



Plan Director de Seguridad - Magerit

V.3

[Introducción](#)

El crecimiento y evolución de las Tecnologías de la Información y Comunicaciones (TIC) durante los últimos años está cambiando nuestro mundo profunda y vertiginosamente. Los nuevos avances en tecnología de comunicaciones, computación, almacenamiento e internet han abierto un nuevo contexto y paradigma de posibilidades que está originando nuevas necesidades a satisfacer a la sociedad y por las empresas.

Conceptos como conectividad, 24x7, globalización, *Cloud*, 5G, social media, IA, blockchain, inmediatez, online, ... se han integrado en nuestro día a día, cambiando nuestros hábitos y forma de vivir, en definitiva; pues vienen a satisfacer o modelar nuevas necesidades y expectativas.

Sin duda la información es el elemento común y la dimensión clave. Es a la vez el objeto de medida, el producto o servicio con el que transaccionar, el activo a proteger, el arma y defensa, el combustible de esta “Era de la información”.

¿Cómo afecta esta etapa a las empresas en sus sistemas y procesos?

La irrupción de nuevos dispositivos, servicios, formas de almacenamiento, transmisión, intercambio, compartición y utilización de esta información conlleva nuevas amenazas (externas e internas), vulnerabilidades, ciberataques y riesgos desconocidos.

Durante este periodo la información ha crecido exponencialmente a la vez que se ha convertido en uno de los activos a proteger más valiosos y estratégicos de cualquier organización, lo cual hace que el tratamiento de la información adquiera especial importancia para asegurar su disponibilidad, confidencialidad e integridad, autenticidad y no repudio, y por ende la protección de los sistemas y espacio que la contienen.

¿Y qué ocurre con la seguridad de esa información?

Esto ha propiciado la transformación de las empresas y sus procesos.

¿Y qué ocurre con la seguridad de esa información?

No es lo mismo “seguridad informática” que “seguridad de la información”.

La familia normativa ISO 2700, utilizada como marco de referencia (no obligatorio aunque aconsejable), para el desarrollo e implementación de la gestión de la seguridad de los activos de información, propone los Sistemas de Gestión de Seguridad de la Información (SGSI) como herramienta que permite gestionar y desarrollar los procesos destinados a organizar y actuar sobre la seguridad de la información de una organización, mediante políticas, procedimientos e instrucciones técnicas que garanticen el aseguramiento de la información.

El análisis de los riesgos es fundamental en el diseño para la gestión de la seguridad y desarrollo de sistemas de información seguros. Conocer los riesgos a los que está expuesta una organización es imprescindible para poder gestionarlos. La gestión de riesgos supone, primero realizar un análisis de riesgos y posteriormente realizar el tratamiento de esos riesgos mediante salvaguardas para llevarlos a un nivel aceptable, agrupando las distintas tareas y acciones en programas de seguridad (o proyectos de seguridad, según nomenclaturas).

Para organizar el SGSI es necesario desarrollar un Plan de Seguridad o Plan Director de Seguridad (PDS), que a su vez se compone de una serie de programas mediante los cuales las decisiones adoptadas para el tratamiento de riesgos se materializan.

No es lo mismo “seguridad informática” que “seguridad de la información”.

Un Plan Director de Seguridad siempre debe tener en cuenta la actividad y funcionamiento de la organización y estar alineado con los objetivos estratégicos de la empresa.

La seguridad absoluta no existe. El nivel de seguridad a alcanzar es proporcional a la inversión para conseguirlo y se debe contar con el compromiso de la dirección, la

concienciación de la compañía, establecimiento de objetivos y dotación de medios tanto económicos como humanos para conseguirlos.

El presente trabajo consistirá en el desarrollo de un SGSI para una empresa pyme del sector de la construcción, anónima e inventada a partir de otras similares existentes, fruto de mi experiencia en empresas de este tipo y la elaboración de una propuesta de Plan de Seguridad.

Este tipo de empresas generan y manejan información relativa a la actividad de negocio propiamente dicha o datos personales de clientes, empleados y proveedores, lo cual hace que tengan la necesidad de protegerlos y estén sujetas a cumplir con la normativa sobre protección y tratamiento de la información.

Para la elaboración del SGSI, siguiendo la metodología *MAGERIT – versión 3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)* [9], se realizará el catálogo de activos, valoración, amenazas, vulnerabilidades, salvaguardas; para a continuación hacer un análisis de riesgos que permita establecer las directrices, controles y medidas de seguridad a adoptar para asegurar la información del sistema. Estas tareas se organizarán en los distintos programas de seguridad que conformarán el plan de seguridad de la empresa que se propondrá a la dirección para su evaluación y futura implantación.

2. Planificación

La presentación del TFM se realizará en la convocatoria extraordinaria de enero.

Al tener que compaginar el trabajo y conciliación familiar con la realización del máster, el planteamiento para poder realizarlo ha sido cursar todas las asignaturas durante el primer año y en este segundo año, abordar el TFM, siempre con el objetivo de defenderlo en la primera convocatoria disponible.

Según esta planificación se implementará el SGSI y desarrollará el Plan Director de Seguridad.

La planificación prevista es la siguiente iniciando a principios de Julio:

Tabla 1. Planificación temporal TFM

Contenidos	Tiempo total	Fecha límite fin
Entrevistas en la empresa Situación actual. (Modelo de madurez)	4 semanas	31-jul-2019
Organización y estructura TFM Planificación Estado del arte Objetivos	4 semanas	29-sep-2019
Motivación, justificación, objetivo general, Introducción Metodología Análisis y especificación Presupuesto, estimaciones	3 semanas	20-oct-2019
Implementación SGSI	5 semanas	24-nov-2019
Análisis del SGSI	1 semana	01-dic-2019
Resultados Conclusiones y trabajo futuro Referencias, bibliografía y apéndices Agradecimientos, citas, índices	2 semanas	15-dic-2019
Último envío tutor	1 semana	23-dic-2019
Solicitud defensa en UAproject		07-ene-2020
Entrega UAproject (versión final)		10-ene-2020
Presentación TFM	2 semanas	23-ene-2020
Defensa TFM		24-ene-2020

3. Estado del arte

En este apartado se describe el contexto en el que se centra el trabajo, el cual gira en torno a la seguridad de la información como activo a proteger y análisis de riesgos. Así como los mecanismos que se pueden utilizar para el desarrollo de un plan director de seguridad que permita mejorar la protección de los activos de información de una empresa, de una forma organizada.

1. Antecedentes

El boom inmobiliario de principio de siglo XXI en España propició la creación de multitud de empresas a partir de otras que diversificaron su actividad principal hacia la promoción inmobiliaria y sector de la construcción. Muchas de ellas crecieron en un sector donde no tenían experiencia y se vieron obligadas a desarrollarse rápidamente mediante la estructura de una Pyme.

En mi caso, contaba con la oportunidad de trabajar en el área de TI de una gran empresa donde actualmente sigo desempeñando mis funciones y con la experiencia de

conocer la realidad y gestión de los sistemas de información desde la perspectiva y recursos de gran empresa.

Hubo un periodo de tiempo en el cual, por circunstancias familiares y profesionales, participé de primera mano en atender las necesidades de servicios informáticos en pymes de este sector emergente.

Durante el tiempo que realicé esta actividad, traté de aplicar mi conocimiento y experiencia en estas empresas cuyo uso de la informática no iba más allá de utilizarla como un medio; me refiero a que no se percibía como una herramienta para obtener una ventaja competitiva o diferenciación. Era un contexto cambiante, se desconocían las amenazas y los riesgos derivados del uso de nuevas tecnologías e impacto real en el negocio. La salvaguarda más reconocida era la copia de seguridad, que por qué no decirlo, a veces ni se sabía lo que guardaba realmente. El criterio de copias era el que inicialmente se estimó en base a una aplicación o necesidad concreta, del cual nunca se había probado su validez y por ende si llegado el caso sería útil; aunque eso sí, seguridad transmitía a todo el personal.

La salvaguarda más reconocida era la copia de seguridad, que por qué no decirlo, a veces ni se sabía lo que guardaba realmente.

Se trataba de un sector en auge en el que se crecía rápido sin estructura empresarial y se pretendía obtener ganancias rápidamente. La situación del mercado lo propiciaba. Conceptos como sistema de información, políticas y gestión de la seguridad o plan de contingencia sonaban a otros ámbitos y se percibían en el mejor de los casos como algo caro, no necesario para el negocio ‘core’, sin un ROI claro, del ámbito de otras empresas grandes y procesos industriales. Lo más parecido a gestión de la seguridad y políticas eran los usuarios individuales para entrar al sistema informático y una ley llamada LOPD [5], para cuyo cumplimiento y evitar sanciones, se contrataba a una empresa que rellenase los formularios y realizará las gestiones oportunas para así cubrir el trámite; y que desde entonces es probable que no hayan sido actualizados. (*También es verdad que a muchas de estas empresas ya no les hace falta hoy en día pues no soportaron el estallido de la burbuja inmobiliaria a finales de 2007*).

Mi aportación en aquel momento fue adoptar las medidas necesarias sobre el sistema de información desde el punto de vista de la seguridad informática, adaptándome a los recursos y necesidades de cada empresa; aunque sin una base fundamentada en la gestión de la seguridad de la información como tal, ni con el soporte argumentado sobre un plan derivado de un análisis de riesgos. Los recursos de este tipo de empresas no lo contemplaban como una necesidad, ni era algo valorado. También por mi desconocimiento de este tipo de metodologías y herramientas de análisis.

Estas empresas utilizaban las tecnologías de la información sin ser conscientes de su dependencia y riesgos; aunque sí tenían claro que las necesitaban para elaborar su “producto final”. Al no contar con un departamento propio ni de IT ni de Seguridad, llevaban esta labor de una manera informal e insuficiente, sin ser conscientes del riesgo que realmente estaban asumiendo (tanto económico como reputacional). No lo tenían cuantificado y desconocían las medidas a adoptar para llevar este riesgo a un nivel aceptable, pensando que los recursos a invertir pudieran llegar a ser excesivos. Además, tampoco sabían cómo actuar cuando estas tecnologías fallaban o cualquier circunstancia les privaba de su uso.

Al cursar la asignatura “*Sistemas de Gestión de Seguridad*” durante el máster universitario en ciberseguridad, tuve claro que una de las aplicaciones que podría tener y que sin duda hubiese sido muy adecuado durante aquella etapa, era precisamente la elaboración de un SGSI adaptado a empresas como las descritas, utilizando la metodología y visión aprendida en la asignatura mediante la que evaluar la empresa y llevar a cabo la implementación del plan director de seguridad para este tipo de empresas.

El contexto actual de globalización, el uso de las tecnologías de la información y la transformación digital en la que las empresas están inmersas, ha derivado en que hayan surgido nuevas amenazas a las que las empresas quedan expuestas y que la ciberseguridad haya adquirido una importancia relevante dentro del día a día de todas las organizaciones.

2. Seguridad de la información

Según la norma española UNE-ISO/IEC 2700,

“se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.” [1]

La información es un activo esencial para el negocio de una empresa, y que por tanto es necesario proteger. Ya sea relativa a la actividad de negocio propiamente dicha o datos personales. Es almacenada en distintos formatos, físico, digital o intangible como el propio conocimiento de las personas; y se genera, transmite, intercambia y accede por diversos medios. En cualquiera de las formas y ubicaciones, es necesario mantener su seguridad.

El término seguridad aplicado a información, se refiere a garantizar sus características dentro de los sistemas de información en las siguientes dimensiones:

Confidencialidad: Propiedad que consiste en garantizar que la información sólo es accesible por aquellas entidades autorizadas.

Disponibilidad: Propiedad que consiste en que la información permanezca accesible para entidades autorizadas.

Integridad: Supone que la información se mantenga inalterada ante errores, accidentes o intentos maliciosos. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.

1. La protección de datos

Cuando se habla de datos personales y su tratamiento por parte de terceros, nos referimos a toda información que permita identificar a una persona o hacerla identificable.

Como ejemplo: Nombre, documento de identidad, dirección, número de teléfono..., email, información enviada a redes sociales, dirección IP, cookies... información física, psicológica, médica, biométrica, genética, ...

El marco legal que regula la protección de datos personales en España viene dado por la norma de referencia para la protección de datos, LOPDGDD - Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales [2], la cual entró en vigor el 6 de diciembre de 2018. Esta norma sustituyó a la antigua LOPD - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

[5].

Uno de los principales objetivos de la LOPDGDD es adaptar la legislación española a la normativa europea, definida por el Reglamento General de Protección de Datos (*RGPD o GDPR – General Data Protection Regulation*). [3][4], el cual está vigente desde el 25 de mayo de 2018, cuya finalidad es aportar un marco único comunitario para la protección de datos.

La obligación de cumplir esta ley es de todas las personas, empresas y entidades públicas y privadas (administraciones y organismos públicos, sociedades mercantiles, autónomos, asociaciones, entidades sin ánimo de lucro, comunidades de propietarios, de bienes), que utilicen cualquier dato personal en el desarrollo de sus actividades profesionales.

Quedan excluidos el tratamiento de datos con fines domésticos, datos referidos a personas jurídicas y las personas de contacto, datos relativos a empresarios individuales y datos relativos a personas fallecidas.

¿Cómo afecta la RGPD a empresas del sector de la construcción?

En lo que aplica a empresas del sector inmobiliario y la construcción, según el portal especializado <https://ayudaleyprotecciondatos.es> cuyo responsable es “Agustín Pérez Silverio” director de ventas y responsable de proyectos en la empresa Grupo Ático34, que ofrece servicios legales de asesoramiento en ámbito nacional en materia de protección de datos y soluciones específicas para la adaptación y asesoramiento a organizaciones, públicas y privadas, sobre el RGPD y LOPD,

“Las empresas de construcción e ingeniería manejan también datos de clientes, empleados y proveedores, por lo que están obligados a adaptarse a la nueva normativa.”

“Las actuaciones para adaptarse serían:

- *Realizar un Registro de actividades de tratamiento*
- *Firmar los contratos con terceros*
- *Firmar los contratos con los empleados*
- *Incluir los textos legales en la página web*
- *Solicitar el consentimiento a los clientes*
- *Realizar un Análisis de riesgos*
- *Notificar las brechas de seguridad”.*

Hace más de año y medio que la RGPD entró en vigor y las estadísticas indican que todavía no se cumple la normativa de protección de datos.

El 79% de las empresas españolas aún no cumple con la RGPD.

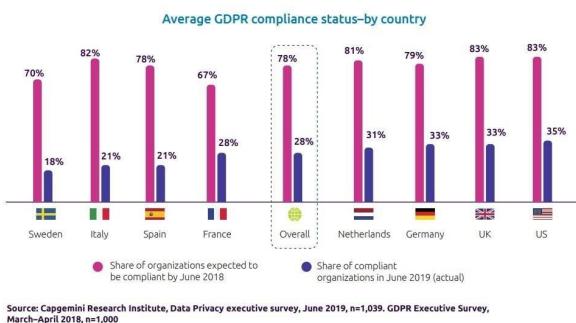


Figura 1. Estado de cumplimiento de la GDPR por país (Fuente Capgemini Research Institute)

Según el estudio “*Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century*” [8] de la consultora Capgemini, a fecha de Junio 2019, solo el 21% de las empresas españolas cumpliría con la normativa; mientras que el 78% de las mismas esperaban cumplir un año antes.

Sin duda los datos personales son uno de los activos a proteger por parte de las empresas, aunque existen otros activos de la información propios del ejercicio de su actividad los cuales son importantes y esenciales para las empresas. En este caso, planos, datos económicofinancieros, comerciales, estrategias, etc.

La utilización de las nuevas tecnologías, la transformación digital de las empresas e irrupción del uso de Internet y conectividad desde cualquier dispositivo y ubicación, digitalización de la información, almacenamiento en la nube, utilización de nuevos elementos y dispositivos en contacto directo con el sistema de información, hace que el paradigma de seguridad vaya cambiando; así como las amenazas y riesgos (tanto externos como internos), a los que están expuestas las empresas.

Todo ello hace que el análisis de riesgos y evaluación del impacto adquiera más importancia y se convierta en una obligación.

Disponer de un buen sistema de gestión de la seguridad de la información y unas medidas adecuadas de ciberseguridad, es esencial para abordar la transformación digital de forma ordenada y segura.

En este punto me gustaría hacer referencia a lo que en su momento indicó en 2018 previo a la entrada en vigor de la RGPD, Mar España, directora de la Agencia Española de Protección de Datos.

“El 25 de mayo, tanto el sector público como el privado, deben tener implementado un análisis de riesgos y una evaluación de impacto” [7]

[1. Sistemas de gestión de la seguridad de la información](#)

La información por tanto es un activo importante de las empresas que hay que proteger. Depende de la tecnología y de las comunicaciones. Esta tecnología facilita su ciclo de vida, creación, almacenamiento, tratamiento, utilización, transmisión, intercambio y destrucción. Durante todas las etapas el valor y riesgo de los activos de información puede variar, aunque la seguridad es importante en todas ellas.

Un ejemplo sería el valor de unos planos de un prototipo de un nuevo producto, los cuales pueden suponer mayor impacto para la empresa, si los roban antes de lanzar el producto, que una vez ya puesto en el mercado. Otro ejemplo sería que las condiciones contractuales y tarifas de determinado proveedor para la subcontratación de un trabajo pudieran llegar a otro proveedor. La pérdida de la información en ambas situaciones, independientemente de la fase del ciclo de vida en la que se encuentre tiene, aunque distintas, implicaciones para la empresa.

El hecho de conocer qué proteger, de qué protegerlo, según el valor e impacto que pueda causar para la empresa su deterioro, adoptando y adaptando las medidas de seguridad y recursos necesarios para evitar/disminuir hasta un nivel asumible la probabilidad de que ocurra, durante todo el ciclo de vida, sería el objetivo de la gestión de la seguridad.

Aplicado a los sistemas de información, llevando a cabo todas las tareas y medidas de forma organizada acorde a la evaluación de unos riesgos, mediante un proceso sistemático, procedural y metódico durante todo el ciclo de vida, alineado con la estrategia y el objetivo de negocio de la Organización, se trataría de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Que según la norma española UNE-ISO/IEC 2700:2019 se define,

“Un SGSI (Sistema de Gestión de la Seguridad de la Información) consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son

gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.” [1]

La normativa ISO 2700, es la norma internacional utilizada como marco de referencia para el desarrollo e implantación de un SGSI.

Con la implantación de un SGSI, se garantiza el aseguramiento de la información. Un SGSI son los procesos cuyo objetivo es organizar y actuar sobre los elementos que constituyen la seguridad.

El desarrollo de un Plan director de Seguridad te lleva a la implementación de un SGSI.

2. Normativas ISO 27000

La familia de normas internacionales ISO/IEC/27000:2019 [1] para los sistemas de gestión proporcionan un modelo que ayuda a la implementación y operación de un sistema de gestión de la seguridad de la información. Se pueden utilizar como marco de referencia para el desarrollo e implementación de la gestión de la seguridad de los activos de información de una empresa o como evaluación independiente de un SGSI ante una certificación por una entidad independiente.

Para la realización de este trabajo se han utilizado las siguientes:

Tabla 2. Familia normas ISO 27000 principales

<i>Norma ISO/IEC 27000 [1]</i>	<i>Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.</i>
<i>Norma ISO/IEC 27001 [21]</i>	<i>Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.</i>
<i>Norma ISO/IEC 27002 [22]</i>	<i>Código de práctica para los controles de seguridad de la información.</i>
<i>Norma ISO/IEC 27003 [23]</i>	<i>Guía para la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI).</i>
<i>Norma ISO/IEC 27005 [2522]</i>	<i>Norma que aporta directrices para la gestión de riesgos de seguridad de la información.</i>

Según ISO/IEC/27000:2019 [1] dentro de la sección que describe qué es un SGSI, hace un resumen muy completo y preciso sobre la finalidad, cómo y por qué se logra el aseguramiento de la información mediante un SGSI.

“La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos que se haya elegido y gestionado por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser especificados, implementados, monitorizados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de negocio de una organización.”

3. Gestión de riesgos

Según MAGERIT – versión 3.0 *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* [9], se puede definir riesgo como “*la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.*” El análisis de riesgos es un paso necesario para la gestión de la seguridad. Para lograr la seguridad de la información, es necesario realizar una gestión del riesgo relacionado con amenazas (ya sean físicas, humanas y tecnológicas), asociadas a cualquier formato de información.

Conocer los riesgos a los que están expuestos los activos de los que depende el trabajo, objetivos y propósito de una organización es imprescindible para poder gestionarlos.

La gestión de riesgos supone, primero realizar un **análisis de riesgos** y posteriormente realizar el **tratamiento de esos riesgos**.

El proceso de **análisis de riesgos** tiene como finalidad estimar el grado de magnitud de los riesgos a los que está expuesta una Organización, ante la ocurrencia de amenazas que puedan dañar sus activos. Básicamente se compone de los siguientes pasos:

- Realizar un inventario de activos y amenazas a las que están expuestos.
- Identificar los activos relevantes para la empresa, su interrelación y su valor.
- Determinar el coste que supondría su degradación si determinadas amenazas se materializaran, para evaluar el riesgo que supondría y las implicaciones de dicho riesgo para la organización.

La gestión de riesgos requiere métodos de valoración y tratamiento del riesgo en los que se pueden tener en cuenta variables como costes, beneficios, requisitos legales, prioridades, aspectos sociales o económicos, etc. con el objetivo de identificarlos, cuantificarlos (cuantitativa o cualitativamente) para poder priorizar su tratamiento teniendo en cuenta los objetivos de la empresa.

El proceso de análisis y evaluación de riesgos se debe plantear de forma metódica y sistemática para contemplar los cambios en los requisitos de seguridad de la información y

en los riesgos; cambios sobre activos, amenazas/vulnerabilidades, impactos y evaluación del riesgo, en definitiva.

La norma ISO/IEC 27005:2018 [22] proporciona directrices para “*la gestión de riesgos de seguridad de la información, incluyendo asesoramiento sobre la apreciación del riesgo, el tratamiento del riesgo, la aceptación del riesgo, la comunicación del riesgo, el seguimiento y supervisión del riesgo y la revisión del riesgo. Se incluyen también ejemplos de metodologías de apreciación del riesgo.*”

El **tratamiento de los riesgos** se refiere a aquellas medidas, procesos o controles cuyo objetivo es modificar el riesgo. Un riesgo se puede tratar de distintas formas:

- Evitando las circunstancias que lo provocan.
- Reduciendo las posibilidades de que ocurra.
- Limitando las consecuencias.
- Compartiéndolo con otros (normalmente subcontratando un servicio o seguro de cobertura).
- Aceptándolo.

Para abordar el tratamiento de los riesgos, se deben decidir los criterios para establecer el umbral de riesgo no asumible.

Una vez se han identificado los requisitos de seguridad de la información, valorados los riesgos asociados a los activos de información y adoptadas las decisiones para su tratamiento, deben implementarse los controles para reducirlos a un nivel aceptable según los criterios establecidos por la organización.

1. Plan director de seguridad

El aseguramiento de la información requiere de la implantación de un Sistema de Gestión de la Seguridad de la Información, que no son más que una serie de procesos destinados a organizar y actuar sobre todos los elementos que componen la seguridad de una organización. Para organizar este Sistema de Gestión de la Seguridad es necesario desarrollar un Plan Director de Seguridad, que a su vez se compone de una serie de documentos o apartados.

En la documentación “*Plan director de seguridad*”, de la colección “*Protege tu empresa*” del INCIBE [13], se define como,

“*Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.*”

Además, se indica que, para la realización de un buen Plan Director de Seguridad, debe estar alineado con los objetivos estratégicos de la empresa, incluir una definición del alcance e incorporar las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la Organización, así como terceros que colaboren con ésta.

Como se ha descrito previamente, la gestión de la seguridad lleva aparejada una gestión de los riesgos. Una vez realizado el análisis y decidido el tratamiento de los riesgos mediante salvaguardas, estas salvaguardas son implantadas mediante una serie de tareas, las cuales se agrupan en programas de seguridad que tienen un objetivo o hacen referencia a un elemento común, aplican a una misma competencia o por conveniencia.

El plan director de seguridad son el conjunto de programas mediante los cuales las decisiones adoptadas para el tratamiento de riesgos se materializan. Se puede abordar en tres fases.

Fase 1: Identificación de proyectos/programas

En cada proyecto de seguridad dependiendo de la complejidad deberían identificarse:

- Objetivo genérico del proyecto
- Detalle de salvaguardas a implantar y objetivo de cada una
- Activos a los que afecta, valoración, amenazas, impacto y riesgo
- Responsable de la ejecución
- Estimación de costes
- Subtareas a realizar
- Planificación temporal de implantación del proyecto
- Estimación riesgo residual una vez implantado
- Indicadores de eficacia y eficiencia de la función de seguridad que permita medir la calidad

Fase 2: Planificación

Se pueden ordenar los programas en base a distintos criterios:

- Priorizando por criticidad, gravedad o conveniencia del tratamiento de los impactos y riesgos que se traten.
- Coste del proyecto
- Disponibilidad de los recursos humanos necesarios para llevar a cabo el proyecto
- Presupuesto para afrontarlo

- Cumplimiento de normativas legales que pueden entrar en vigor en una fecha concreta

La planificación se realiza normalmente con tres niveles de detalle:

- Plan director (3-5 años): El plan director de seguridad
- Plan anual (1-2 años): Planes anuales con los proyectos de seguridad incluidos en cada año
- Plan de proyecto (< 1 año): Conjunto de proyectos con el detalle de ejecución de cada uno **Fase 3: Ejecución**

Una vez aprobado por la dirección, se lleva a cabo siguiendo la ejecución de los distintos planes y proyectos, mediante la planificación, recursos y tareas detallada en cada uno.

Con la ejecución y finalización del plan director, se logrará la nueva situación de riesgo aceptable.

4. Objetivos

El objetivo de este trabajo es el desarrollo de un Plan Director de Seguridad a partir del diseño e implantación de un Sistema de Gestión de la Seguridad de la Información que sirva para mejorar la seguridad en empresas pymes del sector de la construcción.

El alcance incluiría hasta la presentación de una propuesta de Plan Director de Seguridad listo para que la dirección de la empresa lo supervise, apruebe y se proceda a la implantación.

Para ello se realizarán los siguientes pasos:

1. Estudio de la empresa. Su contexto, modelo de negocio, estructura organizativa, aspectos técnicos y tratamiento actual de los datos que gestiona.
2. Elaboración de un catálogo de activos y su valoración. Relación de elementos tecnológicos y de información destacados de un SGSI en función de la importancia para el funcionamiento de la empresa.
3. Identificación de amenazas y vulnerabilidades que pueden afectar a los activos.
4. Análisis de riesgos. Cálculo del impacto y riesgo para cada activo, en función de la probabilidad de que se vea afectado por alguna de las amenazas y el daño que puedan ocasionarles.
5. Listado de salvaguardas. Estudio de las contramedidas aplicables frente a un riesgo, que permitan mitigarlo o reducirlo.
6. Creación de planes de seguridad como parte de un plan director de seguridad, que permita a la empresa la implantación ordenada y justificada de las medidas de

seguridad necesarias para garantizar los niveles aceptables de riesgo según los análisis previos.

7. Proporcionar a la empresa el Plan Director de Seguridad desarrollado con el conjunto de planes de seguridad para evaluación de la implantación de las medidas propuestas en cada plan.
8. Incluir un plan de formación y concienciación en materia de seguridad de la información como parte del Plan Director de Seguridad.

5. Propuesta

En este trabajo se va a generar un plan director de seguridad para la empresa Anonym, S.L. Este plan director será formalizado utilizando herramientas y buenas prácticas del sector de la ciberseguridad, y constará de al menos un análisis detallado de situación de la empresa, un análisis de riesgos y los consiguientes planes de seguridad que permitan mitigar los riesgos en aquello que sea posible o reducirlos hasta niveles aceptables.

Dentro de la gestión de riesgos, existen varias metodologías (CRAMM, EBIOS, MAGERIT v3, MEHARI, NIST SP 800-30, Octave, SP800-30).

Todas ellas tienen como objetivo la integración de buenas prácticas internacionalmente reconocidas, proporcionando un método sistemático y ordenado para abordar el análisis de riesgos e implantación de un sistema de gestión de riesgos.

En ellas quedan recogidas todas las actividades que conforman un método de análisis de riesgos:

- Generar un modelo de valor del sistema, identificando y valorando los activos relevantes
- Proporcionar un mapa de riesgos del sistema identificando y valorando las amenazas sobre los activos
- Conocer el estado actual y aplicable de salvaguardas
- Evaluar el impacto potencial e impacto residual
- Evaluar el riesgo potencial y riesgo residual
- Informar de las áreas que requieren de tratamiento

Para la elaboración del presente trabajo, la propuesta es utilizar la metodología *MAGERIT v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)* [9] para abordar la gestión de riesgos, por ser de las más utilizadas en España para SGSI. Esta metodología es promovida por el CSAE (Consejo Superior de Administración Electrónica),

editada por el Ministerio de Hacienda y Administraciones Públicas y está disponible en el Portal de Administración Electrónica (PAe). [17]

Como se indica en MAGERIT v3 – Libro I [10] se provee una metodología con el fin de facilitar la labor de gestión del riesgo propiciado por la generalización del uso de nuevas TI,

“MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.”

[1. Metodología MAGERIT v3](#)

La gestión de los riesgos es una piedra angular en las guías de buen gobierno [ISO 38500], “*...donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican:*

1.6.12 Propuesta Recopilación de los beneficios, costos, riesgos, oportunidades, y otros factores que deben tenerse en cuenta en las decisiones que se tomen.” [14]

Esto quiere decir que las decisiones de gobierno para cumplir los objetivos de una Organización deben tomarse contextualizadas con la gestión de riesgos.

Es necesario un equilibrio entre los riesgos y oportunidades para tomar las mejores decisiones.

Los fallos en los sistemas causan desconfianza, aunque sería deseable que nunca fallaran, lo que realmente causa más incertidumbre es la sensación de no tener bajo control las incidencias que se puedan producir y qué hacer cuando se produzcan. Es imprescindible conocer los riesgos para poder afrontarlos y controlarlos.

Acorde a la terminología de la normativa [ISO 31000:2018 *Risk management — Principles and guidelines*] [15], MAGERIT implementa el proceso de gestión de riesgos descrito en la misma, dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

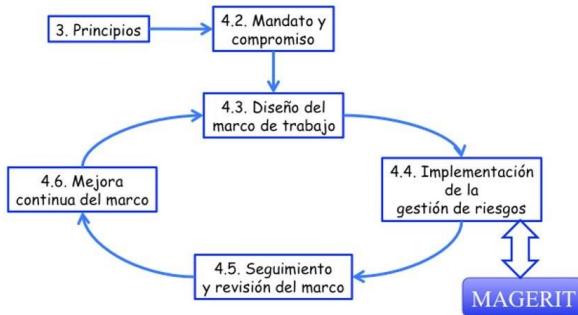


Figura 2. ISO 31000 – Marco de trabajo para la gestión de riesgos

(Fuente MAGERIT – Libro I)

MAGERIT pretende realizar el análisis de riesgos mediante una aproximación metódica, estableciendo una serie de tareas y actividades que definen con exactitud todo lo que se ha de realizar:

Paso 1: Identificación de los activos relevantes para la Organización, sus dependencias y valor, en el sentido de qué perjuicio (coste) supondría su degradación.

Paso 2: Identificación y valoración de las amenazas a las que están expuestos los activos.

Paso 3: Determinar qué salvaguardas hay dispuestas y valoración de su eficacia frente al riesgo.

Paso 4: Estimación del impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

Paso 5: Estimación del riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.



Figura 3. Elementos del análisis de riesgos potenciales

2. Identificación de Activos

La metodología MAGERIT describe como primer paso la elaboración de la lista de elementos a proteger, aquellos que tienen un valor para la organización y serían objeto de aplicarles ciertas medidas de seguridad.

Dentro de la metodología de análisis y gestión de riesgos para los sistemas de información, la norma UNE 71504:2008 [16], define activo como “*Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Esto incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.*”

En un sistema de información hay dos componentes esenciales: la información y los servicios que se prestan. Estos activos marcan los requisitos de seguridad para los demás componentes del sistema.

Según *Magerit – Libro II -Catálogo de Elementos* (pág. 7-13) [11], ésta es la propuesta de categorías inicial en las cuales se propone clasificar los activos:

[D] Datos / Información que materializan la información.

[S] Servicios auxiliares o de soporte para el desempeño del sistema.

[SW] Software - Aplicaciones informáticas que permiten manejar los datos.

[HW] Hardware, equipamiento informático que permite hospedar datos, aplicaciones y servicios.

[Media] Soportes de información que son dispositivos de almacenamiento de datos.

[AUX] Equipamiento auxiliar que complementa el material informático.

[COM] Redes de comunicaciones que permiten intercambiar datos.

[L] Instalaciones que acogen equipos informáticos y de comunicaciones.

[P] Personas que explotan u operan todos los elementos anteriormente citados.

Cada tipo de activo es susceptible de sufrir ciertas amenazas y soporta determinadas salvaguardas.

Existe **dependencia** entre activos cuando el correcto funcionamiento de unos depende de otros. Esta relación se representa en forma de grafo de dependencias en el que los activos de arriba dependen de los de abajo. Por ello la propagación de un daño en caso de materializarse las amenazas, se propaga desde los activos inferiores en el grafo hacia los activos superiores. Un activo A depende de otro B si para cubrir las necesidades de seguridad del activo A se requiere cubrir las necesidades de seguridad del activo B.

El **valor** de los activos viene determinado por la importancia que tiene un activo para la organización desde el punto de vista del perjuicio que le causaría perderlo o su deterioro, lo cual se traduce en la necesidad de protegerlo.

El valor se determina en varias **dimensiones de valoración**, que son las características que hacen valioso un activo. Las dimensiones se utilizan para valorar las consecuencias de la

materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Estas son las dimensiones que se proponen para valorar los activos en los distintos aspectos.

Tabla 3. Dimensiones de valoración según Magerit v3 – Libro II [11]

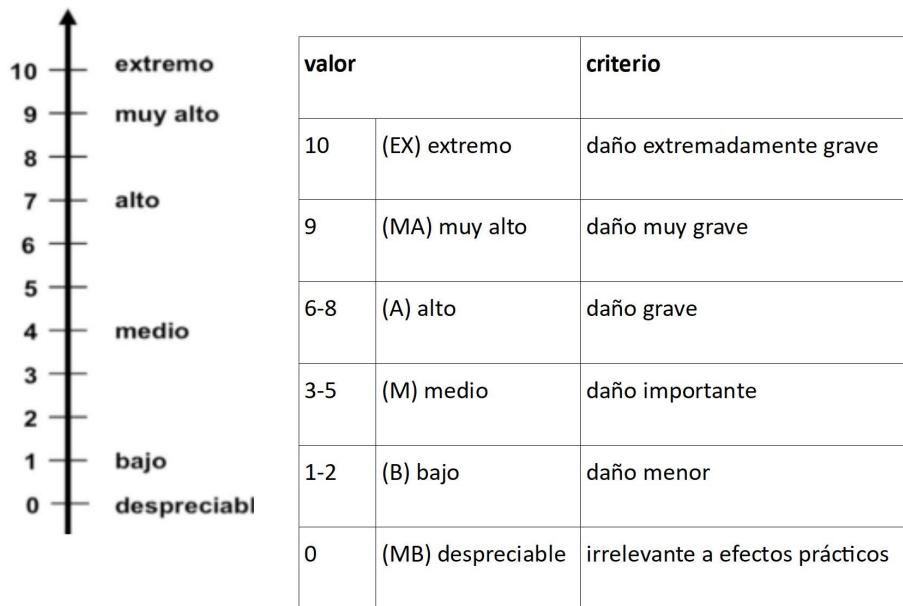
Dimensión	
[D] disponibilidad	<i>"Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren." [UNE 71504:2008] [16]</i>
[I] integridad	<i>"Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada." [ISO/IEC 13335-1:2004] [0]</i>
[C] confidencialidad	<i>"Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados." UNE-ISO/IEC 27001:2017 [21]</i>
[A] autenticidad	<i>"Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos."</i> [UNE 71504:2008] [16]
[T] trazabilidad	<i>"Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad."</i> [UNE 71504:2008] [16]

Para obtener una valoración homogénea de los activos que permita comparar el análisis por separado, MAGERIT sugiere **escalas de valoración** equivalentes (detallada y simplificada). En el presente trabajo, se utilizará la escala simplificada dado que el análisis de riesgos no es muy detallado. La escala va desde un valor despreciable (0) hasta uno extremadamente grave (10).

El valor se puede expresar de forma cuantitativa o cualitativa. Las valoraciones cuantitativas se pueden sumar de forma natural, mientras que las valoraciones cualitativas posicionan el valor de cada activo en un orden relativo respecto a los demás. La ventaja de las cualitativas es que permiten rápido, aunque su inconveniente es que no permiten comparar más allá del orden relativo y no se puede sumar.

En esta tabla se muestra la versión numérica y conversión a nominal de la escala usando la nomenclatura que se utiliza en el presente trabajo, según *MAGERIT v3 – Libro II* [11].

Tabla 4. Escala de valoración de activos. MAGERIT v3 – Libro II



Así pues, este primer paso consistiría en la elaboración del inventario de activos importantes para la organización, determinación de su valor y las dependencias entre sí. Una vez realizada estas tareas, MAGERIT propone la realización de una ficha de catalogación y valoración por cada activo con la siguiente información.

Tabla 5. Ejemplo Ficha de activos. MAGERIT v3 – Libro II [11]

2.1. [info] Activos esenciales		Valoración		
código: I001	nombre: Fichero Clientes	Dimensión	Valor	Justificación
descripción:	Fichero de clientes con información personal	[I]	A	Incumplimiento regulatorio
propietario:	Responsable Administración	[C]	A	Incumplimiento regulatorio
responsable:	Gerente	[D]	M	Es replicable
tipo:	[or][per][M][classified][R]	[A]	A	Incumplimiento regulatorio
		[T]	A	Incumplimiento regulatorio
Dependencias				
Activos: [HW].HW001	Grado: Alto			
¿Por qué?	El maestro de clientes se almacena en el servidor principal dentro del ERP			

En la sección Anexo del presente trabajo, donde se implementan las fichas de cada uno de los activos, se utilizará la siguiente versión simplificada de ficha al tratarse de una PYME; para empresas más grandes con mayor personal disponible se puede utilizar la anterior extendida.

Tabla 6. Ejemplo Ficha de activos simplificada. (fuente propia)

Tipo Activo: [Media] Soportes de información		Valoración - Dimensión				
		[I]	[C]	[D]	[A]	[T]
código:	MEDIA001	nombre:	Memorias USB	A	MA	M
descripción:		Memorias	USB			
propietario:		Responsable	TI			
responsable:		Gerente				
tipo:		[electronic][usb]				

3. Amenazas

En este paso 2 de la metodología MAGERIT, es donde se lleva a cabo la identificación y valoración de las amenazas a las que están expuestos los activos.

La norma [UNE 71504:2008] [16] define amenaza como “*Causa potencial de un incidente que puede causar daños a un sistema de información o una Organización.*”

Según MAGERIT se clasifican en cuatro tipos:

- **De origen natural:** Accidentes naturales como terremotos, inundaciones, incendios, rayos, ... El sistema es víctima pasiva.
- **Del entorno (de origen industrial):** Fallos de la infraestructura auxiliar, contaminación, fallos eléctricos, refrigeración, ...
- **Defectos de las aplicaciones:** Problemas con origen el equipamiento propio por defectos en su diseño o en su implementación. Fallos en las aplicaciones, hardware o equipos de transmisiones, producen consecuencias potencialmente negativas sobre el sistema. También se denominan vulnerabilidades técnicas.
- **Causadas por las personas de forma accidental:** Errores accidentales de las personas que interactúan con la información. Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión.
- **Causadas por las personas de forma deliberada:** Errores deliberados de las personas que interactúan con la información. Las personas con acceso al sistema de información pueden de forma deliberada ser causa de problemas intencionados: acciones no autorizadas como uso de software o hardware no autorizados, funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, información comprometida por robo de equipos, desvelado de secretos, espionaje, etc.

No todas las amenazas son susceptibles de afectar a todos los tipos de activos. Existe una cierta relación entre el tipo de activo y lo que le podría ocurrir. Además, tampoco afectan a

todas las dimensiones (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad) por igual.

Ejemplo, un terremoto afecta a las instalaciones, en la dimensión Disponibilidad, aunque no en el resto de las dimensiones. Sin embargo, no sería considerado una amenaza directa para una aplicación.

En Magerit v3 – Libro II, capítulo 5 (pág. 25-47) [11], se detalla la relación de Amenazas-Tipo de activo-Dimensión.

[N] Desastres naturales, [I] De origen industrial, [E] Errores y fallos no intencionados, [A] Ataques intencionados.

A modo de ejemplo se muestra la siguiente tabla:

Tabla 7. Ejemplo relación Amenazas por tipo de activo/dimensión – [N] Desastres naturales

Código	[N]Desastres Naturales	Tipo Activo	Dimensión
N.1	Fuego	[HW] [Media] [AUX] [L]	[D]
N.2	Daños por agua	[HW] [Media] [AUX] [L]	[D]
N.*	Desastres naturales	[HW] [Media] [AUX] [L]	[D]

Debido a ello es necesario identificar a qué activos puede afectar cada amenaza, que nivel de degradación puede producirle en cada una de sus dimensiones y la probabilidad con la que puede ocurrir.

Para estimar la degradación, se determina en qué medida perdería el valor el activo en caso de que ocurra la amenaza. Para estimar la probabilidad, se estimará cual es la probabilidad de que se materialice. Para ello MAGERIT propone una escala nominal cualitativa o una numérica modelada como una frecuencia de ocurrencia temporal equivalentes.

Tabla 8. Escala de degradación del valor de activos. Magerit v3 – Libro II [11]

Degrado	Descripción
1%	Inapreciable
10%	Perceptible
100%	Total/irrecuperable

Tabla 9. Escala de probabilidad de ocurrencia de activos. Magerit v3 – Libro I [11]

Código		Descripción	
MA	100%	Muy frecuente	A diario
A	10%	Frecuente	Mensualmente
M	1%	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Una vez que se han identificado y valorado los activos, se conocen las amenazas a los que cada tipo de activo puede estar expuesto y valorado el daño que pueden producirles, se puede calcular el impacto y estimar el riesgo.

Tabla 10. Escalas cualitativas de impacto, probabilidad y riesgo. MAGERIT v3 – Libro II [11]

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

1. Impacto

Se denomina impacto al daño causado por la materialización de una amenaza sobre un activo. El impacto se calcula estimando el grado de degradación que una amenaza causaría sobre un determinado activo y dimensión, si se materializara.

El impacto potencial se refiere al impacto que se podría producir considerando que no se está aplicando ningún tipo de salvaguarda.

Es importante tener en cuenta las dependencias de los activos pues hacen que, si una amenaza afecta a un activo, también afecte a otros dependientes, influyendo en el valor del activo en función de todos los que dependen del mismo. Esta dependencia puede producir que una amenaza sobre un activo no muy importante pueda causar un impacto alto sobre otro dependiente.

Estimación del impacto

Se puede utilizar un método cualitativo basado en la misma escala nominal utilizada para la valoración de los activos. Se utilizarán los siguientes valores para el valor global, valor en cada dimensión de los activos, la magnitud del impacto y la magnitud del riesgo:

Tabla 11. Escala nominal de magnitud de impacto/riesgo

MB	muy bajo
B	bajo
M	medio
A	alto
MA	muy alto

Como escala de valoración de la degradación, se utilizará esta otra escala donde dependiendo del grado de afectación ante una amenaza, el daño puede ser prácticamente nulo, reseñable o muy severo. Un daño inapreciable significa que, aunque se produce una amenaza, no tiene casi efecto y puede no advertirse (1%). Un daño perceptible se puede apreciar algo, aunque sin efectos para el funcionamiento 10%. Un daño total afecta al funcionamiento de forma severa o irrecuperable (100%).

Tabla 12. Escala de degradación. MAGERIT v3 – Libro II [11]

Degradación	Descripción
1%	Inapreciable
10%	Perceptible
100%	Total/irrecuperable

Una vez se conoce el valor de los activos y la degradación que causa la amenaza sobre ellos, se puede calcular el impacto que estas amenazas tendrían sobre el SGSI, en base a tablas sencillas de doble entrada (valor, degradación):

Tabla 13. Cálculo del impacto. MAGERIT v3 – Libro II [11]

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

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

2. Cálculo del riesgo

Una vez se conoce el impacto potencial, teniendo en cuenta la probabilidad de que se materialice una amenaza sobre un activo, se calcula el riesgo potencial que es el riesgo estimado a partir del impacto producido por las amenazas sin tener en cuenta el efecto de ningún tipo de salvaguarda.

El cálculo de riesgo potencial normalmente se centra en los activos que hayan obtenido para alguna de las amenazas un impacto potencial (A)alto, (MA)muy alto o (M)medio, en el apartado anterior, dado que según la probabilidad serían susceptibles de alcanzar un riesgo (A)alto/(MA)muy alto.

Esta sería la escala cualitativa con la que se modelarán los valores de impacto, probabilidad y riesgo.

Tabla 14. Escalas cualitativas de impacto, probabilidad y riesgo. MAGERIT v3 – Libro II [11]

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

Estimación del riesgo

La estimación del riesgo resultaría de la combinación del impacto y frecuencia de la amenaza en una tabla.

Tabla 15. Matriz estimación del riesgo (impacto vs probabilidad). MAGERIT v3 – Libro II [11]

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

De esta forma quedaría determinado el riesgo, evaluando el impacto de cada amenaza sobre cada activo en cada una de sus dimensiones, teniendo en cuenta la probabilidad de que suceda. Dentro de los posibles valores de riesgo (MB, B, M, A, MA), los muy altos (MA) deberán ser gestionados inmediatamente.

2. Salvaguardas

Una vez calculado el riesgo potencial, la metodología MAGERIT v3 indica en el paso 3 que hay que determinar qué salvaguardas hay dispuestas y la valoración de su eficacia frente al riesgo. Las salvaguardas permiten hacer frente a las amenazas con el objetivo de reducir el riesgo. Una salvaguarda puede actuar sobre los 2 factores que las condicionan:

- Degradación: limitando o frenando una posible degradación una vez que se materializa la amenaza. Algunas lo que realizan es una pronta recuperación, en este caso la amenaza ocurre, aunque se limitan sus consecuencias.
- Probabilidad: reduciendo la probabilidad con la que puede ocurrir una amenaza. Tienen carácter preventivo, aunque lo ideal es impedir completamente la materialización de la amenaza. En este caso lo que se limita es la frecuencia de la amenaza.

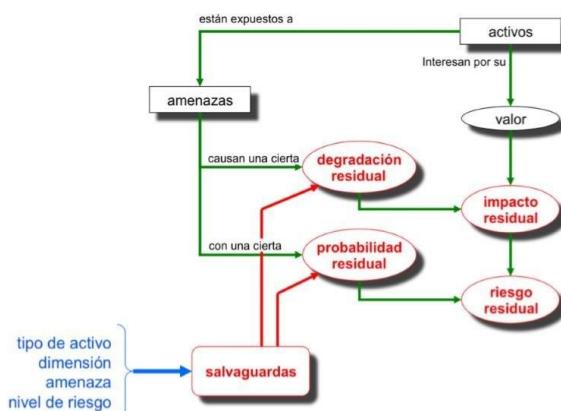


Figura 4. Elementos del análisis del riesgo residual. (Efectos de las salvaguardas)

(Fuente MAGERIT – Libro I)

Las salvaguardas aplicadas sobre un activo y dimensión, para contrarrestar una amenaza, actúan reduciendo la degradación o la probabilidad de que se materialice, reduciendo el nivel de riesgo.

Existen varios tipos de salvaguardas cuyo efecto es distinto:

Tabla 16. Tipos de salvaguardas. MAGERIT v3 – Libro I [10]

Efecto	Tipo	Descripción
Prevenir: Actúa sobre la probabilidad, reduciéndola	[PR] preventivas	Reduce las oportunidades de que la amenaza se produzca.
	[DR] disuasorias	Producen un efecto disuasorio ante los atacantes, antes de que se produzca.
	[EL] eliminatorias	Logra que el incidente se produzca actuando antes.
Limitar: Actúa sobre la degradación, acotándola	[IM] minimizadoras	Reduce el impacto acotando las consecuencias.
	[CR] correctivas	Actúan reparando el daño reduciéndolo, después de que se haya producido.
	[RC] recuperativas	Permiten retornar al estado anterior al incidente para reducir el daño.
Fortalecer: Complementan consolidando el efecto de las demás	[MN] de monitorización	Monitorizan lo que ocurre online o a posteriori sobre el incidente o estado del sistema. Permiten mejorar las salvaguardas o determinar impacto.
	[DC] de detección	Detectan y alertan de que un ataque se está produciendo, permitiendo reaccionar con otras medidas para pararlo o minimizar el impacto.
	[AW] de concienciación	Acciones de formación sobre las personas en contacto con el sistema. Reducen errores y potencian la eficacia de otras salvaguardas al mejorar el conocimiento de las personas que las operan.
	[AD] administrativas	Componentes y procesos de administración de la seguridad del sistema.

Para que una salvaguarda sea eficaz tiene que ser técnicamente adecuada para la amenaza contra la que se aplica, estar desplegada y en uso correctamente, los usuarios deben conocerla y existir controles que alerten ante un mal funcionamiento o nos dé idea de su eficacia. De modo que una eficacia del 0% correspondería a aquellas salvaguardas inexistentes, mientras que un 100% a aquellas idóneas y en uso perfectamente implantadas, mantenidas, controladas y conocidas. Se puede establecer una escala de madurez que refleje el grado de confianza del proceso de gestión de la salvaguarda.

Tabla 17. Eficacia y madurez de las salvaguardas. MAGERIT v3 – Libro I [10]

Factor	Nivel	Significado
0%	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Conforme evolucionan las nuevas tecnologías se producen cambios en los activos, lo cual precisa de una adecuación de las salvaguardas también.

El libro 2, Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, de Magerit v3 [11], proporciona en su capítulo 6 (pág. 53-57), la lista de salvaguardas relacionada con el tipo de activos a los que son aplicables.

Para la aplicación de salvaguardas nos centramos en los activos que hayan obtenido un riesgo Alto/Muy Alto. De todos ellos se analiza si es de aplicación alguna salvaguarda que ayude a reducir el grado de degradación o disminuir su probabilidad, de forma que afecte disminuyendo el impacto y/o riesgo. Del catálogo de salvaguardas se excluyen aquellas que no sean apropiadas para proteger la dimensión necesaria o no protegen frente a una amenaza, o aquellas cuya aplicación sea desproporcionada para el riesgo existente.

Una vez que se han determinado las salvaguardas se puede calcular tanto el impacto como el riesgo residual teniendo en cuenta la disminución del valor de degradación o de probabilidad que se da tras la aplicación de la salvaguarda.

[1. Impacto residual](#)

El paso 4 de MAGERIT establece el impacto residual como el impacto potencial modificado por el efecto de las salvaguardas aplicadas. Se estima calculando el nuevo nivel de degradación tras la aplicación de las salvaguardas.

En el anexo se calculará este valor para cada uno de los activos analizados.

[2. Riesgo residual](#)

El paso 5 de MAGERIT establece el riesgo residual como el riesgo potencial modificado por el efecto de las salvaguardas aplicadas. Se estima calculando el nuevo nivel de riesgo en base al impacto y probabilidad residuales tras aplicación de las salvaguardas.

En el anexo se calculará este valor para cada uno de los activos analizados.

[2. Tratamiento del riesgo](#)

Con el estudio realizado de impactos (lo que podría ocurrir) y riesgos (lo que probablemente ocurra), que da como resultado los activos a proteger (activos valorados), de qué protegerlos (amenazas) y cómo se pueden proteger (salvaguardas), se realizará la evaluación y el tratamiento de los riesgos determinando la acción a adoptar ante cada riesgo.

En función del nivel de criticidad de los riesgos, se valorarán los que deberían ser tratados y cuáles podrían ser asumidos por la empresa. Para ello hay que establecer el umbral de riesgo asumible por la organización.

Una vez se han identificado los requisitos de seguridad de la información, valorados los riesgos asociados a los activos de información y adoptadas las decisiones para su tratamiento, deben implementarse los controles para reducirlos a un nivel aceptable según los criterios establecidos por la organización.

Para cada riesgo se adoptarán medidas con un objetivo:

- **Aceptar:** La decisión de asumir un riesgo puede ser por factores no estrictamente técnicos, como legislación, por motivos políticos o compromisos contractuales con proveedores o usuarios. Cualquier riesgo aceptable debe ser conocido por la Dirección, que es quien será responsable de las consecuencias. Unido a la decisión de asumir un riesgo,

normalmente se ponen en marcha medidas que permitan hacerle frente, si sucediese, como planes de contingencia. También debería preverse una dotación para hacer frente a las consecuencias.

- **Evitar:** Mediante la adopción de medidas encaminadas a eliminar el origen del riesgo. Por ejemplo, eliminando un activo que no es esencial y cuya función puede realizarse con otra alternativa o forma.
- **Mitigar:** Aplicando medidas preventivas enfocadas a reducir las posibilidades de que ocurra o la degradación que causa una amenaza.
- **Compartir:** Se transfiere el riesgo, bien externalizando un servicio o componente del sistema de forma que se comparten responsabilidades, o bien contratando un seguro de forma que se reduce el impacto.

Conforme al análisis de riesgos descrito, para decidir sobre las acciones a adoptar para tratar el riesgo en cada uno de los activos de la empresa descritos en el Anexo, se aplicarán los siguientes criterios:

- Activos cuya estimación del riesgo sea (B)bajo, (MB)muy bajo, debido a que tienen una probabilidad baja de que ocurra o el impacto no es importante: **Aceptar**
- Activos cuya estimación del riesgo sea (M)Medio, no se tratarán con medidas directas para reducirlo, aunque sí que se tendrán en cuenta en los planes de contingencia y formación: **Aceptar**
- Activos cuyo riesgo sea (A)alto, (MA)muy alto, que suponen riesgos graves o críticos, serán tratados evaluando las salvaguardas adecuadas para reducirlos hasta un nivel aceptable: **Mitigar/Compartir**

3. Planes de Seguridad

Tomando como base el inventario de activos, amenazas y riesgos calculado en los apartados anteriores, una vez analizados los riesgos, las salvaguardas y decidido el tratamiento que se hará, se elaborará el plan de seguridad compuesto por los proyectos o programas de seguridad en los que se organizarán las medidas y decisiones adoptadas para el tratamiento de los riesgos.

Según se describe en Magerit – Libro I, capítulo 6 (pág. 73-76) [10], para ello se identificarán y formalizarán cada uno de los programas/proyectos de seguridad que reunirán las salvaguardas afines, complementarias o necesarias para cubrir objetivos comunes.

Para cada programa se implementarán fichas donde se detallará la siguiente información:

- Objetivo, código y nombre del programa
- Descripción del programa

- Activos afectados y amenazas afrontadas
- Salvaguardas para implantar o mejorar en el programa
- Unidad responsable de su ejecución
- Estimación de costes, esfuerzo y económicos
- Tareas que realizar
- Sistema de indicadores o controles que permitan conocer el grado de eficacia de las medidas implantadas

Tras determinar los programas de seguridad, se proporcionará un cronograma con la propuesta de planificación y la ordenación de la ejecución de los distintos programas, teniendo en cuenta criterios como criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, coste de cada programa, disponibilidad del personal que tiene que participar u otros factores como fecha de entrada en vigor de determinadas normativas, objetivos de la Organización, dependencias entre programas o con terceros, etc.

6. Resultados

El objetivo de este trabajo era el desarrollo de un Plan Director de Seguridad a partir de la implantación de un Sistema de Gestión de la Seguridad de la Información que sirviese para mejorar la seguridad en empresas pymes del sector de la construcción.

El alcance ha sido la elaboración de una propuesta de Plan Anual Director de Seguridad, listo para que la dirección de la empresa analizada lo supervise, eleve a aprobación y pueda proceder a su implantación si así lo considera.

El resultado del trabajo queda reflejado en el Anexo I y contempla todo el proceso seguido, utilizando la metodología MAGERIT, para la creación de los distintos programas que componen la propuesta de plan director de seguridad, que permitirán a la empresa la implantación ordenada y justificada de las medidas de seguridad necesarias para garantizar los niveles aceptables de riesgo según los análisis previos realizados.

Otro de los resultados ha sido la aplicación durante el presente trabajo de muchos de los conceptos y conocimientos vistos en todas las asignaturas del máster.

7. Conclusiones y trabajo futuro

A lo largo de la realización de este trabajo, en las entrevistas realizadas en la empresa, la Dirección manifestó la necesidad de abordar la transformación digital de su empresa como una de las líneas de su plan estratégico a 3 años, a la vez que mostró su inquietud sobre la forma de abordarla de forma segura, pues eran conscientes de los posibles riesgos e

impactos que se pudieran producir. La visión que les transmití en aquel momento fue que, para poder responder era importante conocer la situación actual de riesgos de la empresa y que en cualquier caso la mejor forma de abordarla sería habiendo tratado previamente los riesgos actuales.

Una vez realizado el trabajo, la principal conclusión que extraigo es la importancia de implantar un Sistema de Gestión de la Seguridad de la Información y desarrollar un Plan Director de Seguridad, que conste de al menos un análisis detallado de situación de la empresa, un análisis de riesgos y los consiguientes planes de seguridad que permitan mitigar los riesgos en aquello que sea posible o reducirlos hasta niveles aceptables.

Volviendo a la pregunta sobre cómo abordar de forma segura la transformación digital, mi respuesta sería algo así: *"desde la seguridad de la implantación de un SGSI y desarrollo del Plan Director de Seguridad que te permita conocer los riesgos y adoptar las medidas de forma ordenada para tratarlos y reducirlos hasta niveles aceptables"*.

La visión que les transmití en aquel momento fue que, para poder responder era importante conocer la situación actual de riesgos de la empresa y que en cualquier caso la mejor forma de abordarla sería habiendo tratado previamente los riesgos actuales.

Otra conclusión extraída es que la realización de un análisis formal permite justificar la inversión de los recursos de seguridad, además de indicar la priorización de los planes a abordar.

En mi opinión, el objetivo principal ha quedado cubierto formalizándose en una propuesta de Plan Director de Seguridad, que agrupa aquellos programas a abordar de forma prioritaria tras los resultados del análisis de realizado. Además, analizando el resultado también se puede observar que este plan puede ser válido y servir de guía para abordar en otro tipo de empresas similares, el cual era otro de los objetivos.

Como trabajo futuro inmediato, quedaría evaluar, validar y contrastar los resultados en una empresa, implantando los planes y retroalimentando el análisis de riesgos (frecuencias y valoraciones) con los registros de incidencias, ajustando desviaciones que se aprecien en la realidad respecto al trabajo realizado. También habría que identificar nuevos grupos de activos/amenazas clave y si procede habilitar nuevas contramedidas, a la vez que establecer métricas para evaluar la eficiencia.

A largo plazo queda la mejora continua a partir de la evaluación en una empresa y la evolución de la herramienta creada para realizar los cálculos del análisis de riesgos.

Referencias

1. UNE-EN ISO/IEC 27000:2019

ISO/IEC 27000 Family – Sistemas de Gestión de la Seguridad de la Información (SGSI).

Disponible en:

<https://www.aenor.com/normas-y-libros/busador-de-normas/UNE?c=N0061478>

2. BOLETÍN OFICIAL DEL ESTADO LEGISLACIÓN CONSOLIDADA: Jefatura del Estado «BOE» núm. 294, de 6 de diciembre de 2018 Referencia: BOE-A-2018-16673,

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en:

<https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (*Reglamento general de protección de datos*) Disponible en:

<https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>

4. Diario Oficial de la Unión Europea,

Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (*Reglamento general de protección de datos*) Disponible en:

[https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679R\(02\)&from=ES](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679R(02)&from=ES)

5. BOLETÍN OFICIAL DEL ESTADO LEGISLACIÓN CONSOLIDADA: Jefatura del Estado «BOE» núm. 298, de 14 de diciembre de 1999 Referencia: BOE-A-1999-2375,

Disponible en:

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Disponible en:

<https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>

6. Agencia española de protección de datos, <https://www.aepd.es/index.html>

7. ELDERECHO.COM: Artículo RGPD Mar España, febrero 2018. Disponible en:

<https://elderecho.com/mar-espana-el-25-de-mayo-tanto-el-sector-publico-como-el-privado-tiene-que-tener-implementado-un-analisis-de riesgos-y-una-evaluacion-de-impacto>

8. Capgemini Research Institute. 2019.

Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century. Disponible en:

<https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/09/Infographic---GDPR.pdf>

9. Ministerio de Hacienda y Administraciones Públicas. Octubre 2012.

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

10. Ministerio de Hacienda y Administraciones Públicas. Octubre 2012.

MAGERIT – versión 3.0. Libro I – Método. Disponible en:

https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d058567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

11. Ministerio de Hacienda y Administraciones Públicas. Octubre 2012. *MAGERIT – versión 3.0. Libro II – Catálogo de Elementos.* Disponible en:

https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_63012-171-8.pdf

Disponible en:

12. Ministerio de Hacienda y Administraciones Públicas. Octubre 2012.

MAGERIT – versión 3.0. Libro III – Guía de Técnicas. Disponible en:

https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e179cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf

13. INCIBE. Ene 2016. Colección “Protege tu empresa: Plan director de seguridad” Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-directorseguridad.pdf

14. ISO 38500 ISO/IEC 38500:2015. “*Corporate governance of information technology*”. Disponible en: <https://www.iso.org/standard/62816.html>
15. ISO 31000:2018, “*Risk management — Principles and guidelines*”. Disponible en: <https://www.iso.org/standard/65694.html>
16. AENOR – Asociación Española de Normalización y Certificación (2008). UNE 71504:2008 “*Metodología de análisis y gestión de riesgos para los sistemas de información*”. Disponible en:
<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430>
17. Portal de Administración Electrónica - Ministerio de Política Territorial y Función Pública.
<https://administracionelectronica.gob.es/pae/Home>
18. ISO/IEC 13335-1:2004
“*Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*”. Disponible en:
<https://www.iso.org/standard/39066.html>
19. ISO/IEC 27001:2013 ISMS Status,
“*Statement of Applicability (Soak) and Controls Status (gap analysis) workbook*” Disponible en:
https://iso27001security.com/ISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx
20. INCIBE, “Kit de concienciación para empresas.” Disponible en: <https://www.incibe.es/protege-tu-empresa/kit-conciencion>
21. UNE-ISO/IEC 27001:2017
“*Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)*”. Disponible en:
<https://www.aenor.com/normas-y-libros/buscador-de-normas/une?c=N0058428>
22. UNE-EN ISO/IEC 27002:2017

“Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).”

Disponible en:

<https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058429>

23. ISO/IEC 27003:2017

“Information technology -- Security techniques -- Information security management systems – Guidance” Disponible en:

<https://www.aenor.com/normas-y-libros/buscador-de-normas/ISO?c=063417>

24. INCIBE. Ene 2016. Colección *“Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario”* Disponible en:

<https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendoel-rgpd-guia-aproximacion-el-empresario>

25. ISO/IEC 27005:2018

“Information technology -- Security techniques -- Information security risk management”

Disponible en:

<https://www.aenor.com/normas-y-libros/buscador-de-normas/ISO?c=075281>

Anexo 1 – Plan Director de Seguridad

1. Contexto de la organización

[1.1 Introducción](#)

La empresa Anonym S.L. es una empresa que fue fundada en 1989 por parte de los hermanos Anonym (actuales gerentes). Se dedica a la promoción de vivienda y explotación de los activos inmobiliarios de la misma, dentro del ámbito local de Elche.

Esta empresa trabaja principalmente de cara al cliente particular o empresa final, interesado en viviendas, garajes o locales pertenecientes a la misma, ya sea venta o alquiler.

Aprovechando la sinergia del negocio y recursos de ésta, también ofrecen servicios de reformas.

Dentro de la actividad de la empresa, se podría distinguir entre dos líneas de actividad: todas las tareas relacionadas con la compra de suelo, promoción de obra nueva, construcción y comercialización; y otra línea relacionada con trabajos de reformas, gestión de las distintas empresas y explotación de los distintos activos de la empresa (alquiler garajes y locales).

El ejercicio de estas actividades conlleva la relación con clientes, distintos proveedores principalmente relacionados con el sector de la construcción (profesionales de oficios, empresas constructoras, empresas de materiales, estudios de arquitectura), empleados

(administración, internos y subcontratados), gabinetes jurídicos, notarías, consultoría fiscal y laboral, organismos, etc.

Actualmente la empresa tiene un pequeño portal web, cuyo desarrollo y mantenimiento ha sido contratado a una empresa informática especialista en estos servicios. El fin de este portal es simplemente el de publicitar información sobre las distintas promociones, así como los datos de contacto de la empresa.

La empresa cuenta con un Sistema de Planificación de Recursos Empresariales, ERP (por sus siglas en inglés, “Enterprise Resource Planning”), específico para la gestión de la actividad inmobiliaria (módulo de contabilidad, clientes, proveedores y facturación).

Por parte de los usuarios particulares y proveedores, esperan de Anonym, S.L. que toda su información sea protegida adecuadamente permitiéndoles realizar todas las gestiones que así sean necesarias.

Por parte de Anonym, S.L., espera que los servicios prestados por los distintos profesionales y proveedores se adecuen a las condiciones contractuales, por lo que la empresa ha de asegurar que dichas condiciones son suficiente para cubrir sus necesidades y que las garantías que ofrecen sus proveedores permiten cubrir sus servicios; por ejemplo mediante tiempos acotados de reaprovisionamiento de servicios y solución de averías, que las características contratadas son suficientes e incluso dejar un margen para operar con imprevistos, etc.

1.2 Estructura de la empresa

La empresa se organiza con una estructura en la que Anonym S.L. actúa como matriz de un grupo de empresas las cuales van siendo creadas para la gestión de cada promoción inmobiliaria concreta, mientras Anonym, S.L. se encarga del resto de actividades y gestión.

La empresa Anonym, S.L. se organiza mediante los siguientes departamentos.

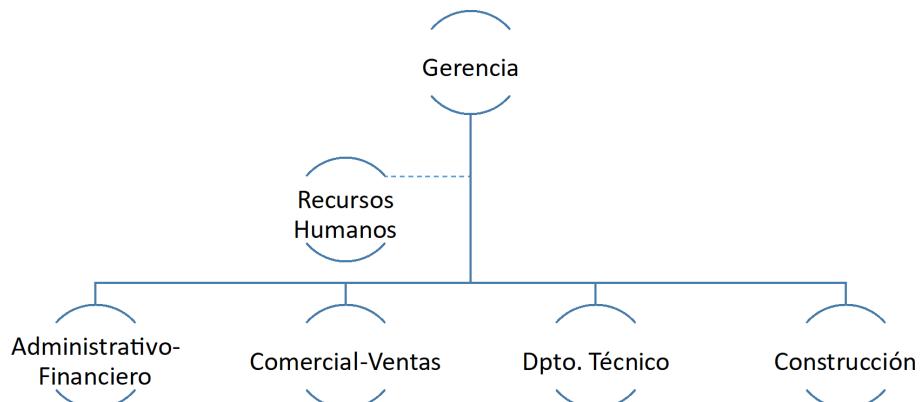


Figura 5. Estructura organizativa de la empresa

(Fuente propia)

Departamento comercial-ventas. Es responsable de la captación de nuevos clientes, mostrar y vender las viviendas. Se distinguen dos líneas de trabajo, la de clientes interesados en obra nueva, y la de clientes interesados en alquiler.

Esta parte se gestiona principalmente a través de herramientas ofimáticas y mediante generación de recursos digitales y emails. Cada cierto tiempo se generan campañas publicitarias para dar a conocer alguna promoción en curso, mediante anuncios en periódicos, vallas publicitarias, buzoneo, publicación de viviendas en portales inmobiliarios especializados (como *idealista.com*).

Departamento administrativo-financiero. Este departamento gestiona toda la información administrativo-contable de la empresa para el cumplimiento con las obligaciones fiscales y societarias. Para ello utiliza el ERP Prinex, software especializado para empresas del sector inmobiliario, el cual incluye módulos de gestión de facturación, contabilidad, clientes, proveedores y ventas. Tiene acceso a toda la información fiscal de todas las partes interesadas. En este departamento se formalizan las ventas y alquileres también. La empresa tiene contratados parte de los servicios financieros a una asesoría fiscal.

Recursos humanos. Este departamento es el responsable de la gestión de personas en la empresa, lo que significa que es responsable de los procesos de selección que en ella se producen. La parte de gestión administrativa relacionada con la generación de nóminas y contratos de personal está subcontratada a una asesoría laboral. El resto de las tareas propias de este ámbito, como pago nóminas, selección de personal, etc. lo asumen uno de los gerentes y una persona de la parte administrativo-financiera.

Departamento técnico. Este departamento se encarga principalmente de las direcciones de obra, relación con los estudios de arquitectura de las diferentes promociones, relación con los proveedores y demás empresas de servicios. La parte de dirección del departamento y relación con los proveedores, la asume el otro gerente. Dependiendo del periodo en el que se encuentra la empresa (principalmente número de promociones en construcción), se puede llegar a tener contratado mayor o menor número de personal técnico interno para las tareas directamente relacionadas con cada una de las obras. Las herramientas que utilizan habitualmente son de diseño gráfico, ofimáticas y email.

Departamento de construcción. Este departamento directamente está ubicado en cada una de las promociones, y está compuesto por personal de la empresa (un responsable y varios obreros), que trabajan y están a cargo de la coordinación y supervisión del resto de empresas y oficios contratados durante las distintas fases de las obras. No cuentan con ninguna herramienta informática para su trabajo, más allá de los smartphones de la empresa.

Gerencia. Este departamento está compuesto por los dos socios de Anonym, S.L. Normalmente uno se encarga de las áreas técnicas y construcción, el otro lo hace de las áreas administrativofinanciera y legal; mientras que la responsabilidad sobre el área

comercial-ventas, queda compartida. En cuanto a las políticas de seguridad de la información, esta área tiene acceso a toda la información y software de la empresa.

El resto de las tareas de mantenimiento de instalaciones, informática, legales, etc., son subcontratadas a otras empresas especializadas.

1.3 Aspectos técnicos

Los aspectos técnicos de la empresa describen los elementos de TI (Tecnologías de la información) con los que cuenta la empresa. La empresa posee una sede central, donde se ubican todos los departamentos excepto el de construcción.

La estructura a nivel técnico está compuesta por: Internet mediante un contrato global con la empresa VodaTel (*nombre ficticio*), a través de fibra óptica y varios equipos informáticos. Dependiendo del departamento y uso de los equipos, puede haber software especializado para cada puesto. Existe software común a todos ellos, normalmente herramientas ofimáticas. Todo el software ofimático de la empresa es software como servicio, por lo que los ordenadores básicos sólo necesitan acceso a internet y un navegador.

El software utilizado por los equipos comercial/ventas, difiere del utilizado por los equipos del departamento técnico o financiero, así como la potencia de equipo requerida.

Los equipos técnicos requieren potencia y software especializado para manejar planos e imágenes. Los equipos del departamento financiero utilizan el ERP Prinex para la gestión administrativo-contable de las empresas.

La sede central de la empresa donde están sus oficinas y la mayoría de los departamentos tiene red LAN y Wifi. Todos tienen acceso a internet. En esta sede se sitúa el servidor principal donde residen los sistemas y datos principales de la empresa, sobre los cuales se realiza una copia de seguridad diaria en las horas nocturnas sin actividad mediante un dispositivo de copias en cinta local al servidor. Adicionalmente, se realizan copias de determinada información a un servicio de almacenamiento en la nube.

Las herramientas que se utilizan son variadas, aunque la mayoría son servicios a través del navegador y ofimáticos, exceptuando el paquete ERP que está instalado en el servidor y los puestos lo ejecutan desde el mismo. Los programas de diseño gráfico están instalados en cada estación local que lo requiera.

El portal web de la empresa se sirve bajo un dominio, ha sido desarrollado y es mantenido por una empresa especializada en este tipo de portales. Está compuesto por páginas con fin publicitario de las promociones y servicios de la empresa, así como sus datos de contacto.

Los equipos informáticos son básicamente de tres tipos según sus características y propósito: Server, Workstation y Desktop.

El servidor es un PowerEdge de Dell en torre, tiene hardware específico de servidor diseñado para estar en funcionamiento 24x7. Tiene algunos componentes redundados

(discos en RAID1, doble tarjeta de red y doble fuente de alimentación). Mantiene todo el software de red, antivirus, dominio Windows y Active Directory. Se encarga de controlar el acceso de usuarios a la LAN y aplicar las políticas de seguridad sobre los diferentes recursos compartidos de la red. Así como de realizar tareas planificadas como copias de seguridad, mantenimiento de base de datos ERP, descarga de actualizaciones, etc.

Los desktops son estaciones básicas de trabajo de la gama profesional de DELL diseñados con componentes estables para uso profesional. La línea base se compone de un monitor de 21" full HD, 8GB RAM, procesador x64 i5, SO Windows 10 Pro, tarjetas gráfica y red GB integradas, disco SSD 128GB. Son utilizados en el departamento comercial-ventas, administrativo-financiero y gerencia.

Las workstations, son estaciones de trabajo Dell con una configuración de hardware más potente, diseñados con componentes estables para uso profesional. La línea base se compone de un monitor de 24" full HD, 16GB RAM, procesador x64 i7, SO Windows 10 Pro, tarjeta red integrada, tarjeta gráfica dedicada, disco SSD 256GB. Son utilizados en el departamento técnico.

Los portátiles, tienen diferentes características y están asignados a usuarios de los departamentos técnicos y gerencia normalmente. Aunque hay alguno de los más antiguos, que están disponibles para uso común.

Existen contextos de trabajo como casetas a pie de obra, en los que personal del departamento comercial y técnicos se desplazan durante determinados períodos. Esto obliga a contratar una línea de internet para la caseta.

Todos los puestos están configurados para trabajar sobre recursos de red u offline (determinadas funciones), de forma que cualquier información en local, debería ser temporal.

Las copias de seguridad se realizan en el servidor, mediante un dispositivo local de copias específico Dell PowerVault. Existe una política de dos tipos de copia, diaria y semanal. La copia diaria es incremental. La copia semanal es completa y mensualmente se guarda una copia completa en una caja fuerte.

Los usuarios y políticas de seguridad los administra la empresa informática con la que se tiene contratados el mantenimiento del sistema informático, según las directrices comentadas con gerencia.

Toda la documentación digital no temporal debe residir en los recursos de red gestionados por el servidor. Aunque también es importante destacar la utilización de unidades de almacenamiento USB para intercambio de información.

El servicio de correo electrónico es externo y se tienen contratados buzones con el dominio de la empresa. Pueden ser buzones nominales de uso personal, o genéricos para distintos

propósitos dentro de la empresa (ej. Buzón de ventas, buzón de contacto con la empresa, buzón de administración, ...)

También existen dispositivos móviles smartphones de empresa, asignados a los distintos usuarios.

1.4 Políticas de seguridad de la información

Las políticas de seguridad no están formalizadas, ni documentadas. La documentación existente son principalmente instrucciones de tipo técnico de algunos procesos. Los únicos procedimientos implantados son relativos a usuarios y permisos en la red. Son llevados a cabo por la empresa administradora de la informática.

Los usuarios deben ser dados de alta en el sistema para tener acceso a los distintos recursos. Además, se les proporciona un buzón personal para uso profesional, y según su función se les da acceso a los buzones genéricos que aplique.

Existen políticas respecto a la seguridad de las passwords: obligatoriedad, expiración, cambio periódico, fortaleza, complejidad, ...

No se ha realizado ninguna formación en materia de seguridad a los empleados de la empresa.

El acceso a internet no está restringido.

No existe una directriz formalizada en cuanto al uso de internet, correo ni redes sociales.

Dependiendo del departamento al que está asignado cada usuario, se le incluye en los grupos de red correspondientes para proporcionarle los privilegios necesarios.

Hay cinco grupos de usuarios básicamente: administradores, gerencia, técnicos, comercial/ventas, administrativo/financiero.

Existen distintos **grupos de recursos**, tanto de datos como de software.

Un grupo de **recursos y programas comunes**: Unidades con información compartida entre todos, software común como antivirus, cuadrante de vacaciones, diversa información común, ...

Grupo de **recursos específico** para cada departamento: Dependiendo del departamento al que pertenece cada usuario, tiene acceso a los recursos comunes, a los recursos propios de su departamento y puede que a algún otro recurso/software de otro departamento.

Por ejemplo, un usuario del departamento técnico tiene acceso a la información común y la técnica. Sin embargo, un usuario del departamento administrativo-financiero puede tener acceso a la común, a la suya específica y a la del departamento de ventas.

2. Situación actual del SGSI

Actualmente, la empresa no cuenta con un departamento de seguridad ni tampoco tiene subcontratada una empresa externa que realice esta tarea.

La responsabilidad de estas funciones y supervisar las tareas relacionadas con la seguridad recae en la gerencia y una persona del departamento administrativo-financiero, asesorados por la empresa de TI a la que se tiene contratado el mantenimiento informático. Esta supervisión se realiza de manera informal y reactiva ante incidentes producidos.

Por tanto, no se dispone de ningún SGSI definido, así como tampoco existe un análisis de riesgos que sirva como base al mismo, más allá de lo concerniente a la normativa de la LOPD.

En cuanto a documentación de seguridad, existe únicamente el documento de seguridad LOPD, que se encuentra desactualizado, el cual fue contratado a una empresa externa con el objetivo de cumplir estrictamente dicha norma y evitar sanciones.

Los requerimientos de seguridad no se encuentran documentados, ni las políticas de seguridad, ni los procedimientos de tratamiento de riesgos y actuación ante incidentes.

Actualmente, la empresa no cuenta con un departamento de seguridad ni tampoco tiene subcontratada una empresa externa que realice esta tarea.

No obstante, la dirección está sensibilizada con la necesidad de la implementación de un SGSI, pues son conscientes de los posibles riesgos e impactos relacionados con la gestión y protección de la información que se puedan producir, tanto económicos como reputacionales.

La implementación del SGSI será la base del proceso de mejora continua en materia de seguridad; que permitirá, conocer la situación de partida en materia de seguridad y medir el nivel de cada uno de los aspectos, así como plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales a los que se encuentre expuesta.

De acuerdo con los puntos de la plantilla “ISO/IEC 27001:2013 ISMS Status” [19] de la normativa ISO27001 [21], que permite analizar de una forma gráfica el nivel de implantación de un SGSI según la norma ISO 27000 [1], ésta sería la situación inicial de la empresa de la que se parte para la implementación del SGSI.

Estado de Implementación ISO 27001

Sección	Requerimientos ISO 27001	Estado
4	Contexto de la organización	
4,1	Comprensión de la organización y de su contexto	

4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial
4,2	Comprensión de las necesidades y expectativas de las partes interesadas	
4,2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Administrado
4,2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Repetible
4,3	Determinación del alcance del SGSI	
4,3	Determinar y documentar el alcance del SGSI	Inicial
4,4	SGSI	
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inexistente
5	Liderazgo	
5,1	Liderazgo y compromiso	
5,1	La administración debe demostrar liderazgo y compromiso por el SGSI	Repetible
5,2	Política	
5,2	Documentar la Política de Seguridad de la Información	Inicial
5,3	Roles, responsabilidades y autoridades en la organización	
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inicial
6	Planificación	
6,1	Acciones para tratar los riesgos y oportunidades	
6,1,1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	Inexistente
6,1,2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente
6,1,3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente
6,2	Objetivos de seguridad de la información y planificación para su consecución	
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inexistente
7	Soporte	
7,1	Recursos	
7,1	Determinar y asignar los recursos necesarios para el SGSI	Repetible
7,2	Competencia	
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Inicial
7,3	Concienciación	
7,3	Implementar un programa de concienciación de seguridad	Inicial
7,4	Comunicación	
7,4	Determinar las necesidades de comunicación internas y externas relacionadas al SGSI	Inexistente
7,5	Información documentada	
7,5,1	Proveer documentación requerida por el estándar más la requerida por la organización	Inexistente
7,5,2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inexistente
7,5,3	Mantener un control adecuado de la documentación	Inexistente
8	Operación	
8,1	Planificación y control operacional	
8,1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	Inexistente
8,2	Apreciación de los riesgos de seguridad de la información	
8,2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inexistente
8,3	Tratamiento de los riesgos de seguridad de la información	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente
9	Evaluación del desempeño	
9,1	Seguimiento, medición, análisis y evaluación	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inicial
9,2	Auditoría interna	
9,2	Planificar y realizar una auditoría interna del SGSI	Inicial
9,3	Revisión por la dirección	
9,3	La administración realiza una revisión periódica del SGSI	Inicial
10	Mejora	
10,1	No conformidad y acciones correctivas	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inicial
10,2	Mejora continua	
10,2	Mejora continua del SGSI	Repetible

1 - Figura 6. Situación actual de implantación de la normativa ISO 27001

(Fuente propia)



Figura 7. Esquema de situación actual de implantación del SGSI

(Fuente propia)

Como se puede observar el estado de implementación del SGSI está en un nivel muy prematuro, con el 75% de requerimientos inexistentes o en una fase inicial.

Lo existente está mayoritariamente en estado repetible, se realiza de un modo totalmente informal (con procedimientos propios, informales). No estando definidos los procedimientos formalmente, ni documentados.

Sería necesario desarrollar la normativa de seguridad en la empresa a través de políticas y procedimientos.

Dentro del SGSI, sería aconsejable realizar un plan de formación y concienciación del personal sobre riesgos y seguridad.

3. Catálogo general de activos

En esta sección se desarrolla la lista de elementos a proteger en un sistema de información, aquellos que tienen un valor para la organización determinado por la importancia que tienen desde el punto de vista del perjuicio que le causaría perderlos o su deterioro, y en consecuencia serían objeto de aplicarles ciertas medidas de seguridad.

El valor se determina en varias dimensiones de valoración (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad), que son las características para preservar que hacen valioso un activo. Las dimensiones se utilizan para valorar las consecuencias de la

materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Cada tipo de activo y dimensión es susceptible de sufrir ciertas amenazas accidental o deliberadamente, y soporta determinadas salvaguardas.

3.1. Inventario de Activos

A continuación, se lista el **catálogo general de activos** valorados de la empresa.

Tabla 18. Catálogo general de activos.

Tipo de Activo	Tipo	Código de Activo	Nombre del Activo	Valor
2.1. [info] Activos esenciales				
[info]	[per]	I001	Fichero Clientes	MA
2.3. [D] Datos / Información				
[D]	[info]	D001	Expediente Cliente	A
[D]	[password]	D002	Datos acceso Servidor	MA
[D]	[password]	D003	Datos acceso Usuarios	A
[D]	[backup]	D004	Backup Servidor	A
[D]	[log]	D005	Fichero log	A
[D]	[conf]	D006	Ficheros configuraciones	A
2.4. [K] Claves criptográficas				
[K]	[info][sign][public _signature]	K001	Certificados FMNT	M
2.6. [SW] Software - Aplicaciones informáticas				
[SW]	[SW]	SW001	ERP	A
[SW]	[std][office]	SW002	Paquete ofimático	M

[SW]	[std][email_client]	SW003	Cliente de correo	A
[SW]	[std][av]	SW004	Antivirus	A
[SW]	[std][backup]	SW005	Sistema de backup	A
[SW]	[std][browser]	SW006	Navegador web	B
[SW]	[web]	SW007	Portal Web	B
[SW]	[std][os]	SW008	Sistema operativo Servidor	A
[SW]	[std][os]	SW009	Sistema operativo cliente	M
2.7. [HW] Equipamiento informático (hardware)				
[HW]	[mid]	HW001	Servidor	MA
[HW]	[pc]	HW002	Desktop	M
[HW]	[pc]	HW003	Workstation	M
[HW]	[pc]	HW004	Laptop	M
[HW]	[backup]	HW005	Unidad Backup	A
[HW]	[peripheral][print]	HW006	Impresora	B
[HW]	[peripheral][scan]	HW007	Plotter	MB
[HW]	[network][router]	HW008	Router	A
[HW]	[network][switch]	HW009	Switch	A
2.8 [COM] Redes de comunicaciones				
[COM]	[PSTN][mobile]	COM001	Servicio de Telefonía	A
[COM]	[LAN]	COM002	Red local	A
[COM]	[ADSL]	COM003	ADSL/Fibra	A
[COM]	[www]	COM004	Red-wifi	M
2.9. [Media] Soportes de información				
[Media]	[usb]	MEDIA001	Memorias USB	A
[Media]	[disk_ext]	MEDIA002	Discos removibles USB	A
2.10. [AUX] Equipamiento auxiliar				
[AUX]	[ups]	AUX001	SAI	M
2.11. [L] Instalaciones				
[L]	[building]	L001	Edificio empresa	A
[L]	[local]	L002	Cuarto de comunicaciones	MA
2.12. [P] Personal				
[P]	[ui]	P001	Personal interno (Gerencia)	MA
[P]	[ui]	P002	Personal interno (Responsables área)	A
[P]	[ui]	P003	Resto personal interno	M
[P]	[ue]	P004	Personal externo (administrador sistemas)	A

3.2. Fichas detalle de activos

Éstas serían las **Fichas de Activo** con información descriptiva y valoración de cada uno.

3.2.1. [info] Activos esenciales

Los tipos de activo [info] son activos **esenciales** que se refieren a la información que se maneja. Pueden clasificarse en datos de carácter personal regulados por leyes y reglamentos, o también pueden tener una confidencialidad relevante y estar sujetos a normativa específica de control de acceso y distribución.

Tabla 19. Ficha de activo [I001]-Fichero Clientes

2.1. [info] Activos esenciales		Valoración - Dimensión						
Código: I001	Nombre: Fichero Clientes	[I]	[C]	[D]	[A]	[T]	Total	
		MA	MA	A	MA	A	MA	
descripción: Fichero de clientes con información personal								
propietario: Responsable Administración responsable: Gerente								
tipo: [vr][per][M][classified][R]								

3.2.2. [arch] Arquitectura del sistema

En esta categoría de activos, no se han censado activos relevantes para el desarrollo del presente trabajo. Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.

3.2.3. [D] Datos / Información

Los tipos de activo [D] Datos / Información se refieren a los que materializan la información.

Tabla 20. Ficha de activo [D001]-Expediente Cliente

2.3. [D] Datos / Información		Valoración - Dimensión						
Código: D001	Nombre: Expediente Cliente	[I]	[C]	[D]	[A]	[T]	Total	
		A	MA	M	MA	A	A	
descripción: Contratos, compraventas, arras, alquiler, ...								
propietario: Responsable Administración responsable: Gerente								
tipo: [info]								

Tabla 21. Ficha de activo [D002]-Datos acceso Servidor

2.3. [D] Datos / Información		Valoración - Dimensión					
Código: D002	Nombre: Datos acceso Servidor	[I]	[C]	[D]	[A]	[T]	Total
		MA	MA	MA	MA	A	MA
descripción:	Credenciales acceso al servidor						
propietario:	Responsable TI	responsable:					
Gerente							
tipo:	[password]						

Tabla 22. Ficha de activo [D003]-Datos acceso Usuarios

2.3. [D] Datos / Información		Valoración - Dimensión					
Código: D003	Nombre: Datos acceso Usuarios	[I]	[C]	[D]	[A]	[T]	Total
		MA	MA	M	MA	A	A
descripción:	Credenciales acceso a los puestos cliente						
propietario:	Usuario responsable:	Usuario					
tipo:	[password]						

Tabla 23. Ficha de activo [D004]-Backup Servidor

Tabla 24. Ficha de activo [D005]-Logs

Tabla 25. Ficha de activo [D006]-Ficheros configuraciones

3.2.4. [K] Claves criptográficas

Los activos [K] Claves criptográficas se emplean para proteger el secreto o autenticar a las partes.

Son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

Tabla 26. Ficha de activo [K001]-Certificados FMNT

3.2.5. [S] Servicios

No se han censado activos de este tipo para su análisis durante el presente trabajo, pues se trata de servicios prestados por el sistema a usuarios del servicio. En este caso la empresa no presta un servicio como tal. En todo caso el portal web clasificado como activo de tipo SW, se podría analizar dentro de este apartado al estar subcontratado el mantenimiento y hosting de la página.

3.2.6. [SW] Software - Aplicaciones informáticas

Los tipos de activo [SW] Software - Aplicaciones informáticas se refieren a aquellas aplicaciones que permiten manejar los datos.

Tabla 27. Ficha de activo [SW001]-ERP

Tabla 28. Ficha de activo [SW002]-Paquete ofimático

Tabla 29. Ficha de activo [SW003]-Cliente de correo

Tabla 30. Ficha de activo [SW004]-Antivirus

Tabla 31. Ficha de activo [SW005]-Software de backup

Tabla 32. Ficha de activo [SW006]-Navegador web

Tabla 33. Ficha de activo [SW007]-Portal Web

Tabla 34. Ficha de activo [SW008]-Sistema operativo servidor

Tabla 35. Ficha de activo [SW009]- Sistema operativo cliente

[**3.2.7. \[HW\] Equipamiento informático \(hardware\)**](#)

Los tipos de activo [HW] Hardware se refieren al equipamiento informático que permite hospedar datos, aplicaciones y servicios.

Tabla 36. Ficha de activo [HW001]-Servidor

Tabla 37. Ficha de activo [HW002]-Desktop

Tabla 38. Ficha de activo [HW003]-Workstation

Tabla 39. Ficha de activo [HW004]-Laptop

Tabla 40. Ficha de activo [HW005]-Unidad de Backup

Tabla 41. Ficha de activo [HW006]-Impresora

Tabla 42. Ficha de activo [HW007]-Plotter

Tabla 43. Ficha de activo [HW008]-Router

Tabla 44. Ficha de activo [HW009]-Switch

[**3.2.8. \[COM\] Redes de comunicaciones**](#)

Los tipos de activo [COM] Redes de comunicaciones, se refieren a aquellos elementos que permiten intercambiar datos.

Tabla 45. Ficha de activo [COM001]-Línea telefónica

Tabla 46. Ficha de activo [COM002]-Red Local

Tabla 47. Ficha de activo [COM003]-ADSL/Fibra

Tabla 48. Ficha de activo [COM004]-Red Wifi

3.2.9. [Media] Soportes de información

Los tipos de activo [Media] Soportes de información se refieren a dispositivos de almacenamiento de datos.

Tabla 49. Ficha de activo [MEDIA001]-Memorias USB

Tabla 50. Ficha de activo [MEDIA002]-Discos removibles USB

3.2.10. [AUX] Equipamiento auxiliar

Los tipos de activo [AUX] Equipamiento auxiliar se refieren al equipamiento que complementa el material informático.

Tabla 51. Ficha de activo [AUX001]-SAI

3.2.11. [L] Instalaciones

Los tipos de activo [L] Instalaciones se refieren a las instalaciones que acogen equipos informáticos y de comunicaciones.

Tabla 52. Ficha de activo [L001]-Edificio empresa

Tabla 53. Ficha de activo [L002]-Cuarto de comunicaciones

3.2.12. [P] Personal

Los tipos de activo [P] Personas se refieren a los que explotan u operan todos los elementos anteriormente citados.

Tabla 54. Ficha de activo [P001]- Personal interno (Gerencia)

Tabla 55. Ficha de activo [P002]-Personal interno (Responsables de Área)

Tabla 56. Ficha de activo [P003]-Resto empleados internos

Tabla 57. Ficha de activo [P004]-Personal externo

4. Identificación de amenazas

En este apartado se lleva a cabo la identificación y valoración de las amenazas a las que están expuestos los activos en cada una de sus dimensiones y la probabilidad de que se materialicen. Se define amenaza como “*Causa potencial de un incidente que puede causar daños a un sistema de información o a una Organización.*”, según la norma [UNE 71504:2008] [16].

Las amenazas pueden tener un origen diverso, tanto interno como externo a la organización, (accidentes naturales, del entorno, fallos y vulnerabilidades en aplicaciones y equipamiento, accidentales o intencionadas causadas por personas).

No todas las amenazas son susceptibles de afectar a todos los tipos de activos. Existe una cierta relación entre el tipo de activo y lo que le podría ocurrir. Además, tampoco afectan a

todas las dimensiones (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad) por igual.

Es por lo que es necesario identificar a qué activos puede afectar cada amenaza, qué nivel de degradación puede producirle en cada una de sus dimensiones y la probabilidad con la que puede ocurrir. Para estimar la degradación se determina en qué medida perdería el valor el activo en caso de que ocurra la amenaza. Para estimar la probabilidad se estimará cual es la probabilidad de que se materialice.

A continuación, se detalla el nivel de degradación de los activos (y dimensión) del sistema de información de la empresa y probabilidad de que se vean afectados por las amenazas de tipo Desastres naturales, [I] De origen industrial, [E] Errores y fallos no intencionados, [A] Ataques intencionados, según el catálogo de amenazas propuesto por Magerit v3.

Para ello se utilizará la siguiente plantilla y escalas de valores:

Tabla 58. Escala de degradación del valor de activos. Magerit v3 – Libro II [11]

Degrado	Descripción
1%	Inapreciable
10%	Perceptible
100%	Total/irrecuperable

Tabla 59. Escala de probabilidad de ocurrencia de activos. Magerit v3 – Libro I [11]

Código		Descripción	
MA	100%	Muy frecuente	A diario
A	10%	Frecuente	Mensualmente
M	1%	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Tabla 60. Plantilla de Ficha amenazas de tipo [N.1] Amenaza ejemplo

[N.1]Amenaza ejemplo				
Descripción:	Breve descripción de la amenaza y sus consecuencias			
Tipos Activo:	[Códigos de cada tipo de activo que puede ser vulnerable ante la amenaza] (*)	Dimensiones:	[a las que afecta]	
Activos afectados		Probabilidad	% Degrado	
			[I]	[C]
< Código – Nombre Activo >			1	10
			100	

(*) Códigos de tipos de activo utilizados en la sección anterior "3. Catálogo general de activos."

4.1. [N] Desastres naturales

Tabla 61. Ficha amenazas de tipo [N] Desastres naturales

[N] Desastres naturales							
Posibilidad de que se acabe con recursos del sistema por el efecto de inundaciones, fuego u otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...							
Amenazas							
N.1	Fuego						
N.2	Daños por agua						
N.*	Desastres naturales						
Tipos de Activo afectados		Dimensiones					
[HW] [Media] [AUX] [L]		[D]					
Activo		Probabilidad (Frec)	% Degradación				
[I]		[C]	[D]	[A]	[T]		
HW001-Servidor		MB	100				
HW002-Desktop		MB	100				
HW003-Workstation		MB	100				
HW004-Laptop		MB	100				
HW005-Unidad Backup		MB	100				
HW006-Impresora		MB	100				
HW007-Plotter		MB	100				
HW008-Router		MB	100				
HW009-Switch		MB	100				
MEDIA001-Memorias removibles USB		MB	100				
MEDIA002-Discos duros removibles		MB	100				
AUX001-SAI		MB	100				
L001-Edificio empresa		MB	100				
L002-Cuarto de comunicaciones		MB	100				

4.2. [I] De origen industrial

Tabla 62. Ficha amenazas de tipo [I.1] Fuego

[I.1] Fuego						
Descripción:	Incendio: Posibilidad de que el fuego acabe con recursos del sistema por el efecto de sucesos que pueden ocurrir derivados de la actividad humana de tipo industrial, ya sea de forma accidental o deliberada.					
Tipos Activo:	[HW] [Media] [AUX] [L]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
HW001-Servidor		B			100	
HW002-Desktop		B			100	
HW003-Workstation		B			100	
HW004-Laptop		B			100	
HW005-Unidad Backup		B			100	
HW006-Impresora		B			100	
HW007-Plotter		B			100	
HW008-Router		B			100	
HW009-Switch		B			100	
MEDIA001-Memorias removibles USB		B			100	
MEDIA002-Discos duros removibles		B			100	
AUX001-SAI		B			100	
L001-Edificio empresa		MB			100	
L002-Cuarto de comunicaciones		B			100	

Tabla 63. Ficha amenazas de tipo [I.2] Agua

[I.2] Agua						
Descripción:	Escapes, fugas, inundaciones: Posibilidad de que el agua acabe con recursos del sistema por el efecto de sucesos que pueden ocurrir derivados de la actividad humana de tipo industrial, ya sea de forma accidental o deliberada.					
Tipos Activo:	[HW] [Media] [AUX] [L]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
HW001-Servidor		B			100	
HW002-Desktop		B			100	
HW003-Workstation		B			100	
HW004-Laptop		B			100	
HW005-Unidad Backup		B			100	
HW006-Impresora		B			100	
HW007-Plotter		B			100	
HW008-Router		B			100	
HW009-Switch		B			100	
MEDIA001-Memorias removibles USB		B			100	
MEDIA002-Discos duros removibles		B			100	
AUX001-SAI		B			100	
L001-Edificio empresa		MB			10	
L002-Cuarto de comunicaciones		MB			10	

Tabla 64. Ficha amenazas de tipo [I.*] Desastres industriales

[I.*] Desastres industriales						
Descripción:	Otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...					
Tipos Activo:	[HW] [Media] [AUX] [L]			Dimensiones: [D]		
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A]
HW001-Servidor	MB			100		
HW002-Desktop	MB			100		
HW003-Workstation	MB			100		
HW004-Laptop	MB			100		
HW005-Unidad Backup	MB			100		
HW006-Impresora	MB			100		
HW007-Plotter	MB			100		
HW008-Router	MB			100		
HW009-Switch	MB			100		
MEDIA001-Memorias removibles USB	MB			100		
MEDIA002-Discos duros removibles	MB			100		
AUX001-SAI	MB			100		
L001-Edificio empresa	MB			10		
L002-Cuarto de comunicaciones	MB			10		

Tabla 65. Ficha amenazas de tipo [I.3] Contaminación mecánica

[I.3] Contaminación mecánica						
Descripción:	Daños causados por vibraciones, polvo, suciedad, ...					
Tipos Activo:	[HW] [Media] [AUX]			Dimensiones: [D]		
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A]
HW001-Servidor	M				10	
HW002-Desktop	M				10	
HW003-Workstation	M				10	
HW004-Laptop	M				10	
HW005-Unidad Backup	M				10	
HW006-Impresora	B				10	
HW007-Plotter	B				10	
HW008-Router	B				10	
HW009-Switch	B				10	
MEDIA001-Memorias removibles USB	B				1	
MEDIA002-Discos duros removibles	M				10	
AUX001-SAI	MB				100	

Tabla 66. Ficha amenazas de tipo [I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética					
Descripción:	Daños causados por interferencias de radio, campos magnéticos, luz ultravioleta, ...				
Tipos Activo:	[HW] [Media] [AUX]	Dimensiones: [D]			
Activos afectados		Probabilidad	% Degradación		
			[I]	[C]	[D]
HW001-Servidor		MB		10	
HW002-Desktop		MB		10	
HW003-Workstation		MB		10	
HW004-Laptop		MB		10	
HW005-Unidad Backup		MB		10	
HW006-Impresora		B		10	
HW007-Plotter		B		10	
HW008-Router		B		10	
HW009-Switch		B		10	
MEDIA001-Memorias removibles USB		MB		100	
MEDIA002-Discos duros removibles		MB		100	
AUX001-SAI		MB		100	

Tabla 67. Ficha amenazas de tipo [I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico					
Descripción:	Fallos en los equipos y/o programas, que pueden deberse a un defecto de origen o durante el funcionamiento del sistema.				
Tipos Activo:	[SW] [HW] [Media] [AUX]	Dimensiones: [D]			
Activos afectados		Probabilidad	% Degradación		
			[I]	[C]	[D]
SW001-ERP		MB		10	
SW002-Paquete ofimático		B		10	
SW003-Cliente de correo		MB		10	
SW004-Antivirus		MB		10	
SW005-Sistema de backup		MB		10	
SW006-Navegador web		MB		10	
SW007-Portal web		MB		10	
SW008-Sistema operativo Servidor		MB		10	
SW009-Sistema operativo cliente		MB		10	
HW001-Servidor		B		100	
HW002-Desktop		B		100	
HW003-Workstation		B		100	
HW004-Laptop		B		100	
HW005-Unidad Backup		B		100	
HW006-Impresora		MB		100	
HW007-Plotter		MB		100	
HW008-Router		MB		100	
HW009-Switch		MB		100	
MEDIA001-Memorias removibles USB		MB		10	
MEDIA002-Discos duros removibles		MB		10	
AUX001-SAI		B		100	

Tabla 68. Ficha amenazas de tipo [I.6] Corte de suministro eléctrico

[I.6] Corte de suministro eléctrico					
Descripción:	Daño causado por un corte de la energía eléctrica				
Tipos Activo:	[HW] [Media] [AUX]	Dimensiones: [D]			
Activos afectados		% Degradación			
		[I]	[C]	[D]	[A]
HW001-Servidor	B		100		
HW002-Desktop	B		100		
HW003-Workstation	B		100		
HW004-Laptop	MB		10		
HW005-Unidad Backup	B		100		
HW006-Impresora	B		100		
HW007-Plotter	B		100		
HW008-Router	B		100		
HW009-Switch	B		100		
MEDIA001-Memorias removibles USB	B		100		
MEDIA002-Discos duros removibles	B		100		
AUX001-SAI	MB		10		

Tabla 69. Ficha amenazas de tipo [I.7] Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura o humedad					
Descripción:	Daños causados cuando las condiciones de climatización afectan el trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...				
Tipos Activo:	[HW] [Media] [AUX]	Dimensiones: [D]			
Activos afectados		% Degradación			
		[I]	[C]	[D]	[A]
HW001-Servidor	MB		10		
HW002-Desktop	MB		10		
HW003-Workstation	MB		10		
HW004-Laptop	MB		10		
HW005-Unidad Backup	MB		10		
HW006-Impresora	MB		10		
HW007-Plotter	MB		10		
HW008-Router	MB		100		
HW009-Switch	MB		100		
MEDIA001-Memorias removibles USB	MB		10		
MEDIA002-Discos duros removibles	MB		10		
AUX001-SAI	B		100		

Tabla 70. Ficha amenazas de tipo [I.8] Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones						
Descripción:	Daños producidos por el cese de las comunicaciones: línea, servicio, sobrecarga, ...					
Tipos Activo:	[COM]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
COM001-Servicio de telefonía		MB			100	
COM002-Red local		MB			100	
COM003-Fibra óptica		MB			100	
COM004-Red wifi		MB			10	

Tabla 71. Ficha amenazas de tipo [I.9] Interrupción de otros servicios y suministros esenciales /

[I.9] Interrupción de otros servicios y suministros esenciales						
Descripción:	Averías provocadas por otros servicios o recursos de los que depende la operación de los equipos: papel para las impresoras, tóner, refrigerante, ...					
Tipos Activo:	[AUX]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
AUX001-SAI		MB			10	

Tabla 72. Ficha amenazas de tipo [I.10] Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información						
Descripción:	Degradoación propia del uso a consecuencia del paso del tiempo.					
Tipos Activo:	[Media]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
MEDIA001 - Memorias removibles USB		B			10	
MEDIA002 - Discos duros removibles		MB			10	

Tabla 73. Ficha amenazas de tipo [I.11] Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas								
Descripción:	Un dispositivo electrónico emite radiaciones que pueden ser interceptadas por otros equipos terceros y derivar en una fuga de información. Es una amenaza donde el emisor actúa como víctima pasiva del ataque. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, ..., que estarán amenazadas de interceptación.							
	Tipos Activo:		Dimensiones:		[C]			
Activos afectados			% Degradación					
			[I]	[C]	[D]	[A]		
HW001-Servidor			MB	1				
HW002-Desktop			MB	1				
HW003-Workstation			MB	1				
HW004-Laptop			MB	1				
HW005-Unidad Backup			MB	1				
HW006-Impresora			MB	1				
HW007-Plotter			MB	1				
HW008-Router			MB	1				
HW009-Switch			MB	1				
MEDIA001-Memorias removibles USB			MB	1				
MEDIA002-Discos duros removibles			MB	1				
AUX001-SAI			MB	1				
L001-Edificio empresa			MB	1				
L002-Cuarto de comunicaciones			MB	1				

4.3. [E] Errores y fallos no intencionados

Tabla 74. Ficha amenazas de tipo [E.1] Errores de los usuarios

[E.1] Errores de los usuarios							
Descripción:	Errores de las personas al utilizar los servicios, datos, ...						
Tipos Activo:	[D] [Info] [keys] [S] [SW] [Media]		Dimensiones:		[I]	[C]	[D]
Activos afectados		Probabilidad	% Degradación				
			[I]	[C]	[D]	[A]	
						[T]	
I001-Fichero Clientes	M	10	10	10			
D001-Expediente Cliente	A	10	1	10			
D002-Datos acceso Servidor	MB	1	1	1			
D003-Datos acceso Usuarios	B	10	10	10			
D004-Backup Servidor	MB	1	1	1			
D005-Fichero log	MB	1	1	1			
D006-Ficheros configuraciones	MB	1	1	1			
K001-Certificados FMNT	MB	10	1	10			
SW001-ERP	M	10	10	10			
SW002-Paquete ofimático	M	1	10	10			
SW003-Cliente de correo	M	1	1	10			
SW004-Antivirus	MB	1	1	1			
SW005-Sistema de backup	MB	1	1	1			
SW006-Navegador web	M	1	10	1			
SW007-Portal web	MB	1	1	1			
SW008-Sistema operativo Servidor	MB	1	1	1			
SW009-Sistema operativo cliente	M	1	1	1			
MEDIA001-Memorias USB	M	10	100	10			
MEDIA002-Discos USB	B	10	100	10			

Tabla 75. Ficha amenazas de tipo [E.2] Errores del administrador

[E.2] Errores del administrador											
Descripción:	Errores de las personas que tienen responsabilidades de instalación y operación en el ejercicio de su función.										
Tipos Activo:	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	Dimensiones:	[D]	[I]	[C]
Activos afectados		Probabilidad						% Degradación			
		[I]	[C]	[D]	[A]	[T]					
I001-Fichero Clientes	B	10	10	10							
D001-Expediente Cliente	B	10	10	10							
D002-Datos acceso Servidor	B	10	100	10							
D003-Datos acceso Usuarios	MB	1	1	1							
D004-Backup Servidor	B	100	10	10							
D005-Fichero log	B	10	10	10							
D006-Ficheros configuraciones	B	10	10	10							
K001-Certificados FMINT	MB	100	1	10							
SW001-ERP	MB	10	10	10							
SW002-Paquete ofimático	MB	1	10	10							
SW003-Cliente de correo	MB	1	10	10							
SW004-Antivirus	B	10	10	10							
SW005-Sistema de backup	B	10	10	10							
SW006-Navegador web	MB	1	10	10							
SW007-Portal web	MB	10	10	10							
SW008-Sistema operativo Servidor	B	10	10	10							
SW009-Sistema operativo cliente	MB	1	10	10							
HW001-Servidor	MB	10	10	10							
HW002-Desktop	MB	1	10	10							
HW003-Workstation	MB	1	10	10							
HW004-Laptop	MB	1	10	10							
HW005-Unidad Backup	MB	1	10	10							
HW006-Impresora	MB	1	1	1							
HW007-Plotter	MB	1	1	1							
HW008-Router	B	10	10	10							
HW009-Switch	MB	1	1	10							
COM001-Servicio de telefonía	MB	1	1	1							
COM002-Red local	B	10	10	10							
COM003-Fibra óptica	MB	1	1	1							
COM004-Red wifi	B	10	10	10							
MEDIA001-Memorias USB	MB	10	100	10							
MEDIA002-Discos USB	MB	1	10	1							

Tabla 76. Ficha amenazas de tipo [E.3] Errores de monitorización (log)

[E.3] Errores de monitorización (log)						
Descripción:	Uso inadecuado del registro de actividades: registros con información incompleta o inexistente.					
Tipos Activo:	[D.log]			Dimensiones:	[I] [T]	
Activos afectados		Probabilidad	% Degradación			
D005-Fichero log		MB	[I]	[C]	[D]	[A] [T]
			10			10

Tabla 77. Ficha amenazas de tipo [E.4] Errores de configuración

[E.4] Errores de configuración						
Descripción:	Errores relacionados con la configuración de cada activo, normalmente introducida por el administrador.					
Tipos Activo:	[D.conf]			Dimensiones:	[I]	
Activos afectados		Probabilidad	% Degradación			
D006-Ficheros configuraciones		B	[I]	[C]	[D]	[A] [T]
			10			

Tabla 78. Ficha amenazas de tipo [E.7] Deficiencias en la organización

[E.7] Deficiencias en la organización						
Descripción:	Cuando la definición de funciones y tareas no están claras, qué hacer y cuándo, incluido informar a superiores o decisiones sobre los activos.					
Tipos Activo:	[P]			Dimensiones:	[D]	
Activos afectados		Probabilidad	% Degradación			
P001-Personal interno (Gerencia)		B	[I]	[C]	[D]	[A] [T]
P002-Personal interno (Responsables área)		B			10	
P003-Resto personal interno		B			10	
P004-Personal externo (administrador sistemas)		B			10	

Tabla 79. Ficha amenazas de tipo [E.8] Difusión de software dañino

[E.8] Difusión de software dañino						
Descripción:	Propagación no intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, ...					
Tipos Activo:	[SW]		Dimensiones: [D] [I] [C]			
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A] [T]
SW001-ERP		MB	100	100	100	
SW002-Paquete ofimático		B	10	1	10	
SW003-Cliente de correo		B	10	100	10	
SW004-Antivirus		MB	10	1	10	
SW005-Sistema de backup		MB	10	10	10	
SW006-Navegador web		M	10	100	1	
SW007-Portal web		MB	10	1	10	
SW008-Sistema operativo Servidor		MB	100	100	100	
SW009-Sistema operativo cliente		B	10	100	10	

Tabla 80. Ficha amenazas de tipo [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento						
Descripción:	Errores de envío de información a través de un sistema de red causados por un encaminamiento incorrecto; ya sean mensajes entre personas, entre procesos o entre unos y otros. Esto supone un riesgo de que la información pueda terminar en manos de quien no se espera.					
Tipos Activo:	[S] [SW] [COM]		Dimensiones: [C]			
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A] [T]
SW001-ERP		MB		1		
SW002-Paquete ofimático		MB		100		
SW003-Cliente de correo		MB		10		
SW004-Antivirus		MB		1		
SW005-Sistema de backup		MB		1		
SW006-Navegador web		MB		10		
SW007-Portal web		MB		1		
SW008-Sistema operativo Servidor		MB		100		
SW009-Sistema operativo cliente		MB		10		
COM001-Servicio de telefonía		MB		100		
COM002-Red local		MB		100		
COM003-Fibra óptica		MB		100		
COM004-Red wifi		MB		100		

Tabla 81. Ficha amenazas de tipo [E.10] Errores de secuencia

[E.10] Errores de secuencia						
Descripción:	Errores debidos a la alteración accidental del orden de los mensajes enviados.					
Tipos Activo:	[S][SW][COM]	Dimensiones: [I]				
Activos afectados		Probabilidad	% Degradación			
		[I]	[C]	[D]	[A]	[T]
SW001-ERP		MB	1			
SW002-Paquete ofimático		MB	1			
SW003-Cliente de correo		MB	1			
SW004-Antivirus		MB	1			
SW005-Sistema de backup		MB	1			
SW006-Navegador web		MB	1			
SW007-Portal web		MB	1			
SW008-Sistema operativo Servidor		MB	1			
SW009-Sistema operativo cliente		MB	1			
COM001-Servicio de telefonía		MB	10			
COM002-Red local		MB	10			
COM003-Fibra óptica		MB	10			
COM004-Red wifi		MB	10			

Tabla 82. Ficha amenazas de tipo [E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información					
Descripción:	Alteración de información que suele darse en los datos en general. Para amenazas sobre los soportes se aplican otras.				
Tipos Activo:	[D] [Info] [keys] [S] [SW] [COM] [Media] [L]	Dimensiones: [I]			
Activos afectados		Probabilidad	% Degradación		
			[I]	[C]	[D]
I001-Fichero Clientes	M	10			
D001-Expediente Cliente	M	10			
D002-Datos acceso Servidor	MB	10			
D003-Datos acceso Usuarios	MB	10			
D004-Backup Servidor	B	1			
D005-Fichero log	MB	1			
D006-Ficheros configuraciones	B	10			
K001-Certificados FMNT	MB	100			
SW001-ERP	B	10			
SW002-Paquete ofimático	MB	1			
SW003-Cliente de correo	B	1			
SW004-Antivirus	MB	1			
SW005-Sistema de backup	B	1			
SW006-Navegador web	MB	1			
SW007-Portal web	B	10			
SW008-Sistema operativo Servidor	MB	10			
SW009-Sistema operativo cliente	MB	10			
COM001-Servicio de telefonía	MB	10			
COM002-Red local	MB	1			
COM003-Fibra óptica	MB	1			
COM004-Red wifi	MB	1			
[MEDIA001]-Memorias USB	M	100			
[MEDIA002]-Discos USB	B	10			
L001-Edificio empresa	MB	100			
L002-Cuarto de comunicaciones	MB	10			

Tabla 83. Ficha amenazas de tipo [E.18] Destrucción de información

[E.18] Destrucción de información						
Descripción:	Pérdida accidental de información, suele identificarse sólo para datos, pues cuando la información reside en algún soporte informático, hay otras amenazas específicas.					
Tipos Activo:	[D] [Info] [keys] [S] [SW] [COM] [Media] [L]	Dimensiones: [D]				
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A]
I001-Fichero Clientes	MB			100		
D001-Expediente Cliente	B			10		
D002-Datos acceso Servidor	MB			100		
D003-Datos acceso Usuarios	MB			100		
D004-Backup Servidor	MB			100		
D005-Fichero log	B			10		
D006-Ficheros configuraciones	B			100		
K001-Certificados FMNT	MB			100		
SW001-ERP	MB			100		
SW002-Paquete ofimático	MB			10		
SW003-Cliente de correo	MB			10		
SW004-Antivirus	MB			10		
SW005-Sistema de backup	MB			10		
SW006-Navegador web	MB			10		
SW007-Portal web	MB			10		
SW008-Sistema operativo Servidor	MB			100		
SW009-Sistema operativo cliente	MB			100		
COM001-Servicio de telefonía	MB			1		
COM002-Red local	MB			1		
COM003-Fibra óptica	MB			1		
COM004-Red wifi	MB			1		
[MEDIA001]-Memorias USB	M			100		
[MEDIA002]-Discos USB	MB			100		
L001-Edificio empresa	B			100		
L002-Cuarto de comunicaciones	B			100		

Tabla 84. Ficha amenazas de tipo [E.19] Fugas de información

[E.19] Fugas de información					
Descripción:	Revelación de información por indiscreción, incontinencia verbal, sobre medios electrónicos, sobre papel, ...				
Tipos Activo:	[D] [Info] [keys] [S] [SW] [COM] [Media] [L] [P]	Dimensiones: [C]			
Activos afectados		Probabilidad	% Degradación		
			[I]	[C]	[D]
I001-Fichero Clientes	MB		10		
D001-Expediente Cliente	MB		10		
D002-Datos acceso Servidor	MB		100		
D003-Datos acceso Usuarios	MB		10		
D004-Backup Servidor	MB		10		
D005-Fichero log	MB		1		
D006-Ficheros configuraciones	MB		10		
K001-Certificados FMNT	MB		1		
SW001-ERP	MB		100		
SW002-Paquete ofimático	MB		100		
SW003-Cliente de correo	B		100		
SW004-Antivirus	MB		1		
SW005-Sistema de backup	MB		100		
SW006-Navegador web	MB		100		
SW007-Portal web	MB		1		
SW008-Sistema operativo Servidor	MB		1		
SW009-Sistema operativo cliente	MB		1		
COM001-Servicio de telefonía	MB		10		
COM002-Red local	MB		10		
COM003-Fibra óptica	MB		10		
COM004-Red wifi	MB		10		
[MEDIA001]-Memorias USB	B		100		
[MEDIA002]-Discos USB	MB		100		
L001-Edificio empresa	M		10		
L002-Cuarto de comunicaciones	B		100		
P001-Personal interno (Gerencia)	MB		100		
P002-Personal interno (Responsables área)	B		100		
P003-Resto personal interno	B		10		
P004-Personal externo (administrador sistemas)	B		100		

Tabla 85. Ficha amenazas de tipo [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)						
Descripción:	Errores en el código fuente que no intencionadamente provoca operatoria defectuosa por parte del usuario, con consecuencias sobre la integridad de los datos o la capacidad de operar.					
Tipos Activo:	[SW]		Dimensiones: [I] [D] [C]			
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A] [T]
SW001-ERP		B	10	100	10	
SW002-Paquete ofimático		B	1	10	10	
SW003-Cliente de correo		B	10	100	10	
SW004-Antivirus		B	100	10	10	
SW005-Sistema de backup		B	10	100	10	
SW006-Navegador web		MB	10	100	10	
SW007-Portal web		MB	10	10	10	
SW008-Sistema operativo Servidor		MB	10	100	10	
SW009-Sistema operativo cliente		B	1	100	1	

Tabla 86. Ficha amenazas de tipo [E.21] Errores de mantenimiento/actualización de programas (software)

[E.21] Errores de mantenimiento/actualización de programas (software)						
Descripción:	Defectos en los procedimientos o controles de actualización de versiones de programas con defectos conocidos y ya reparados por el fabricante. Por ejemplo, no actualización de los parches de seguridad en los sistemas o versiones últimas de aplicaciones que corren errores.					
Tipos Activo:	[SW]		Dimensiones: [I] [D]			
Activos afectados		Probabilidad	% Degradación			
			[I]	[C]	[D]	[A] [T]
SW001-ERP		B	10		10	
SW002-Paquete ofimático		B	10		10	
SW003-Cliente de correo		MB	10		10	
SW004-Antivirus		B	100		10	
SW005-Sistema de backup		B	10		10	
SW006-Navegador web		B	10		1	
SW007-Portal web		MB	10		10	
SW008-Sistema operativo Servidor		B	10		10	
SW009-Sistema operativo cliente		B	1		1	

Tabla 87. Ficha amenazas de tipo [E.23] Errores de mantenimiento/actualización de equipos (hardware)

[E.23] Errores de mantenimiento/actualización de equipos (hardware)					
Descripción:	Defectos en los procedimientos o controles de actualización de los equipos que permiten que se utilicen más tiempo nominal de uso. Esto dificulta la mantenibilidad del sistema de información.				
Tipos Activo:	[HW] [Media] [AUX]	Dimensiones:		[D]	
Activos afectados		Probabilidad	% Degradación		
		[I]	[C]	[D]	[A] [T]
HW001-Servidor		B		10	
HW002-Desktop		M		10	
HW003-Workstation		M		10	
HW004-Laptop		M		10	
HW005-Unidad Backup		B		10	
HW006-Impresora		B		10	
HW007-Plotter		M		10	
HW008-Router		B		10	
HW009-Switch		MB		10	
MEDIA001-Memorias removibles USB		MB		10	
MEDIA002-Discos duros removibles		B		10	
AUX001-SAI		MB		10	

Tabla 88. Ficha amenazas de tipo [E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos					
Descripción:	La falta de recursos suficientes provoca la caída del sistema cuando la carga de trabajo aumenta.				
Tipos Activo:	[S] [HW] [COM]	Dimensiones:		[D]	
Activos afectados		Probabilidad	% Degradación		
		[I]	[C]	[D]	[A] [T]
HW001-Servidor		MB		10	
HW002-Desktop		B		1	
HW003-Workstation		B		1	
HW004-Laptop		B		1	
HW005-Unidad Backup		B		10	
HW006-Impresora		B		10	
HW007-Plotter		MB		10	
HW008-Router		MB		10	
HW009-Switch		MB		10	
COM001-Servicio de telefonía		MB		100	
COM002-Red local		B		100	
COM003-Fibra óptica		B		10	
COM004-Red wifi		B		10	

Tabla 89. Ficha amenazas de tipo [E.25] Pérdidas de equipos

[E.25] Pérdidas de equipos						
Descripción:	La pérdida de equipos provoca directamente indisponibilidad de los servicios. La pérdida de equipos y soportes de información suelen ser los más habituales. Si los equipos contienen datos, además puede producirse una fuga de información.					
Tipos Activo:	[HW] [Media] [AUX]		Dimensiones:		[D] [C]	
Activos afectados		Probabilidad	% Degradación			
[I]		[C]	[D]	[A]	[T]	
HW001-Servidor	MB		100	100		
HW002-Desktop	MB		100	100		
HW003-Workstation	MB		100	100		
HW004-Laptop	B		100	100		
HW005-Unidad Backup	MB		100	100		
HW006-Impresora	MB		1	100		
HW007-Plotter	MB		1	100		
HW008-Router	MB		10	100		
HW009-Switch	MB		1	100		
MEDIA001-Memorias removibles USB	A		100	100		
MEDIA002-Discos duros removibles	MB		100	100		
AUX001-SAI	MB		1	1		

Tabla 90. Ficha amenazas de tipo [E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal						
Descripción:	Ausencia accidental del puesto de trabajo: enfermedad, causas ajenas, ...					
Tipos Activo:	[P]		Dimensiones:		[D]	
Activos afectados		Probabilidad	% Degradación			
[I]		[C]	[D]	[A]	[T]	
P001-Personal interno (Gerencia)	B			10		
P002-Personal interno (Responsables área)	B			100		
P003-Resto personal interno	B			100		
P004-Personal externo (administrador sistemas)	B			100		

4.4. [A] Ataques intencionados

Tabla 91. Ficha amenazas de tipo [A.3] Manipulación de los registros de actividad (log)

[A.3] Manipulación de los registros de actividad (log)						
Descripción:	Alteración de los registros de log.					
Tipos Activo:	[D.log]	Dimensiones:		[I] [T]		
Activos afectados		Probabilidad		% Degradación		
		[I]	[C]	[D]	[A]	[T]
D005-Fichero log	MB	10				10

Tabla 92. Ficha amenazas de tipo [A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración						
Descripción:	Alteración de la configuración de los activos, la cual depende de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de la actividad, enrutamiento, ...					
Tipos Activo:	[D.conf]	Dimensiones:		[I] [C] [A]		
Activos afectados		Probabilidad		% Degradación		
		[I]	[C]	[D]	[A]	[T]
D006-Ficheros configuraciones	MB	100	100		100	

Tabla 93. Ficha amenazas de tipo [A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario						
Descripción:	Un atacante consigue hacerse pasar por un usuario autorizado suplantando su identidad y disfrutando de los privilegios de este para sus fines propios. Esta amenaza puede ser llevada a cabo por personal interno como externo.					
Tipos Activo:	[D] [info] [keys] [S] [SW] [COM]	Dimensiones:		[C] [A] [I]		
Activos afectados		Probabilidad		% Degradación		
		[I]	[C]	[D]	[A]	[T]
I001-Fichero Clientes	MB	10	100		10	
D001-Expediente Cliente	B	10	10		10	
D002-Datos acceso Servidor	MB	10	100		100	
D003-Datos acceso Usuarios	B	10	100		100	
D004-Backup Servidor	MB	10	100		10	
D005-Fichero log	MB	10	100		10	
D006-Ficheros configuraciones	MB	10	100		10	
K001-Certificados FMNT	B	100	1		100	
SW001-ERP	MB	10	100		100	
SW002-Paquete ofimático	B	10	100		100	
SW003-Cliente de correo	MB	10	100		100	
SW004-Antivirus	MB	10	10		100	
SW005-Sistema de backup	MB	1	100		100	
SW006-Navegador web	B	10	10		100	
SW007-Portal web	A	10	10		100	
SW008-Sistema operativo Servidor	B	10	100		100	
SW009-Sistema operativo cliente	B	1	100		100	
COM001-Servicio de telefonía	MB	10	100		100	
COM002-Red local	M	10	100		100	
COM003-Fibra óptica	MB	10	100		100	
COM004-Red wifi	A	10	100		100	

Tabla 94. Ficha amenazas de tipo [A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso						
Descripción:	Los privilegios de los que disfruta un usuario son para un propósito determinado, normalmente por sus funciones. Cuando un usuario utiliza estos privilegios para realizar tareas que no son de su competencia, se produce esta amenaza.					
	Tipos Activo:		Dimensiones:		% Degradación	
Activos afectados	Probabilidad	[I]	[C]	[D]	[A]	[T]
I001-Fichero Clientes	MB	10	10	10		
D001-Expediente Cliente	MB	10	10	10		
D002-Datos acceso Servidor	MB	10	10	10		
D003-Datos acceso Usuarios	MB	10	10	10		
D004-Backup Servidor	MB	10	100	10		
D005-Fichero log	MB	10	10	10		
D006-Ficheros configuraciones	MB	10	10	10		
K001-Certificados FMNT	MB	100	1	10		
SW001-ERP	B	10	100	10		
SW002-Paquete ofimático	MB	10	10	10		
SW003-Cliente de correo	MB	10	10	1		
SW004-Antivirus	MB	100	10	10		
SW005-Sistema de backup	MB	10	100	10		
SW006-Navegador web	B	1	10	1		
SW007-Portal web	B	10	1	100		
SW008-Sistema operativo Servidor	B	10	100	10		
SW009-Sistema operativo cliente	B	1	10	1		
HW001-Servidor	B	10	100	10		
HW002-Desktop	M	10	10	10		
HW003-Workstation	B	10	10	10		
HW004-Laptop	B	10	100	10		
HW005-Unidad Backup	MB	10	100	10		
HW006-Impresora	B	10	1	10		
HW007-Plotter	B	10	1	10		
HW008-Router	B	100	100	10		
HW009-Switch	MB	10	100	10		
COM001-Servicio de telefonía	B	10	10	10		
COM002-Red local	M	10	100	10		
COM003-Fibra óptica	MB	1	100	1		
COM004-Red wifi	B	10	100	10		

Tabla 95. Ficha amenazas de tipo [A.7] Uso no previsto

[A.7] Uso no previsto						
Descripción:	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: películas, música, juegos, uso personal de Internet, aplicaciones personales, almacenamiento de datos personales, ...					
Tipos Activo:	[S] [SW] [HW] [COM] [Media] [AUX] [L]	Dimensiones: [D] [C] [I]				
Activos afectados		Probabilidad % Degradación				
		[I]	[C]	[D]	[A]	[T]
SW001-ERP	B	10	10	10		
SW002-Paquete ofimático	MB	10	10	10		
SW003-Cliente de correo	B	10	100	10		
SW004-Antivirus	MB	100	10	10		
SW005-Sistema de backup	MB	10	100	10		
SW006-Navegador web	B	10	10	1		
SW007-Portal web	MB	1	1	10		
SW008-Sistema operativo Servidor	MB	10	100	10		
SW009-Sistema operativo cliente	B	10	100	10		
HW001-Servidor	B	10	100	10		
HW002-Desktop	M	10	10	10		
HW003-Workstation	B	10	100	10		
HW004-Laptop	B	10	100	10		
HW005-Unidad Backup	MB	10	100	10		
HW006-Impresora	M	10	10	10		
HW007-Plotter	MB	10	10	10		
HW008-Router	MB	10	100	10		
HW009-Switch	MB	10	100	10		
COM001-Servicio de telefonía	M	10	10	10		
COM002-Red local	B	10	100	10		
COM003-Fibra óptica	M	10	100	10		
COM004-Red wifi	B	10	10	10		
[MEDIA001]-Memorias USB	A	100	100	10		
[MEDIA002]-Discos USB	B	100	100	100		
AUX001-SAI	B	10	1	10		
L001-Edificio empresa	MB	10	10	10		
L002-Cuarto de comunicaciones	B	10	10	10		

Tabla 96. Ficha amenazas de tipo [A.8] Difusión de software dañino

[A.8] Difusión de software dañino						
Descripción:	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, ...			Dimensiones: [D] [I] [C]		
Tipos Activo:	[SW]	Probabilidad	% Degradación			
Activos afectados			[I]	[C]	[D]	[A]
SW001-ERP	MB	100	100	100		
SW002-Paquete ofimático	MB	10	1	10		
SW003-Cliente de correo	MB	10	100	10		
SW004-Antivirus	MB	10	1	10		
SW005-Sistema de backup	MB	10	100	100		
SW006-Navegador web	M	10	100	1		
SW007-Portal web	MB	10	1	10		
SW008-Sistema operativo Servidor	MB	100	100	100		
SW009-Sistema operativo cliente	MB	10	100	10		

Tabla 97. Ficha amenazas de tipo [A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes						
Descripción:	Errores de envío de información a través de un sistema de red causados por un encaminamiento incorrecto; ya sean mensajes entre personas, entre procesos o entre unos y otros. Un reenvío intencionado puede hacer que un mensaje se encamine por una ruta de la red donde pueda ser interceptado. Pudiendo terminar la información en manos de quien no se espera.			Dimensiones: [C]		
Tipos Activo:	[S] [SW] [COM]	Probabilidad	% Degradación			
Activos afectados			[I]	[C]	[D]	[A]
SW001-ERP	MB		1			
SW002-Paquete ofimático	MB		100			
SW003-Cliente de correo	MB		10			
SW004-Antivirus	MB		1			
SW005-Sistema de backup	MB		1			
SW006-Navegador web	MB		10			
SW007-Portal web	MB		1			
SW008-Sistema operativo Servidor	MB		100			
SW009-Sistema operativo cliente	MB		10			
COM001-Servicio de telefonía	MB		100			
COM002-Red local	B		100			
COM003-Fibra óptica	MB		100			
COM004-Red wifi	B		100			

Tabla 98. Ficha amenazas de tipo [A.10] Alteración de secuencia

[A.10] Alteración de secuencia						
Descripción:	Se trata de una alteración del orden de los mensajes transmitidos con ánimo de alterar el significado del conjunto de mensajes, afectando a la integridad de los datos.			Dimensiones: [I]		
Tipos Activo:	[S] [SW] [COM]	Probabilidad	% Degradación			
Activos afectados			[I]	[C]	[D]	[A]
SW001-ERP	MB	1				
SW002-Paquete ofimático	MB	1				
SW003-Cliente de correo	MB	1				
SW004-Antivirus	MB	1				
SW005-Sistema de backup	MB	1				
SW006-Navegador web	MB	1				
SW007-Portal web	MB	1				
SW008-Sistema operativo Servidor	MB	1				
SW009-Sistema operativo cliente	MB	1				
COM001-Servicio de telefonía	MB	10				
COM002-Red local	B	10				
COM003-Fibra óptica	MB	10				
COM004-Red wifi	B	10				

Tabla 99. Ficha amenazas de tipo [A.11] Acceso no autorizado

[A.11] Acceso no autorizado						
Descripción:	Un atacante accede a los recursos del sistema sin autorización, típicamente aprovechando un fallo del sistema de identificación y autorización.					
	Tipos Activos:		Dimensiones: [I] [C]			
Activos afectados	Probabilidad		% Degradación			
		[I]	[C]	[D]	[A]	[T]
I001-Fichero Clientes	MB	10	100			
D001-Expediente Cliente	MB	10	100			
D002-Datos acceso Servidor	MB	10	100			
D003-Datos acceso Usuarios	MB	10	100			
D004-Backup Servidor	MB	10	100			
D005-Fichero log	MB	10	100			
D006-Ficheros configuraciones	MB	10	100			
K001-Certificados FMNT	MB	100	1			
SW001-ERP	MB	10	100			
SW002-Paquete ofimático	MB	10	10			
SW003-Cliente de correo	MB	10	100			
SW004-Antivirus	MB	100	10			
SW005-Sistema de backup	MB	10	100			
SW006-Navegador web	B	10	10			
SW007-Portal web	M	10	1			
SW008-Sistema operativo Servidor	MB	100	100			
SW009-Sistema operativo cliente	B	10	100			
HW001-Servidor	M	10	100			
HW002-Desktop	B	10	10			
HW003-Workstation	B	10	100			
HW004-Laptop	B	10	10			
HW005-Unidad Backup	B	10	100			
HW006-Impresora	MB	10	10			
HW007-Plotter	MB	10	1			
HW008-Router	B	10	100			
HW009-Switch	B	10	100			
COM001-Servicio de telefonía	B	10	10			
COM002-Red local	M	10	100			
COM003-Fibra óptica	B	1	100			
COM004-Red wifi	M	10	100			
[MEDIA001]-Memorias USB	MB	100	100			
[MEDIA002]-Discos USB	B	100	100			
AUX001-SAI	B	10	1			
L001-Edificio empresa	B	10	100			
L002-Cuarto de comunicaciones	B	10	100			

Tabla 100. Ficha amenazas de tipo [A.12] Análisis de tráfico

[A.12] Análisis de tráfico						
Descripción:	A veces un atacante, se sitúa en medio del tráfico de datos por la red (canal) y mediante una monitorización/análisis obtiene acceso a datos confidenciales.					
Tipos Activo:	[COM]				Dimensiones:	[C]
Activos afectados		Probabilidad	% Degradación			
COM001-Servicio de telefonía	MB		[I]	[C]	[D]	[A]
COM002-Red local	MB		100			
COM003-Fibra óptica	MB		100			
COM004-Red wifi	MB		100			

Tabla 101. Ficha amenazas de tipo [A.13] Repudio

[A.13] Repudio						
Descripción:	Es el hecho de negar a posteriori, actuaciones realizadas. 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.					
Tipos Activo:	[S] [D.log]				Dimensiones:	[I] [T]
Activos afectados		Probabilidad	% Degradación			
D005-Fichero log	B		[I]	[C]	[D]	[A]
			10			100

Tabla 102. Ficha amenazas de tipo [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)						
Descripción:	Un atacante accede a información para la que no tiene autorización, sin que la información se vea alterada.					
Tipos Activo:	[COM]				Dimensiones:	[C]
Activos afectados		Probabilidad	% Degradación			
COM001-Servicio de telefonía	MB		[I]	[C]	[D]	[A]
COM002-Red local	MB		100			
COM003-Fibra óptica	MB		100			
COM004-Red wifi	MB		100			

Tabla 103. Ficha amenazas de tipo [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información

Descripción:	Alteración intencionada de la información, con ánimo de obtener un beneficio o causar un perjuicio.				
Tipos Activo:	[D] [info] [keys] [S] [SW] [COM] [Media] [L]			Dimensiones:	[I]
Activos afectados		Probabilidad	% Degradoación		
			[I]	[C]	[D]
I001-Fichero Clientes	MB	100			
D001-Expediente Cliente	MB	100			
D002-Datos acceso Servidor	MB	100			
D003-Datos acceso Usuarios	MB	100			
D004-Backup Servidor	MB	100			
D005-Fichero log	MB	100			
D006-Ficheros configuraciones	MB	100			
K001-Certificados FMNT	MB	100			
SW001-ERP	MB	100			
SW002-Paquete ofimático	B	10			
SW003-Cliente de correo	MB	100			
SW004-Antivirus	MB	100			
SW005-Sistema de backup	MB	100			
SW006-Navegador web	MB	10			
SW007-Portal web	MB	10			
SW008-Sistema operativo Servidor	MB	100			
SW009-Sistema operativo cliente	MB	10			
COM001-Servicio de telefonía	MB	10			
COM002-Red local	B	10			
COM003-Fibra óptica	MB	10			
COM004-Red wifi	B	10			
[MEDIA001]-Memorias USB	MB	100			
[MEDIA002]-Discos USB	MB	100			
L001-Edificio empresa	MB	100			
L002-Cuarto de comunicaciones	MB	10			

Tabla 104. Ficha amenazas de tipo [A.18] Destrucción de información

[A.18] Destrucción de información						
Descripción:	Eliminación intencionada de información, con ánimo de obtener un beneficio o causar un perjuicio.					
Tipos Activo:	[D] [info] [keys] [S] [SW] [Media] [L]	Dimensiones: [D]				
Activos afectados	Probabilidad	% Degradación				
		[I]	[C]	[D]	[A]	[T]
I001-Fichero Clientes	MB			100		
D001-Expediente Cliente	MB			100		
D002-Datos acceso Servidor	MB			100		
D003-Datos acceso Usuarios	MB			100		
D004-Backup Servidor	MB			100		
D005-Fichero log	MB			100		
D006-Ficheros configuraciones	MB			100		
K001-Certificados FMNT	MB			10		
SW001-ERP	MB			10		
SW002-Paquete ofimático	MB			100		
SW003-Cliente de correo	MB			100		
SW004-Antivirus	MB			10		
SW005-Sistema de backup	MB			100		
SW006-Navegador web	MB			10		
SW007-Portal web	B			100		
SW008-Sistema operativo Servidor	MB			100		
SW009-Sistema operativo cliente	MB			100		
MEDIA001 - Memorias removibles USB	MB			100		
MEDIA002 - Discos duros removibles	MB			100		
L001-Edificio empresa	MB			100		
L002-Cuarto de comunicaciones	MB			100		

Tabla 105. Ficha amenazas de tipo [A.19] Divulgación de información

[A.19] Divulgación de información						
Descripción:	Se produce revelación de información.					
Tipos Activo:	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	Dimensiones: [C]				
Activos afectados	Probabilidad	% Degradación				
		[I]	[C]	[D]	[A]	[T]
I001-Fichero Clientes	MB	100				
D001-Expediente Cliente	MB	100				
D002-Datos acceso Servidor	MB	100				
D003-Datos acceso Usuarios	MB	100				
D004-Backup Servidor	MB	100				
D005-Fichero log	MB	100				
D006-Ficheros configuraciones	MB	100				
K001-Certificados FMNT	MB	1				
SW001-ERP	MB	100				
SW002-Paquete ofimático	MB	100				
SW003-Cliente de correo	MB	100				
SW004-Antivirus	MB	1				
SW005-Sistema de backup	MB	100				
SW006-Navegador web	MB	10				
SW007-Portal web	MB	1				
SW008-Sistema operativo Servidor	MB	100				
SW009-Sistema operativo cliente	MB	100				
COM001-Servicio de telefonía	B	10				
COM002-Red local	M	10				
COM003-Fibra óptica	MB	10				
COM004-Red wifi	M	10				
MEDIA001-Memorias USB	B	100				
MEDIA002-Discos USB	MB	100				
L001-Edificio empresa	MB	100				
L002-Cuarto de comunicaciones	MB	100				

Tabla 106. Ficha amenazas de tipo [A.22] Manipulación de programas

[A.22] Manipulación de programas						
Descripción:	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.					
Tipos Activo:	[SW]			Dimensiones: [C] [I] [D]		
Activos afectados		Probabilidad	% Degradación			
[I]		[C]	[D]	[A]	[T]	
SW001-ERP	MB	10	100	10		
SW002-Paquete ofimático	MB	10	100	10		
SW003-Cliente de correo	MB	10	100	10		
SW004-Antivirus	MB	1	1	1		
SW005-Sistema de backup	MB	10	10	10		
SW006-Navegador web	MB	1	1	1		
SW007-Portal web	MB	1	1	1		
SW008-Sistema operativo Servidor	MB	1	1	1		
SW009-Sistema operativo cliente	MB	1	1	1		

Tabla 107. Ficha amenazas de tipo [A.23] Manipulación de los equipos

[A.23] Manipulación de los equipos						
Descripción:	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.					
Tipos Activo:	[HW] [Media] [AUX]			Dimensiones: [C] [D]		
Activos afectados		Probabilidad	% Degradación			
[I]		[C]	[D]	[A]	[T]	
HW001-Servidor	MB		10	10		
HW002-Desktop	MB		10	10		
HW003-Workstation	MB		10	10		
HW004-Laptop	MB		10	10		
HW005-Unidad Backup	MB		10	10		
HW006-Impresora	MB		1	10		
HW007-Plotter	MB		1	10		
HW008-Router	MB		100	100		
HW009-Switch	MB		100	10		
[MEDIA001]-Memorias USB	MB		100	10		
[MEDIA002]-Discos USB	MB		100	10		
AUX001-SAI	B		1	10		

Tabla 108. Ficha amenazas de tipo [A.24] Denegación de servicio

[A.24] Denegación de servicio						
Descripción:	Se produce caída del sistema o no respuesta ante el agotamiento de los recursos, provocado por un ataque con tal intención.					
Tipos Activo:	[S][HW][COM]			Dimensiones: [D]		
Activos afectados		Probabilidad	% Degradación			
[I]		[C]	[D]	[A]	[T]	
HW001-Servidor	MB		100			
HW002-Desktop	MB		100			
HW003-Workstation	MB		100			
HW004-Laptop	MB		100			
HW005-Unidad Backup	MB		10			
HW006-Impresora	MB		10			
HW007-Plotter	MB		1			
HW008-Router	M		100			
HW009-Switch	MB		100			
COM001-Servicio de telefonía	MB		100			
COM002-Red local	B		100			
COM003-Fibra óptica	M		100			
COM004-Red wifi	M		100			

Tabla 109. Ficha amenazas de tipo [A.25] Robo

[A.25] Robo							
Descripción:	Sustracción de todo tipo de equipamiento o documentos provocan directamente indisponibilidad de un servicio. El robo de equipos y de soportes de información suelen ser los más habituales. El robo puede producirse por personal interno, externo 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 contienen datos, además se puede producir una fuga de información.						
Tipos Activo:	[HW] [Media] [AUX]	Dimensiones: [D] [C]					
Activos afectados		Probabilidad	% Degradación				
HW001-Servidor	MB	[I]	[C]	[D]	[A]	[T]	
HW002-Desktop	MB	100	100				
HW003-Workstation	MB	100	100				
HW004-Laptop	B	100	100				
HW005-Unidad Backup	B	100	100				
HW006-Impresora	B	1	100				
HW007-Plotter	MB	1	100				
HW008-Router	MB	10	100				
HW009-Switch	MB	1	100				
[MEDIA001]-Memorias USB	B	100	100				
[MEDIA002]-Discos USB	B	100	100				
AUX001-SAI	B	1	100				

Tabla 110. Ficha amenazas de tipo [A.26] Ataque destructivo

[A.26] Ataque destructivo							
Descripción:	Acciones de vandalismo, terrorismo, acción militar, ... de destrucción de hardware o soportes. Esta amenaza puede ser perpetrada por personal tanto interno como externo.						
Tipos Activo:	[HW] [Media] [AUX] [L]	Dimensiones: [D]					
Activos afectados		Probabilidad	% Degradación				
HW001-Servidor	MB	[I]	[C]	[D]	[A]	[T]	
HW002-Desktop	MB			100			
HW003-Workstation	MB			100			
HW004-Laptop	MB			100			
HW005-Unidad Backup	MB			100			
HW006-Impresora	MB			100			
HW007-Plotter	MB			100			
HW008-Router	MB			100			
HW009-Switch	MB			100			
[MEDIA001]-Memorias USB	MB			100			
[MEDIA002]-Discos USB	MB			100			
AUX001-SAI	MB			100			
L001-Edificio empresa	MB			100			
L002-Cuarto de comunicaciones	MB			100			

Tabla 111. Ficha amenazas de tipo [A.27] Ocupación enemiga

[A.27] Ocupación enemiga							
Descripción:	Las instalaciones y locales han sido invadidas y se carece de control sobre los propios medios de trabajo.						
Tipos Activo:	[L]	Dimensiones: [D] [C]					
Activos afectados		Probabilidad	% Degradación				
L001-Edificio empresa	MB	[I]	[C]	[D]	[A]	[T]	
L002-Cuarto de comunicaciones	MB	100	100				
		100	100				

Tabla 112. Ficha amenazas de tipo [A.28] Indisponibilidad del personal

[A.28] Indisponibilidad del personal						
Descripción:	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos...					
Tipos Activo:	[P]	Dimensiones:				
Activos afectados		% Degradación				
		[I]	[C]	[D]	[A]	[T]
P001-Personal interno (Gerencia)	MB			10		
P002-Personal interno (Responsables área)	B			10		
P003-Resto personal interno	B			100		
P004-Personal externo (administrador sistemas)	B			100		

Tabla 113. Ficha amenazas de tipo [A.29] Extorsión

[A.29] Extorsión						
Descripción:	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.					
Tipos Activo:	[P]	Dimensiones:				
Activos afectados		% Degradación				
		[I]	[C]	[D]	[A]	[T]
P001-Personal interno (Gerencia)	MB	100	100	100		
P002-Personal interno (Responsables área)	MB	10	100	10		
P003-Resto personal interno	MB	10	100	10		
P004-Personal externo (administrador sistemas)	MB	10	100	10		

Tabla 114. Ficha amenazas de tipo [A.30] Ingeniería social (picarescas)

[A.30] Ingeniería social (picarescas)						
Descripción:	Amenaza que consiste en el abuso de la buena fe de las personas para que actúen en favor del interés de un tercero.					
Tipos Activo:	[P]	Dimensiones:				
Activos afectados		% Degradación				
		[I]	[C]	[D]	[A]	[T]
P001-Personal interno (Gerencia)	MB	100	100	100		
P002-Personal interno (Responsables área)	MB	10	100	100		
P003-Resto personal interno	MB	100	100	100		
P004-Personal externo (administrador sistemas)	MB	100	100	100		

5. Cálculo del riesgo

Se denomina impacto al daño causado por la materialización de una amenaza sobre un activo. El impacto se calcula estimando el grado de degradación que una amenaza causaría sobre un determinado activo y dimensión, si se materializara.

Una vez se conoce el valor de los activos y la degradación que causa cada amenaza sobre ellos, en esta sección se calculará el impacto que las amenazas tendrían sobre éstos, en base a tablas sencillas de doble entrada (valor, degradación):

Tabla 115. Cálculo del impacto. MAGERIT v3 – Libro II [11]

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

Con el impacto calculado y teniendo en cuenta la probabilidad de que se materialice una amenaza sobre un activo en cada una de sus dimensiones, se calculará el riesgo potencial, (estimado a partir del impacto producido por las amenazas sin tener en cuenta el efecto de ningún tipo de salvaguarda).

Para el cálculo del riesgo potencial nos centraremos en los activos que hayan obtenido para alguna de las amenazas un impacto potencial (A)alto, (MA)muy alto o (M)medio, dado que según la probabilidad serían susceptibles de alcanzar un riesgo (A)alto/(MA)muy alto.

Así pues, la estimación del riesgo resultará de la siguiente tabla combinando el impacto sobre un activo y frecuencia de que la amenaza se materialice.

Tabla 116. Matriz estimación del riesgo (impacto vs probabilidad). MAGERIT v3 – Libro II [11]

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

Dentro de los posibles valores de riesgo, los muy altos (MA) deberán ser gestionados prioritariamente.

A continuación, se detallan las fichas para cada activo con la información sobre las amenazas que pueden sufrir, el impacto y riesgo potencial.

5.1 [info] Activos esenciales (impacto y riesgo)

Tabla 117. Impacto y Riesgo (potencial) del activo I001-Fichero Clientes

[info] Activos esenciales	I001-Fichero Clientes											
	Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
	I001-Fichero Clientes											
[E.1] Errores de los usuarios	M	10	10	10	A	A	M	A	A	M		
[E.2] Errores del administrador	B	10	10	10	A	A	M	A	A	M		
[E.15] Alteración accidental de la información	M	10			A			A				
[E.18] Destrucción de información	MB			100			A					M
[E.19] Fugas de información	MB			10			A					M
[A.5] Suplantación de la identidad del usuario	MB	10	100		A	MA		M	A			
[A.6] Abuso de privilegios de acceso	MB	10	10	10	A	A	M	M	M	B		
[A.11] Acceso no autorizado	MB	10	100		A	MA		M	A			
[A.15] Modificación deliberada de la información	MB	100			MA			A				
[A.18] Destrucción de información	MB			100			A					M
[A.19] Divulgación de información	MB			100			MA					A

5.2. [D] Datos / Información (impacto y riesgo)

Tabla 118. Impacto y Riesgo (potencial) del activo D001-Expediente Cliente

[D] Datos / Información	D001-Expediente Cliente											
	Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
	D001-Expediente Cliente											
[E.1] Errores de los usuarios	A	10	1	10	M	M	B	A	A	M		
[E.2] Errores del administrador	B	10	10	10	M	A	B	M	A	B		
[E.15] Alteración accidental de la información	M	10			M			M				
[E.18] Destrucción de información	B			10			B					B
[E.19] Fugas de información	MB			10			A					M
[A.5] Suplantación de la identidad del usuario	B	10	10		M	A		M	A			
[A.6] Abuso de privilegios de acceso	MB	10	10	10	M	A	B	B	M	MB		
[A.11] Acceso no autorizado	MB	10	100		M	MA		B	A			
[A.15] Modificación deliberada de la información	MB	100			A			M				
[A.18] Destrucción de información	MB			100			M					B
[A.19] Divulgación de información	MB			100			MA					A

Tabla 119. Impacto y Riesgo (potencial) del activo D002-Datos acceso Servidor

D002-Datos acceso Servidor							
AMENAZAS	Frecuencia	Impacto (potencial)			Riesgo (potencia)		
		[I]	[C]	[D]	[I]	[C]	[D]
D002-Datos acceso Servidor							
[E.1] Errores de los usuarios	MB	1	1	1	M	M	M
[E.2] Errores del administrador	B	10	100	10	A	MA	A
[E.15] Alteración accidental de la información	MB	10			A		M
[E.18] Destrucción de información	MB			100		MA	
[E.19] Fugas de información	MB		100			MA	
[A.5] Suplantación de la identidad del usuario	MB	10	100		A	MA	
[A.6] Abuso de privilegios de acceso	MB	10	10	10	A	A	A
[A.11] Acceso no autorizado	MB	10	100		A	MA	M
[A.15] Modificación deliberada de la información	MB	100			MA		A
[A.18] Destrucción de información	MB			100		MA	
[A.19] Divulgación de información	MB		100			MA	A

Tabla 120. Impacto y Riesgo (potencial) del activo D003-Datos acceso Usuarios

[D] Datos / Información		D003-Datos acceso Usuarios									
AMENAZAS		Probabilidad		Degradoación		Impacto (potencial)			Riesgo (potencia)		
		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
D003-Datos acceso Usuarios											
[E.1] Errores de los usuarios		B	10	10	10	M	A	B	M	A	B
[E.2] Errores del administrador		MB	1	1	1	B	M	MB	MB	B	MB
[E.15] Alteración accidental de la información		MB	10			M			B		
[E.18] Destrucción de información		MB			100			M			B
[E.19] Fugas de información		MB		10			A			M	
[A.5] Suplantación de la identidad del usuario		B	10	100		M	MA		M	MA	
[A.6] Abuso de privilegios de acceso		MB	10	10	10	M	A	B	B	M	MB
[A.11] Acceso no autorizado		MB	10	100		M	MA		B	A	
[A.15] Modificación deliberada de la información		MB	100			A			M		
[A.18] Destrucción de información		MB			100			M			B
[A.19] Divulgación de información		MB			100		MA			A	

Tabla 121. Impacto y Riesgo (potencial) del activo D004-Backup Servidor

[D] Datos / Información			D004-Backup Servidor									
AMENAZAS	Probabilidad	Degradación	Impacto (potencial)			Riesgo (potencia)						
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]		
D004-Backup Servidor												
[E.1] Errores de los usuarios	MB	1	1	1	B	M	B	MB	B	MB		
[E.2] Errores del administrador	B	100	10	10	A	A	M	A	A	M		
[E.15] Alteración accidental de la información	B	1			B			B				
[E.18] Destrucción de información	MB			100			A				M	
[E.19] Fugas de información	MB		10			A					M	
[A.5] Suplantación de la identidad del usuario	MB	10	100		M	MA		B	A			
[A.6] Abuso de privilegios de acceso	MB	10	100	10	M	MA	M	B	A	B		
[A.11] Acceso no autorizado	MB	10	100		M	MA		B	A			
[A.15] Modificación deliberada de la información	MB	100			A						M	
[A.18] Destrucción de información	MB			100			A				M	
[A.19] Divulgación de información	MB		100			MA					A	

Tabla 122. Impacto y Riesgo (potencial) del activo D005-Fichero log

[D] Datos / Información	D005-Fichero log									
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
D005-Logs										
[E.1] Errores de los usuarios	MB	1	1	1	M	M	MB	B	B	MB
[E.2] Errores del administrador	B	1	1	1	M	M	MB	M	M	MB
[E.3] Errores de monitorización (log)	B	10			A			A		
[E.15] Alteración accidental de la información	B	1			M			M		
[E.18] Destrucción de información	B			10			B			B
[E.19] Fugas de información	MB		1		M				B	
[A.3] Manipulación de los registros de actividad	MB	10			A			M		
[A.5] Suplantación de la identidad del usuario	MB	10	100		A	MA		M	A	
[A.6] Abuso de privilegios de acceso	MB	10	10	10	A	A	B	M	M	MB
[A.11] Acceso no autorizado	MB	10	100		A	MA		M	A	
[A.13] Repudio	MB	10			A			M		
[A.15] Modificación deliberada de la información	MB	100			MA			A		
[A.18] Destrucción de información	MB			100			M			B
[A.19] Divulgación de información	MB		100		MA				A	

Tabla 123. Impacto y Riesgo (potencial) del activo D006-Ficheros configuraciones

[D] Datos / Información	D006-Ficheros configuraciones									
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
D006-Ficheros configuraciones										
[E.1] Errores de los usuarios	MB	1	1	1	M	B	B	B	MB	MB
[E.2] Errores del administrador	B	10	1	1	A	B	B	A	B	B
[E.4] Errores de configuración	B	10			A			A		
[E.15] Alteración accidental de la información	MB	10			A			M		
[E.18] Destrucción de información	B			100			A			A
[E.19] Fugas de información	MB		1		B				MB	
[A.4] Manipulación de la configuración	MB	10	10		A	M		M	B	
[A.5] Suplantación de la identidad del usuario	B	10	10		A	M		A	M	
[A.6] Abuso de privilegios de acceso	MB	10	10	10	A	M	M	M	B	B
[A.11] Acceso no autorizado	MB	10	100		A	A		M	M	
[A.15] Modificación deliberada de la información	MB	10			A			M		
[A.18] Destrucción de información	MB			100			A			M
[A.19] Divulgación de información	MB		100		A				M	

5.3. [K] Claves criptográficas (impacto y riesgo)

Tabla 124. Impacto y Riesgo (potencial) del activo K001-Certificados FMNT

[K] Claves criptográficas	K001-Certificados FMNT									
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
K001-Certificados FMNT										
[E.1] Errores de los usuarios	MB	10	1	10	A	MB	B	M	MB	MB
[E.2] Errores del administrador	MB	100	1	10	MA	MB	B	A	MB	MB
[E.15] Alteración accidental de la información	MB	100			MA			A		
[E.18] Destrucción de información	MB			100			M			B
[E.19] Fugas de información	MB		1			MB			MB	
[A.5] Suplantación de la identidad del usuario	B	100	1		MA	MB		MA	MB	
[A.6] Abuso de privilegios de acceso	MB	100	1	10	MA	MB	B	A	MB	MB
[A.11] Acceso no autorizado	MB	100	1		MA	MB		A	MB	
[A.15] Modificación deliberada de la información	MB	100			MA			A		
[A.18] Destrucción de información	MB			10			B			MB
[A.19] Divulgación de información	MB		1			MB			MB	

5.4. [SW] Software - Aplicaciones informáticas (impacto y riesgo)

Tabla 125. Impacto y Riesgo (potencial) del activo SW001-ERP

[SW] Software - Aplicaciones informáticas	Probabilidad	Degradación	Impacto (potencial)			Riesgo (potencial)			
			[I]	[C]	[D]	[I]	[C]	[D]	[I]
AMENAZAS	Frecuencia								
SW001-ERP									
[I.5] Avería de origen físico o lógico	MB			10		M			B
[E.1] Errores de los usuarios	M	10	10	10	M	M	M	M	M
[E.2] Errores del administrador	MB	10	10	10	M	M	M	B	B
[E.8] Difusión de software dañino	MB	100	100	100	A	A	A	M	M
[E.9] Errores de [re-]encaminamiento	MB			1	B			MB	
[E.10] Errores de secuencia	MB	1			B			MB	
[E.15] Alteración accidental de la información	B	10			M			M	
[E.18] Destrucción de información	MB			100		A			M
[E.19] Fugas de información	MB			100	A			M	
[E.20] Vulnerabilidades de los programas (softw	B	10	100	10	M	A	M	M	A
[E.21] Errores de mantenimiento/actualización	B	10		10	M		M	M	M
[A.5] Suplantación de la identidad del usuario	MB	10	100		M	A		B	M
[A.6] Abuso de privilegios de acceso	B	10	100	10	M	A	M	M	A
[A.7] Uso no previsto	B	10	10	10	M	M	M	M	M
[A.8] Difusión de software dañino	MB	100	100	100	A	A	A	M	M
[A.9] [Re-]encaminamiento de mensajes	MB			1	B			MB	
[A.10] Alteración de secuencia	MB	1			B			MB	
[A.11] Acceso no autorizado	MB	10	100		M	A		B	M
[A.15] Modificación deliberada de la informació	MB	100			A			M	
[A.18] Destrucción de información	MB			10		M			B
[A.19] Divulgación de información	MB			100	A			M	
[A.22] Manipulación de programas	MB	10	100	10	M	A	M	B	M

Tabla 126. Impacto y Riesgo (potencial) del activo SW002-Paquete ofimático

[SW] Software - Aplicaciones informáticas	Probabilidad	SW002-Paquete ofimático								
		Degradación	Impacto (potencial)	Riesgo (potencial)						
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW002-Paquete ofimático										
[I.5] Avería de origen físico o lógico	B			10				B		B
[E.1] Errores de los usuarios	M	1	10	10	MB	B	B	MB	B	B
[E.2] Errores del administrador	MB	1	10	10	MB	B	B	MB	MB	MB
[E.8] Difusión de software dañino	B	10	1	10	B	MB	B	B	MB	B
[E.9] Errores de [re]-encaminamiento	MB			100		M				B
[E.10] Errores de secuencia	MB	1			MB				MB	
[E.15] Alteración accidental de la información	MB	1			MB				MB	
[E.18] Destrucción de información	MB			10				B		MB
[E.19] Fugas de información	MB			100		M				B
[E.20] Vulnerabilidades de los programas (softw	B	1	10	10	MB	B	B	MB	B	B
[E.21] Errores de mantenimiento/actualización	B	10		10	B			B	B	B
[A.5] Suplantación de la identidad del usuario	B	10	100		B	M		B	M	
[A.6] Abuso de privilegios de acceso	MB	10	10	10	B	B	B	MB	MB	MB
[A.7] Uso no previsto	MB	10	10	10	B	B	B	MB	MB	MB
[A.8] Difusión de software dañino	MB	10	1	10	B	MB	B	MB	MB	MB
[A.9] [Re]-encaminamiento de mensajes	MB			100		M				B
[A.10] Alteración de secuencia	MB	1			MB				MB	
[A.11] Acceso no autorizado	MB	10	10		B	B			MB	MB
[A.15] Modificación deliberada de la información	B	10			B				B	
[A.18] Destrucción de información	MB			100			M			B
[A.19] Divulgación de información	MB			100		M				B
[A.22] Manipulación de programas	MB	10	100	10	B	M	B	MB	B	MB

Tabla 127. Impacto y Riesgo (potencial) del activo SW003-Cliente de correo

[SW] Software - Aplicaciones informáticas	Probabilidad	SW003-Cliente de correo								
		Degradación	Impacto (potencial)	Riesgo (potencial)						
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW003-Cliente de correo										
[I.5] Avería de origen físico o lógico	MB			10				B		MB
[E.1] Errores de los usuarios	M	1	1	10	B	B	B	B	B	B
[E.2] Errores del administrador	MB	1	10	10	B	M	B	MB	B	MB
[E.8] Difusión de software dañino	B	10	100	10	M	A	B	M	A	B
[E.9] Errores de [re]-encaminamiento	MB			10		M				B
[E.10] Errores de secuencia	MB	1			B				MB	
[E.15] Alteración accidental de la información	B	1			B				B	
[E.18] Destrucción de información	MB			10				B		MB
[E.19] Fugas de información	B			100		A			A	
[E.20] Vulnerabilidades de los programas (softw	B	10	100	10	M	A	B	M	A	B
[E.21] Errores de mantenimiento/actualización	MB	10		10	M		B	B		MB
[A.5] Suplantación de la identidad del usuario	MB	10	100		M	A		B	M	
[A.6] Abuso de privilegios de acceso	MB	10	10	1	M	M	MB	B	B	MB
[A.7] Uso no previsto	B	10	100	10	M	A	B	M	A	B
[A.8] Difusión de software dañino	MB	10	100	10	M	A	B	B	M	MB
[A.9] [Re]-encaminamiento de mensajes	MB			10		M				B
[A.10] Alteración de secuencia	MB	1			B				MB	
[A.11] Acceso no autorizado	MB	10	100		M	A		B	M	
[A.15] Modificación deliberada de la información	MB	100			A			M		
[A.18] Destrucción de información	MB			100			M			B
[A.19] Divulgación de información	MB			100		A			M	
[A.22] Manipulación de programas	MB	10	100	10	M	A	B	B	M	MB

Tabla 128. Impacto y Riesgo (potencial) del activo SW004-Antivirus

[SW] Software - Aplicaciones informáticas			SW004-Antivirus								
AMENAZAS	Probabilidad	Frecuencia	Degradación			Impacto (potencial)			Riesgo (potencial)		
			[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW004-Antivirus											
[I.5] Avería de origen físico o lógico	MB			10			M				B
[E.1] Errores de los usuarios	MB	1	1	1	B	MB	B		MB	MB	MB
[E.2] Errores del administrador	B	10	10	10	M	B	M	M	B	M	
[E.8] Difusión de software dañino	MB	10	1	10	M	MB	M		B	MB	B
[E.9] Errores de [re]-encaminamiento	MB			1			MB				MB
[E.10] Errores de secuencia	MB	1			B				MB		
[E.15] Alteración accidental de la información	MB	1			B				MB		
[E.18] Destrucción de información	MB			10			M				B
[E.19] Fugas de información	MB			1			MB				MB
[E.20] Vulnerabilidades de los programas (softw	B	100	10	10	A	B	M	A	B	M	
[E.21] Errores de mantenimiento/actualización	B	100		10	A		M	A			M
[A.5] Suplantación de la identidad del usuario	MB	10	10		M	B		MB	MB		
[A.6] Abuso de privilegios de acceso	MB	100	10	10	A	B	M	M	MB	B	
[A.7] Uso no previsto	MB	100	10	10	A	B	M	M	MB	B	
[A.8] Difusión de software dañino	MB	10	1	10	M	MB	M		B	MB	B
[A.9] [Re]-encaminamiento de mensajes	MB			1			MB				MB
[A.10] Alteración de secuencia	MB	1			B				MB		
[A.11] Acceso no autorizado	MB	100	10		A	B		M		MB	
[A.15] Modificación deliberada de la informació	MB	100			A			M			
[A.18] Destrucción de información	MB			10			M				B
[A.19] Divulgación de información	MB			1			MB				MB
[A.22] Manipulación de programas	MB	1	1	1	B	MB	B	MB	MB	MB	

Tabla 129. Impacto y Riesgo (potencial) del activo SW005-Sistema de backup

[SW] Software - Aplicaciones informáticas			SW005-Sistema de backup								
AMENAZAS	Probabilidad	Frecuencia	Degradación			Impacto (potencial)			Riesgo (potencial)		
			[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW005-Sistema de backup											
[I.5] Avería de origen físico o lógico	MB			10			M				B
[E.1] Errores de los usuarios	MB	1	1	1	B	B	B	MB	MB	MB	
[E.2] Errores del administrador	B	10	10	10	M	M	M	M	M	M	
[E.8] Difusión de software dañino	MB	10	10	10	M	M	M		B	B	B
[E.9] Errores de [re]-encaminamiento	MB			1			B				MB
[E.10] Errores de secuencia	MB	1			B				MB		
[E.15] Alteración accidental de la información	B	1			B				B		
[E.18] Destrucción de información	MB			10			M				B
[E.19] Fugas de información	MB			100			A				M
[E.20] Vulnerabilidades de los programas (softw	B	10	100	10	M	A	M	M	A	M	
[E.21] Errores de mantenimiento/actualización	B			10			M				M
[A.5] Suplantación de la identidad del usuario	MB	1	100		B	A		MB	M		
[A.6] Abuso de privilegios de acceso	MB	10	100	10	M	A	M	M	B	M	B
[A.7] Uso no previsto	MB	10	100	10	M	A	M	M	B	M	B
[A.8] Difusión de software dañino	MB	10	100	100	M	A	A	B	M	M	
[A.9] [Re]-encaminamiento de mensajes	MB			1			B				MB
[A.10] Alteración de secuencia	MB	1			B				MB		
[A.11] Acceso no autorizado	MB	10	100		M	A		B	M		
[A.15] Modificación deliberada de la informació	MB	100			A			M			
[A.18] Destrucción de información	MB			100			A				M
[A.19] Divulgación de información	MB			100			A				M
[A.22] Manipulación de programas	MB	10	10	10	M	M	M	B	B	B	

Tabla 130. Impacto y Riesgo (potencial) del activo SW006-Navegador web

[SW] Software - Aplicaciones informáticas	SW006-Navegador web										
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)			
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW006-Navegador web											
[I.5] Avería de origen físico o lógico	MB			10			MB			MB	
[E.1] Errores de los usuarios	M	1	10	1	MB	B	MB	MB	B	MB	
[E.2] Errores del administrador	MB	1	10	10	MB	B	MB	MB	MB	MB	
[E.8] Difusión de software dañino	M	10	100	1	MB	M	MB	MB	M	MB	
[E.9] Errores de [re]-encaminamiento	MB			10		B			MB		
[E.10] Errores de secuencia	MB	1			MB				MB		
[E.15] Alteración accidental de la información	MB	1			MB				MB		
[E.18] Destrucción de información	MB			10			MB			MB	
[E.19] Fugas de información	MB		100			M			B		
[E.20] Vulnerabilidades de los programas (softw	MB	10	100	10	MB	M	MB	MB	B	MB	
[E.21] Errores de mantenimiento/actualización	B	10		1	MB		MB	MB	MB	MB	
[A.5] Suplantación de la identidad del usuario	B	10	10		MB	B			MB	B	
[A.6] Abuso de privilegios de acceso	B	1	10	1	MB	B	MB	MB	B	MB	
[A.7] Uso no previsto	B	10	10	1	MB	B	MB	MB	B	MB	
[A.8] Difusión de software dañino	M	10	100	1	MB	M	MB	MB	M	MB	
[A.9] [Re]-encaminamiento de mensajes	MB			10		B			MB		
[A.10] Alteración de secuencia	MB	1			MB				MB		
[A.11] Acceso no autorizado	B	10	10		MB	B			MB	B	
[A.15] Modificación deliberada de la información	MB	10			MB				MB		
[A.18] Destrucción de información	MB			10			MB			MB	
[A.19] Divulgación de información	MB			10		B			MB		
[A.22] Manipulación de programas	MB	1	1	1	MB	MB	MB	MB	MB	MB	

Tabla 131. Impacto y Riesgo (potencial) del activo SW007-Portal web

[SW] Software - Aplicaciones informáticas	SW007-Portal web										
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)			
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW007-Portal web											
[I.5] Avería de origen físico o lógico	MB			10			MB			MB	
[E.1] Errores de los usuarios	MB	1	1	1	MB	MB	MB	MB	MB	MB	
[E.2] Errores del administrador	MB	10	10	10	MB	MB	MB	MB	MB	MB	
[E.8] Difusión de software dañino	MB	10	1	10	MB	MB	MB	MB	MB	MB	
[E.9] Errores de [re]-encaminamiento	MB			1		MB			MB		
[E.10] Errores de secuencia	MB	1			MB				MB		
[E.15] Alteración accidental de la información	B	10			MB				MB		
[E.18] Destrucción de información	MB			10			MB			MB	
[E.19] Fugas de información	MB			1		MB			MB		
[E.20] Vulnerabilidades de los programas (softw	MB	10	10	10	MB	MB	MB	MB	MB	MB	
[E.21] Errores de mantenimiento/actualización	MB	10		10	MB		MB	MB	MB	MB	
[A.5] Suplantación de la identidad del usuario	A	10	10		MB	MB		B	B		
[A.6] Abuso de privilegios de acceso	B	10	1	100	MB	MB	B	MB	MB	B	
[A.7] Uso no previsto	MB	1	1	10	MB	MB	MB	MB	MB	MB	
[A.8] Difusión de software dañino	MB	10	1	10	MB	MB	MB	MB	MB	MB	
[A.9] [Re]-encaminamiento de mensajes	MB			1		MB			MB		
[A.10] Alteración de secuencia	MB	1			MB				MB		
[A.11] Acceso no autorizado	M	10	1		MB	MB		MB	MB		
[A.15] Modificación deliberada de la información	MB	10			MB				MB		
[A.18] Destrucción de información	B			100			B			B	
[A.19] Divulgación de información	MB			1		MB			MB		
[A.22] Manipulación de programas	MB	1	1	1	MB	MB	MB	MB	MB	MB	

Tabla 132. Impacto y Riesgo (potencial) del activo SW008-Sistema operativo Servidor

[SW] Software - Aplicaciones informáticas	SW008-Sistema operativo Servidor										
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)			
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW008-Sistema operativo Servidor											
[I.5] Avería de origen físico o lógico	MB			10			M			B	
[E.1] Errores de los usuarios	MB	1	1	1	B	B	B	MB	MB	MB	
[E.2] Errores del administrador	B	10	10	10	M	M	M	M	M	M	
[E.8] Difusión de software dañino	MB	100	100	100	A	A	A	M	M	M	
[E.9] Errores de [re-]encaminamiento	MB	100			A			M			
[E.10] Errores de secuencia	MB	1			B			MB			
[E.15] Alteración accidental de la información	MB	10			M			B			
[E.18] Destrucción de información	MB			100			A			M	
[E.19] Fugas de información	MB		1		B			MB			
[E.20] Vulnerabilidades de los programas (softw	MB	10	100	10	M	A	M	B	M	B	
[E.21] Errores de mantenimiento/actualización	B	10		10	M		M	M		M	
[A.5] Suplantación de la identidad del usuario	B	10	100		M	A		M	A		
[A.6] Abuso de privilegios de acceso	B	10	100	10	M	A	M	M	A	M	
[A.7] Uso no previsto	MB	10	100	10	M	A	M	B	M	B	
[A.8] Difusión de software dañino	MB	100	100	100	A	A	A	M	M	M	
[A.9] [Re-]encaminamiento de mensajes	MB			100	A			M			
[A.10] Alteración de secuencia	MB	1			B			MB			
[A.11] Acceso no autorizado	MB	100	100		A	A		M	M		
[A.15] Modificación deliberada de la información	MB	100			A			M			
[A.18] Destrucción de información	MB			100			A			M	
[A.19] Divulgación de información	MB			100			A			M	
[A.22] Manipulación de programas	MB	1	1	1	B	B	B	MB	MB	MB	

Tabla 133. Impacto y Riesgo (potencial) del activo SW009-Sistema operativo cliente

[SW] Software - Aplicaciones informáticas	SW009-Sistema operativo cliente										
	Probabilidad	Degradación			Impacto (potencial)			Riesgo (potencial)			
AMENAZAS		Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
SW009-Sistema operativo Cliente											
[I.5] Avería de origen físico o lógico	MB			10			B			MB	
[E.1] Errores de los usuarios	M	1	1	1	B	MB	MB	B	MB	MB	
[E.2] Errores del administrador	MB	1	10	10	B	B	B	MB	MB	MB	
[E.8] Difusión de software dañino	B	10	100	10	M	M	B	M	M	B	
[E.9] Errores de [re-]encaminamiento	MB	10			B			MB			
[E.10] Errores de secuencia	MB	1			B			MB			
[E.15] Alteración accidental de la información	MB	10			M			B			
[E.18] Destrucción de información	MB			100			M			B	
[E.19] Fugas de información	MB		1		MB			MB			
[E.20] Vulnerabilidades de los programas (softw	B	1	100	1	B	M	MB	B	M	MB	
[E.21] Errores de mantenimiento/actualización	B	1		1	B		MB	B		MB	
[A.5] Suplantación de la identidad del usuario	B	1	100		B	M		B	M		
[A.6] Abuso de privilegios de acceso	B	1	10	1	B	B	MB	B	B	MB	
[A.7] Uso no previsto	B	10	100	10	M	M	B	M	M	B	
[A.8] Difusión de software dañino	MB	10	100	10	M	M	B	B	B	MB	
[A.9] [Re-]encaminamiento de mensajes	MB	10			B			MB			
[A.10] Alteración de secuencia	MB	1			B			MB			
[A.11] Acceso no autorizado	B	10	100		M	M		M	M		
[A.15] Modificación deliberada de la información	MB	10			M			B			
[A.18] Destrucción de información	MB			100			M			B	
[A.19] Divulgación de información	MB			100			M			B	
[A.22] Manipulación de programas	MB	1	1	1	B	MB	MB	MB	MB	MB	

5.5. [HW] Equipamiento informático (hardware) (impacto y riesgo)

Tabla 134. Impacto y Riesgo (potencial) del activo HW001-Servidor

AMENAZAS	HW001-Servidor			Impacto (potencial)			Riesgo (potencial)		
	Probabilidad	Degradación	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]
HW001-Servidor									
[N] Desastres naturales([N.*],[N.1]-Fuego,[N.2]-A)	MB		100				MA		A
[I.1] Fuego	B		100				MA		A
[I.2] Agua	B		100				MA		A
[I.*] Desastres industriales	MB		100				MA		A
[I.3] Contaminación mecánica	M		10				A		A
[I.4] Contaminación electromagnética	MB		10				A		M
[I.5] Avería de origen físico o lógico	B		100				MA		A
[I.6] Corte de suministro eléctrico	B		100				MA		A
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10				A		M
[I.11] Emanaciones electromagnéticas	MB		1				M		B
[E.2] Errores del administrador	MB	10	10	10	M	A	A	B	M
[E.23] Errores de mantenimiento/actualización	B		10				A		A
[E.24] Caída del sistema por agotamiento de recursos	MB		10				A		M
[E.25] Pérdidas de equipos	MB	100	100				MA	MA	A
[A.6] Abuso de privilegios de acceso	B	10	100	10	M	MA	A	M	A
[A.7] Uso no previsto	B	10	100	10	M	MA	A	M	A
[A.11] Acceso no autorizado	M	10	100		M	MA		M	MA
[A.23] Manipulación de los equipos	MB		10				A		M
[A.24] Denegación de servicio	MB		100				MA		A
[A.25] Robo	MB	100	100				MA	MA	A
[A.26] Ataque destructivo	MB		100				MA		A

Tabla 135. Impacto y Riesgo (potencial) del activo HW002-Desktop

AMENAZAS	HW002-Desktop			Impacto (potencial)			Riesgo (potencial)		
	Probabilidad	Degradación	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]
HW002-Desktop									
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB		100				A		M
[I.1] Fuego	B		100				A		A
[I.2] Agua	B		100				A		A
[I.*] Desastres industriales	MB		100				A		M
[I.3] Contaminación mecánica	M		10				M		M
[I.4] Contaminación electromagnética	MB		10				M		B
[I.5] Avería de origen físico o lógico	B		100				A		A
[I.6] Corte de suministro eléctrico	B		100				A		A
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10				M		B
[I.11] Emanaciones electromagnéticas	MB		1				MB		MB
[E.2] Errores del administrador	MB	1	10	10	MB	B	M	MB	B
[E.23] Errores de mantenimiento/actualización	M		10				M		M
[E.24] Caída del sistema por agotamiento de recursos	B		1				B		B
[E.25] Pérdidas de equipos	MB	100	100				M	A	B
[A.6] Abuso de privilegios de acceso	M	10	10	10	MB	B	M	MB	M
[A.7] Uso no previsto	M	10	10	10	MB	B	M	MB	B
[A.11] Acceso no autorizado	B	10	10		MB	B		MB	B
[A.23] Manipulación de los equipos	MB	10	10				B	M	MB
[A.24] Denegación de servicio	MB		100				A		M
[A.25] Robo	MB	100	100				M	A	B
[A.26] Ataque destructivo	MB		100				A		M

Tabla 136. Impacto y Riesgo (potencial) del activo HW003-Workstation

AMENAZAS	HW003-Workstation			Impacto (potencial)			Riesgo (potencial)		
	Probabilidad	Degradación	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]
HW003-Workstation									
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB		100				A		M
[I.1] Fuego	B		100				A		A
[I.2] Agua	B		100				A		A
[I.*] Desastres industriales	MB		100				A		M
[I.3] Contaminación mecánica	M		10				M		M
[I.4] Contaminación electromagnética	MB		10				M		B
[I.5] Avería de origen físico o lógico	B		100				A		A
[I.6] Corte de suministro eléctrico	B		100				A		A
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10				M		B
[I.11] Emanaciones electromagnéticas	MB		1				MB		MB
[E.2] Errores del administrador	MB	1	10	10	MB	B	M	MB	B
[E.23] Errores de mantenimiento/actualización	M		10				M		M
[E.24] Caída del sistema por agotamiento de recursos	B		1				B		B
[E.25] Pérdidas de equipos	MB	100	100				M	A	B
[A.6] Abuso de privilegios de acceso	B	10	10	10	MB	B	M	MB	M
[A.7] Uso no previsto	B	10	100	10	MB	M	M	MB	M
[A.11] Acceso no autorizado	B	10	100		MB	M		MB	M
[A.23] Manipulación de los equipos	MB	10	10				B	M	MB
[A.24] Denegación de servicio	MB		100				A		M
[A.25] Robo	MB	100	100				M	A	B
[A.26] Ataque destructivo	MB		100				A		M

Tabla 137. Impacto y Riesgo (potencial) del activo HW004-Laptop

AMENAZAS	HW004-Laptop			Impacto (potencial)			Riesgo (potencial)		
	Frecuencia	Degrado	Ción	I	C	D	I	C	D
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB		100		M		B		
[I.1] Fuego	B		100		M		M		
[I.2] Agua	B		100		M		M		
[I.*] Desastres industriales	MB		100		M		B		
[I.3] Contaminación mecánica	M		10		B		B		
[I.4] Contaminación electromagnética	MB		10		B		MB		
[I.5] Avería de origen físico o lógico	B		100		M		M		
[I.6] Corte de suministro eléctrico	MB		10		B		MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10		B		MB		
[I.11] Emanaciones electromagnéticas	MB	1		B			MB		
[E.2] Errores del administrador	MB	1	10	10	MB	M	B	MB	B
[E.23] Errores de mantenimiento/actualización	M		10			B			B
[E.24] Caida del sistema por agotamiento de recursos	B		1			MB			MB
[E.25] Pérdidas de equipos	B		100	100	A	M	A	M	
[A.6] Abuso de privilegios de acceso	B	10	100	10	MB	A	B	MB	A
[A.7] Uso no previsto	B	10	100	10	MB	A	B	MB	A
[A.11] Acceso no autorizado	B	10	10		MB	M		MB	M
[A.23] Manipulación de los equipos	MB	10	10		M	B		B	MB
[A.24] Denegación de servicio	MB		100			M			B
[A.25] Robo	B		100	100	A	M		A	M
[A.26] Ataque destructivo	MB		100		M				B

Tabla 138. Impacto y Riesgo (potencial) del activo HW005-Unidad Backup

AMENAZAS	HW005-Unidad Backup			Impacto (potencial)			Riesgo (potencial)		
	Frecuencia	Degrado	Ción	I	C	D	I	C	D
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB		100		A		M		
[I.1] Fuego	B		100		A		A		
[I.2] Agua	B		100		A		A		
[I.*] Desastres industriales	MB		100		A		M		
[I.3] Contaminación mecánica	M		10		M		M		
[I.4] Contaminación electromagnética	MB		10		M		B		
[I.5] Avería de origen físico o lógico	B		100		A		A		
[I.6] Corte de suministro eléctrico	B		100		A		A		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10		M		B		
[I.11] Emanaciones electromagnéticas	MB	1		B			MB		
[E.2] Errores del administrador	MB	1	10	10	MB	M	B	B	B
[E.23] Errores de mantenimiento/actualización	B		10		M			M	
[E.24] Caida del sistema por agotamiento de recursos	B		10		M			M	
[E.25] Pérdidas de equipos	MB		100	100	A	A	M	M	M
[A.6] Abuso de privilegios de acceso	MB	10	100	10	MB	A	M	MB	B
[A.7] Uso no previsto	MB	10	100	10	MB	A	M	MB	M
[A.11] Acceso no autorizado	B	10	100		MB	A		MB	A
[A.23] Manipulación de los equipos	MB	10	10		M	M		B	B
[A.24] Denegación de servicio	MB		10		M			B	
[A.25] Robo	B		100	100	A	A	A	A	A
[A.26] Ataque destructivo	MB		100		A			M	

Tabla 140. Impacto y Riesgo (potencial) del activo HW007-Plotter

AMENAZAS	HW007-Plotter			Impacto (potencial)			Riesgo (potencial)		
	Frecuencia	Degrado	Ción	I	C	D	I	C	D
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB		100		B		MB		
[I.1] Fuego	B		100		B		B		
[I.2] Agua	B		100		B		B		
[I.*] Desastres industriales	MB		100		B		MB		
[I.3] Contaminación mecánica	B		10		MB		MB		
[I.4] Contaminación electromagnética	B		10		MB		MB		
[I.5] Avería de origen físico o lógico	MB		100		B		MB		
[I.6] Corte de suministro eléctrico	B		100		B		B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10		MB		MB		
[I.11] Emanaciones electromagnéticas	MB	1		MB			MB		
[E.2] Errores del administrador	MB	1	1	1	MB	MB	MB	MB	MB
[E.23] Errores de mantenimiento/actualización	M		10		MB		MB		
[E.24] Caida del sistema por agotamiento de recursos	MB		10		MB		MB		
[E.25] Pérdidas de equipos	MB		1	100	MB	B	MB	MB	MB
[A.6] Abuso de privilegios de acceso	B	10	1	10	MB	MB	MB	MB	MB
[A.7] Uso no previsto	MB	10	10	10	MB	MB	MB	MB	MB
[A.11] Acceso no autorizado	MB	10	1		MB	MB	MB	MB	MB
[A.23] Manipulación de los equipos	MB	1	10		MB	MB	MB	MB	MB
[A.24] Denegación de servicio	MB		1		MB		MB		MB
[A.25] Robo	MB		1	100	MB	B	MB	MB	MB
[A.26] Ataque destructivo	MB		100		B				MB

Tabla 141. Impacto y Riesgo (potencial) del activo HW008-Router

AMENAZAS	HW008-Router			HW008-Router			Impacto (potencial)			Riesgo (potencial)			
	Frecuencia	I	C	D	I	C	D	I	C	D	I	C	D
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB			100				A			M		
[I.1] Fuego	B			100				A			A		
[I.2] Agua	B			100				A			A		
[I.*] Desastres industriales	MB			100				A			M		
[I.3] Contaminación mecánica	B			10				M			M		
[I.4] Contaminación electromagnética	B			10				M			M		
[I.5] Avería de origen físico o lógico	MB			100				A			M		
[I.6] Corte de suministro eléctrico	B			100				A			A		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			100				A			M		
[I.11] Emanaciones electromagnéticas	MB	1						B			MB		
[E.7] Errores del administrador	B	10	10	10	M	M	M	M	M	M	M		
[E.23] Errores de mantenimiento/actualización	B			10				M			M		
[E.24] Caída del sistema por agotamiento de recursos	MB			10				M			B		
[E.25] Pérdidas de equipos	MB			100				M	A		B	M	
[A.6] Abuso de privilegios de acceso	B	100	100	10	A	A	M	A	A	M	M		
[A.7] Uso no previsto	MB	10	100	10	M	A	M	B	M	B			
[A.11] Acceso no autorizado	B	10	100		M	A		M	A				
[A.23] Manipulación de los equipos	MB			100				A			M		
[A.24] Denegación de servicio	M			100				A			M		
[A.25] Robo	MB			10	100			M	A		B	M	
[A.26] Ataque destructivo	MB				100			A			M		

Tabla 142. Impacto y Riesgo (potencial) del activo HW009-Switch

AMENAZAS	HW009-Switch			HW009-Switch			Impacto (potencial)			Riesgo (potencial)			
	Frecuencia	I	C	D	I	C	D	I	C	D	I	C	D
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB			100				A			M		
[I.1] Fuego	B			100				A			A		
[I.2] Agua	B			100				A			A		
[I.*] Desastres industriales	MB			100				A			M		
[I.3] Contaminación mecánica	B			10				M			M		
[I.4] Contaminación electromagnética	B			10				M			M		
[I.5] Avería de origen físico o lógico	MB			100				A			M		
[I.6] Corte de suministro eléctrico	B			100				A			A		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB			100				A			M		
[I.11] Emanaciones electromagnéticas	MB	1			B						MB		
[E.2] Errores del administrador	MB	1	1	10	B	B	M	MB	MB	B			
[E.23] Errores de mantenimiento/actualización	MB			10				M			B		
[E.24] Caída del sistema por agotamiento de recursos	MB			10				M			B		
[E.25] Pérdidas de equipos	MB			100				B	A		MB	M	
[A.6] Abuso de privilegios de acceso	MB	10	100	10	M	A	M	B	M	B	B		
[A.7] Uso no previsto	MB	10	100	10	M	A	M	B	M	B	B		
[A.11] Acceso no autorizado	B	10	100		M	A		M	A				
[A.23] Manipulación de los equipos	MB			100				A	M		M		
[A.24] Denegación de servicio	MB			100				A			M		
[A.25] Robo	MB			1	100			B	A		MB	M	
[A.26] Ataque destructivo	MB				100			A			M		

5.6. [COM] Redes de comunicaciones (impacto y riesgo)

Tabla 143. Impacto y Riesgo (potencial) del activo COM001-Servicio de telefonía

AMENAZAS	COM001-Servicio de comunicaciones			COM001-Servicio de telefonía			Impacto (potencial)			Riesgo (potencial)			
	Frecuencia	I	C	D	I	C	D	I	C	D	I	C	D
[I.8] Fallo de servicios de comunicaciones	MB			100				A			M		
[E.2] Errores del administrador	MB	1	1	1	MB	B	B	MB	MB	MB			
[E.9] Errores de [re]-encaminamiento	MB			100				A			M		
[E.10] Errores de secuencia	MB			10				B			MB		
[E.15] Alteración accidental de la información	MB			10				B			MB		
[E.18] Destrucción de información	MB			1				B			MB		
[E.19] Fugas de información	MB			10				M			B		
[E.24] Caída del sistema por agotamiento de recursos	MB			100				A			M		
[A.5] Suplantación de la identidad del usuario	MB	10	100	10	B	A		MB	MB	MB	M		
[A.6] Abuso de privilegios de acceso	B	10	10	10	B	M	M	B	M	M	M		
[A.7] Uso no previsto	M	10	10	10	B	M	M	B	M	M	M		
[A.9] [re]-encaminamiento de mensajes	MB			100				A			M		
[A.10] Alteración de secuencia	MB			10				B			MB		
[A.11] Acceso no autorizado	B	10	10		B	M		B	M				
[A.12] Análisis de tráfico	MB			100				A			M		
[A.14] Intercepción de información (escucha)	MB			100				A			M		
[A.15] Modificación deliberada de la información	MB			10				B			MB		
[A.19] Divulgación de información	B			10				M			M		
[A.24] Denegación de servicio	MB			100				A			M		

Tabla 144. Impacto y Riesgo (potencial) del activo COM002-Red local

[COM] Redes de comunicaciones	COM002-Red local											
	Probabilidad			Degradoación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia			[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
	COM002-Red local											
[I.8] Fallo de servicios de comunicaciones	MB			100			A			M		
[E.2] Errores del administrador	B	10	10	10	M	M	M	M	M	M	M	
[E.9] Errores de [re]-encaminamiento	MB	100			A					M		
[E.10] Errores de secuencia	MB	10		M						B		
[E.15] Alteración accidental de la información	MB	1		B						MB		
[E.18] Destrucción de información	MB			1			B					MB
[E.19] Fugas de información	MB	10			M					B		
[E.24] Caida del sistema por agotamiento de re	B			100			A			A		
[A.5] Suplantación de la identidad del usuario	M	10	100		M	A	M	M	A			
[A.6] Abuso de privilegios de acceso	M	10	100	10	M	A	M	M	A	M		
[A.7] Uso no previsto	B	10	100	10	M	A	M	M	A	M		
[A.9] [Re]-encaminamiento de mensajes	B	100			A					A		
[A.10] Alteración de secuencia	B	10		M						M		
[A.11] Acceso no autorizado	M	10	100		M	A		M	A			
[A.12] Análisis de tráfico	MB	100			A					M		
[A.14] Intercepción de información (escucha)	MB	100			A					M		
[A.15] Modificación deliberada de la informació	MB	10		M					M			
[A.19] Divulgación de información	M	10			M					M		
[A.24] Denegación de servicio	B			100			A			A		

Tabla 145. Impacto y Riesgo (potencial) del activo COM003-Fibra óptica

[COM] Redes de comunicaciones	COM003-Fibra óptica											
	Probabilidad			Degradoación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia			[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
	COM003-ADSL											
[I.8] Fallo de servicios de comunicaciones	MB			100			M			B		
[E.2] Errores del administrador	MB	1	1	1	MB	B	MB	MB	MB	MB		
[E.9] Errores de [re]-encaminamiento	MB	100			A					M		
[E.10] Errores de secuencia	MB	10		B						MB		
[E.15] Alteración accidental de la información	MB	1		MB						MB		
[E.18] Destrucción de información	MB			1			MB			MB		
[E.19] Fugas de información	MB	10			M					B		
[E.24] Caida del sistema por agotamiento de re	B			10			B			B		
[A.5] Suplantación de la identidad del usuario	MB	10	100		B	A	MB	MB	M			
[A.6] Abuso de privilegios de acceso	MB	1	100	1	MB	A	MB	MB	M	MB		
[A.7] Uso no previsto	M	10	100	10	B	A	B	B	A	B		
[A.9] [Re]-encaminamiento de mensajes	MB	100			A					M		
[A.10] Alteración de secuencia	MB	10	100		MB	A	MB	MB	A			
[A.11] Acceso no autorizado	B	1	100		MB	A	MB	MB	A			
[A.12] Análisis de tráfico	MB	100			A				M			
[A.14] Intercepción de información (escucha)	MB	100			A				M			
[A.15] Modificación deliberada de la informació	MB	10		M					MB			
[A.19] Divulgación de información	M	10			M				B			
[A.24] Denegación de servicio	M			100			M			M		

Tabla 146. Impacto y Riesgo (potencial) del activo COM004-Red wifi

[COM] Redes de comunicaciones	COM004-Red wifi											
	Probabilidad			Degradoación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia			[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
	COM004-Red wifi											
[I.8] Fallo de servicios de comunicaciones	MB			10			MB			MB		
[E.2] Errores del administrador	B	10	10	10	MB	M	MB	MB	M	MB		
[E.9] Errores de [re]-encaminamiento	MB	100			A					M		
[E.10] Errores de secuencia	MB	10		MB						MB		
[E.15] Alteración accidental de la información	MB	1		MB						MB		
[E.18] Destrucción de información	MB			1			MB			MB		
[E.19] Fugas de información	MB	10			M					B		
[E.24] Caida del sistema por agotamiento de re	B			10			MB			MB		
[A.5] Suplantación de la identidad del usuario	A	10	100		MB	A	B	M	A			
[A.6] Abuso de privilegios de acceso	B	10	100	10	MB	A	MB	MB	A	MB		
[A.7] Uso no previsto	B	10	10	10	MB	M	MB	MB	M	MB		
[A.9] [Re]-encaminamiento de mensajes	B	100			A					A		
[A.10] Alteración de secuencia	B	10		MB						MB		
[A.11] Acceso no autorizado	M	10	100		MB	A	MB	MB	A			
[A.12] Análisis de tráfico	MB	100			A				M			
[A.14] Intercepción de información (escucha)	MB	100			A				M			
[A.15] Modificación deliberada de la informació	B	10		MB					MB			
[A.19] Divulgación de información	M	10			M				B			
[A.24] Denegación de servicio	M			100			B			M		

5.7. [Media] Soportes de información (impacto y riesgo)

Tabla 147. Impacto y Riesgo (potencial) del activo MEDIA001-Memorias USB

[Media] Soportes de información	MEDIA001-Memorias USB											
	Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
[MEDIA001]-Memorias USB												
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-Aqua,[I.3]-Contaminación mecánica,[I.4]-Contaminación electromagnética,[I.5]-Avería de origen físico o lógico,[I.6]-Corte de suministro eléctrico,[I.7]-Condiciones inadecuadas de temperatura o humedad,[I.10]-Degradación de los soportes de almacenamiento,[I.11]-Emanaciones electromagnéticas,[E.1]-Errores de los usuarios,[E.2]-Errores del administrador,[E.15]-Alteración accidental de la información,[E.18]-Destrucción de información,[E.19]-Fugas de información,[E.23]-Errores de mantenimiento/actualización,[E.25]-Pérdidas de equipos,[A.7]-Uso no previsto,[A.11]-Acceso no autorizado,[A.15]-Modificación deliberada de la información,[A.18]-Destrucción de información,[A.19]-Divulgación de información,[A.23]-Manipulación de los equipos,[A.25]-Robo,[A.26]-Ataque destructivo	MB		100				B			MB		
[I.1] Fuego	B		100				B			B		
[I.2] Agua	B		100				B			B		
[I.*] Desastres industriales	MB		100				M			B		
[I.3] Contaminación mecánica	B		1				MB			MB		
[I.4] Contaminación electromagnética	MB		100				B			MB		
[I.5] Avería de origen físico o lógico	MB		10				MB			MB		
[I.6] Corte de suministro eléctrico	B		100				B			B		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10				MB			MB		
[I.10] Degradación de los soportes de almacenamiento	B		10				MB			MB		
[I.11] Emanaciones electromagnéticas	MB		1				M			B		
[E.1] Errores de los usuarios	M	10	100	10			B	MA	MB	B	MA	MB
[E.2] Errores del administrador	MB	10	100	10			B	MA	MB	MB	A	MB
[E.15] Alteración accidental de la información	M	100					M			M		
[E.18] Destrucción de información	M			100						B		
[E.19] Fugas de información	B		100				MA			MA		
[E.23] Errores de mantenimiento/actualización	MB		10							MB		
[E.25] Pérdidas de equipos	A	100	100	100			MA	B		MA	M	
[A.7] Uso no previsto	A	100	100	100			M	MA	MB	A	MA	B
[A.11] Acceso no autorizado	MB	100	100	100			M	MA	MB	B	A	MB
[A.15] Modificación deliberada de la información	MB	100					M			B		
[A.18] Destrucción de información	MB			100						B		MB
[A.19] Divulgación de información	B		100				MA			MA		
[A.23] Manipulación de los equipos	MB		100	10			MA	MB		A	MB	
[A.25] Robo	B		100	100			MA	B		MA	B	
[A.26] Ataque destructivo	MB			100			B			MA	M	

Tabla 148. Impacto y Riesgo (potencial) del activo MEDIA002-Discos USB

[Media] Soportes de información	MEDIA002-Discos USB											
	Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
[MEDIA002]-Discos USB												
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-Aqua,[I.3]-Contaminación mecánica,[I.4]-Contaminación electromagnética,[I.5]-Avería de origen físico o lógico,[I.6]-Corte de suministro eléctrico,[I.7]-Condiciones inadecuadas de temperatura o humedad,[I.10]-Degradación de los soportes de almacenamiento,[I.11]-Emanaciones electromagnéticas,[E.1]-Errores de los usuarios,[E.2]-Errores del administrador,[E.15]-Alteración accidental de la información,[E.18]-Destrucción de información,[E.19]-Fugas de información,[E.23]-Errores de mantenimiento/actualización,[E.25]-Pérdidas de equipos,[A.7]-Uso no previsto,[A.11]-Acceso no autorizado,[A.15]-Modificación deliberada de la información,[A.18]-Destrucción de información,[A.19]-Divulgación de información,[A.23]-Manipulación de los equipos,[A.25]-Robo,[A.26]-Ataque destructivo	MB		100				M			B		
[I.1] Fuego	B		100				M			M		
[I.2] Agua	B		100				M			M		
[I.*] Desastres industriales	MB		100				M			B		
[I.3] Contaminación mecánica	M		10				B			B		
[I.4] Contaminación electromagnética	MB		100				M			B		
[I.5] Avería de origen físico o lógico	MB		10				B			MB		
[I.6] Corte de suministro eléctrico	B		100				M			M		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		10				B			MB		
[I.10] Degradación de los soportes de almacenamiento	MB		10				B			MB		
[I.11] Emanaciones electromagnéticas	MB		1				M			B		
[E.1] Errores de los usuarios	B	10	100	10			M	MA	B	M	MA	B
[E.2] Errores del administrador	MB	1	10	1			B	A	MB	MB	M	MB
[E.15] Alteración accidental de la información	B	10					M			M		
[E.18] Destrucción de información	MB			100						B		
[E.19] Fugas de información	MB		100				MA			A		
[E.23] Errores de mantenimiento/actualización	B		10							B		
[E.25] Pérdidas de equipos	MB		100	100			MA	M		A	MB	
[A.7] Uso no previsto	B	100	100	100			A	MA	M	A	MA	M
[A.11] Acceso no autorizado	B	100	100	100			A	MA	M	A	MA	M
[A.15] Modificación deliberada de la información	MB	100					A			M		
[A.18] Destrucción de información	MB			100						B		
[A.19] Divulgación de información	MB		100				MA			A		
[A.23] Manipulación de los equipos	MB		100	10			MA	B		A	MB	
[A.25] Robo	B		100	100			MA	M		MA	M	
[A.26] Ataque destructivo	MB			100			M			B		

5.8. [AUX] Equipamiento auxiliar (impacto y riesgo)

Tabla 149. Impacto y Riesgo (potencial) del activo AUX001-SAI

[AUX] Equipamiento auxiliar	AUX001-SAI											
	Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)		
AMENAZAS	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
AUX001-SAI												
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-Aqua,[I.3]-Contaminación mecánica,[I.4]-Contaminación electromagnética,[I.5]-Avería de origen físico o lógico,[I.6]-Corte de suministro eléctrico,[I.7]-Condiciones inadecuadas de temperatura o humedad,[I.9]-Interrupción de otros servicios y suministros,[I.11]-Emanaciones electromagnéticas,[E.2]-Errores del administrador,[E.25]-Pérdidas de equipos,[A.7]-Uso no previsto,[A.11]-Acceso no autorizado,[A.15]-Modificación deliberada de la información,[A.18]-Destrucción de información,[A.19]-Divulgación de información,[A.23]-Manipulación de los equipos,[A.25]-Robo,[A.26]-Ataque destructivo	MB		100				M			B		
[I.1] Fuego	B		100				M			M		
[I.2] Agua	B		100				M			M		
[I.*] Desastres industriales	MB		100				M			B		
[I.3] Contaminación mecánica	MB		100				M			B		
[I.4] Contaminación electromagnética	MB		100				M			B		
[I.5] Avería de origen físico o lógico	B		100				M			M		
[I.6] Corte de suministro eléctrico	MB		10				B			MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	MB		100				M			M		
[I.9] Interrupción de otros servicios y suministros	MB		10				B			MB		
[I.11] Emanaciones electromagnéticas	MB		1				MB			MB		
[E.2] Errores del administrador	MB		1	10			MB	MB	B	MB	MB	B
[E.25] Pérdidas de equipos	MB	10	1	10			MB	MB	B	MB	MB	B
[A.7] Uso no previsto	B	10	1	10			MB	MB	B	MB	MB	B
[A.11] Acceso no autorizado	B	10	1	10			MB	MB	B	MB	MB	B
[A.15] Modificación deliberada de la información	MB		1	100			MB	M		MB	M	
[A.18] Destrucción de información	MB			100			M			B		
[A.19] Divulgación de información	MB						MA			A		
[A.23] Manipulación de los equipos	MB			1	100		MB	M		MB	M	
[A.25] Robo	B			1	100		MB	M		MB	M	
[A.26] Ataque destructivo	MB				100		M			B		

5.9. [L] Instalaciones (impacto y riesgo)

Tabla 150. Impacto y Riesgo (potencial) del activo L001-Edificio empresa

AMENAZAS	[L] Instalaciones			L001-Edificio empresa									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
L001-Edificio empresa													
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB			100			A			M			
[I.1] Fuego	MB			100			A			M			
[I.2] Agua	MB			10			M			B			
[I.*] Desastres industriales	MB			10			M			B			
[I.11] Emanaciones electromagnéticas	MB		1				M			B			
[E.15] Alteración accidental de la información	MB	100			MA								
[E.18] Destrucción de información	B			100			A			A			
[E.19] Fugas de información	M		10				A			A			
[A.7] Uso no previsto	MB	10	10	10	A	A	M	M	M	B			
[A.11] Acceso no autorizado	B	10	100		A	MA		A	MA				
[A.15] Modificación deliberada de la información	MB	100			MA								
[A.18] Destrucción de información	MB			100			A			M			
[A.19] Divulgación de información	MB	100			MA								
[A.26] Ataque destructivo	MB			100			A			M			
[A.27] Ocupación enemiga	MB	100	100		MA	A		A	M				

Tabla 151. Impacto y Riesgo (potencial) del activo L002-Cuarto de comunicaciones

AMENAZAS	[L] Instalaciones			L002-Cuarto de comunicaciones									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
L002-Cuarto de comunicaciones													
[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-A)	MB			100			A			M			
[I.1] Fuego	B			100			A			A			
[I.2] Agua	MB		10				M			B			
[I.*] Desastres industriales	MB		10				M			B			
[I.11] Emanaciones electromagnéticas	MB		1				M			B			
[E.15] Alteración accidental de la información	MB	10			M								
[E.18] Destrucción de información	B			100			A			A			
[E.19] Fugas de información	B	100			MA								
[A.7] Uso no previsto	B	10	10	10	M	A	M	M	M	A	M		
[A.11] Acceso no autorizado	B	10	100		M	MA		M	MA				
[A.15] Modificación deliberada de la información	MB	10			M								
[A.18] Destrucción de información	MB			100			A			M			
[A.19] Divulgación de información	MB	100			MA								
[A.26] Ataque destructivo	MB			100			A			M			
[A.27] Ocupación enemiga	MB	100	100		MA	A		A	M				

5.10. [P] Personal (impacto y riesgo)

Tabla 152. Impacto y Riesgo (potencial) del activo P001-Personal interno (Gerencia)

AMENAZAS	[P] Personal			P001-Personal interno (Gerencia)									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
P001-Personal interno (Gerencia)													
[E.7] Deficiencias en la organización	B			10			B			B			
[E.19] Fugas de información	MB			100			MA			A			
[E.28] Indisponibilidad del personal	B			10			B			B			
[A.28] Indisponibilidad del personal	MB			10			B			M			
[A.29] Extorsión	MB	100	100	100	A	MA	M	M	A	B			
[A.30] Ingeniería social (picareza)	MB	100	100	100	A	MA	M	M	A	B			

Tabla 153. Impacto y Riesgo (potencial) del activo P002-Personal interno (Responsables área)

AMENAZAS	[P] Personal			P002-Personal interno (Responsables área)									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
P002-Personal interno (Responsables área)													
[E.7] Deficiencias en la organización	B			10			M			M			
[E.19] Fugas de información	B			100			A			A			
[E.28] Indisponibilidad del personal	B			100			A			A			
[A.28] Indisponibilidad del personal	B			10			M			M			
[A.29] Extorsión	MB	10	100	10	M	A	M	B	M	B	M		
[A.30] Ingeniería social (picareza)	MB	10	100	100	M	M	M	B	B	B	B		

Tabla 154. Impacto y Riesgo (potencial) del activo P003-Resto personal interno

AMENAZAS	[P] Personal			P003-Resto personal interno									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
P003-Resto personal interno													
[E.7] Deficiencias en la organización	B			10			B			B			
[E.19] Fugas de información	B			100			MA			A			
[E.28] Indisponibilidad del personal	B			100			A			A			
[A.28] Indisponibilidad del personal	B			100			A			A			
[A.29] Extorsión	MB	10	100	10	M	A	M	B	M	B	M		
[A.30] Ingeniería social (picareza)	MB	100	100	100	A	A	A	M	M	M	M		

Tabla 155. Impacto y Riesgo (potencial) del activo P004-Personal externo (admin. sistemas)

AMENAZAS	[P] Personal			P004-Personal externo (administrador sistemas)									
				Probabilidad			Degradación			Impacto (potencial)			Riesgo (potencial)
	Frecuencia	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]
P004-Personal externo (administrador sistemas)													
[E.7] Deficiencias en la organización	B			10			M			M			
[E.19] Fugas de información	B			100			A			A			
[E.28] Indisponibilidad del personal	B			100			A			A			
[A.28] Indisponibilidad del personal	B			100			A			A			
[A.29] Extorsión	MB	10	100	10	M	A	M	B	M	B	M		
[A.30] Ingeniería social (picareza)	MB	100	100	100	A	A	A	M	M	M	M		

6. Evaluación de salvaguardas

Una vez calculado el riesgo potencial e identificados aquellos activos con un riesgo mayor, se puede evaluar la aplicación de posibles salvaguardas o contramedidas que permitan reducir este riesgo hasta niveles aceptables.

Las salvaguardas aplicadas sobre un activo y dimensión para contrarrestar una amenaza actúan reduciendo, o bien la degradación, o la probabilidad de que la amenaza se materialice, disminuyendo de este modo el nivel de riesgo. Así pues, existen distintos tipos de salvaguardas que se pueden aplicar, con efectos distintos (prevención, limitación del daño, fortalecimiento y complementación del efecto de las demás).

A continuación, se resume la relación de posibles salvaguardas a aplicar para contrarrestar las amenazas que suponen un mayor riesgo en cada activo según el apartado anterior. Del catálogo de salvaguardas se excluyen aquellas que no sean apropiadas para proteger la dimensión necesaria o no protegen frente a una amenaza, o aquellas cuya aplicación sea desproporcionada para el riesgo existente.

Una vez que se han determinado las salvaguardas se calcula tanto el impacto como el riesgo residual teniendo en cuenta la disminución que producen sobre el valor de degradación o de probabilidad, considerando la efectividad que pueda darnos cada salvaguarda.

La efectividad de una salvaguarda viene determinada por varios parámetros tales como, que sea técnicamente adecuada para la amenaza frente a la que se aplica, estar desplegada y en uso correctamente. Los usuarios deben conocerla y existir controles que alerten ante un mal funcionamiento o nos dé idea de su eficacia.

En los datos estimados que se proporcionan, una eficacia cercana al 0% correspondería a aquellas salvaguardas inexistentes, mientras que un 100% a aquellas idóneas y en uso perfectamente implantadas, mantenidas, controladas y conocidas.

En las tablas siguientes se indica con color verde aquellos valores de probabilidad o degradación que se hayan visto modificados por el efecto de las salvaguardas. Además, se calcula el impacto y riesgo residual que quedaría si se implementaran estas salvaguardas.

6.1. [D][info] Datos / Información (salvaguardas)

156. Salvaguardas: Impacto y riesgo residual de los activos [D][info] Datos / Información (001-Fichero Clientes, D001-Expediente Cliente)										
AMENAZAS	001-Fichero Clientes					D001-Expediente Cliente				
	Probabilidad	Degravación	Impacto (potencial)	Impacto (real)	Riesgo	Probabilidad	Degravación	Impacto (potencial)	Impacto (real)	Riesgo
[E.1] Errores de los usuarios	M	10	10	10	A	M	1	1	0	M
[E.2] Errores del administrador	B	10	10	10	A	M	1	1	0	M
[E.3] Alteración accidental de la información	M	10	10	10	A	M	1	1	0	M
[E.4] Errores de programación	M	100	100	100	A	M	1	1	0	M
[E.5] Fugas de información	MB	10	10	10	A	M	1	1	0	M
[A.5] Suplantación de la identidad del usuario	M	10	10	10	A	M	1	1	0	M
[A.6] Robo de privilegios de acceso	MB	10	10	10	A	M	1	1	0	M
[A.7] Acceso no autorizado	MB	10	100	100	A	MA	1	1	0	M
[A.8] Destrucción deliberada de la información	MB	100	100	100	A	M	1	1	0	M
[A.9] Difusión de información	MB	100	100	100	MA	M	1	1	0	M
002-Expediente Cliente										
[E.1] Errores de los usuarios	A	10	1	10	M	M	B	A	M	
[E.2] Errores del administrador	B	10	10	10	M	M	B	A	M	
[E.3] Alteración accidental de la información	M	10	10	10	M	M	B	A	M	
[E.4] Errores de programación	M	100	100	100	A	M	1	1	0	M
[E.5] Fugas de información	MB	10	10	10	A	M	1	1	0	M
[A.5] Suplantación de la identidad del usuario	B	10	10	10	M	A	M	1	1	M
[A.6] Robo de privilegios de acceso	MB	10	10	10	M	A	M	1	1	M
[A.7] Acceso no autorizado	MB	10	100	100	MA	M	1	1	0	M
[A.8] Destrucción deliberada de la información	MB	100	100	100	A	M	1	1	0	M
[A.9] Difusión de información	MB	100	100	100	MA	M	1	1	0	M
003-Expediente Cliente										
[E.1] Errores de los usuarios	M	10	10	10	A	M	1	1	0	M
[E.2] Errores del administrador	B	10	10	10	M	M	B	A	M	
[E.3] Alteración accidental de la información	M	10	10	10	M	M	B	A	M	
[E.4] Errores de programación	M	100	100	100	A	M	1	1	0	M
[E.5] Fugas de información	MB	10	10	10	A	M	1	1	0	M
[A.5] Suplantación de la identidad del usuario	B	10	10	10	M	A	M	1	1	M
[A.6] Robo de privilegios de acceso	MB	10	10	10	M	A	M	1	1	M
[A.7] Acceso no autorizado	MB	10	100	100	MA	M	1	1	0	M
[A.8] Destrucción deliberada de la información	MB	100	100	100	A	M	1	1	0	M
[A.9] Difusión de información	MB	100	100	100	MA	M	1	1	0	M

6.9. [P] Personal (salvaguardas)

[P] Personal		177. Salvaguardas: Impacto y riesgo residual de los activos (P) Personal																						
AMENAZAS	Probabilidad	Degrado/Impacto						Protección/Intervención						Salvaguardias	Probabilidad	Degrado/Impacto						Protección/Intervención		
		[0]	[1]	[2]	[3]	[4]	[5]	[0]	[1]	[2]	[3]	[4]	[5]			[0]	[1]	[2]	[3]	[4]	[5]			
POD-Personal interno (Gerencia)																								
[1,1] Defensas en la organización	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[1,19] Fuga de información	MB	100	MA	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[1,20] Ataque informático	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[A,20] Indisponibilidad del personal	MB	50	MA	B	M	A	MA	B	M	A	MA	B	M	MB	10	10	10	M	MA	B	M	MB	M	MB
[A,29] Exteriores	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	10	10	10	M	MA	B	M	MB	M	MB
[A,30] Organización social (personal)	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	1	10	10	M	MA	B	M	MB	M	MB
POD-Personal interno (Responsables área)																								
[1,1] Defensas en la organización	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[1,19] Fuga de información	MB	100	MA	B	M	A	MA	B	M	A	MA	B	M	MB	10	M	M	M	M	MB	M	MB	M	
[1,20] Ataque informático	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[A,20] Indisponibilidad del personal	MB	50	MA	B	M	A	MA	B	M	A	MA	B	M	MB	10	10	10	M	MA	B	M	MB	M	MB
[A,29] Exteriores	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	1	10	10	M	MA	B	M	MB	M	MB
[A,30] Organización social (personal)	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	1	10	10	M	MA	B	M	MB	M	MB
POD-Personal externo (Administrador sistemas)																								
[1,1] Defensas en la organización	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[1,19] Fuga de información	MB	100	MA	B	M	A	MA	B	M	A	MA	B	M	MB	10	M	M	M	M	MB	M	MB	M	
[1,20] Ataque informático	B	10	M	B	M	A	MA	B	M	A	MA	B	M	MB	1	M	MB	MB	M	MB	MB	M	MB	
[A,20] Indisponibilidad del personal	MB	50	MA	B	M	A	MA	B	M	A	MA	B	M	MB	10	10	10	M	MA	B	M	MB	M	MB
[A,29] Exteriores	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	1	10	10	M	MA	B	M	MB	M	MB
[A,30] Organización social (personal)	MB	100	100	100	M	A	MA	M	A	MA	M	A	MA	MB	1	10	10	M	MA	B	M	MB	M	MB

7. Tratamiento del riesgo

Una vez realizado el estudio de impactos, riesgos, activos a proteger, amenazas y salvaguardas, en este apartado se realizará la evaluación y el tratamiento de los riesgos determinando la acción y objetivo (aceptar, evitar, mitigar, compartir) a adoptar ante cada riesgo para reducirlo a un nivel aceptable según los criterios establecidos por la organización. La evaluación y tratamiento se realizará tomando como base las tablas con las salvaguardas y riesgos residuales calculados incluidas en el apartado anterior.

En función del nivel de criticidad de los riesgos, se valorarán los que deberían ser tratados y cuáles podrían ser asumidos por la empresa. Para ello hay que establecer el umbral de riesgo asumible por la organización. Según el nivel riesgo, se adoptará un tratamiento u otro.

Según el análisis de riesgos descrito, en el presente trabajo se seguirá como criterio general para decidir sobre las acciones a adoptar en el tratamiento de los riesgos en cada uno de los activos de la empresa, aplicar el siguiente criterio de tratamiento:

- Activos cuya estimación del riesgo haya sido (B)bajo, (MB)muy bajo, debido a que tienen una probabilidad baja de que ocurra o el impacto no es importante: **Aceptar**
- Activos cuya estimación del riesgo sea (M)Medio, no se tratarán con medidas directas para reducirlo, aunque sí que se tendrán en cuenta en los planes de contingencia y formación: **Aceptar**
- Activos cuyo riesgo sea (A)alto, (MA)muy alto, que suponen riesgos graves o críticos, serán tratados evaluando las salvaguardas adecuadas para reducirlos hasta un nivel aceptable: **Mitigar/Compartir**

A continuación, se detalla el análisis de salvaguardas a aplicar por activo en base a los datos calculados en los apartados anteriores.

7.1. [D][info] Datos / Información (tratamiento del riesgo)

7.1.1. Activos I001-Fichero Clientes, D001-Expediente Cliente

Estos activos se refieren a la información relacionada con información de clientes, sensible y carácter personal. Además del resto de información relacionada que podría considerarse expediente de un cliente, (información financiera, contractual, comercial, contacto, etc.).

Los riesgos que presentan son Altos en las dimensiones de confidencialidad e integridad y están relacionados con las siguientes amenazas: [E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.15] Alteración accidental de la información, [A.5] Suplantación de la identidad del usuario, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.19] Divulgación de información.

Por ello las medidas que se pueden adoptar van encaminadas al control y aseguramiento de la seguridad de acceso a la esta información.

Las salvaguardas que se contemplan son:

[H.AC] Control de acceso lógico, [H.IA] Identificación y autenticación: Mediante esta salvaguarda establecerán y revisarán los mecanismos de autenticación en el sistema (contraseñas, tokens, certificados), para gestionar los permisos y establecer las medidas de seguridad necesarias sobre cada nivel de información. Se realizará la revisión de la política actual de usuarios, grupos y perfiles de seguridad en el sistema, para garantizar que se satisfacen los requerimientos de seguridad para estos activos; adaptándola al nivel de confidencialidad de la información, las funciones de cada empleado, departamento, propietario de la información, etc.

[H.AU] Registro y auditoría: Mediante el establecimiento de un sistema de auditoría y registro de eventos de seguridad relacionados con el acceso y manipulación de los datos más críticos. El sistema debería registrar datos como:

- - Acceso, modificación y borrado de información categorizada con nivel alto de confidencialidad.
- - Datos generales sobre las conexiones de usuarios al sistema, intentos fallidos y otra información de conexión (fecha/hora, aplicaciones utilizadas, información confidencial accedida, ...).
- - Registro de la modificación de permisos sobre los recursos del sistema.

[D.C] Cifrado de información: Según el grado de confidencialidad de la información se plantea la necesidad de cifrar al menos aquella información sensible de carácter personal para mitigar el riesgo de confidencialidad con los datos más sensibles. Este aspecto debería quedar contemplado en la política de seguridad.

[D.A] Copias de seguridad de los datos (backup): Con la implementación de esta salvaguarda se garantizarán la disponibilidad e integridad de estos activos de información ante incidencias. Será necesario adecuar la política de copias de seguridad al nivel de criticidad de los datos.

[PS.AT] Formación y concienciación: La formación y concienciación en materia de seguridad es necesaria para conocer las amenazas, ayudando a reducir/evitar riesgos y a hacer frente a determinadas amenazas; siendo obligatorio el cumplimiento del Reglamento general de protección de datos (RGPD) [3].

Política de Seguridad: Elaboración de las políticas con la normativa interna en materia de seguridad de los datos que garanticen el cumplimiento del reglamento RGPD y regulen las medidas a adoptar para la protección de estos activos de información. Tienen que quedar contemplados aspectos como política de copias, usuarios, contraseñas, nivel de permisos, auditoría sobre los datos, etc.

Con este conjunto de salvaguardas todos los riesgos de este activo quedarían reducidos a niveles aceptables (medios o bajos).

7.1.2. Activos D002-Datos acceso Servidor, D003-Datos acceso Usuarios

Estos activos se refieren a la gestión y custodia de credenciales de acceso a la red, de usuarios y administradores. Los riesgos presentan un nivel Alto/Muy Alto en todas las dimensiones, aunque son más en el caso del activo *[D002-Datos acceso Servidor]* pues otorgan acceso a una activo más crítico y un nivel de privilegios mayor.

Será necesario adecuar la política de copias de seguridad al nivel de criticidad de los datos.

Están **relacionados con las siguientes amenazas:** *[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.18] Destrucción de información, [E.19] Fugas de información, [A.5] Suplantación de la identidad del usuario, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.18] Destrucción de información, [A.19] Divulgación de información.* Por ello las medidas que se pueden adoptar van encaminadas al control y aseguramiento de la seguridad de acceso.

Las salvaguardas que se contemplan son:

[PS.AT] Formación y concienciación: Dentro de la formación en materia de seguridad a impartir al personal, es necesario incluir contenido sobre la gestión de las credenciales, políticas de contraseñas, contraseñas seguras y amenazas.

[H.AC] Control acceso lógico, [H.IA] Identificación y autenticación: El acceso al sistema se debe realizar con credenciales seguras, (usuario de dominio y contraseña segura, certificados, tokens, etc.). Las cuentas de usuario/Administrador deben ser personales e intransferibles. Los accesos y actividad de todos los usuarios deben ser auditados.

Política de Seguridad corporativa: Se debe crear el procedimiento de alta (y baja) de cuentas de usuario y cuentas de administrador y definir política de contraseñas (complejidad, número de intentos, bloqueo, longitud, caducidad, repetición, envío de contraseña, custodia de las credenciales de administrador, ...). También definir el nivel de auditoría necesario sobre las acciones que realice cada uno de los tipos de cuenta (usuarios y administradores), alertas a notificar, gestión de la seguridad sobre los recursos mediante grupos de usuarios de dominio.

Con este conjunto de salvaguardas todos los riesgos de estos activos quedarían reducidos a niveles aceptables.

7.1.3. Activo D004-Backup Servidor

Las copias de seguridad de datos del servidor presentan riesgos de nivel Alto en las dimensiones de integridad y principalmente confidencialidad, debido a que la información crítica y sensible es parte de las copias. Se trata de un activo básico en el plan de recuperación, por lo que es crucial su protección como medida de contingencia ante una pérdida de información.

Las amenazas relacionadas para estos riesgos son: *[E.2] Errores del administrador, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, [A.19] Divulgación de información.*

Por ello las medidas que se pueden adoptar van encaminadas al aseguramiento de la confidencialidad ante una pérdida y a su integridad.

Las salvaguardas que se contemplan son:

[H.AC] Control de acceso lógico: Se establecerán las medidas de seguridad oportunas de acceso a la gestión, configuración, operación y mantenimiento de las copias.

[D.C] Cifrado de la información: Se establecerá un mecanismo de cifrado a las copias debido al riesgo que supone la pérdida o robo por el nivel de confidencialidad de la información que contienen.

Política de Seguridad corporativa: Es necesario revisar la política de copias actual para que se adecue a cada tipo de información según el nivel de confidencialidad y criticidad, garantizando que se cumple el reglamento RGPD; adaptando también las frecuencias y retención de las copias teniendo en cuenta tanto aspectos legales sobre periodo de preservación de los datos, como para la estrategia de recuperación. Además de revisar la

información que se copia y cuándo, se deben analizar las configuraciones, aplicaciones o equipos a incluir; así como establecer un nivel adecuado de log que permita revisar el estado y analizar errores.

Las salvaguardas que se contemplan son:

Todo debe quedar debidamente documentado mediante los procedimientos oportunos.

Plan de contingencia: En el plan de contingencia se deberá prever la comprobación de la validez de las copias mediante recuperaciones periódicas planificadas y contempladas en la política de seguridad corporativa.

Sería conveniente guardar los juegos de copias en ubicaciones seguras fuera del edificio (*actualmente se guardan en una caja fuerte en el mismo edificio*).

Con este conjunto de salvaguardas todos los riesgos de este activo quedarían reducidos a niveles aceptables.

7.1.4. Activos D005-Logs, D006-Ficheros configuraciones

Estos activos se refieren a los archivos de log y de configuraciones. El nivel de riesgo que presentan es Alto en ambos activos.

En el activo **D005-Logs**, los riesgos Altos están **relacionados con las amenazas:** [E.3] *Errores de monitorización (log)*, [A.5] *Suplantación de la identidad del usuario*, [A.11] *Acceso no autorizado*, [A.15] *Modificación deliberada de la información*, [A.19] *Divulgación de información*.

En el activo **D006-Ficheros configuraciones**, los riesgos Altos están **relacionados con las amenazas:** [E.2] *Errores del administrador*, [E.4] *Errores de configuración*, [E.18] *Destrucción de información*, [A.5] *Suplantación de la identidad del usuario*.

Para mitigarlos o reducirlos, **se considera la implementación de las siguientes salvaguardas:**

En los logs y en algunos archivos de configuración puede haber información confidencial.

[H.AC] Control de acceso lógico, [H.IA] Identificación y autenticación: Se establecerán permisos adecuados para garantizar que no se manipula esta información y mantener su confidencialidad, preservando la trazabilidad y autenticidad. En los logs y en algunos archivos de configuración puede haber información confidencial.

[H.AU] Registro y auditoría: Se establecerá el nivel de auditoría suficiente para tener la trazabilidad y garantizar el no repudio. En los archivos de configuración, se mantendrá registro de cambios y modificaciones. Las salvaguardas del punto anterior, control de acceso, identificación y autenticación, permitirán dejar registro de acciones y logs sobre el sistema por parte de los usuarios con la granularidad y seguridad suficiente.

[H.tools.LA] Herramienta para análisis de logs: Se utilizará una herramienta para analizar y gestionar los eventos de logs y monitorizar el sistema. La información de los logs y registro de eventos es información básica para analizar incidentes, depurar responsabilidades o determinar la afectación de un ataque, por ejemplo.

[D.A] Copias de seguridad de los datos (backup): La política de copias de seguridad debe contemplar el respaldo de aquellos archivos de configuraciones importantes; así como mantener copia de los logs.

Política de Seguridad corporativa: En las políticas debe quedar contemplado las configuraciones sensibles a proteger, las medidas de copias y permisos sobre estos activos. Así como el nivel de auditoría y registro de eventos necesario.

7.2. [K] Claves criptográficas (tratamiento del riesgo)

7.2.1. Activo K001-Certificados FMNT

En el análisis de riesgos de este activo se detecta nivel de riesgo Alto en la dimensión de integridad **relacionado con las amenazas:** *[E.2] Errores del administrador, [E.15] Alteración accidental de la información, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información.*

Las salvaguardas contempladas son: **[H.AC] Control de acceso lógico, [H.IA] Identificación y autenticación, [D.A] Copias de seguridad de los datos (backup), [K.DS] Gestión de claves de firma de información, Política de seguridad**

Con la aplicación de estas salvaguardas, todos los riesgos quedarían mitigados o reducidos a nivel Medio aceptable, pues una vez se tiene copia, los certificados se pueden volver a instalar o en otro caso, solicitar de nuevo.

7.3. [SW] Software – Aplicaciones informáticas (tratamiento del riesgo)

7.3.1. Activo SW001-ERP

Este activo corresponde al software Prinex Real State (software de gestión inmobiliaria). Es el ERP donde reside y se gestiona toda información administrativo-financiera de la empresa

(contabilidad, transacciones comerciales de ventas, compras, ...). Es un activo crítico desde el punto de vista de la gestión del negocio de la empresa. De él dependen los departamentos administrativo-financiero y comercial, principalmente.

En el análisis de riesgos de este activo, se detectan riesgos Altos **relacionados con las amenazas:**

[E.20] Vulnerabilidades de los programas (software), [A.6] Abuso de privilegios de acceso

Para los cuales **se estiman las siguientes salvaguardas:**

[SW] Protección de las Aplicaciones Informáticas: Aunque la configuración para ejecución de la herramienta en los clientes no es trivial, se procederá a proteger mediante un grupo de dominio específico para gestionar los usuarios de Prinex (Anonym/grp_Prinex) y su permiso de ejecución. Se han detectado riesgos relacionados con la reutilización de puestos donde la herramienta ha sido previamente instalada, y los nuevos usuarios no deberían tener acceso.

[SW.A] Copias de seguridad (backup): Se revisará que la restauración de la copia de seguridad es válida para que el software y base de datos quede operativo mediante la restauración, ante un desastre.

[H.AC] Control de acceso lógico, [SW.SC] Se aplican perfiles de seguridad: Además del grupo de red específico, la herramienta cuenta con usuarios propios y perfiles por funcionalidad dentro de esta. Es necesario revisar y definir los distintos perfiles base necesarios dentro del ERP asignables a cada persona según su función/departamento y alinear los usuarios actuales a estos.

[SW.CM] Cambios (actualizaciones y mantenimiento), [H.tools.LA] Herramienta para análisis de logs, [H.AU] Registro y auditoría, [H.tools.AV] Herramienta contra código dañino: Ya existen medidas que implementan estas salvaguardas. Habría que revisarlas.

Manuales y Procedimientos: Es importante confeccionar los manuales de procedimiento de las tareas de cada equipo dentro de la herramienta ante indisponibilidad del personal; así como las instrucciones técnicas para la configuración de usuarios y asignación de perfiles dentro del ERP. Esta función puede recaer en un responsable de Administración.

Con la aplicación de estas salvaguardas, todos los riesgos quedarían mitigados o reducidos a nivel Bajo o inferior.

7.3.2. Activos SW002-Paquete ofimático, SW003-Cliente de correo, SW006- Navegador web

En el análisis de riesgos de este grupo de activos se detecta nivel de riesgo Medio en **SW002- Paquete ofimático y SW006- Navegador web, relacionado con las amenazas:**

[E.8] Difusión de software dañino y [A.5] Suplantación de la identidad del usuario.

Con la aplicación de estas **salvaguardas [H.tools.AV] Herramienta contra código dañino y [H.AC] Control de acceso lógico**, se mitigaría el riesgo en estos dos activos. El resto de los riesgos quedaría en niveles Bajos junto con el resto de las medidas adoptadas.

En el caso del **SW003-Cliente de correo**, los riesgos que se dan son de nivel Alto relacionados con las amenazas: *[E.8] Difusión de software dañino, [E.19] Fugas de información, [E.20] Vulnerabilidades de los programas (software), [A.7] Uso no previsto*.

Para estima aplicar las siguientes **salvaguardas**:

[H.tools.AV] Herramienta contra código dañino y [H.AC] Control de acceso lógico: Se mitigaría los riesgos relacionado con virus.

[SW.A] Copias de seguridad (backup): Garantizaría la integridad del software ante una degradación que requiriese reinstalación.

[SW.SC] Se aplican perfiles de seguridad: Se utilizarán los perfiles de usuario de red para asignar políticas de uso relacionadas con la navegación y uso de internet (utilización de un proxy).

[SW.CM] Cambios (actualizaciones y mantenimiento), [SW] Protección de las Aplicaciones Informáticas: Con una política de actualizaciones de últimas versiones se mejorará la estabilidad, reducirá los errores del software y solucionará las vulnerabilidades de seguridad que se vayan produciendo y solventando por parte del fabricante.

[D.C] Cifrado de la información: Es aconsejable la utilización de protocolos seguros SSL, HTTPS y regulación de su uso en la política de seguridad.

[H.tools.LA] Herramienta para análisis de logs, [H.AU] Registro y auditoría: Mejorará el análisis ante incidentes o errores que se estén produciendo.

Política de seguridad, Manuales y Procedimientos: Es importante que en la política de seguridad queden contempladas las normas sobre el uso del correo electrónico y sus riesgos.

[PS.AT] Formación y concienciación: En este ámbito también es de aplicación la formación y concienciación en materia de seguridad, ayudando a reducir riesgos detectados y a hacer frente a determinadas amenazas. Por ejemplo, respecto al riesgo que supone un mal uso del correo y conocimiento de las amenazas a las que se está expuesto como puerta de entrada para instalar software dañino.

Con la implantación de estas medidas todos los riesgos quedarían mitigado o reducidos a niveles bajos.

7.3.3. Activo SW004-Antivirus

En el análisis de riesgos de este grupo de activos se detecta nivel de riesgo Alto **relacionado con las amenazas**: [E.20] *Vulnerabilidades de los programas (software)*, [E.21] *Errores de mantenimiento/actualización de programas (software)*.

Estas serían las **salvaguardas consideradas**: [H.tools.AV] *Herramienta contra código dañino*, [H.AC], *Control de acceso lógico*, [SW] *Protección de las Aplicaciones Informáticas*, [SW.A] *Copias de seguridad (backup)*, [SW.SC] *Se aplican perfiles de seguridad*, [SW.CM] *Cambios (actualizaciones y mantenimiento)*, [H.tools.LA] *Herramienta para análisis de logs*, [H.AU] *Registro y auditoría*, [H.AC] *Control de acceso lógico, Política de seguridad, Manuales y Procedimientos*.

Actualmente la empresa ya utiliza un software antivirus server centralizado en el servidor que permite distribuir e instalar los clientes antivirus, mantener actualizadas las firmas y la gestión de los escaneos en la red (opciones y programación); así como la monitorización del estado y análisis de cada puesto, supervisión de logs, registro de incidencias o archivos sospechosos. Además, se controla por directivas que el software antivirus cliente no se pueda desactivar, ni desinstalar. Sería necesario formalizar la política de seguridad al respecto.

Con la revisión y aplicación de estas salvaguardas quedarían todos los riesgos mitigados o reducidos a niveles Bajos.

7.3.4. Activo SW005-Sistema de backup

Este activo se refiere al software de backup donde se configuran, planifican y revisan el conjunto de copias de seguridad. En el análisis de riesgos del activo se obtienen un riesgo de nivel **Alto** relacionado con la **amenaza**: [E.20] *Vulnerabilidades de los programas (software)*, y el resto riesgos de nivel **Medio relacionados con las amenazas**: [E.2] *Errores del administrador* [E.19] *Fugas de información*, [E.21] *Errores de mantenimiento/actualización de programas (software)*, [A.5] *Suplantación de la identidad del usuario*, [A.6] *Abuso de privilegios de acceso*, [A.7] *Uso no previsto*, [A.8] *Difusión de software dañino*, [A.11] *Acceso no autorizado*, [A.15]

Modificación deliberada de la información, [A.18] *Destrucción de información*, [A.19] *Divulgación de información*.

Aunque es un nivel que puede ser aceptable, la importancia del software en cuanto a la función que realiza hace que apliquemos **las siguientes salvaguardas** para reducirlos a **Bajos**:

[SW] *Protección de las Aplicaciones Informáticas*, [H.tools.AV] *Herramienta contra código dañino*: Como cualquier otro software debe estar protegido por el antivirus y herramientas

de análisis de vulnerabilidades. Debido al alto nivel de riesgo que presenta ante la amenaza de vulnerabilidades por la información que maneja para realizar la copia, se realizará un análisis específico.

[SW.SC] Se aplican perfiles de seguridad, [H.AC] Control de acceso lógico: Se deben configurar los permisos de acceso al software sólo para administradores, pues un acceso no autorizado puede permitir acceso a la información de las copias y la configuración de éstas.

[SW.A] Copias de seguridad (backup): Es importante que se tenga copia del software para restaurarlo en caso de necesidad, volver a una versión estable tras una actualización, etc.

[SW.CM] Cambios (actualizaciones y mantenimiento): Deben aplicarse las últimas actualizaciones y correcciones de versiones existentes para evitar errores en funcionalidades o vulnerabilidades solucionables.

[D.C] Cifrado de la información: La herramienta actual no cifra las copias. Dependiendo de la solución de cifrado que se adopte para la empresa, se tendrá que ver la posibilidad de que sea compatible con este software. Puede derivar en comprar otro software o que la propia solución de cifrado ya disponga de funcionalidades de copias de seguridad.

[H.tools.LA] Herramienta para análisis de logs, [H.AU] Registro y auditoría: Hay que evaluar la posibilidad de integrar los logs del software de backup en la herramienta de análisis de log.

Política de seguridad: Las características, permisos de acceso y administración deben estar contempladas en la política de seguridad.

Manuales y Procedimientos: Es necesario que quede formalizado el procedimiento de instalación y configuración del software y conjuntos de copias, y los manuales de uso de la herramienta.

7.3.5. Activo SW007-Portal Web

Este activo no presenta ningún riesgo pues se trata de páginas con información comercial de las distintas promociones, así como los datos de contacto de la empresa. Su desarrollo y mantenimiento ha sido contratado a una empresa informática, así pues, el riesgo bajo existente estaría compartido con ésta.

7.3.6. Activo SW008-Sistema operativo Servidor

En el análisis de riesgos del activo relativo al sistema operativo del servidor da como resultado niveles de riesgo Altos **relacionados con las amenazas:** *[A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso.*

No en vano, el acceso al servidor es donde residen los activos críticos de información y proporciona acceso a funciones de administración del sistema. Por ello las medidas van encaminadas a la estabilidad y robustez su sistema operativo. Además, es donde se configura y mantiene la seguridad del resto de la red.

Estas son las salvaguardas que se consideran:

[H.AC] Control acceso lógico, [H.IA] Identificación y autenticación, [SW.SC] Se aplican perfiles de seguridad: Sólo usuarios administradores deben tener acceso. Es donde se configuran los perfiles de seguridad y políticas de los usuarios. Es necesario revisar los servicios por defecto del sistema que no sean necesarios para deshabilitarlos y revisar configuraciones para reforzar la seguridad en caso de que las configuraciones por defecto no sean seguras.

[SW] Protección de las Aplicaciones Informáticas, [H.tools.VA] Herramientas análisis vulnerabilidades, [H.tools.AV] Herramienta contra código dañino: Actualmente está protegido por software antivirus, no obstante, se debería complementar con otras herramientas de prevención, análisis de vulnerabilidades, detección de intrusos y SIEM. Se debería realizar un test de penetración (Pentest).

[SW.A] Copias de seguridad: Es necesario una política específica de copias para el sistema servidor que, en caso de un desastre, garantice su recuperación a partir del backup con todas las funciones, servicios y elementos de configuración que se mantienen o proporcionan por este sistema.

[SW.CM] Cambios (actualizaciones y mantenimiento): Por política debe contemplarse que el sistema operativo esté actualizado con las últimas actualizaciones de seguridad o de corrección de errores, lo cual mejora su estabilidad.

[D.C] Cifrado información: Se aplicará cifrado sobre la información sensible. Se debe integrar con la solución de cifrado que se adquiera.

[H.tools.LA] Herramienta análisis logs, [H.AU] Registro y auditoría: La herramienta de análisis de logs, ayudará en la monitorización de los eventos registrados. Se debe configurar el log con la auditoría suficiente requerida.

Plan de contingencia: Es necesario contemplar un plan de recuperación del sistema con todas las funciones y servicios.

Manuales y Procedimientos: Es necesario documentar por parte de la empresa que realiza la administración de sistemas, la documentación de todos los procedimientos, manuales sobre las distintas tareas y configuraciones.

Con la implementación de estas salvaguardas, los niveles de riesgo del sistema servidor quedarían reducidos a niveles aceptables.

7.3.7. Activo SW009-Sistema operativo Cliente

En el análisis de riesgos de este activo relativo al sistema operativo de los puestos cliente, los riesgos que se detectan son de nivel Medio y están **relacionados con las amenazas:** [E.8] *Difusión de software dañino*, [E.20] *Vulnerabilidades de los programas (software)*, [A.5]

Suplantación de la identidad del usuario, [A.7] *Uso no previsto* y [A.11] *Acceso no autorizado*

Se considera las siguientes salvaguardas:

[SW] Protección de las Aplicaciones Informáticas, [H.tools.AV] Herramienta contra código dañino:

Todos los puestos deben tener software antivirus actualizado y operativo para conexión a la red. Este aspecto debe quedar contemplado en la política de seguridad.

[SW.A] Copias seguridad: Realmente esta salvaguarda aplicaría a los portátiles, pues por política los puestos de red deben trabajar con los datos en recursos de red y el ERP se utiliza desde el servidor.

[H.AC] Ctrl acceso lógico, [H.IA] Identificación y autenticación, [SW.SC] Se aplican perfiles de seguridad: Los usuarios se configurarán en grupos de red y perfiles. Según el perfil determinado para cada usuario, pertenecerá a un grupo distinto. Cuando un usuario conecte, se configurará automáticamente el sistema cliente, habilitando los recursos de red y aplicaciones según su perfil de usuario. Es necesario revisar los perfiles de seguridad de los usuarios de red y alinearlos con sus funciones/departamento.

[SW.CM] Cambios (actualizaciones y mantenimiento): Debe quedar regulado por política la obligación de mantener actualizado el sistema operativo con las últimas actualizaciones de seguridad.

[H.tools.LA] Herramienta análisis logs: La utilización de herramientas de análisis de logs ayudará en el análisis, monitorización y alerta de incidencias o errores producidos en los puestos.

[H.AU] Registro y auditoría: El nivel de auditoria y registro de eventos debe permitir la traza de acciones con el nivel de auditoría necesario.

Política de seguridad: La política de seguridad debe contemplar las normas de uso, configuración y protección de los puestos.

Plan de contingencia: Se puede estudiar la posibilidad de mantener imágenes (snapshots) de cada puesto con el software base, para en caso de un incidente, ante la infección o degradación de este, poder restaurarlo o regenerarlo a partir de la imagen.

Aunque el nivel de riesgo para este activo, no obstante, se considera tratarlo por la importancia que tiene en el funcionamiento de los puestos clientes y el resto de las aplicaciones que se ejecutan. Con la aplicación de estas salvaguardas, los riesgos quedarían mitigados o reducidos a niveles Bajos/Muy Bajos.

7.4. [HW] Equipamiento informático (hardware) (tratamiento del riesgo)

En este ámbito de activos hardware, se pueden distinguir cinco grupos diferentes: Servidor, Puestos cliente, Impresoras y hardware de Red.

7.4.1. Activo HW001-Servidor

Los **riesgos Altos o Muy Altos** afectan a las dimensiones de disponibilidad/confidencialidad y están **relacionados con las siguientes amenazas**: *[N] Desastres naturales([N.*], [N.1]Fuego,N.2]-Agua), [I.1] Fuego, [I.2] Agua, [I.*] Desastres industriales, [I.3] Contaminación mecánica, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico, [E.23] Errores de mantenimiento/actualización de equipos (hardware), [E.25] Pérdidas de equipos, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, A.24] Denegación de servicio, [A.25] Robo y [A.26] Ataque destructivo*

Por ello las medidas que se pueden adoptar van encaminadas a su disponibilidad y al aseguramiento de la seguridad de acceso a éste y la información que contiene.

Las salvaguardas que se contemplan son:

[L.AC] Control acceso físico, Ubicación correcta, Mantenimiento Extintores: El acceso al edificio y movimiento dentro de éste por parte del personal y visitas, hace que el servidor pueda estar alcance de cualquier persona que vaya a la planta del departamento técnico o gerencia. La ubicación actual del servidor no es adecuada, pues se encuentra en una sala abierta con otros usos (microondas, material oficina y archivo, ...) sin ninguna medida de seguridad física. La principal salvaguarda para proteger al servidor físicamente será el cambio de ubicación junto con el resto de los elementos críticos a la sala *[L002-Cuarto de comunicaciones]*, una vez este activo haya sido reconvertido como una sala acondicionada para uso exclusivo de CPD (como se indica más adelante), con las condiciones de seguridad y ambientales oportunas (sistema de acceso restringido, sistema antiincendios, climatización, ...).

[D.A] Copias de seguridad de los datos (backup), [D.C] Cifrado información: La protección de la confidencialidad de la información que guarda el servidor ante pérdidas, robo o fugas de información vendrá proporcionada por salvaguardas este tipo. Para ello es necesario adaptar la política de copias de seguridad según el nivel de criticidad de cada tipo de información, unido a medidas de cifrado de la información más sensible.

(AUX.power) Suministro eléctrico: Es necesario destinar un SAI exclusivo para el servidor para reducir el riesgo sobre la disponibilidad del servidor ante cortes de suministro eléctrico.

[HW.A] Aseguramiento de la disponibilidad: Debido a la criticidad de las funciones que concentra el servidor (repositorio principal de información sensible, servidor del ERP,

controla de dominio del Active Directory que gestiona la seguridad y recursos de la red, ...), es urgente establecer un mecanismo de alta disponibilidad como contingencia ante un desastre. La opción que se propone a corto plazo es la instalación de un servidor en *cluster*, aunque hay alguna otra alternativa a medio plazo que pasa por mover alguna función/servicio crítico a otra ubicación y repartir el riesgo.

[H.AC] Control acceso lógico: Evaluación de la instalación de una solución NAC (Network Access Control) a medio plazo, para controlar y gestionar mediante políticas el acceso de los distintos dispositivos y usuarios a la red.

[H.tools.AV] Herramienta contra código dañino, [S.www] Protección de servicios y aplicaciones web: Como medidas preventivas se plantea junto con el antivirus ya existente, la instalación de herramientas de análisis de vulnerabilidades y de un proxy para filtrar los accesos a internet por parte de los usuarios.

[HW.CM] Cambios (actualizaciones y mantenimiento): Política para mantener actualizado el sistema con los últimos drivers y actualizaciones de seguridad. Chequeos periódicos de los elementos hardware.

[H.AU] Registro y auditoría, [H.tools.LA] Herramienta para análisis de logs y monitorización: Se plantea la utilización de una herramienta de gestión de logs y eventos. También es necesario definir el nivel de eventos de log y auditoría requerido por la política de seguridad, sobre los accesos, los distintos recursos del servidor y sobre el acceso a la información, así como base de información de registro para analizar incidentes, monitorizar el sistema o como una de las fuentes de información de eventos de seguridad para un SIEM (si se instala en un futuro).

Política de Seguridad Corporativa, Registro actuaciones: Es necesario implementar la organización física de la información y permisos, creando las distintas directivas y permisos de acceso a la información según el nivel de seguridad y propietario definido; adaptando también la política de copias de seguridad y el plan de contingencia.

Plan de contingencia: Una vez implantadas las salvaguardas, es necesario definir el plan de contingencia y recuperación del servidor.

Con la aplicación de estas salvaguardas todos los riesgos quedarían mitigados o reducidos a niveles aceptables, excepto los riesgos residuales de disponibilidad frente a las amenazas **[I.1] Fuego y [I.2] Agua**; pues aun habiendo implementado alta disponibilidad con un servidor en *Cluster*, ante un fuego o inundación pueden verse afectados los dos nodos, pues no se ha planteado que se ubiquen geográficamente en zonas distintas. Este riesgo se puede asumir dada la baja probabilidad de estas amenazas y el coste que supondría la opción de un *Cluster* geográfico.

No obstante, se plantea otra forma de disminuir este riesgo mediante la disminución de la criticidad del servidor. Para ello se puede estudiar llevar al Cloud determinados servicios que

lo hacen crítico como el ERP o la disponibilidad de determinada información. De esta forma el valor del activo sería menor, lo cual supondría un impacto menor ante cualquier amenaza, y en consecuencia quedaría reducido el riesgo.

Esta salvaguarda será objeto de un plan específico para analizar las alternativas y mejor opción.

7.4.2. Activos HW002-Desktop, HW003-Workstation, HW004-Laptop

En este grupo de activos (*HW002-Desktop, HW003-Workstation, HW004-Laptop*), los riesgos son de nivel Alto o inferior, afectando a la disponibilidad en el caso de los puestos de sobremesa y a la confidencialidad en el caso de los portátiles.

Estarían relacionados con las siguientes amenazas:

- Puestos sobremesa (HW002-Desktop y HW003-Workstation): *[I.1] Fuego, [I.2] Agua, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico.*
- Portátiles HW004-Laptop: *[E.25] Pérdidas de equipos, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.25] Robo.*

Por ello las medidas que se pueden adoptar van encaminadas a su disponibilidad y a la confidencialidad de la información ante una pérdida.

Las salvaguardas que se contemplan son:

[L.AC] Control acceso físico: El control del acceso físico es importante. Regular por políticas la normativa en cuanto a las visitas, su recepción y acompañamiento por el edificio hasta la salida de éste. En el caso de los portátiles son más propensos al robo en las propias dependencias.

[D.C] Cifrado discos: Es necesario la utilización de una herramienta de cifrado de discos para el caso de los portátiles pues son dispositivos que tienen mayor riesgo de pérdida/robo que, al no estar conectados siempre a la red corporativa, son susceptibles de guardar información en local. Con esta salvaguarda se reducirían los riesgos provocados por la pérdida de los portátiles.

[D.A] Copias de seguridad de los datos (backup): Debería hacerse backup de la información, pues al no utilizarse siempre conectados a la red corporativa pueden contener información en local.

Esta salvaguarda aplica a los portátiles dado que el resto de los puestos guardan la información en los recursos de red.

Protección física: Cerradura de seguridad para portátil con cable de seguridad para asegurar los portátiles a la mesa de trabajo.

(AUX.power) Suministro eléctrico: Puestos de sobremesa conectados a SAI. Portátiles no es necesario.

[H.tools.AV] Herramienta contra código dañino, [HW.CM] Cambios (actualizaciones y mantenimiento), [S.www] Protección de servicios y aplicaciones web: Todas estas medidas de protección van encaminadas a hacer frente a amenazas de errores, software dañino, o uso de los dispositivos, como en el caso de la utilización de un proxy. Aplican a todos los puestos.

[H.AC] Control acceso lógico: El control de acceso mediante contraseñas fuertes y seguras, políticas de usuarios/contraseñas. Utilización de certificados en redes wifis reduce los riesgos de accesos no autorizados. La utilización de un NAC, permitiría aplicar políticas a portátiles que se conectarán a la red y no cumpliesen determinadas condiciones (antivirus, nivel de parches, ...).

Política de Seguridad: La política sobre el uso de los equipos deberá contemplar las normas, directrices, instrucciones técnicas, guías de actuación ante incidentes. Por ejemplo, aspectos como política de actualización de equipos, guardar toda la información en recursos de red, hacer backup y/o sincronización de la información de los portátiles a la red cuando estén conectados.

También se podrían considerar otro tipo de sincronizaciones mediante el *Cloud*.

Ubicación correcta: Evita averías relacionadas con condiciones ambientales, suciedad, ...

Registro actuaciones: Es importante mantener un registro de actuaciones e incidencias, como medida de análisis de incidentes y plan de mejora. Y que así esté especificado en la política de seguridad.

Mantenimiento Extintores: Para reducir consecuencias ante un fuego.

Con la implementación de estas salvaguardas quedarán todos los riesgos mitigados o reducidos hasta niveles bajos. Sólo habría dos riesgos residuales aceptables de nivel Medio para las amenazas *[N] Desastres naturales([N.*],[I.1]-Fuego,[I.2]-Agua)* y *[I.1] Fuego*. Como contingencia se propone guardar algún equipo de los últimos retirados para utilizarlo en caso de avería de otro o necesidad.

7.4.3. Activo HW005-Unidad de Backup

En este activo HW005-Unidad de Backup, los riesgos son de nivel Alto o inferior, relacionados con la pérdida/robo o avería de la unidad y la confidencialidad de la

información en los soportes, **amenazas**: [I.1] Fuego, [I.2] Agua, [I.5] Avería de origen físico o lógico, [I.6] Corte de suministro eléctrico, [A.25] Robo

Para reducir todos los riesgos a niveles aceptables, se contemplan las siguientes **salvaguardas**:

Plan de contingencia: Disponibilidad de una segunda unidad de backup, configuración de las copias de seguridad contra un servicio en *Cloud* o combinación de ambas.

[D.C] Cifrado información de la información contenida en los soportes.

(AUX.power) Suministro eléctrico: Disponibilidad ante un corte de suministro eléctrico.

Mantenimiento Extintores: Para reducir consecuencias ante un fuego.

7.4.4. Activos HW006-Impresora, HW007-Plotter

Estos activos no suponen riesgos reseñables que tratar pues sus riesgos son aceptables. Su disponibilidad está garantizada pues hay varias en red. En cualquier caso, como el resto de los elementos, su uso y normas quedarán contempladas dentro de la normativa de la política de seguridad.

7.4.5. Activos HW008-Router, HW009-Switch

En este grupo de activos (*HW008-Router, HW009-Switch*), los riesgos son de nivel Alto o inferior, afectando a la disponibilidad o confidencialidad. Estarían **relacionados con las siguientes amenazas**:

- *HW008-Router*: [I.1] Fuego, [I.2] Agua, [I.6] Corte de suministro eléctrico, [A.6] Abuso de privilegios de acceso, [A.11] Acceso no autorizado, [A.24] Denegación de servicio
- *HW009-Switch*: [I.1] Fuego, [I.2] Agua, [I.6] Corte de suministro eléctrico, [A.11] Acceso no autorizado

Por ello las medidas que se pueden adoptar van encaminadas a su disponibilidad y a la confidencialidad de la información que transita por ellos.

El *router* es un elemento importante pues además de ser la conexión con el exterior, también puede ser la puerta de entrada de múltiples amenazas; contiene un firewall y se sitúa en la primera línea de defensa. Su disponibilidad es cada vez más importante, no en vano hay medidas y salvaguardas que se han planteado basadas en servicios exteriores (en *Cloud*), etc. Aunque el uso para el negocio no es crucial.

El *switch* es otro elemento con menos “*inteligencia*”, aunque más importante si cabe. Su indisponibilidad dejaría si interconexión a los ordenadores y sin red LAN a la empresa.

Además, es un elemento a través del cual se puede tener acceso directo al tráfico que circula por la red interna.

Las salvaguardas que se contemplan son:

[L.AC] Control acceso físico: El control del acceso físico es importante. Regular por políticas la normativa en cuanto a las visitas, su recepción y acompañamiento por el edificio hasta la salida de este. En el caso del *router* y *switch* es transcendental no tener acceso físico para la seguridad pues conectar un dispositivo directamente, puede dar lugar a múltiples amenazas, desde acceso directo a la red hasta visualización del tráfico que circula por ésta.

[SW.A] Copias de seguridad (backup): En el caso del *router*, es necesario tener guardada la configuración como contingencia formando parte de la política de seguridad. Se trata de información que puede ser sensible como reglas del firewall, direcciones MAC de dispositivos autorizados, credenciales de acceso a la red Wifi, configuraciones, ...

(AUX.power) Suministro eléctrico: Un corte de suministro en router y switch, causa indisponibilidad. En el caso del switch, provocaría una caída de la red LAN.

(H.IA) Identificación y autenticación: Es importante asegurar que el router está protegido con usuario y password que cumplan la política de seguridad.

Ubicación correcta: Esta salvaguarda referida a la accesibilidad física al *switch/router* y a las condiciones de temperatura, humedad, etc., quedará implementada mediante un plan de seguridad propuesto relacionado con el activo *[L002-Cuarto de comunicaciones]*, cuyo objetivo es reconvertir este activo en una sala acondicionada para uso exclusivo de CPD (como se indica más adelante), con las condiciones de seguridad y ambientales oportunas (sistema de acceso restringido, sistema antiincendios, climatización, ...).

Política de seguridad: La Política de Seguridad debe contemplar toda la normativa y políticas a implementar respecto a estos dispositivos, medidas de seguridad, configuraciones y sus backups, uso y manipulación, ubicación, etc.

Plan de contingencia: Dentro del plan de contingencia, la principal salvaguarda que se considera es la reposición de los dispositivos para hacer frente a amenazas relacionadas con averías o desastres que causen indisponibilidad. En el caso del *router*, se debe prever en el contrato con la empresa de telefonía, que esté contemplada su reposición con un SLA suficiente. En el caso del *switch*, se puede tener uno en reserva o redundado ante cualquier incidencia. La política debe garantizar las instrucciones para llevar a cabo el cambio.

Con la implementación de estas salvaguardas los riesgos se mitigan o reducen hasta niveles aceptables. En el caso del *router*, parte del riesgo quedaría compartido con la empresa que presta el servicio ADSL.

7.5. [COM] Redes de comunicaciones (tratamiento del riesgo)

En este ámbito de las redes y comunicaciones, se pueden distinguir dos grupos de riesgos que afectan a redes LAN/Wifi, líneas telefonía y ADSL/Fibra.

7.5.1. Activos COM002-Red local y COM004-Red Wifi

Los **riesgos más altos** afectan a las dimensiones de confidencialidad y disponibilidad y están **relacionados con las siguientes amenazas:** *[E.24] Caída del sistema por agotamiento de recursos, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.9] [Re-]encaminamiento de mensajes, [A.11] Acceso no autorizado, [A.24] Denegación de servicio*

Por ello las medidas que se pueden adoptar van encaminadas al reforzamiento de la seguridad de las redes (arquitectura y acceso), uso de las redes, prevención y alerta. **Las salvaguardas que se contemplan son:**

[COM.DS] Segregación de las redes en dominios: La división de la red en una parte interna y otra externa separada por un firewall interior, a la vez que la creación de dos wifis una para invitados (sin acceso a la red interna) y otra conectada a la red LAN interior, reduce una mayoría de los riesgos.

[H.AC] Control de acceso lógico, [L.AC] Control de los accesos físicos, [COM.SC] Se aplican perfiles de seguridad: El acceso con mecanismos de control de la seguridad de acceso y perfilado juntamente con el uso de certificados y claves en las redes inalámbricas, reducen los riesgos relacionados con la suplantación, abuso de privilegios, acceso no autorizado y sus posibles consecuencias como ataques de denegación de servicios (DoS), ...

[H.tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión, [H.tools.VA] Herramienta de análisis de vulnerabilidades: La finalidad de estas medidas es la detección y prevención de amenazas.

La instalación de un sistema de detección de intrusos (IDS) y un SIEM para gestión de los eventos y alertas de seguridad, permitirá analizar patrones, alertar y predecir ataques, no sólo de amenazas externas sino también de las internas (fuga de información, ...).

La implantación de un SIEM, los hay asequibles para empresas de cualquier tamaño, es una buena medida para anticiparse a posibles ataques (tanto externos como internos). Se puede prever un ataque gracias a la información y eventos que va registrando en el sistema, siendo capaz de emitir alertas, permitiendo así su análisis antes de que ocurra un incidente.

También se podría evaluar la instalación de un IDS, herramienta que se integra con el firewall y es un buen complemento, pues añade inteligencia (análisis del contenido de firmas de ataques conocidos y comportamientos sospechosos), a la capacidad de bloqueo del firewall.

[COM.CM] Cambios (actualizaciones y mantenimiento): Las actualizaciones y mantenimiento de los distintos componentes de red, es fundamental para mitigar las vulnerabilidades que hayan sido corregidas en los firmwares por parte de los fabricantes. Así como el cambio de aquellos componentes obsoletos y amortizados, que ya no se siguen actualizando o no son válidos para hacer frente a nuevas amenazas.

[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados: Se establecerán directrices para que el tráfico en la red viaje más protegido, por ejemplo, mediante la utilización de protocolos seguros (*SSL, WAP2, SFTP, HTTPS*).

[H.AU] Registro y auditoría: El registro de conexiones también es una salvaguarda para análisis de los incidentes y para determinar la afectación y causa tras un ataque, garantizar el no repudio, El registro de incidentes siempre ayuda a la mejora en las medidas y toma de decisiones.

Política de Seguridad corporativa: La política de seguridad es otra de las salvaguardas que reduce el riesgo que puede producir un mal uso del sistema, como por ejemplo descargas ilegales, acceso a dominios no recomendados, uso personal de los recursos del sistema, envío de archivos adjuntos con información sensible hacia el exterior por correo ...

7.5.2. Activos COM001-Servicio de Telefonía y COM003-ADSL

Los riesgos altos están **relacionados con las siguientes amenazas:** *[I.8] Fallo de servicios de comunicaciones, [E.9] Errores de [re-]encaminamiento, [E.24] Caída del sistema por agotamiento de recursos, [A.5] Suplantación de la identidad del usuario, [A.6] Abuso de privilegios de acceso, [A.7] Uso no previsto, [A.9] [Re-]encaminamiento de mensajes, [A.11] Acceso no autorizado, [A.12] Análisis de tráfico, [A.14] Interceptación de información (escucha), [A.24] Denegación de servicio.*

Como salvaguardas se plantean:

[H.AU] Registro y auditoría: Para control de las llamadas.

Política de Seguridad corporativa: Para establecer las normas de uso correctas.

[H.AC] Control de acceso lógico: La configuración y control de acceso mediante usuario a los terminales.

[L.AC] Control de los accesos físicos: El control de acceso físico evita que se pueda tener acceso a terminales (realización llamadas, registro llamadas, ...) a personal que no esté autorizado.

Los riesgos de **nivel Alto** se ven reducidos a niveles aceptables, con la aplicación de estas salvaguardas.

Los riesgos de **nivel Medio**, (*[E.9] Errores de [re-]encaminamiento, [A.9] [Re-]encaminamiento de mensajes, [A.12] Análisis de tráfico, [A.14] Interceptación de información (escucha)*), si bien son aceptables, también quedan compartidos con la empresa telefónica proveedora del servicio Telefónico y ADSL.

7.6. [Media] Soportes de información (tratamiento del riesgo)

7.6.1. Activos [MEDIA001]-Memorias USB y [MEDIA002]-Discos USB

En este ámbito, para todos los activos **[Media] Soportes de información** se estiman riesgos de nivel Alto/Muy Alto relacionados sobre todo con la dimensión de **confidencialidad**.

Las amenazas que los producen son:

[E.1] Errores de los usuarios, [E.2] Errores del administrador, [E.19] Fugas de información, [E.25] Pérdidas de equipos, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.19] Divulgación de información, [A.23] Manipulación de los equipos, [A.25] Robo

Las salvaguardas que se contemplan son:

[D.A] Copias de seguridad de los datos: Los soportes removibles no deben ser utilizados para guardar información importante que no esté en otro lugar. Ante la pérdida del soporte, si los datos que contienen están en un backup o en su ubicación de red asignada, el daño de perder los datos será recuperable. Esta salvaguarda nos protege de la disponibilidad e integridad de los datos en estos soportes ante una pérdida/robo y errores o modificaciones de los datos (ya sean intencionadas o no).

[H.AC] Control de acceso lógico, [L.AC] Control de los accesos físicos: Con el control de acceso tanto lógico como físico, se reduce el riesgo de acceso a los dispositivos, o a copiar información para la que no se tenga autorización.

[D.C] Cifrado de la información: Sin duda esta es quizás la salvaguarda más eficaz para estos activos, pues mitiga prácticamente el riesgo de confidencialidad ante una pérdida, robo o uso indebido del soporte. Si además la información reside en una copia, el riesgo de perderla es menor.

Políticas y Normas de uso dispositivos: Dentro de la política general de seguridad de la empresa deben existir directrices y normas relativas al uso de los soportes removibles. Por ejemplo, utilizarlos siempre para guardar información de forma temporal, que estén cifrados, normas sobre un uso adecuado, normas antivirus, ...

[PS.AT] Formación y concienciación: En este ámbito también es de aplicación la formación y concienciación en materia de seguridad, ayudando a reducir riesgos detectados y a hacer

frente a determinadas amenazas. Por ejemplo, respecto al riesgo que entraña la utilización de dispositivos removibles como vector de ataque al sistema.

Adicionalmente, también se pueden considerar otras medidas como el registro de incidencias de seguridad relacionadas con los soportes removibles.

Con la implementación de estas salvaguardas se estima que su efectividad en la frecuencia de las amenazas puede ser de hasta el 75%. En cuanto a la efectividad en la degradación causada a los activos, estaría entre el 25%-50%, excepto en el caso del cifrado de la información que sería del 100% sobre las amenazas que comprometan la confidencialidad.

7.7. [AUX] Equipamiento auxiliar (tratamiento del riesgo)

7.7.1. Activo AUX001-SAI

En este ámbito, para el activo **AUX001-SAI** se estiman riesgos de nivel Medio como máximo.

Las amenazas que los producen son: *[I.1] Fuego, [I.2] Agua, [I.5] Avería de origen físico o lógico, [I.7] Condiciones inadecuadas de temperatura o humedad, [A.25] Robo.*

Las salvaguardas que se contemplan son: *[L.AC] Control de los accesos físicos, [AUX.AC] Climatización, Mantenimiento/manipulación por personal/servicio técnico autorizado.*

7.8. [L] Instalaciones (tratamiento del riesgo)

7.8.1. Activo L001-Edificio empresa

Para el edificio de la empresa los riesgos son altos/muy altos y vienen provocados por las **amenazas:** *[E.15] Alteración accidental de la información, [E.18] Destrucción de información, [E.19] Fugas de información, [A.11] Acceso no autorizado, [A.15] Modificación deliberada de la información, [A.19] Divulgación de información, [A.27] Ocupación enemiga.*

Por un lado, el edificio alberga todos los activos de la empresa, lo que le suceda al edificio puede repercutir en los activos críticos. Por otro lado, otra causa de parte de estos riesgos es consecuencia del control de acceso físico. Por ejemplo, al edificio general se accede desde el área comercial y para ir a cualquier otro departamento en otras plantas (técnicos, gerencia, administración), hay veces que los clientes circulan de forma independiente hasta el sitio de trabajo de cada empleado que visitan, donde puede haber accesible diversa información. Tampoco existe un registro de acceso, motivo, persona visitada, horario, ...

Las salvaguardas que se contemplan en este ámbito son del tipo: *[L] Protección de las Instalaciones, [L.AC] Control de los accesos físicos, Política de Seguridad de la empresa,*

Registro incidencias de seguridad, y van encaminadas a reforzar el control de acceso y adecuar la normativa, así como reubicar ciertos elementos esenciales en espacios restringidos.

7.8.2. Activo L002-Cuarto de comunicaciones

Este activo se refiere a la sala donde residen actualmente los elementos físicos de la red y el SAI. Los riesgos altos o muy altos vienen **provocados por las amenazas:** [I.1] Fuego, [E.18] Destrucción de información, [E.19] Fugas de información, [A.7] Uso no previsto, [A.11] Acceso no autorizado, [A.19] Divulgación de información, [A.26] Ataque destructivo, [A.27] Ocupación enemiga

El nivel de riesgo es consecuencia principalmente de los elementos que alberga y de la ausencia de medidas de seguridad que impidan el paso, dado que es accesible por personal que no le compete sin ninguna medida de seguridad más allá de una puerta sin cerradura. Además, el uso es compartido para diversos propósitos (almacén, material de oficina, materia de limpieza, ...), lo cual aumenta la probabilidad de que se produzcan incidentes no intencionados, o que en el caso de daños intencionados esté todo más accesible.

En este ámbito **las salvaguardas contempladas son:** [L] Protección de las Instalaciones, [L.AC] Control de los accesos físicos, Registro incidencias de seguridad y Política de Seguridad de la empresa.

Con estas salvaguardas se proporcionará por una lado, protección y acceso restringido a determinados espacios con elementos sensibles. Por otro lado, es necesario contemplar en la política de seguridad de la empresa, normativa sobre el acceso y circulación de personal externo por las instalaciones (recepción de las visitas en la entrada, acompañamiento por las dependencias y durante la salida), acceso a zonas restringidas como el cuarto de comunicaciones, registro de visitas externas, así como manuales de uso de las instalaciones. Sería aconsejable reforzar con un sistema de cámaras de seguridad.

En el caso de los riesgos derivados de desastres naturales para los que no se establece una salvaguarda concreta, el riesgo se asume, al ser la probabilidad muy baja; se contratará un seguro acorde para compartir riesgo, seguro también para vandalismo o ataque destructivo.

El riesgo por la amenaza ocupación enemiga, se acepta ante la baja probabilidad y teniendo en cuenta las medidas existentes.

Adicionalmente, es imprescindible que en general todos los empleados se formen en materia de seguridad. Esta formación concienciaría sobre las amenazas, riesgos y prácticas no seguras las cuales pueden provocar fuga de información fortuita. Además de hacerles conocedores de la normativa en materia de seguridad sobre gestión de la información que deben cumplir. Esta iniciativa también ayudará a reducir riesgos detectados en este ámbito.

7.9. [P] Personal (tratamiento del riesgo)

En este ámbito, **para todos los activos** los riesgos altos y muy altos vienen provocados por las **amenazas:** *[E.19] Fugas de información, [A.30] Ingeniería social (picaresca), [E.28] Indisponibilidad del personal.*

Así pues, hay dos líneas de riesgos, el riesgo relacionado con la revelación de información a través de la intervención propia del personal, y el riesgo derivado de la no disponibilidad del personal.

Las **salvaguardas** consideradas para hacer frente a estas amenazas son: *[PS.AT] Formación y concienciación, Política de Seguridad de la Empresa, [PS.A] Aseguramiento de la disponibilidad, Elaboración procedimientos.*

Es imprescindible que en general todos los empleados se formen en materia de seguridad. Esta formación concienciaría sobre las amenazas, riesgos y prácticas no seguras las cuales pueden provocar fuga de información fortuita. Además de hacerles conocedores de la normativa en materia de seguridad sobre gestión de la información que deben cumplir.

En cuanto a la indisponibilidad del personal, se hace necesario que los procesos estén documentados mediante procedimientos y con instrucciones y guías de actuación ante diversas incidencias.

Planes de seguridad

A partir de las entrevistas realizadas en la empresa, la Dirección ha manifestado su deseo de aprovechar las nuevas posibilidades y herramientas que ofrecen hoy en día las TIC (Tecnologías de la Información y Comunicación), como palanca para diferenciarse dentro de su sector ofreciendo servicios más innovadores, formas de trabajo más adecuadas a la movilidad, trabajo deslocalizado, utilización de dispositivos móviles, etc.

No obstante, es consciente del desconocimiento de los nuevos riesgos que ello puede implicar y quiere hacerlo de forma ordenada sin asumir riesgos innecesarios o no evaluados.

Para ello están diseñando un plan estratégico a 3 años mediante el que definir su modelo de empresa a futuro. En este plan, una de las líneas estratégicas estaría compuesta por la transformación digital de la empresa. Abordar esta transformación digital requiere hacerlo de una forma ordenada y segura. Es por lo que uno de los objetivos estratégicos marcados es el desarrollo de Plan Director de Seguridad que refuerce y mejore el SGSI de la empresa, garantice que todos los riesgos son gestionados hasta un nivel aceptable, bajo el que se gobiernen y lleven a cabo todas las tareas en materia de seguridad de la empresa necesarias para ello.

La definición del presente Plan Director de Seguridad viene a dar respuesta a este objetivo.

Las líneas principales de actuación identificadas dentro del mismo serían las siguientes:

- Desarrollar e implementar la política de seguridad de la empresa.
- Plan de concienciación en materia de seguridad de la información, tanto para personal de los departamentos como para la Dirección.
- Documentación e implantación de un procedimiento para la gestión de incidentes de seguridad.
- Mejora de la seguridad de la red corporativa. Mejora de la infraestructura de red corporativa, segmentación e instalación de sistemas de prevención y control (IDS, SIEM, ...).
- Plan de contingencia y continuidad del negocio. Mejora de la capacidad de respuesta de la empresa frente a una contingencia.
- Plan de recuperación.
- Clasificación de la información en distintos niveles de seguridad (público, privado y confidencial). Este sistema debe contemplar aspectos como el etiquetado, acceso, destrucción de la información, uso de cifrado, etc.
- Definición e implantación de una nueva política de copias de seguridad adecuada, basada en el nivel de confidencialidad y criticidad de la información corporativa, que contemple la realización de restauraciones periódicas
- Regulación de los servicios de Tecnología de la Información y Comunicaciones prestados por terceros: revisar y homogeneizar los contratos establecidos con los proveedores TIC externos a fin de garantizar que estos son adecuados a las necesidades de la organización

Este Plan Director de Seguridad se organizará en 3 fases o planes anuales con los siguientes objetivos.

Plan Anual primer año (Plan objetivo TFM):

- Abordar planes prioritarios enfocados a tratar riesgos críticos detectados.
- Implementación de los planes orientados al robustecimiento de la seguridad estructural o básica (redes, copias, ...).
- Concienciación y formación en seguridad de la información para preparar la organización.
- Elaboración de políticas de seguridad.
- Clasificación de la información.
- Sistemas de prevención y control de la seguridad (detección de intrusos, SIEM, ...).

Plan Anual segundo año:

- Plan de contingencia y continuidad de negocio.

- Plan de recuperación.
- Planes menos prioritarios que, bien por presupuesto o capacidad no se han podido abordar en el año anterior.
- Regulación de los servicios de Tecnología de la Información y Comunicaciones prestados por terceros.
- Planes orientados a preparar la seguridad futura sobre la que asentar otros servicios y formas de trabajo en la organización (dispositivos móviles, deslocalización del trabajo, ...).

Plan Anual tercer año:

- Planes menos prioritarios que o bien por presupuesto o capacidad no se han podido abordar en el año anterior.
- Gestión documental.

A continuación, como parte del Plan Director de Seguridad, se desarrollan los distintos planes de seguridad dirigidos a la reducción del riesgo a un nivel aceptable en base al análisis de riesgos realizado, agrupando tareas de forma homogénea y eficiente en cada plan.

Para describir cada plan se utilizarán las siguientes fichas con las que se pretende que la Dirección tenga la propuesta resumen con los objetivos, tareas a realizar y forma de abordarlas, así como que les sirva para la toma de decisiones.

8.1. Plan [SEC20-SEG.PRO01] Protección de cifrado

Tabla 178. Plan SEC20-SEG.PRO01 - Protección de cifrado

Nombre:	Protección de cifrado	Grupo:	[SecInfo]
			Planificación 2020
Código:	SEC20-SEG.PRO01	Prioridad	[1T] [2T] [3T] [4T]
Responsable: Responsable TI			
Objetivos/Hitos			
<ul style="list-style-type: none"> - Adquisición e instalación herramienta de cifrado que dé cobertura a las necesidades detectadas para asegurar la confidencialidad de la información en soportes (removibles, discos, copias de seguridad, portátiles y móviles). - Cifrado de soportes removibles (memorias y discos USB). - Adaptación la política de uso de los soportes removibles y portátiles. 			
Activos afectados			
MED001 – Memorias, MED002 - Discos removibles USB HW004-Laptop, HW005-Unidad Backup [D] Datos / Información HW001-Servidor, HW002-Desktop, HW003-Workstation			
Salvaguardas			
[MP.IC] Protección criptográfica del contenido [D.C] Cifrado de la información			
Descripción			
<p>Este plan tiene como objetivo prioritario mitigar el riesgo de confidencialidad sobre la información almacenada en los dispositivos removibles. Para ello es necesario la instalación de una herramienta de cifrado de los dispositivos removibles, portátiles, backup y discos para reducir el riesgo a niveles aceptables ante la pérdida o robo de éstos.</p> <p>Como parte del plan es preciso estudiar la adquisición de la solución de cifrado. Se tendrá en cuenta que sea válida para atender el resto de las necesidades de cifrado detectadas (copias, información sensible), para conforme el resto de los planes se desarrollen, estar en disposición de utilizarla.</p> <p><i>Ejemplo:</i> cuando se lleve a cabo el plan de gestión de la información, se utilizará la solución de cifrado adquirida.</p> <p>Durante el desarrollo de este plan se cifrarán los soportes removibles por ser uno de los riesgos altos detectados. Se podría abordar de inmediato al no tener dependencias ni afectar a otros planes.</p>			
Coste			
Estudio y evaluación de soluciones de mercado válidas: 1 semana de empresa servicios TI Instalación y configuración: 1 semana de empresa servicios TI El coste de adquisición puede variar dependiendo de la solución: Un dispositivo USB con cifrado puede costar unos 100€ dependiendo de la capacidad. Una licencia de Windows 10 Pro, unos 279€ Un software de cifrado de datos para estas necesidades los hay por menos 100€.			
Tareas			
<ul style="list-style-type: none"> - Análisis de mercado y evaluación de soluciones: <ul style="list-style-type: none"> o Herramienta de cifrado que soporte diferentes dispositivos y sea compatible con la copia de seguridad. o Unidades USB con encriptación hardware, (ej. Ironkey de Kington) o Opciones del SO ej. BitLocker para Windows 10 Pro) - Compra unidades cifradas USB (si procede). - Instalación y cifrado de todos los dispositivos removibles. - Instalación y cifrado de los portátiles. 			
Controles			
<ul style="list-style-type: none"> - Control periódico del cifrado en las unidades instaladas. - Registro de incidentes de seguridad que permita controlar la frecuencia de estos incidentes y eficacia de esta medida. 			

<ul style="list-style-type: none"> - Análisis de mercado y evaluación de soluciones: <ul style="list-style-type: none"> o Herramienta de cifrado que soporte diferentes dispositivos y sea compatible con la copia de seguridad. o Unidades USB con encriptación hardware, (ej. Ironkey de Kington) o Opciones del SO ej. BitLocker para Windows 10 Pro) - Compra unidades cifradas USB (si procede). - Instalación y cifrado de todos los dispositivos removibles. - Instalación y cifrado de los portátiles.
<ul style="list-style-type: none"> - Control periódico del cifrado en las unidades instaladas. - Registro de incidentes de seguridad que permita controlar la frecuencia de estos incidentes y eficacia de esta medida.

8.2. Plan [SEC20-DOC.PR002] Política de Seguridad Corporativa

Tabla 179. Plan SEC20-DOC.PR002 - Política de Seguridad Corporativa

Nombre:	Política de Seguridad Corporativa	Grupo:	[Políticas]
Código:	SEC20-DOC_PR002	Prioridad	Planiificación 2020 [1T] [2T] [3T] [4T]
Responsable:	Responsable Seguridad	1	
Objetivos/Hitos			
- Creación y formalización de las Políticas de Seguridad.			
Activos afectados			
En general todos los activos del sistema de información tienen asociadas políticas o procedimientos. Dependiendo del tipo de activo, tendrán políticas diferentes o específicas que le afecten para su cometido (backup, gestión de las claves, uso aplicaciones, credenciales de acceso, etc.).			
<p>I001-Fichero Clientes, D001-Expediente Cliente, D002-Datos acceso Servidor, D003-Datos acceso Usuarios, D004-Backup Servidor, SW005-Sistema de backup, HW005-Unidad Backup, D005-Fichero log, D006-Ficheros configuraciones, K001-Certificados FMNT, SW003-Cliente de correo, SW004-Antivirus, SW006-Navegador web, SW007-Portal web, SW008-Sistema operativo Servidor, SW009-Sistema operativo cliente, HW001-Servidor, HW002-Desktop, HW003-Workstation, HW004-Laptop, HW006-Impresora, HW007-Plotter, HW008-Router, HW009-Switch, COM002-Red local, COM001-Telefonía, COM003-ADSL/Fibra, COM004-Red wifi, [MEDIA001]-Memorias USB, [MEDIA002]-Discos USB, AUX001SAI, L001-Edificio empresa, L002-Cuarto de comunicaciones, P001-Personal interno (Gerencia), P002-Personal interno (Responsables Área) P003-Resto personal interno, P004-Personal externo</p>			
Salvaguardas			
Descripción			
Creación de la Política de Seguridad de la empresa: Documento global en el que se recogen los objetivos de seguridad, se definen controles (en base al análisis de riesgos realizado) y se establecen directrices básicas acordes tanto a los requisitos del negocio como a la legislación y normativa vigente.			
Creación de las políticas, procedimientos y guías técnicas en materia de seguridad de la empresa, pues no existen. Actualmente existen "normas" de actuación no escritas, que deberían estar formalizadas como procedimientos y ser parte de la política de seguridad interna. Adicionalmente, es necesario contemplar políticas que permitan cumplir los nuevos requerimientos regulatorios y marco de seguridad.			

<p>Una vez definidas las políticas, procedimientos e instrucciones, es necesario distribuir y concienciar a toda la empresa.</p> <p>Esta iniciativa de divulgación se abordará durante el programa SEC20-PRG003 conforme se avance en este programa y se vayan librando políticas.</p>
Coste
<p>1 especialista en la tarea, por parte de la empresa de servicios TI, durante 5 meses, para la elaboración de las políticas y documentación de soporte, la revisión junto al Responsable de Seguridad, más la difusión y explicación al resto de la empresa.</p> <p>20% durante 4 meses, dedicación Responsable de Seguridad para revisión de la documentación.</p>

Tareas
<ul style="list-style-type: none"> - Creación de la Política de seguridad de la empresa. - Definir proceso de revisión, actualización y aprobación. - Elaboración de las diversas políticas, procedimientos y guías, como ejemplo:

<p>Políticas</p> <ul style="list-style-type: none"> o Política de seguridad de la empresa: Objetivos de seguridad. o Política de cumplimiento de RGPD: Documentación de seguridad y manuales asociados para el cumplimiento con la normativa RGPD. o Política de copias de seguridad: Política para la realización de los backups. o Política de uso de Internet y correo electrónico: Normas y reglas sobre el uso. o Política de gestión de contraseñas: medidas de seguridad de las contraseñas (longitud, caracteres, caducidad, repetibilidad, almacenamiento, ...). o Política de gestión de usuarios, grupos y perfiles, permisos, ... o Política de antivirus: Gestión de antivirus, actualización, ... o Política de gestión de claves: Claves de cifrado, certificados, ... o Política de actualización de software. o Código de uso aceptable: Normativa general de seguridad a cumplir por todos los empleados. o Política de acceso de personal externo. o Política de respuesta ante incidentes de seguridad.
<p>Procedimientos</p> <ul style="list-style-type: none"> o Procedimientos de copias de seguridad: cómo hacer las copias. o Procedimiento de altas/bajas de usuarios: cómo gestionar los usuarios. o Procedimiento de cifrado de la información: criterios de cuándo y cómo cifrar la información. o Procedimiento de usuarios administradores: detalle de la gestión de los usuarios administradores. o Procedimiento de actuación ante la pérdida de un equipo: Pasos a realizar ante la pérdida de un equipo con información sensible. o Procedimiento de registro de incidente: detalle de información sobre el incidente y su resolución (fecha y hora de aparición, tipología y gravedad, recursos afectados, posibles orígenes, estado actual del incidente, acciones realizadas para solventarlo y quienes las ejecutaron, fecha y hora de resolución y cierre del incidente).

<p>Guías de instrucciones técnicas</p> <ul style="list-style-type: none"> o Guía de aseguración de aplicaciones (navegador, correo, ...) o Guía de aseguración de red o Guía de configuración del correo
Controles
<ul style="list-style-type: none"> - Checklist de políticas, procedimientos y guías a implementar para dar cobertura a todas las áreas y procesos. - Registro y revisión de incidentes de seguridad que permita mejorar las políticas, procedimientos y guías existentes, o la creación de nuevas donde se requiera. - Auditoría de cumplimiento de políticas. - Auditoría de vulnerabilidades.

8.3. Plan [SEC20-DOC.PR003] Formación y concienciación

Tabla 180. Plan SEC20-DOC PR003 - Formación y concienciación

Nombre:	Formación y concienciación	Grupo:	[Form]
Código:	SEC20-DOC_PR003	Prioridad	Planificación 2020
Responsable:	Responsable TI	2	[1T] [2T] [3T] [4T]
Objetivos/Hitos			
- Formación y concienciación del personal sobre riesgos y seguridad.			
Activos afectados			
P001-Personal interno (Gerencia), P002-Personal interno (Responsables Área) P003-Resto personal interno			
Salvaguardas			
[PS] Gestión del Personal [PS.AT] Formación y concienciación			
Descripción			
<p>Una de las brechas y vectores de ataque dentro de la seguridad de la información, se plantea en el personal interno de la empresa. Errores no intencionados, malas prácticas, ingeniería social, desconocimiento de amenazas y políticas de seguridad.</p> <p>Parte de los riesgos pueden ser limitados por políticas o medidas específicas, aunque otra buena parte puede abordarse desde el ámbito de la concienciación y la formación del personal.</p> <p>El planteamiento es establecer una formación continua sobre distintas materias dentro del ámbito de la seguridad de la información para dar cobertura a los distintos aspectos.</p> <p>Dentro del programa de concienciación y formación se plantean distintas iniciativas enfocadas a disminuir el riesgo en este punto:</p> <ul style="list-style-type: none"> - Kit de concienciación del INCIBE. [20] Se trata de una iniciativa gratuita para ayudar a las empresas llevar a cabo la tarea de concienciación en materia de seguridad y que proporciona los materiales necesarios, incluso un manual para implantarlo que incluye: cómo montar la simulación de un ataque dirigido inicial para concienciar al personal de la empresa de la necesidad de la seguridad, los trípticos y posters a poner en la empresa, proceso formativo, consejos de seguridad mensuales, ataque dirigido recordatorio, videos, píldoras, test de autoevaluación y encuestas de valoración. Está planificado para desarrollarlo durante 9 meses, con una dedicación parcial entre 1-3 días por mes, en los que o bien se lanza un proceso, o se realiza una píldora, ... - Formación específica sobre nueva normativa RGPD para todos los empleados. La puede impartir la empresa a la que se les tienen contratados los servicios TI y puede ser inicialmente basada en la guía “<i>Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario</i>” de la colección “<i>Protege tu empresa</i>” del INCIBE. [24] 			
<ul style="list-style-type: none"> - Divulgar Políticas de Seguridad Definidas, conforme vaya avanzando el programa SEC20-PRG002-Políticas de Seguridad, mediante formación y explicación sobre las distintas políticas que se formalicen. - Charlas de seguridad periódicas o píldoras informando sobre aspectos específicos de seguridad. En este sentido son muy interesantes, las Guías de seguridad del INCIBE de la colección “<i>Protege tu empresa</i>”. Es una temática interesante tanto para el empresario como para los empleados, cada uno desde su rol. 			
Coste			
<ul style="list-style-type: none"> - Kit de concienciación INCIBE (Gratis). Dedicación parcial durante 10 días por empleado a lo largo de 9 meses para leer las píldoras, consejos y lectura guías. Dedicación de 12 días dedicación parcial del responsable TI para organizar distintas tareas, distribuir consejos y guías según planificación kit. - Formación específica sobre normativa RGPD: 6h * nº empleados + coste impartir curso por parte de la empresa de servicios TI. - Explicación y formación políticas de seguridad definidas: 8h * nº empleados + coste divulgación por parte de la empresa de servicios TI 			
<p>(*) <i>Todas las formaciones y horas pueden ser distribuidas y planificadas a lo largo del año, dentro de los períodos marcados en la planificación.</i></p>			
Tareas			
<ul style="list-style-type: none"> - Organización y preparación tareas “<i>Kit de concienciación</i>” INCIBE. - Preparación formación curso RGPD. - Descarga guías seguridad INCIBE - Confeccionar y realizar formación sobre las políticas de seguridad de la empresa definidas. 			
Controles			
<ul style="list-style-type: none"> - Seguimiento de incidencias de seguridad para evaluar la efectividad del programa y detectar temáticas sobre las que impartir formación, refuerzo, leyes, instrucciones o normativa interna. 			

8.4. Plan [SEC20-BAK.PRO004] Copias de Seguridad

Tabla 181. Plan SEC20-BAK.PRO004 - Copias de seguridad						
Nombre:	Copias de seguridad	Grupo:	[Backup]			
Código:	SEC20-BAK.PRO004	Prioridad	[1T]	[2T]	[3T]	[4T]
Responsable:	Responsable TI	2				
Objetivos/Hitos						
<ul style="list-style-type: none"> - Implementación nueva política de copias de seguridad según ubicación y nivel de confidencialidad y criticidad de la información. - Añadir seguridad adicional a los soportes de las copias (cifrado de las copias). - Sincronización copias "on Cloud". - Verificación y validación procedimiento de restauración backups. 						
Activos afectados						
I001-Fichero Clientes, D001-Expediente Cliente, D004-Backup Servidor, SW005-Sistema de backup, HW005-Unidad Backup, HW001-Servidor, D005-Logs, D006-Fichero configuraciones, HW009-Router						
Salvaguardas						
<ul style="list-style-type: none"> [D.A] Copias de seguridad de los datos (backup) [D.I] Aseguramiento de la integridad [SW.A] Copias de seguridad (backup) [D.C] Cifrado de la información 						
Descripción						
<p>Actualmente la empresa ya cuenta con una política de copias de seguridad, si bien precisa de una revisión para cerciorarnos de que cumple su función correctamente.</p> <p>Aunque no hay una política formalizada, los datos de todos los departamentos se encuentran en los recursos de red configurados en el servidor. Además, el ERP con toda la información administrativo-financiera también reside en el servidor.</p> <p>Es por lo que la política actual de copias considera sólo el servidor. Cualquier otra información residente en los puestos locales o dispositivos removibles es considerada temporal.</p> <p>Este plan tiene como finalidad varios objetivos:</p> <ul style="list-style-type: none"> - Revisar la política actual de copias, los distintos parámetros y adecuarlos a las necesidades. - Actualmente se realiza una copia incremental diaria y completa semanalmente (guardando una como mensual). La retención de las copias mensuales es de un año. Cada año se guarda la primera mensual con una retención de 5 años. - Establecer un procedimiento de verificación de las copias periódico que garantice su validez ante un incidente, para asegurar la continuidad de negocio. - Mejorar seguridad del backup frente a un incidente de robo, mediante un mecanismo de cifrado. - Deslocalización de una de las copias fuera de las instalaciones de la empresa sincronizando con un servicio "on Cloud". Actualmente las copias se guardan en una caja de seguridad en la empresa. 						

<ul style="list-style-type: none"> - Establecer distintas políticas de copias considerando el nivel de sensibilidad de cada tipo de información. Este punto está directamente relacionado con el programa SEC20-PROG005-Clasificación de la información, que tiene como objetivo clasificar la información en diferentes niveles de seguridad (público, privado y confidencial) y cumplimiento del RGPD.
Coste
<ul style="list-style-type: none"> - Servicio almacenamiento "on Cloud": 600€ - Dedicación por empresa de servicios TI para la realización de las distintas tareas: 40h - Ejecución del procedimiento de restauración periódico y revisión: 10h cada semestre.
Tareas
<ul style="list-style-type: none"> - Revisión y adaptación de la política actual de copias y nuevos parámetros para adecuarlos a las necesidades. - Establecer distintas políticas de copias (frecuencia) según el nivel de criticidad y sensibilidad de la información. - Establecer un procedimiento periódico de restauración de copias para verificación del proceso de copias. - Contratación del servicio de almacenamiento "on Cloud". - Aplicar cifrado a la copia antes para copiar al sistema de backups o su sincronización al Cloud. - Adaptar la política de seguridad para sincronizar las copias con el Cloud.
Controles
<ul style="list-style-type: none"> - Monitorización del proceso de copias - Revisión de los errores - Informe de restauración periódico

8.5. Plan [SEC20-CPD.PR005] Zona CPD

Tabla 182. Plan SEC20 - CPD.PR005 - Zona CPD

Nombre:	Zona CPD	Grupo:	[CPD]					
			Planificación 2020					
Código:	SEC20-CPD.PR005	Prioridad	[1T]	[2T]	[3T]	[4T]		
Responsable:	Responsable TI	1						
Objetivos/Hitos								
<ul style="list-style-type: none"> - Habilitar espacio físico como CPD exclusivo para servidor y elementos críticos de la red, con acceso restringido. - Adecuar las condiciones de temperatura, humedad y antiincendios. - Restringir acceso sólo a personal autorizado con responsabilidades sobre los elementos. 								
Activos afectados								
L002-Cuarto de comunicaciones Además del cableado red local y resto de dispositivos reubicados. HW001-Servidor, HW005-Unidad Backup, HW008-Router, HW009-Switch, AUX001SAI								
Salvaguardas								
[LAC] Control de los accesos físicos								
Descripción								
<p>Actualmente, tanto servidor como elementos críticos de la red están en habitáculos no compartidos, aunque sin acceso restringido. Estos espacios se utilizan también para otros propósitos (material oficina, archivo, zona de microondas, limpieza, etc.) lo cual supone un riesgo pues son elementos sensibles a ataques físicos intencionados o accidentales que están al alcance de personal interno y externo.</p> <p>Es necesario habilitar un espacio exclusivo para servidor, unidad de copias, dispositivos críticos de red (router, switch) y SAI.</p> <p>Este programa tiene como finalidad habilitar la actual zona de comunicaciones (donde se sitúan router, switch y SAI actualmente), convirtiéndola en CPD, creando un espacio exclusivo con acceso restringido a personal autorizado con responsabilidades sobre el equipamiento y los elementos críticos del sistema.</p> <p>Para llevar a cabo, será necesario:</p> <ul style="list-style-type: none"> - Acondicionar zona para todos los dispositivos de comunicaciones y Servidor. - Adecuar las condiciones de temperatura, humedad y antiincendios. - Trasladar todos los elementos de comunicaciones, servidor, dispositivos de copia sensibles a ataques físicos deben estar protegidos y con acceso restringido. - Instalar medidas de seguridad y control del acceso físico que permita registro de los accesos, con acceso sólo a personal con responsabilidades (administración y mantenimiento). 								
Coste								
Pendiente de presupuestar según proyecto								

Tareas
<ul style="list-style-type: none"> - Instalación armario en rack para situar los elementos de comunicaciones, servidor, unidad backup y SAI. - Instalación cableado red desde el resto de los equipos. - Instalación SAI e instalaciones eléctricas hacia éste. - Climatización del espacio con condiciones de temperatura, humedad. - Sistema antiincendios. - Instalar sistema control de acceso
Controles
Registro de accesos a personal autorizado.

8.6. Plan [SEC20-COM.PR006] Fortalecimiento Red

Tabla 183. Plan SEC20-COM.PR006 - Fortalecimiento Red

Además, se debería contemplar, dentro de la política de seguridad, la revisión de las franjas horarias de funcionamiento, así como el reenvío de alertas del log y su revisión por parte de los administradores. Esta es una tarea para incluir dentro del contrato de servicios de TI.

Switch: Es un elemento cuyo riesgo es alto por dejar la LAN inoperativa, aunque es aceptable, por tener una probabilidad muy baja de daño. Además, la solución sería sencilla (sustitución por otro).

Para acortar el tiempo de inactividad se propone incluir en el plan, la instalación de un segundo switch que actúe como backup, de forma que, ante el fallo de uno, se tenga el otro disponible para dar servicio.

Políticas Wifi: Dentro del programa de creación de políticas, en la política específica de la red Wifi, habría que contemplar al menos 2 aspectos:

- Conexiones a red wifi-invitados.
- Conexión a la red wifi-interna con mecanismos de seguridad adicionales como certificados, habilitar filtrado de MAC, franjas horarias, ...

Coste
Pendiente de análisis detallado para presupuestar.
Tareas
<ul style="list-style-type: none">- Segmentación red interna<ul style="list-style-type: none">o Instalación Router/Firewall internoo Configuración- Instalación switch redundado<ul style="list-style-type: none">o Cablear doble tarjeta red servidor a switches distintos.o Definición procedimiento de contingencia en caso de incidencia.- Revisión mantenimiento router en contrato línea ADSL/Fibra- Separación Wifi-interna e invitados.<ul style="list-style-type: none">o Creación ambas áreas Wifio Configuración usuarios, franjas horarias, certificados, filtrados MAC- Adaptación política de seguridad red Wifi
Controles
Revisión alertas y logs de conexión, intentos de intrusión Realización Pentest periódico

8.7. Plan [SEC20-DOC.PR007] Gestión de la Información

Tabla 184. Plan SEC20-DOC.PR007 - Gestión de la Información

Nombre:	Gestión de la Información	Prioridad	Grupo:	[SEG]
			Planificación 2020	
Código:	SEC20-DOC.PR007		[1T]	[2T]
Responsable:	Responsable Administración	1	[3T]	[4T]
Objetivos/Hitos				
<ul style="list-style-type: none"> - Análisis y clasificación información existente (física y digital). - Adaptar políticas de acceso/restricción de la información. - Verificación cumplimiento de la normativa RGPD. - Procedimiento de destrucción de información. - Adaptar política de copias de seguridad. 				
Activos afectados				
<p>[info] [I001]-Fichero Clientes, [D001]-Expediente Cliente</p>				
Salvaguardas				
<p>[D] Protección de la Información</p>				
Descripción				
<p>Durante la implementación de este programa se definirá un sistema de clasificación de la información según tipología, nivel de confidencialidad y propietario que contemple al menos tres niveles de seguridad (público, privado y confidencial). Este sistema debe contemplar aspectos como el etiquetado, acceso, destrucción de la información, uso de cifrado para datos sensibles de carácter personal, protección de los datos críticos, etc.</p>				
<p>La finalidad principal de este programa es garantizar el cumplimiento de la normativa en cuanto a protección de la información. Para ello es necesario realizar el análisis de la información existente en la empresa y su clasificación según tipología, nivel de confidencialidad y propietario.</p>				
<p>La implementación del plan permitirá adecuar la política de seguridad sobre la información de la empresa, así como la reorganización de los permisos y ubicación de la información.</p>				
<p>Este programa es requisito de otro futuro para implantar un gestor documental, que se abordará en un plan anual posterior (por determinar). Además, impacta directamente en la actualización de los programas [SEC20-DOC.PR002]Políticas de Seguridad y [SEC20-BAK.PR004]Copias de Seguridad.</p>				
<p>(!) Para abordar este programa, es necesario que el personal de la empresa haya comenzado el programa de Formación y Concienciación y se haya formado en materia de seguridad de la información, habiendo recibido al menos los contenidos sobre RGPD.</p>				
Coste				
<p>2 meses, 1 persona especialista en la materia de la empresa de servicios TI.</p>				
<p>4 meses, 50 persona interna de Administración</p>				
<p>4 meses, 20% Responsable TI.</p>				

Tareas
- Identificación y clasificación de la información existente según tipología, nivel de confidencialidad y propietario. - Adaptar políticas de acceso/restricción de la información. - Reubicación información en la red según tipología. - Configurar permisos de acceso. - Adaptación política backup (según tipología). - Definición proceso destrucción información.
Controles
- Verificación cumplimiento RGPD. - Auditoría periódica cumplimiento política de seguridad definida. - Registro de incidencias de seguridad.

8.8. Plan [SEC20-SW.PRO08] ERP on Cloud

Tabla 185. Plan SEC20-SW.PRO08 - ERP on Cloud

Nombre:	ERP on Cloud	Grupo:	[SW]
Código:	SEC20-SW.PR008	Prioridad	Planificación 2020
Responsable:	Responsable TI	2	[1T] [2T] [3T] [4T]
Objetivos/Hitos			
- Análisis coste-beneficio y evaluación Prinex Cloud vs Prinex Real Estate.			
Activos afectados			
SW001-ERP, HW001-Servidor			
Salvaguardas			
[SW] Protección de las Aplicaciones Informáticas			
Descripción			
Dentro de la estrategia de TI de la empresa de mover servicios a la nube, una de las líneas de trabajo sería evaluar la versión del ERP Prinex Cloud (solución en modalidad de pago por uso: Software as a Service (SaaS)).			
El ERP es un activo crítico para la empresa que se encuentra actualmente instalado en el servidor <i>on premise</i> , en su versión Prinex (Real State). Además de hacer crítico el activo HW001-Servidor.			
El hecho de utilizar este servicio desde la nube supondría "compartir" el riesgo con el proveedor (Grupo Shebel) en materia de seguridad y alta disponibilidad de este servicio. Además, abriría la posibilidad para la utilización desde fuera de las oficinas de la empresa; lo cual sería un avance en otra de las líneas estratégicas marcadas en el plan estratégico de la empresa, como es la deslocalización del trabajo.			
La finalidad de este proyecto es realizar un análisis ventajas/inconvenientes y coste-beneficio de la versión Prinex Cloud vs Prinex Real State, para poder tomar la decisión.			
El resultado del análisis se tendrá en cuenta, en caso de decidir migrar al <i>Cloud</i> , para:			
- Incluir en el plan anual 2021, otro programa específico para llevar a cabo la migración.			
- Evaluar y actualizar el riesgo del Servidor, dado que se reduciría. Este impacto se deberá tener en cuenta en el programa "[SEC20-HA.PR009] Alta disponibilidad del Servidor", para adoptar la solución de alta disponibilidad adecuada.			
Coste			
Coste de realizar el análisis y evaluación: 1 mes, 50% un recurso de la empresa de servicios TI			
Tareas			
Evaluar versión.			
Analizar costes y funcionalidades.			
Controles			
Validación de las funcionalidades con el departamento de Administración			

8.9. Plan [SEC20-HA.PRO09] Alta disponibilidad del Servidor

Tabla 186. Plan SEC20-HA.PR009 - Alta disponibilidad del Servidor

Nombre:		Alta disponibilidad del Servidor	Grupo:	[HA]
Código:	SEC20-HA.PR009	Prioridad	Planificación 2020	
Responsable:	Responsable TI	1	[1T]	[2T]
Objetivos/Hitos				
<ul style="list-style-type: none"> - Implementación alta disponibilidad del Servidor - Planificación Disaster recovery del Servidor 				
Activos afectados				
HW001-Servidor				
Salvaguardas				
[HW.A] Aseguramiento de la disponibilidad				
Descripción				
El servidor es un elemento crítico dentro de la empresa, pues tiene varias funciones importantes:				
<ul style="list-style-type: none"> - Es donde reside la información sensible y documentación compartida en los recursos de red de los distintos departamentos y el ERP con la información administrativo-financiera. - Mantiene todo el software de red, antivirus, dominio Windows y Active Directory. - Se encarga de controlar el acceso de usuarios al dominio y la LAN y aplicar las políticas de seguridad sobre los diferentes recursos compartidos de la red. - Realiza tareas planificadas como copias de seguridad, mantenimiento de base de datos ERP, descarga de actualizaciones, etc. 				
El plan de contingencia actual está basado en copias de seguridad y su restauración, aunque ante determinadas amenazas, el impacto y riesgo sigue siendo alto.				
Para implementar la salvaguarda (<i>HW.A - Aseguramiento de la disponibilidad</i>) y reducir el riesgo hasta un nivel aceptable, es necesario dotar al sistema de alta disponibilidad, con un servidor en clúster.				
También sería necesario evaluar la instalación de un servidor que adopte la función de Backup Domain Controller del AD.				
<p><i>(I) Sería aconsejable que este programa se aborde después del programa "[SEC20-COM.PR005] Zona CPD" para instalar el nuevo servidor en su ubicación definitiva.</i></p> <p><i>(II) Este programa está condicionado por el resultado del programa "SEC20-SW.PR008 ERP on Cloud", pues si se decidiese migrar el ERP a la nube, el servidor pasaría a ser un activo menos crítico, el riesgo sobre el servidor se reduciría y la solución a adoptar habría que adecuarla a las necesidades.</i></p>				
Coste				
Clúster 2 nodos Servidor 5000€				
1 persona, 2 mes, de empresa de servicios TI				
Tareas				

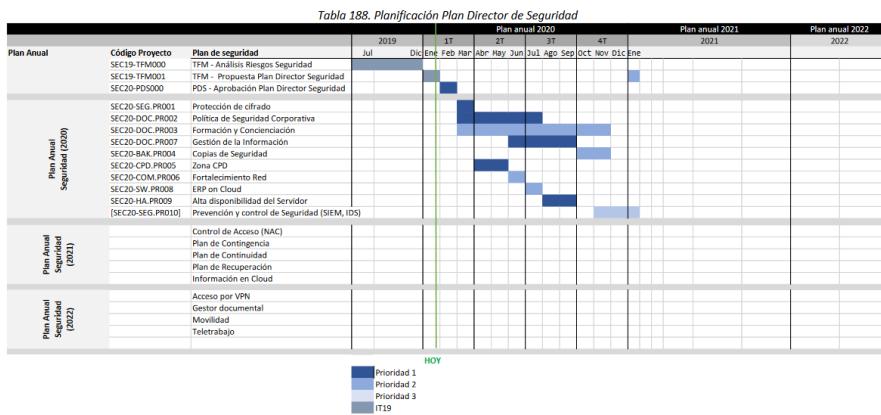
- Análisis de las opciones para implementar la alta disponibilidad del Servidor y servicios críticos.
- Comprar hardware necesario
- Configurar e instalar clúster
- Instalar software
- Migrar datos
- Instalar y configurar servidor actual como Domain Backup Controller.
- Elaboración procedimiento de Disaster recovery del servidor, como parte del plan de contingencia y recuperación.
- Realizar prueba del procedimiento de Disaster recovery

8.10. Plan [SEC20-SEG.PR010] Prevención-Control Seguridad(SIEM/IDS)

Tabla 187. Plan SEC20-SEG.PRO10 - Prevención - Control Seguridad[SIEM/IDS]								
Nombre:	Prevención-Control de Seguridad (SIEM/IDS)	Grupos:	[SEG]	Planificación 2020				
Código:	[SEC20-SEG.PRO10]	Prioridad	[1T] [2T] [3T] [4T]					
Responsable:	Responsable TI	2						
Objetivos/Hitos								
- Evaluación/instalación solución de sistema de información y gestión de eventos (SIEM)	<ul style="list-style-type: none"> o Proporcionar una visión global de la seguridad de la tecnología de la información de la empresa. o Detección y neutralización de las amenazas informáticas (externas e internas). o Recopilar datos para su análisis sobre los distintos eventos relevantes de seguridad. o Detección de accesos no autorizados al sistema de la empresa. 							
- Evaluación solución de sistema de detección de intrusos (IDS)								
Activos afectados								
En general todos los activos del sistema de información de los que se registren eventos de seguridad y sean susceptibles de ser atacados.								
I001-Fichero Clientes, D001-Expediente Cliente,								
D002-Datos acceso Servidor, D003-Datos acceso Usuarios,								
D004-Backup Servidor, SW005-Sistema de backup, HW005-Unidad Backup,								
D005-Fichero log, D006-Ficheros configuraciones,								
SW003-Cliente de correo, SW004-Antivirus, SW006-Navegador web,								
SW008-Sistema operativo Servidor, SW009-Sistema operativo cliente,								
HW001-Servidor, HW002-Desktop, HW003-Workstation, HW004-Laptop,								
HW008-Router, HW009-Switch, COM002-Red local, COM004-Red WiFi,								
Salvaguardias								
[H.tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión								
[H.tools.LA] Herramienta para análisis de logs								
Descripción								
La finalidad de este plan es la evaluación e instalación de herramientas de prevención y detección de intrusos para reforzar la seguridad.								
- SIEM como solución para unificar la recopilación de eventos y alertas de seguridad de todas las tecnologías que intervienen en la red (aplicaciones antivirus, firewalls, soluciones de prevención de intrusiones, etc.).								
La solución actuará como orquestador ofreciendo visibilidad completa del estado de la seguridad en los distintos activos y dispositivos, mediante: recolección de logs, informes, dashboards, monitorización, cumplimiento de políticas, alertas, correlación de eventos, análisis forense.								
Son una parte importante del ecosistema de seguridad de datos: agregan datos de múltiples sistemas y soluciones, y analizan y correlacionan esos datos para detectar comportamientos anormales o sospechosos que puedan traducirse en ataques cibernéticos.								

- IDS: Sistema de detección de intrusos
Coste
Análisis soluciones adecuada a necesidades empresa: 50% 1 persona, 1 mes de empresa de servicios TI Instalación y configuraciones: 1 persona, 2 mes de empresa servicios TI
Tareas
- Evaluación solución SIEM - Evaluación solución IDS - Instalación y configuración
Controles
- Reportes - Métricas de detección, alertas

8.11. Planificación Plan Director de Seguridad



Anexo 2 – Tablas auxiliares

En este anexo se adjuntan las tablas de salvaguardas y tipos de activos con la codificación utilizada de MAGERIT, para que estén accesibles a consulta en el propio trabajo.

Catálogo de Amenazas de Magerit (relación Tipo Activo y Dimensión)

Tabla 189. Catálogo Amenazas-Tipo Activo-Dimensión. Magerit v3 – Libro II, capítulo 5 (pág. 25-47) [11]

Amenaza	Tipo Activo afectado	Dimensión
Desastres Naturales		
[N.1] Fuego	[HW] [Media] [AUX] [L]	[D]
[N.2] Daños por agua	[HW] [Media] [AUX] [L]	[D]
[N.*] Desastres naturales	[HW] [Media] [AUX] [L]	[D]
De origen industrial	Tipo Activo	Dimensión
[I.1] Fuego	[HW] [Media] [AUX] [L]	[D]
[I.2] Daños por agua	[HW] [Media] [AUX] [L]	[D]
[I.*] Desastres industriales	[HW] [Media] [AUX] [L]	[D]
[I.3] Contaminación Mecánica	[HW] [Media] [AUX]	[D]
[I.4] Contaminación Electromagnética	[HW] [Media] [AUX]	[D]
[I.5] Avería de origen físico o lógico	[SW] [HW] [Media] [AUX]	[D]
[I.6] Corte del suministro eléctrico	[HW] [Media] [AUX]	[D]
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] [Media] [AUX]	[D]
[I.8] Fallo de servicios de comunicaciones	[COM]	[D]
[I.9] Interrupción de otros servicios y suministros esenciales	[AUX]	[D]
[I.10] Degradación de los soportes de almacenamiento de la información	[Media]	[D]
[I.11] Emanaciones electromagnéticas	[HW] [Media] [AUX] [L]	[C]
Errores y fallos no intencionados	Tipo Activo	Dimensión
[E.1] Errores de los usuarios	[D] [info] [keys] [S] [SW] [Media]	[I] [C] [D]
[E.2] Errores del administrador	[D] [info] [keys] [S] [SW] [HW] [COM] [Media]	[D] [I] [C]
[E.3] Errores de monitorización (log)	[D.log]	[I] [T]
[E.4] Errores de configuración	[D.conf]	[I]
[E.7] Deficiencias en la organización	[P]	[D]
[E.8] Difusión de software dañino	[SW]	[D] [I] [C]
[E.9] Errores de [re]-encamamiento	[S] [SW] [COM]	[C]
[E.10] Errores de secuencia	[S] [SW] [COM]	[I]
[E.15] Alteración accidental de la información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[I]
[E.18] Destrucción de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[D]
[E.19] Fugas de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L] [P]	[C]

[E.20] Vulnerabilidades de los programas (software)	[SW]	[I] [D] [C]
[E.21] Errores de mantenimiento / actualización de programas (software)	[SW]	[I] [D]
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] [Media] [AUX]	[D]
[E.24] Caída del sistema por agotamiento de recursos	[S] [HW] [COM]	[D]
[E.25] Pérdida de equipos (robo)	[HW] [Media] [AUX]	[D] [C]
[E.28] Indisponibilidad del personal	[P]	[D]
Ataques intencionados	Tipo Activo	Dimensión
[A.3] Manipulación de los registros de actividad (log)	[D.log]	[I] [T]
[A.4] Manipulación de la configuración	[D.log]	[I] [C] [A]
[A.5] Suplantación de la identidad del usuario	[D] [info] [keys] [S] [SW] [COM]	[C] [A] [I]
[A.6] Abuso de privilegios de acceso	[D] [info] [keys] [S] [SW] [HW] [COM]	[C] [I] [D]
[A.7] Uso no previsto	[S] [SW] [HW] [COM] [Media] [AUX] [L]	[D] [C] [I]
[A.8] Difusión de software dañino	[SW]	[D] [I] [C]
[A.9] [Re]-encamamiento de mensajes	[S] [SW] [COM]	[C]
[A.10] Alteración de secuencia	[S] [SW] [COM]	[I]
[A.11] Acceso no autorizado	[D] [info] [keys] [S] [SW] [HW] [COM] [Media] [AUX] [L]	[I] [C]
[A.12] Análisis de tráfico	[COM]	[C]
[A.13] Repudio	[S] [D.log]	[I] [T]
[A.14] Interceptación de información (escucha)	[COM]	[C]
[A.15] Modificación deliberada de la información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[I]
[A.18] Destrucción de información	[D] [info] [keys] [S] [SW] [Media] [L]	[D]
[A.19] Divulgación de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[C]
[A.22] Manipulación de programas	[SW]	[C] [I] [D]
[A.23] Manipulación de los equipos	[HW] [Media] [AUX]	[C] [D]
[A.24] Denegación de servicio	[S] [HW] [COM]	[D]
[A.25] Robo	[HW] [Media] [AUX]	[D] [C]
[A.26] Ataque destructivo	[HW] [Media] [AUX] [L]	[D]
[A.27] Ocupación enemiga	[L]	[D] [C]
[A.28] Indisponibilidad del personal	[P]	[D]
[A.29] Extorsión	[P]	[C] [I] [D]
[A.30] Ingeniería social (picardía)	[P]	[C] [I] [D]
Amenaza	Tipo Activo afectado	Dimensión
[N.1] Fuego	[HW] [Media] [AUX] [L]	[D]
[N.2] Daños por agua	[HW] [Media] [AUX] [L]	[D]
[N.*] Desastres naturales	[HW] [Media] [AUX] [L]	[D]
Amenaza	Tipo Activo	Dimensión

[I.1] Fuego	[HW] [Media] [AUX] [L]	[D]
[I.2] Daños por agua	[HW] [Media] [AUX] [L]	[D]
[I.*] Desastres industriales	[HW] [Media] [AUX] [L]	[D]
[I.3] Contaminación Mecánica	[HW] [Media] [AUX]	[D]
[I.4] Contaminación Electromagnética	[HW] [Media] [AUX]	[D]
[I.5] Avería de origen físico o lógico	[SW] [HW] [Media] [AUX]	[D]
[I.6] Corte del suministro eléctrico	[HW] [Media] [AUX]	[D]
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] [Media] [AUX]	[D]
[I.8] Fallo de servicios de comunicaciones	[COM]	[D]
[I.9] Interrupción de otros servicios y suministros esenciales	[AUX]	[D]
[I.10] Degradación de los soportes de almacenamiento de la información	[Media]	[D]
[I.11] Emanaciones electromagnéticas	[HW] [Media] [AUX] [L]	[C]
Amenaza	Tipo Activo	Dimensión
[E.1] Errores de los usuarios	[D] [info] [keys] [S] [SW] [Media]	[I] [C] [D]
[E.2] Errores del administrador	[D] [info] [keys] [S] [SW] [HW] [COM] [Media]	[D] [I] [C]
[E.3] Errores de monitorización (log)	[D.log]	[I] [T]
[E.4] Errores de configuración	[D.conf]	[I]
[E.7] Deficiencias en la organización	[P]	[D]
[E.8] Difusión de software dañino	[SW]	[D] [I] [C]
[E.9] Errores de re-encaminamiento	[S] [SW] [COM]	[C]
[E.10] Errores de secuencia	[S] [SW] [COM]	[I]
[E.15] Alteración accidental de la información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[I]
[E.18] Destrucción de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[D]
[E.19] Fugas de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L] [P]	[C]
[E.20] Vulnerabilidades de los programas (software)	[SW]	[I] [D] [C]
[E.21] Errores de mantenimiento / actualización de programas (software)	[SW]	[I] [D]
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] [Media] [AUX]	[D]
[E.24] Caída del sistema por agotamiento de recursos	[S] [HW] [COM]	[D]
[E.25] Pérdida de equipos (robo)	[HW] [Media] [AUX]	[D] [C]
[E.28] Indisponibilidad del personal	[P]	[D]
Amenaza	Tipo Activo	Dimensión
[A.3] Manipulación de los registros de actividad (log)	[D.log]	[I] [T]
[A.4] Manipulación de la configuración	[D.log]	[I] [C] [A]
[A.5] Suplantación de la identidad del usuario	[D] [info] [keys] [S] [SW] [COM]	[C] [A] [I]

[A.6] Abuso de privilegios de acceso	[D] [info] [keys] [S] [SW] [HW] [COM]	[C] [I] [D]
[A.7] Uso no previsto	[S] [SW] [HW] [COM] [Media] [AUX] [L]	[D] [C] [I]
[A.8] Difusión de software dañino	[SW]	[D] [I] [C]
[A.9] (Re-)encaminamiento de mensajes	[S] [SW] [COM]	[C]
[A.10] Alteración de secuencia	[S] [SW] [COM]	[I]
[A.11] Acceso no autorizado	[D] [info] [keys] [S] [SW] [HW] [COM] [Media] [AUX] [L]	[I] [C]
[A.12] Análisis de tráfico	[COM]	[C]
[A.13] Repudio	[S] [D.log]	[I] [T]
[A.14] Intercepción de información (escucha)	[COM]	[C]
[A.15] Modificación deliberada de la información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[I]
[A.18] Destrucción de información	[D] [info] [keys] [S] [SW] [Media] [L]	[D]
[A.19] Divulgación de información	[D] [info] [keys] [S] [SW] [COM] [Media] [L]	[C]
[A.22] Manipulación de programas	[SW]	[C] [I] [D]
[A.23] Manipulación de los equipos	[HW] [Media] [AUX]	[C] [D]
[A.24] Denegación de servicio	[S] [HW] [COM]	[D]
[A.25] Robo	[HW] [Media] [AUX]	[D] [C]
[A.26] Ataque destructivo	[HW] [Media] [AUX] [L]	[D]
[A.27] Ocupación enemiga	[L]	[D] [C]
[A.28] Indisponibilidad del personal	[P]	[D]
[A.29] Extorsión	[P]	[C] [I] [D]
[A.30] Ingeniería social (pícarosca)	[P]	[C] [I] [D]
Amenaza	Tipo Activo afectado	Dimensión
[N.1] Fuego	[HW] [Media] [AUX] [L]	[D]
[N.2] Daños por agua	[HW] [Media] [AUX] [L]	[D]
[N.*] Desastres naturales	[HW] [Media] [AUX] [L]	[D]
Amenaza	Tipo Activo	Dimensión

Catálogo de Salvaguardas de Magerit

Tabla 190. Catálogo de Salvaguardas. Magerit v3 – Libro II, capítulo 6 (pág. 53-57) [11]

Código	Salvaguarda
H	Protecciones Generales
H.IA	Identificación y autenticación
H.AC	Control de acceso lógico
H.ST	Segregación de tareas
H.IR	Gestión de incidencias
H.tools	Herramientas de seguridad
H.tools.AV	Herramienta contra código dañino
H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
H.tools.CC	Herramienta de chequeo de configuración
H.tools.VA	Herramienta de análisis de vulnerabilidades
H.tools.TM	Herramienta de monitorización de tráfico
H.tools.DLP	DLP: Herramienta de monitorización de contenidos
H.tools.LA	Herramienta para análisis de logs
H.tools.HP	Honey net / honey pot
H.tools.SFV	Verificación de las funciones de seguridad
H.VM	Gestión de vulnerabilidades
H.AU	Registro y auditoría
D	Protección de la Información
D.A	Copias de seguridad de los datos (backup)
D.I	Aseguramiento de la integridad
D.C	Cifrado de la información
D.DS	Uso de firmas electrónicas
D.TS	Uso de servicios de fechado electrónico (time stamping)
K	Gestión de claves criptográficas
K.IC	Gestión de claves de cifra de información
K.DS	Gestión de claves de firma de información
K.disk	Gestión de claves para contenedores criptográficos
K.comms	Gestión de claves de comunicaciones
K.509	Gestión de certificados
S	Protección de los Servicios
S.A	Aseguramiento de la disponibilidad
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.CM	Gestión de cambios (mejoras y sustituciones)
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.email	Protección del correo electrónico
S.dir	Protección del directorio
S.dns	Protección del servidor de nombres de dominio (DNS)
S.TW	Teletrabajo
S.voip	Voz sobre IP

SW	Protección de las Aplicaciones Informáticas
SW.A	Copias de seguridad (backup)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
SW.CM	Cambios (actualizaciones y mantenimiento)
SW.end	Terminación
HW	Protección de los Equipos Informáticos
HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.op	Operación
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.end	Terminación
HW.PCD	Informática móvil
HW.print	Reproducción de documentos
HW.pabx	Protección de la centralita telefónica (PABX)
COM	Protección de las Comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.aut	Autenticación del canal
COM.I	Protección de la integridad de los datos intercambiados
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op	Operación
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.end	Terminación
COM.internet	Internet: uso de ? acceso a
COM.wifi	Seguridad Wireless (WiFi)
COM.mobile	Telefonía móvil
COM.DS	Segregación de las redes en dominios
IP	Puntos de interconexión: conexiones entre zonas de confianza
IP.SPP	Sistema de protección perimetral
IP.BS	Protección de los equipos de frontera
MP	Protección de los Soportes de Información
MP.A	Aseguramiento de la disponibilidad
MP.IC	Protección criptográfica del contenido
MP.clean	Limpieza de contenidos
MP.end	Destrucción de soportes
AUX	Elementos Auxiliares
AUX.A	Aseguramiento de la disponibilidad
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.AC	Climatización

AUX.wires	Protección del cableado
L	Protección de las Instalaciones
L.design	Diseño
L.depth	Defensa en profundidad
L.AC	Control de los accesos físicos
L.A	Aseguramiento de la disponibilidad
L.end	Terminación
PS	Gestión del Personal
PS.AT	Formación y concienciación
PS.A	Aseguramiento de la disponibilidad
G	Organización
G.RM	Gestión de riesgos
G.plan	Planificación de la seguridad
G.exam	Inspecciones de seguridad
BC	Continuidad del negocio
BC.BIA	Análisis de impacto (BIA)
BC.DRP	Plan de Recuperación de Desastres (DRP)
E	Relaciones Externas
E.1	Acuerdos para intercambio de información y software
E.2	Acceso externo
E.3	Servicios proporcionados por otras organizaciones
E.4	Personal subcontratado
NEW	Adquisición / desarrollo
NEW.S	Servicios: Adquisición o desarrollo
NEW.SW	Aplicaciones: Adquisición o desarrollo
NEW.HW	Equipos: Adquisición o desarrollo
NEW.COM	Comunicaciones: Adquisición o contratación
NEW.MP	Soportes de Información: Adquisición
NEW.C	Productos certificados o acreditados
Código	Salvaguardas