratamiento del mismo

Responsable: Responsable de sistemas y Dirección

Prioridad del proyecto: Media

Objetivo:

- Mejorar el tratamiento de los datos almacenados en los servidores y el acceso a los mismos. Cumplimiento de normativas de seguridad y auditoría de acceso a los datos.

Descripción:

Se ha comprobado que actualmente la empresa no está realizando una clasificación de la información de forma estructurada. Por esto mismo se propone un proyecto de re clasificación de la información en base a distintos niveles de seguridad en base a grupos de directorio activo que definan los permisos de los usuarios y departamentos a los datos de los servidores. Además se quiere controlar el acceso a la información que esté categorizada como "sensible" para la empresa para lo que se plantea habilitar la auditoría de acceso y modificaciones de los datos almacenados en servidores de ficheros y BBDD.

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Revisión anual de documentación de recursos informáticos
- Revisión semestral de infracciones en acceso a la información

Tiempo: 3 meses

Coste: 3000€ (equipo dinamización y asesoría externa incluida)

Proyecto 5: Acceso seguro a la información externa / interna

Responsable: Responsable de sistemas

Prioridad del proyecto: Media

Objetivo:

- Mejorar la seguridad de las comunicaciones externas a servicios internos mediante el uso de certificados y tunelización de las comunicaciones
- Mejorar la seguridad de las comunicaciones internas entre puestos de trabajo y servidores con información sensible

Descripción:

Se ha comprobado que actualmente se está utilizando comunicaciones cifrados susceptibles de ser víctimas de un ataque denominado *Man In The Middle* el cual realiza la imperforación de origen y destino pudiendo descifrar el contenido de la comunicación sin que estos tengan conocimiento de estar siendo interceptados. Para ello se propone lo siguiente:

- Creación de una entidad certificadora interna según especificaciones de Microsoft
- Uso de certificados con mayor cifrado en las páginas web externas (renovación de actuales certificados)
- Uso de certificados entre el entorno de la DMZ y la intranet
- Introducción de certificados firmados por la CA interna en los terminales de acceso al correo electrónico.
- Mejora en las conexiones RDP internas mediante la instalación de certificados de máquina y el uso de SSL en las comunicaciones de acceso remoto
- Utilización de certificados generados con la CA interna para el acceso a entornos WEB desarrollados internamente para securizar el entorno.
- Forzar el uso de HTTPS en todos los entornos que sea posible

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Revisión de logs externos
- Revisión de logs internos

Tiempo: 2 mes

Coste: 2000 € certificados externos + 500 € gestión interna + 500 € auditoría posterior

Proyecto 6: Limitación de permisos en los puestos de trabajo para los usuarios

Responsable: Responsable de sistemas y técnicos asociados
Prioridad del proyecto: Baja
Objetivo:

- Mejorar la seguridad de los distintos portátiles y ordenadores de sobremesa
- Securización de los ordenadores de los usuarios
- Centralización de la información

Descripción:

Se ha podido observar que algunos usuarios están almacenando información en sus ordenadores de sobremesa los cuales son susceptibles actualmente de poder sufrir ataques por mal uso del mismo. Para ello se quiere realizar las siguientes acciones:

Seguridad en base a antivirus

- Adquisición de antivirus con opciones de firewall gestionados por consola central
- Distribución de los clientes antivirus por los clientes
- Configuración centralizada

Configuración seguridad a nivel de puesto

- Generación de políticas restrictivas de uso a los usuarios a nivel de imagen base
- Generación de políticas cambios de contraseña y seguridad a nivel del dominio
- Script de logon que en base a la seguridad que tenga acceso el usuario le dé acceso a los distintos recursos de la empresa alojados en los servidores. Evitando almacenar información en los puestos.
- Inhabilitar el acceso a las unidades de disco de portátiles y sobremesa para uso de servidores de empresa o entornos Web de la misma.

Motivación:

Mejora de los resultados del análisis de riesgos
Mejora puntos 5.1.1 / 5.1.2 de ISO 27002

Controles:

- Revisión anual de seguridad lógica en puestos

Tiempo: 4 meses (definición de permisos 2 meses + 1 mes de aplicación)

Coste: 3000€ (gestión del proyecto y definición de documentación)

Proyecto 7: Planes de mantenimiento mensuales de sistemas de la información

Responsable: Responsable de sistemas y técnicos asociados

Prioridad del proyecto: Baja
Objetivo:

- Comprobar que no haya desviaciones de la seguridad y entornos de sistemas
- Detectar posibles carencias del entorno para generar tareas y proyectos de mejora

Descripción:

Con el fin de poder mantener una gestión correcta de los distintos controles que se han implantado y con el de tener una forma de generar proyectos de mejora se va a proceder a establecer un plan de mantenimiento por departamento de los distintos sistemas de gestión de la información. En este plan cada departamento es responsable de los sistemas que ellos gestionan y darán reporte del departamento de informática para poder generar un informe general que se presentará a dirección.

El documento consta de las siguientes partes:

- Estado de los controles de información
- Seguridad / auditoría de acceso a la información sensible departamental
- Resumen general con el estado actual del sistema
- Informe con presentación de proyectos de mejora

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Revisión de logs servidores y auditoría

Tiempo: 3 meses (planificación y activación de reportes)

Coste: 1500€ (equipo de dinamización, generación de informes y análisis inicial)

Proyecto 8: Plan de continuidad de negocio

Responsable: Responsable de sistemas y técnicos asociados

Prioridad del proyecto: Media

Objetivo:

- Creación de un plan de continuidad de negocio para reaccionar adecuadamente ante incidentes que puedan proceder a interrumpir la actividad de la empresa.

Descripción:

Con el fin de poder hacer frente a los posibles problemas que interrumpan la actividad de negocio de la empresa se ha visto la necesidad de generar un plan de continuidad de negocio. Para ello se requiere realizar un estudio complejo con la dirección de la empresa y el departamento de sistemas de la información. Se deben de detectar los distintos puntos de fallo que pueden generarse y sus posibles soluciones y todo ello consensuado con dirección.

Como resultado de este plan de continuidad de negocio se generarán proyectos nuevos de mejora que dependen de los distintos puntos que se detecten en la revisión general del negocio de la empresa. Además se generarán controles adicionales por cada uno de los proyectos además de documentación para solucionar los problemas que puedan surgir.

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Prueba anual ante incidentes de seguridad

Tiempo: 3 meses

Coste: 4000€ (coste de gestión de dirección, dinamizadores, aplicación de automatismos y formación a distintos departamentos)

Proyecto 9: Informes mensuales del estado de los sistemas de la información

Responsable: Responsable de sistemas y técnicos asociados

Prioridad del proyecto: Baja

Objetivo:

- Comprobar que no haya desviaciones de la seguridad y entornos de sistemas
- Detectar posibles carencias del entorno para generar tareas y proyectos de mejora

Descripción:

Con el fin de poder mantener una gestión correcta de los distintos controles que se han implantado y con el de tener una forma de generar proyectos de mejora se va a proceder a establecer un plan de mantenimiento por departamento de los distintos sistemas de gestión de la información. En este plan cada departamento es responsable de los sistemas que ellos gestionan y darán reporte del departamento de informática para poder generar un informe general que se presentará a dirección.

El documento consta de las siguientes partes:

- Estado de los controles de información
- Resumen general con el estado actual del sistema
- Informe con presentación de proyectos de mejora

Motivación:

Mejora de los resultados del análisis de riesgos

Controles:

- Informe mensual del plan de mantenimiento

Tiempo: 2 meses

Coste: 1000€ (equipo de dinamización)

3. Evolución y desarrollo de los proyectos

La realización de los proyecto se realizará de forma serial en base al número de proyecto y a la prioridad que se le ha sido asignado. A tener en cuenta que los proyectos de prioridad alta tendrían gran impacto en la empresa con lo que realmente deben de hacer de forma serial.

Tiempo de proyectos

- ✓ Proyecto 1 → 3 meses
- ✓ Proyecto 2 → 2 meses
- ✓ Proyecto 3 → 4 meses
- ✓ Proyecto 4 → 3 meses
- ✓ Proyecto 5 → 2 meses
- ✓ Proyecto 6 → 4 meses
- ✓ Proyecto 7 → 3 meses
- ✓ Proyecto 8 → 3 meses
- ✓ Proyecto 9 → 2 meses

- ➢ ***Total*** → 26 meses → 2 años y 2 meses

A tener en cuenta que pueden surgir desviaciones de los proyectos que se han ido indicando como por ejemplo la adquisición de nuevo material, la demora en los envíos o elementos imprevisto con lo que se puede prever una adaptación de la duración total del plan de proyecto a 3 años. En el siguiente punto podemos ver el diagrama de Gantt con los tiempos y fechas aproximadas de ejecución de los distintos proyectos.

4. Diagrama de Gantt

En este esquema podemos ver la evolución prevista para los proyectos sin tener en cuenta las posibles desviaciones. En el que caso de haber desviaciones en los proyectos se pueden iniciar los siguientes proyectos planificados si no tienen vinculación unos con otros, consiguiendo de esta forma no desviarnos de las fechas de finalización de los proyectos.

		AÑO 2015 (AGO-DIC)					AÑO 2016											AÑO 2017								
ID	**Proyectos**																									
1	Mejora en mantenimiento eléctrico del CPD																									
	Fase 1 - instalación hardware																									
	Fase 2 - contratación y pruebas																									
2	Mejora de acceso de datos de Internet																									
3	Plan de contingencia de datos - Backups y Restores																									
	Fase 1 - centralización de copias																									
	Fase 2 - librería de cintas																									
4	Plan de clasificación de la información y tratamiento del mismo																									
5	Acceso seguro a la información externa / interna																									
6	Limitación de permisos en los puestos de trabajo para los usuarios																									
7	Planes de mantenimiento mensuales de sistemas de la información																									
8	Plan de continuidad de negocio																									
9	Planes de mantenimiento mensuales de sistemas de la información																									

Tabla 109 Diagrama de Gantt

Auditoría de cumplimiento

1. Introducción y metodología

En esta fase del proyecto se quiere proceder a realizar nuevamente un análisis del estado de la empresa en relación a los distintos controles de la ISO/IEC 27002:2013 para poder comprobar si efectivamente tras la consecución de los distintos proyectos realizado y los controles que se han añadido han producido efectos en el SGSI. En este apartado ya conocemos los activos de la empresa y el estado de la misma con lo que no sería necesario la modificación y especificación de los mismos.

La metodología empleada previamente fue MAGERIT y será la que continuaremos utilizando con los valores previamente indicados.

2. Evaluación de la madurez

Para poder realizar la evaluación de madurez utilizaremos los valores establecida previamente en la *Tabla 110 Modelo de Madurez de la capacidad* donde podemos ver la madurez de los controles que vamos a comprobar de la ISO/IEC 27002:2013

NOMBRE DE LOS CONTROLES	CUMPLIDOS
5. POLITICAS DE SEGURIDAD.	
5.1 Directrices de la Dirección en seguridad de la información.	
5.1.1 Conjunto de políticas para la seguridad de la información.	L3
5.1.2 Revisión de las políticas para la seguridad de la información.	L2
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	
6.1 Organización interna.	
6.1.1 Asignación de responsabilidades para la segur. de la información.	L3
6.1.2 Segregación de tareas.	L3
6.1.3 Contacto con las autoridades.	L3
6.1.4 Contacto con grupos de interés especial.	L3
6.1.5 Seguridad de la información en la gestión de proyectos.	L2
6.2 Dispositivos para movilidad y teletrabajo.	
6.2.1 Política de uso de dispositivos para movilidad.	L2
6.2.2 Teletrabajo.	L2
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	L5
7.1.2 Términos y condiciones de contratación.	L5
7.2 Durante la contratación.	
7.2.1 Responsabilidades de gestión.	L5
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	L3
7.2.3 Proceso disciplinario.	L3
7.3 Cese o cambio de puesto de trabajo.	

NOMBRE DE LOS CONTROLES	CUMPLIDOS
7.3.1 Cese o cambio de puesto de trabajo.	L5
8. GESTION DE ACTIVOS.	
8.1 Responsabilidad sobre los activos.	
8.1.1 Inventario de activos.	L4
8.1.2 Propiedad de los activos.	L5
8.1.3 Uso aceptable de los activos.	L5
8.1.4 Devolución de activos.	L3
8.2 Clasificación de la información.	
8.2.1 Directrices de clasificación.	L3
8.2.2 Etiquetado y manipulado de la información.	L4
8.2.3 Manipulación de activos.	L5
8.3 Manejo de los soportes de almacenamiento.	
8.3.1 Gestión de soportes extraíbles.	L3
8.3.2 Eliminación de soportes.	L5
8.3.3 Soportes físicos en tránsito.	L5
9. CONTROL DE ACCESOS.	
9.1 Requisitos de negocio para el control de accesos.	
9.1.1 Política de control de accesos.	L3
9.1.2 Control de acceso a las redes y servicios asociados.	L3
9.2 Gestión de acceso de usuario.	
9.2.1 Gestión de altas/bajas en el registro de usuarios.	L5
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	L4
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	L4
9.2.4 Gestión de información confidencial de autenticación de usuarios.	L3
9.2.5 Revisión de los derechos de acceso de los usuarios.	L3
9.2.6 Retirada o adaptación de los derechos de acceso	L5
9.3 Responsabilidades del usuario.	
9.3.1 Uso de información confidencial para la autenticación.	L5
9.4 Control de acceso a sistemas y aplicaciones.	
9.4.1 Restricción del acceso a la información.	L3
9.4.2 Procedimientos seguros de inicio de sesión.	L5
9.4.3 Gestión de contraseñas de usuario.	L5
9.4.4 Uso de herramientas de administración de sistemas.	L3
9.4.5 Control de acceso al código fuente de los programas.	L5
10. CIFRADO.	
10.1 Controles criptográficos.	
10.1.1 Política de uso de los controles criptográficos.	L5
10.1.2 Gestión de claves.	L4
11. SEGURIDAD FISICA Y AMBIENTAL.	
11.1 Áreas seguras.	
11.1.1 Perímetro de seguridad física.	L5
11.1.2 Controles físicos de entrada.	L5
11.1.3 Seguridad de oficinas, despachos y recursos.	L5
11.1.4 Protección contra las amenazas externas y ambientales.	L5
11.1.5 El trabajo en áreas seguras.	L5

NOMBRE DE LOS CONTROLES	CUMPLIDOS
11.1.6 Áreas de acceso público, carga y descarga.	L5
11.2 Seguridad de los equipos.	
11.2.1 Emplazamiento y protección de equipos.	L5
11.2.2 Instalaciones de suministro.	L5
11.2.3 Seguridad del cableado.	L3
11.2.4 Mantenimiento de los equipos.	L5
11.2.5 Salida de activos fuera de las dependencias de la empresa.	L3
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	L5
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	L5
11.2.8 Equipo informático de usuario desatendido.	L5
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	L3
12. SEGURIDAD EN LA OPERATIVA.	
12.1 Responsabilidades y procedimientos de operación.	
12.1.1 Documentación de procedimientos de operación.	L5
12.1.2 Gestión de cambios.	L3
12.1.3 Gestión de capacidades.	L3
12.1.4 Separación de entornos de desarrollo, prueba y producción.	L5
12.2 Protección contra código malicioso.	
12.2.1 Controles contra el código malicioso.	L5
12.3 Copias de seguridad.	
12.3.1 Copias de seguridad de la información.	L3
12.4 Registro de actividad y supervisión.	
12.4.1 Registro y gestión de eventos de actividad.	L5
12.4.2 Protección de los registros de información.	L5
12.4.3 Registros de actividad del administrador y operador del sistema.	L3
12.4.4 Sincronización de relojes.	L5
12.5 Control del software en explotación.	
12.5.1 Instalación del software en sistemas en producción.	L3
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Gestión de las vulnerabilidades técnicas.	L3
12.6.2 Restricciones en la instalación de software.	L3
12.7 Consideraciones de las auditorias de los sistemas de información.	
12.7.1 Controles de auditoria de los sistemas de información.	L4
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	
13.1.1 Controles de red.	L5
13.1.2 Mecanismos de seguridad asociados a servicios en red.	L5
13.1.3 Segregación de redes.	L5
13.2 Intercambio de información con partes externas.	
13.2.1 Políticas y procedimientos de intercambio de información.	L3
13.2.2 Acuerdos de intercambio.	L2
13.2.3 Mensajería electrónica.	L2
13.2.4 Acuerdos de confidencialidad y secreto.	L5

NOMBRE DE LOS CONTROLES	CUMPLIDOS
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
14.1 Requisitos de seguridad de los sistemas de información.	
14.1.1 Análisis y especificación de los requisitos de seguridad.	L4
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	L5
14.1.3 Protección de las transacciones por redes telemáticas.	L5
14.2 Seguridad en los procesos de desarrollo y soporte.	
14.2.1 Política de desarrollo seguro de software.	L2
14.2.2 Procedimientos de control de cambios en los sistemas.	L2
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L5
14.2.4 Restricciones a los cambios en los paquetes de software.	L3
14.2.5 Uso de principios de ingeniería en protección de sistemas.	L5
14.2.6 Seguridad en entornos de desarrollo.	L3
14.2.7 Externalización del desarrollo de software.	L5
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	L5
14.2.9 Pruebas de aceptación.	L5
14.3 Datos de prueba.	
14.3.1 Protección de los datos utilizados en pruebas.	L5
15. RELACIONES CON SUMINISTRADORES.	
15.1 Seguridad de la información en las relaciones con suministradores.	
15.1.1 Política de seguridad de la información para suministradores.	L5
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	L5
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	L5
15.2 Gestión de la prestación del servicio por suministradores.	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	L5
15.2.2 Gestión de cambios en los servicios prestados por terceros.	L5
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION.	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	
16.1.1 Responsabilidades y procedimientos.	L3
16.1.2 Notificación de los eventos de seguridad de la información.	L5
16.1.3 Notificación de puntos débiles de la seguridad.	L3
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	L2
16.1.5 Respuesta a los incidentes de seguridad.	L3
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	L3
16.1.7 Recopilación de evidencias.	L5
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO	
17.1 Continuidad de la seguridad de la información.	
17.1.1 Planificación de la continuidad de la seguridad de la información.	L3
17.1.2 Implantación de la continuidad de la seguridad de la información.	L3
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L2

NOMBRE DE LOS CONTROLES	CUMPLIDOS
17.2 Redundancias.	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	L3
18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	
18.1.1 Identificación de la legislación aplicable.	L5
18.1.2 Derechos de propiedad intelectual (DPI).	L5
18.1.3 Protección de los registros de la organización.	L3
18.1.4 Protección de datos y privacidad de la información personal.	L3
18.1.5 Regulación de los controles criptográficos.	L5
18.2 Revisiones de la seguridad de la información.	
18.2.1 Revisión independiente de la seguridad de la información.	L3
18.2.2 Cumplimiento de las políticas y normas de seguridad.	L2
18.2.3 Comprobación del cumplimiento.	L3

Tabla 111 Controles ISO/IEC 27002 tras aplicación de controles

3. Presentación de resultados

Podemos ver que los proyectos y controles que se han aplicado han generado una mejoría en todas las áreas haciendo especial esfuerzo en el dominio 5 de políticas de seguridad en la gestión de la seguridad de la información. Uno de los principales objetivos era poder involucrar a la dirección en la toma de decisiones que conciernen a la seguridad y podemos indicar que efectivamente ha habido una mejoría en este campo.

Podemos ver el siguiente gráfico donde ver las áreas de la ISO/IEC 27002:2013 tras la aplicación de los cambios.

Tabla 112 Análisis posterior ISO/IEC 27002:2013

Si realizamos un análisis de la situación previa a la actual podemos apreciar una considerable mejoraría. Sin duda, gracias a la implicación de Dirección y personal tras los proyectos acometidos.

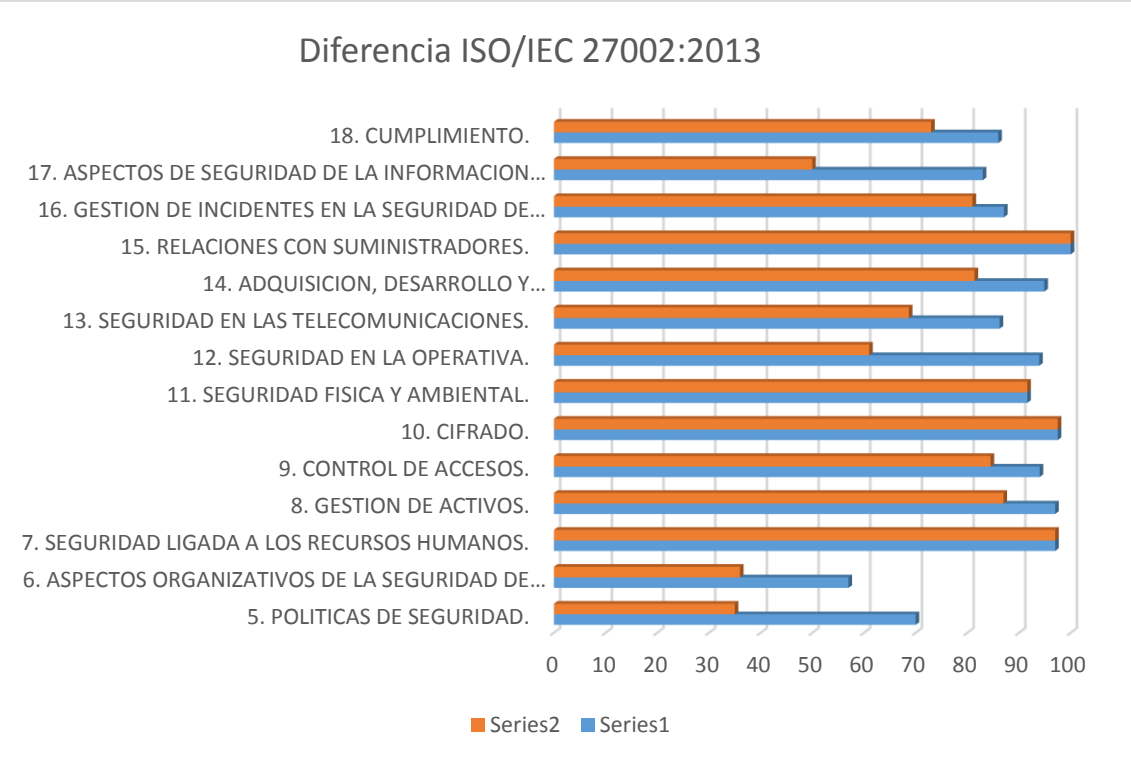

Tabla 113 Diferencial ISO/IEC 27002:2013

En la siguiente podemos ver como la *Series1* que corresponde a la actual situación de la empresa ha sufrido una mejora principalmente en las siguientes áreas:

- Políticas de seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad Operativa
- Aspectos de seguridad de la información en la gestión de la continuidad de negocio

Los controles que actualmente están establecidos en la empresa tienen la siguiente madurez:

Tabla 114 Madurez previa de los controles

Tras la aplicación de los distintos controles mejorados además de los proyectos que han incidido en casi todos los puntos de control podemos ver cómo ha mejorado considerablemente la situación de los controles, lo cual posibilita a la empresa alcanzar sus objetivos iniciales y futuros.

Tabla 115 Madurez actual de los controles

No conformidades

Las no conformidad que hemos encontrad han sido un total de cinco y de categoría media.

Dominio	5. Políticas de seguridad
Punto de control	5.1.1 (L3) y 5.1.2(L2)
Comentarios	5.1.1(L3) Existe actualmente documentación indicando el funcionamiento de las políticas de seguridad de la información pero no dispone de líneas de actuación globales pudiendo dejar libre interpretación en determinados casos. 5.1.2 (L2) Existe un sistema de revisión pero no queda claro los puntos a seguir en el proceso.
Tipo de no conformidad	Mayor
Acción correctora	5.1.1 (L3) Revisión de la política para alinearla con los intereses y objetivos de la empresa en materia de negocio y gestión de seguridad de la información. 5.1.2(L2) Establecer un plan de acción a seguir para poder definir correctamente la forma de revisar las políticas de seguridad

Tabla 116 No conformidad dominio políticas de seguridad

Dominio	6. Aspectos organizativos de la seguridad de la información
Punto de control	6.2.2 (L2)
Comentarios	La forma de proceder para la conexión de los usuario queda clara pero no se establecen medidas adicionales de seguridad cuando se establece la conexión entre máquinas personales y el dominio del cliente
Tipo de no conformidad	Menor
Acción correctora	Revisar la política actual para poder incluir la gestión de la seguridad del cliente que se conecta antes de proceder a permitirle acceso al dominio. Se pueden un proyecto de seguridad mediante accesos VPN y revisión de políticas locales mediante tecnologías como Juniper y su gestión de políticas de cliente.

Tabla 117 No conformidad dominio aspectos organizativos

Dominio	13. Seguridad en las telecomunicaciones
Punto de control	13.2.2 (L2) y 13.2.3 (L2)
Comentarios	13.2.2 (L2) Existe una política o guía de buena conducta pero no se han establecido canales seguros para la transferencia de ficheros o documentación. 13.2.3 (L2) Existe una guía de buena conducta pero no se ha establecido una correcta política de gestión del uso de la mensajería electrónica.
Tipo de no conformidad	Menor
Acción correctora	13.2.2 (L2) Establecer un correcto cauce para el envío de información a terceros mediante el uso de canales cifrados como pueda ser FTPS o SFTP. 13.2.3 (L2) Establecer políticas de correo saliente para poder añadir medidas de protección añadidas en el caso de que un usuario por descuido o voluntariamente envie información calificada como confidencial.

Tabla 118 No conformidad Seguridad en las telecomunicaciones

Bibliografía, referencias y definición de términos

Bibliografía y referencias

INCIBE

https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html

Portal Web ISO27000 en Español

http://www.iso27000.es/

Controles de ISO 27002

http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Definiciones y explicaciones de ISO 27002

http://www.iso27000.es/iso27002.html

Proceso de auditoría

http://www.iso27000.es/certificacion.html

Portal de Administración electrónica gobierno de España

http://administracionelectronica.gob.es/pae_Home#.VWf5Qs_tn_w

LIBRO 3 MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

LIBRO 2 MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Documentación asignatura Sistemas de gestión de la seguridad de la información de la UOC

Normativa ISO 27001:2013 de ISO

Agencia española de protección de datos -LOPD

http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Esquema Nacional de seguridad

https://www.ccn-cert.cni.es/publico/ens/ens/index.html

ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management.

ISO 31010 ISO/IEC 31010:2009, Risk management — Risk assessment techniques.

UNE-ISO/IEC 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo. B.29 Matriz de consecuencia / probabilidad

Definición de términos

Para el correcto entendimiento de algunas partes de la documentación podemos remitir a un glosario muy completo en el que se incluyen todos los apartados que puedan estar relacionados con un plan director de seguridad de la información. El glosario de términos podría ser muy extenso para adjuntarlo por ello haremos referencia a las principales y dejaremos el siguiente enlace de consulta.

http://www.iso27000.es/glosario.html

Algunas palabras serían:

SGSI: Sistema de gestión de la seguridad de la información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Activo: cualquier bien que tiene valor para la organización.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Seguridad de la información: la preservación de la confidencialidad, la integridad y la disponibilidad de la información pudiendo abarcar propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Evento de seguridad: ocurrencias detectadas en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información.

Incidencia de seguridad de la información: un evento o serie de ellos que tienen una probabilidad considerable de comprometer las operaciones empresariales y amenazar la seguridad de la información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Aceptación del riesgo: decisión informada de asumir un riesgo concreto.

Riesgo Residual: riesgo que tenemos después de haber aplicado las medidas oportunas para mitigar el riesgo inicial.

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

ISO/IEC: International Organization of Standardization / International Electrotechnical Comission

PDCA: Ciclo de Deming que indica Plan (planear) – Do (hacer) – Check (comprobar) – Act (actuar)