Escuela Politécnica Superior de Jaén
Grado en Ingeniería Informática

Universidad de Jaén
Escuela Politécnica Superior
de Jaén

TRABAJO FIN DE GRADO

# REALIZACIÓN DE UNA AUDITORÍA INFORMÁTICA AL SISTEMA DE INFORMACIÓN DE UNA PYME REAL.

Alumno

**Antonio Muñoz Segura**

Tutor

**Francisco de Asís Conde Rodríguez**
(Departamento de Informática)

**Junio, 2020**

*(Página intencionalmente en blanco)*


Universidad de Jaén

Departamento de Informática

Don Francisco de Asís Conde Rodríguez, tutor del Trabajo Fin de Grado titulado: '**Realización de una auditoría informática al sistema de información de una PYME real.**', que presenta Don Antonio Muñoz Segura, otorga el visto bueno para su entrega y defensa en la Escuela Politécnica Superior de Jaén.

Jaén, Junio de 2020

El alumno: El tutor:

Antonio Muñoz Segura Francisco de Asís Conde Rodríguez

*(Página intencionalmente en blanco)*

## Agradecimientos

*Lo primero de todo quiero agradecer a las personas que me han ayudado en la recopilación de la información para la elaboración de este Trabajo Fin de Grado. Concretamente a la empresa auditada y sus trabajadores, por dejarme realizar esta auditoría a la misma.*

*A mi tutor, Francisco de Asís Conde Rodríguez, por sus directrices, consejos y dedicación en la elaboración de este proyecto.*

*Finalmente, agradecer a mi familia y amigos por todo el apoyo que me han dado en este largo camino que está a punto de finalizar, y en especial a mis padres que sin su apoyo no hubiera sido posible realizar.*

| FICHA DEL TRABAJO FIN DE TÍTULO | |
|---|---|
| **Titulación** | Grado en Ingeniería Informática |
| **Modalidad** | Proyecto de Ingeniería |
| **Especialidad** (solo TFG) | Ingeniería del Software |
| **Mención** (solo TFG) | Informática Empresarial |
| **Idioma** | Español |
| **Tipo** | Específico |
| **TFT en equipo** | No |
| **Autor/a** | Antonio Muñoz Segura |
| **Fecha de asignación** | 03/04/2020 |
| **Descripción corta** | Hoy en día todas las empresas, no importa su tamaño, son altamente dependientes de su Sistema de Información, ya que les proporcionan la capacidad de procesar grandes volúmenes de datos e información, y les brindan nuevas oportunidades de negocio.<br><br>Los Sistemas de información están en cambio permanente, ya que surgen nuevas tecnologías, nuevas amenazas, cambia la legislación que los regula, etc. Por ello, hay que revisarlos periódicamente para asegurarse de que siguen cumpliendo sus objetivos adecuadamente.<br><br>En este trabajo fin de grado se va a realizar una auditoría informática al sistema de información de una pequeña y mediana empresa dedicada al sector sanitario, para comprobar su correcto funcionamiento en los siguientes temas:<br>• Cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.<br>• Grados de protección de la empresa frente a pérdidas de datos.<br>• Grado de seguridad de su red Wifi. |

| NORMAS APLICADAS EN ESTE DOCUMENTO | |
|---|---|
| **LOCALES** | |
| TFT-UJA:2017 | Normativa de Trabajos Fin de Grado, Fin de Máster y otros Trabajos Fin de Título de la Universidad de Jaén (Normativa marco UJA aprobada en Consejo de Gobierno) |
| TFT-EPSJ:2017 | Normativa sobre Trabajos Fin de Grado y Fin de Máster en la Escuela Politécnica Superior de Jaén (Normativa EPSJ aprobada en Junta de Escuela) |
| TFT-EPSJ | Criterios de evaluación y normas de estilo para TFG y TFM de la Escuela Politécnica Superior de Jaén |
| **NACIONALES E INTERNACIONALES** | |
| ISO 2145:1978 | Documentación - Numeración de divisiones y subdivisiones en documentos escritos |
| UNE 50132:1994 | Traducción de la ISO 2145 |
| APA 6ª edición | Estilo de referencias y citas de APA (American Psychological Association) |

| NORMAS UTILIZADAS COMO BASE O REFERENCIA | |
|---|---|
| **NACIONALES** | |
| UNE 157001:2014 | Criterios generales para la elaboración formal de los documentos que constituyen un proyecto técnico |
| UNE 157801:2007 | Criterios generales para la elaboración de proyectos de sistemas de información |
| UNE-ISO 19011:2018 | Directrices para la auditoría de los sistemas de gestión |
| UNE-ISO 31000:2018 | Gestión del riesgo |
| *Estas normas se han utilizado **como base o referencia** para la inclusión de algunos contenidos y definiciones sobre elaboración de proyectos, entendiendo como **proyecto** la documentación consensuada entre una empresa y un cliente, que da lugar al perfeccionamiento de un contrato para la elaboración de una obra o la prestación de un servicio. Por consiguiente, no debe esperarse la aplicación de estas normas en cuanto a la completitud de los contenidos ni a la organización de los mismos.* | |

# Contenido

# Índice de ilustraciones

# Índice de tablas

# 1 ESPECIFICACIÓN DEL TRABAJO

En este capítulo se presenta la especificación del trabajo, con una estructura y contenidos **inspirados** en los criterios y recomendaciones que establece la norma UNE 157801:2007 - "*Criterios Generales para la elaboración de proyectos de Sistemas de Información*".

A lo largo del documento se utilizarán términos y acrónimos cuya descripción aparecen en el apartado 5 (Definiciones y abreviaturas).

## 1.1 Introducción

En este documento se va a tratar un Trabajo de Fin de Grado para el Grado en Ingeniería Informática de la Universidad de Jaén. Por lo tanto, cumple con los requisitos establecidos por la Escuela Politécnica Superior de la Universidad de Jaén para la elaboración y evaluación de un Trabajo de Fin de Grado.

Concretando un poco más con respecto al tema sobre el que se va a realizar en este trabajo, se va a realizar una auditoría informática al sistema de información de un pequeña y mediana empresa dedicada al sector sanitario. En cuanto a los aspectos que se van a tratar dentro de la auditoría y se comprobará el correcto funcionamiento de los siguientes temas:

- Cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Grado de protección de la empresa frente a pérdidas de datos.
- Grado de seguridad de su red Wifi.

## 1.2 Objetivos del trabajo

Hoy en día todas las empresas, no importa su tamaño, son altamente dependientes de su Sistema de Información, ya que les proporcionan la capacidad de procesar grandes volúmenes de datos e información, y les brindan nuevas oportunidades de negocio.

Los Sistemas de información están en cambio permanente, ya que surgen nuevas tecnologías, nuevas amenazas, cambia la legislación que los regula, etc. Por ello, hay que revisarlos periódicamente para asegurarse de que siguen cumpliendo sus objetivos adecuadamente.

Por lo tanto, cuando este trabajo fin de grado se haya finalizado se deberá haber realizado una auditoría informática al sistema de información de una PYME real, dedicada al sector sanitario, con el siguiente alcance:

- Grado de cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Grado de protección de la empresa frente a pérdidas de datos.
- Grado de seguridad de la red Wifi.

Además, en cuanto a los objetivos de aprendizaje del alumno, este deberá haber ampliado sus conocimientos sobre la realización de auditorías informáticas y habrá llevado a la práctica en un caso real, los conocimientos sobre auditorías aprendidos en el grado.

## 1.3 Antecedentes y estado del arte

### 1.3.1 Covid-19

Actualmente España se encuentra en un estado de alarma debido a la existencia de un virus llamado "*SARS-CoV-2*", este virus provoca una nueva enfermedad de 2019 la "*COVID-19",* también conocida como "*Coronavirus"*, debido a este estado, todos los habitantes del país debemos estar en un confinamiento total, lo que afecta a este TFG a la hora de realizar el estudio de campo en la empresa auditada.

Debido a esta situación, se han tenido que tomar algunas alternativas con respecto a la planificación inicial del proyecto, concretamente en la planificación de la auditoría, reuniones y entrevistas.

En cuanto a la planificación, nos hemos tenido que ajustar a las restricciones actuales y hemos debido planificar la auditoría para hacerla en su gran medida de manera telemática, para ello hemos hecho uso de videollamadas con los trabajadores de la empresa, hemos usado la herramienta que nos proporciona la Universidad de Jaén, "Google Meet".

Con respecto a las reuniones y entrevistas con los trabajadores de la empresa, en condiciones normales estas reuniones se deben realizar en las instalaciones de la empresa

auditada y cara a cara, pero debido a la situación descrita anteriormente, todas ellas las hemos tenido que realizar de manera telemática con el uso de la herramienta “Google Meet”.

Además, para realizar comprobaciones en los ordenadores y terminales de la empresa hemos usado la aplicación de escritorio remoto “TeamViewer”, esta es un software informático “privado” de fácil acceso, que dispone de una versión gratuita para uso personal, que permite conectarse remotamente y controlar escritorios, reuniones en línea, video conferencias y transferencia de archivos entre ordenadores.

### 1.3.2 Privacidad de los datos

Por otro lado, debemos especificar que a lo largo de todo el documento no aparecerán los datos reales de la empresa auditada y se utilizarán unos datos totalmente ficticios. Esta medida se lleva a cabo para preservar la privacidad de la empresa, ya que vamos a usar datos de carácter sensible y su publicación podría tener repercusiones negativas para la misma.

Cabe definir que los datos de cálculo y todos los datos del Sistema de información, sí son reales, los datos ficticios son todos los relativos a la identificación de la empresa, como es su razón social, nombre comercial, ubicación, entre otros.

## 1.4 Descripción del entorno actual

**Empresa sobre la que se va a realizar la auditoría:**

La empresa “Sanitaria AMS SL” es una pequeña empresa de Loja, Granada dedicada a la distribución al por menor de artículos de óptica y audiología. Además, su gama de productos abarca desde productos propios de dicho grupo y una amplia gama de productos generalistas, todos estos completamente personalizados para cada cliente.

En cuanto a sus ventas, se dedican únicamente a la venta física. Para la gestión de su base de datos y toda información relativa a su empresa, como son los datos de los clientes, compras y ventas, citas, facturación, pedidos y almacén usan el programa *“Optiplus”*, el cual está instalado en un servidor con sistema operativo Windows 10. Toda la configuración relativa a la base de datos y al sistema operativo la realizó y la realiza actualmente, uno de los dos dueños de la empresa.

Después de hablar con la empresa para pedirles información sobre la misma para poder realizar la planificación de la auditoría correctamente, nos han dado los siguientes datos:

La empresa está ubicada en un establecimiento comercial ubicado en la calle principal de la ciudad, compuesto por un espacio en el que hay un taller y una parte donde se encuentra instalado el servidor, además tiene una parte de mostrador y otro espacio con dos puntos de venta. Por otro lado, hay una sala en la que se encuentra el gabinete de optometría y otra sala para el gabinete de audiometría.

Con respecto al personal de “Sanitaria AMS SL” hay cuatro trabajadores, dos dueños de la empresa, el primero es óptico y el segundo es técnico en óptica de anteojería y audioprotesista, además, hay dos personas en el departamento comercial que se encargan de las ventas y atención al cliente. Por otro lado, uno de los dueños es el encargado de la administración del sistema de información. Una gestoría externa es la encargada de llevar la contabilidad, pero está no trabaja en la sede de la empresa “Sanitaria AMS SL”.

En relación a los ordenadores que componen el sistema de información de la empresa, hay un servidor con 8 GB de RAM, un procesador Intel i7 7ª generación 3 GHz y un disco duro de 1 TB con tecnología SSD y una velocidad de lectura y escritura de 540 MB/s y 510 MB/s respectivamente; los dos terminales de los puestos de ventas tienen 8 GB de RAM, un procesador Intel i5 6ª generación 2.30 GHz, con tecnología turbo boost hasta 2.40 GHz y un disco duro de 512 GB a 7200 rpm; en el gabinete de optometría hay un ordenador con 4 GB de RAM, un procesador Intel i5 4ª generación 3.10 GHz y un disco duro de 512 GB a 7200rpm; en el mostrador principal hay otro ordenador con 4 Gb de RAM, procesadores Intel Core 2 Quad 2.50GHz y un disco duro de 256 GB a 5400rpm; y por último, en el taller hay un portátil con 8 GB de RAM, procesadores Intel i5 8ª generación 1.60 GHz, con tecnología turbo boost hasta 1.80 GHz. Todos los equipos tienen instalado el sistema operativo Windows 10 y antivirus Windows Defender.

Todos los equipos, excepto el portátil que está mediante conexión wifi, están conectados mediante clave a una red local que se conecta a internet mediante una conexión de fibra óptica de 600 Mb simétricos proporcionada por Movistar.

Además, tenemos dos impresoras láser, una en el gabinete de optometría y otra en el mostrador; y una multifunción en el servidor.

Por otro lado, la empresa tiene registrados un total de 13351 clientes. El cliente promedio realiza compras por un valor de 183.90€ al año. La empresa tiene una facturación anual de 303993.15 €.

### 1.4.1 Resumen de las deficiencias y carencias identificadas

Cómo se ha descrito anteriormente, los tres aspectos en los que se va a basar la realización de la auditoría informática son:

- Grado de cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Grado de protección de la empresa frente a pérdidas de datos.
- Grado de seguridad de la red Wifi.

Por lo tanto, esto conlleva que, tras la realización de la misma, se consigan las siguientes mejoras: conseguir que la empresa cumpla con todos los requisitos necesarios para el cumplimiento de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales; garantizar la total protección de la empresa frente a las pérdidas de datos mejorando todo el sistema de copias de seguridad de la misma; y, por último, aumentar la seguridad de la red wifi.

Para la realización de todas estas mejoras se realizará un estudio exhaustivo del sistema de información y se aplicarán una serie de medidas y controles.

## 1.5 Hipótesis y restricciones

El TFT se define como una asignatura de 12 créditos, lo que supone que la duración total del proyecto será de 300 horas, incluyendo todas las etapas del ciclo de vida, con la excepción del mantenimiento. Por consiguiente, la principal restricción aplicable es la limitación de la duración del trabajo.

Además, debemos añadir la situación actual en la que se encuentra España, como ya hemos descrito anteriormente debido a la *"Covid-19".*

## 1.6 Material y métodos

Para la realización de este trabajo vamos a utilizar una serie de documentos que nos sirven como guía para la realización de una correcta auditoría.

- ISO 19011 Directrices para la auditoría sistemas de gestión (ISO, 2008)
- Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
    - Libro I: Método (Magerit, 2012b)

  - Libro II: Catálogo de Elementos (Magerit, n.d.)
  - Libro III: Guía de Técnicas (Magerit, 2012a)

- BOE núm. 294, de 06/1272018. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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)

Además, también se han usado como referencia para la realización de controles una serie de guías elaboradas y publicadas por el Instituto Nacional de Ciberseguridad:

- Contraseñas (INCIBE, n.d.-c)
- Guía de almacenamiento seguro de la información (INCIBE, n.d.-b)
- Copias de seguridad (INCIBE, 2018a)
- Seguridad en redes wifi (INCIBE, 2019)
- Ganar en competitividad cumpliendo el RGPD (INCIBE, 2018b)

## 1.7 Normas y referencias

A continuación, se presentan las normas, reglamentos y referencias de cualquier tipo que han sido de aplicación en la elaboración del trabajo y/o en la puesta en práctica del mismo.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- UNE-ISO 19011:2018. Directrices para la auditoría de los sistemas de gestión.
- UNE-ISO 31000:2018. Gestión del riesgo

### 1.7.1 Métodos, herramientas, modelos, métricas y prototipos

Con respecto a las herramientas utilizadas para el desarrollo de los diversos cálculos y estimación de trabajo, hemos usado principalmente dos:

En primer lugar, “XMind 8”, es una herramienta bastante reconocida para la realización de mapas mentales, la cual hemos usado en nuestro trabajo para elaborar nuestro árbol de partición de la auditoría.

En segundo lugar, “Google Drive”, para la realización de todas las hojas de cálculos necesarias en nuestro trabajo.

En tercer lugar, “Documentos de Google Drive”, para el desarrollo de las tablas, gráficas y memoria.

En cuarto lugar, “TeamViewer” para las comprobaciones remotas de los terminales y ordenadores de la empresa.

# 2 DESARROLLO

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza

Con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos 2 y 3. Estas valoraciones son “teóricas”: en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo. (Magerit, 2012b)

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

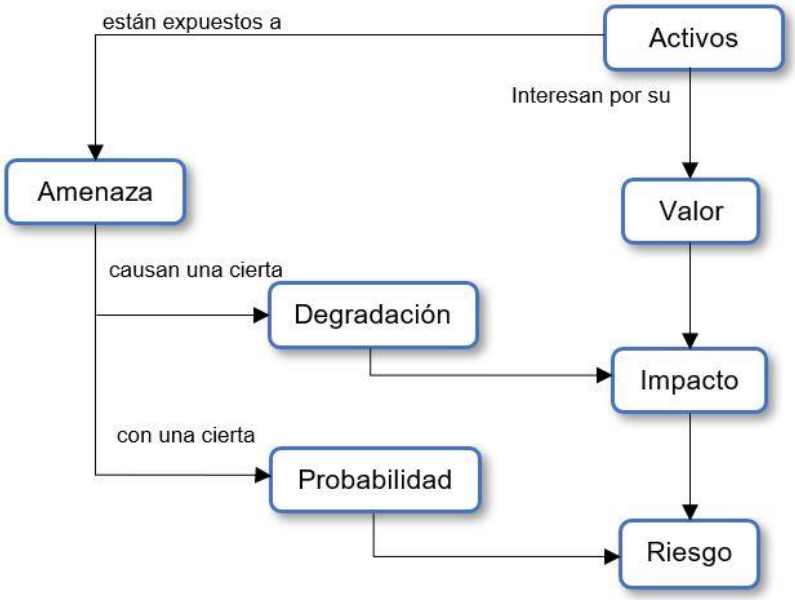



***Ilustración 1. Elementos del análisis de riesgos potenciales***

Fórmula del análisis de riesgos

$$Riesgo = Activos\ x\ Amenaza\ x\ Vulnerabilidad \quad (2.1)$$

Activos, puede afectar a varios

Amenaza, se tantas veces como amenazas haya, porcentaje de que se produzca la amenaza y como de expuesto estoy

Vulnerabilidad, como de “bueno o malos” son mis controles.

### 2.1.1 Activos

En un sistema de información hay 2 cosas esenciales:

- la información que maneja
- y los servicios que presta

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- Datos que materializan información
- Servicios auxiliares que se necesitan para organizar el sistema

- Las aplicaciones informáticas (*software*) que permiten manejas los datos
- Los equipos informáticos (*hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático
- Las redes de comunicaciones que permiten intercambiar datos
- Las instalaciones que acogen equipos informáticos y de comunicaciones
- Las personas que explotan u operan todos los elementos anteriormente citados

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Siguiendo las especificaciones anteriormente expuestas, en la empresa se han considerados los siguientes activos: información de pacientes, pedidos, citas, facturación, control compra-ventas y almacén. (Magerit, 2012b)

#### 2.1.1.1 Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos, de manera que los activos forman árboles de manera que los activos que se encuentran en la zona superior dependen de los activos que se encuentran más abajo. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientras que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas. (Magerit, 2012b)

Las dependencias entre los activos, si un activo A depende, significativamente, o no de otro activo B.

$$(A \rightarrow B) \text{ ^ } (B \rightarrow C) \tag{2.2}$$

Por lo tanto, para la empresa “Sanitaria AMS S.L.” se ha construido el siguiente árbol de dependencias de activos.

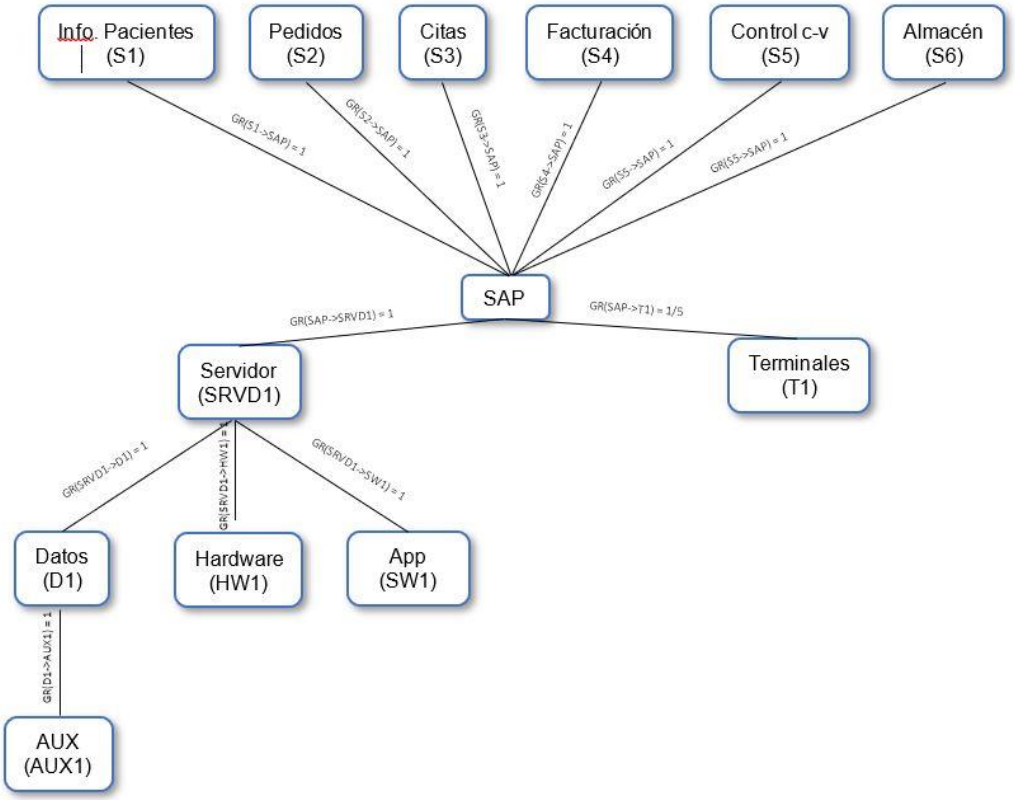



*Ilustración 2. Árbol de dependencias de los activos*

De manera aclaratoria, se añade una tabla para que se aprecie perfectamente el grado de dependencia que hay entre unos nodos y otros.

| **Nombre** | | **Dependencia** |
|---|---|---|
| **Nodo superior** | **Nodo inferior** | |
| Datos (D1) | AUX (AUX1) | 1 |
| Servidor (SRVD1) | Datos (D1) | 1 |
| | Hardware (HW1) | 1 |
| | APP (SW1) | 1 |
| SAP | Servidor (SRVD1) | 1 |
| | Terminales (T1) | 1/5 |
| Info. Pacientes (S1) | SAP | 1 |
| Pedidos (S2) | SAP | 1 |
| Citas (S3) | SAP | 1 |
| Facturación (S4) | SAP | 1 |
| Control c-v (S5) | SAP | 1 |
| Almacén (S6) | SAP | 1 |

*Tabla 1. Grado dependencia de los activos*

Para aclarar un poco el funcionamiento del árbol anterior, vamos a explicar la primera rama. En el nodo superior tenemos lo que serían los activos de la empresa, estos van dependiendo de las ramas inferiores siguiendo una serie de directrices. Se empiezan a estudiar las dependencias desde los nodos hoja hacia arriba. Dos nodos tienen un grado de dependencia el uno del otro, esto es el nodo superior tiene un grado de dependencia con respecto al nodo inferior. De esta manera, vamos calculando una sumatoria teniendo en cuenta los valores de cada nodo y el grado de dependencia de los mismos, desde el nodo hoja al nodo superior y de esta manera obtenemos los valores de cada uno de los activos de la empresa, que están representados en el árbol por los nodos superiores.

Con respecto a los nodos App (SW1) y AUX (AUX1), que puede quedar algo más abstracto a que partes del sistema de información identifican. El nodo AUX (AUX1) representa un disco duro auxiliar el cual se utiliza para realizar las copias de seguridad y tenemos conectado al servidor. El nodo App (SW1) representa todos los programas de gestión y aplicaciones que se utilizan en nuestro servidor para la administración y gestión de nuestro sistema de información.

#### 2.1.1.2 Valoración

¿Por qué interesa un activo? Por lo que vale. No nos referimos a lo que cuestan, sino a lo que valen. Si no se puede prescindir de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

*¿Cuánto vale la "salud" de los activos?*

La valoración es la determinación del coste que supondría recuperarse de una incidencia que destroza el activo. Hay que considerar muchos factores:

- Coste de reposición: cuánto cuesta reponerlo
- Coste de mano de obra: gasto del trabajo invertido en recuperar el valor del activo
- Lucro cesante: cuánto dejamos de ganar mientras el activo está dañado
- Pérdida de confianza: si falla puede que perdamos confianza de los clientes, usuarios, proveedores
- Sanciones: podemos incumplir contratos, incumplir una ley

La valoración de los activos se puede hacer de manera cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles) (Magerit, 2012b). En este caso hemos seleccionado una valoración cuantitativa debido a que es más detalla y más fácil valorar el valor de los activos.

Por lo tanto, a continuación, se va a definir el proceso que se ha seguido para realizar dicha valoración para cada activo.

En primer lugar, hemos separado cada nodo del árbol para calcular su valor total teniendo en cuenta los factores de los que depende cada activo. De esta manera hemos calculado todos los valores para cada nodo.

Para el cálculo de cada valor, se han utilizado datos obtenidos de fuentes de conocimiento fiables, de esta manera conseguimos que los datos estén respaldados en todo momento por organizaciones especializadas y de reputación.

A continuación, se muestra una tabla con el resumen de valores, desglosado y valor total de cada uno de los componentes y activos del sistema de información de la empresa, los cuales forman el árbol de dependencias de activos.

| ***ID*** | **NOMBRE** | | **VALOR (€)** |
|---|---|---|---|
| *S1* | INFORMACIÓN PACIENTES | *Lucro cesante* | 0 |
| | | *Mano de obra* | 1245.25 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31.57 |
| | | *Sanciones* | 601012.10 |
| | | **TOTAL** | **602288.92** |
| *S2* | PEDIDOS | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 830,16 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1885,28** |
| *S3* | CITAS | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 830,16 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31.57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1885,28** |

| | | | |
|---|---|---|---|
| *S4* | FACTURACIÓN | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 830,16 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 0 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1853,71** |
| *S5* | CONTROL COMPRA-VENTAS | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 830,16 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1885,28** |
| *S6* | ALMACÉN | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 830,16 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1885,28** |
| *T1* | TERMINALES | *Lucro cesante* | 0 |
| | | *Mano de obra* | 350,14 |
| | | *Coste de reposición* | 637,50 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1019,22** |
| *SRVD1* | SERVIDOR | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 608,56 |
| | | *Coste de reposición* | 807,99 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **2471,67** |
| *SW1* | APLICACIÓN | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 498,10 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **1553,22** |
| *HW1* | HARDWARE | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 350,14 |

| | | | |
|---|---|---|---|
| | | *Coste de reposición* | 800,00 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 0 |
| | | **TOTAL** | **2205,26** |
| *D1* | DATOS | *Lucro cesante* | 1023,55 |
| | | *Mano de obra* | 1217,12 |
| | | *Coste de reposición* | 0 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 601012,10 |
| | | **TOTAL** | **603284,34** |
| *AUX1* | AUXILIAR (DISCO EXTERNO) | *Lucro cesante* | 0 |
| | | *Mano de obra* | 377,00 |
| | | *Coste de reposición* | 58.99 |
| | | *Pérdida de confianza* | 31,57 |
| | | *Sanciones* | 601012,10 |
| | | **TOTAL** | **601420,67** |

***Tabla 2. Resumen valores activos***

En la tabla anterior, como podemos ver se ha especificado cada activo del árbol de dependencias con sus respectivos factores. A continuación, vamos a explicar cómo se ha calculado el valor del servidor a modo de explicación, hemos elegido este ya que es uno de los más completos y significativo.

En primer lugar, hemos calculado el lucro cesante que se trata de lo que la empresa deja de ganar en caso de que el servidor falle, para ello, se ha calculado la facturación diaria a partir de la facturación anual y ya obtendríamos el lucro cesante.

En segundo lugar, la mano de obra es lo que costaría volver a poner en marcha el servidor en caso de fallo, por lo tanto, para su cálculo, se ha buscado el salario medio de un administrador de servidor en España y con este salario y las horas de trabajo anual en España, se ha calculado el precio por hora de este trabajador. A continuación, se ha buscado cuantas horas puede tardar el trabajador en reparar la avería y las hemos multiplicado por el precio por hora anterior y de esta manera obtenemos el valor de la mano de obra.

En tercer lugar, el coste de reposición, en caso de que el servidor tenga un fallo o avería y haya que sustituirlo, se hará por uno igual. Por lo tanto, se ha buscado el precio del servidor actual y de esta manera obtenemos el valor del coste de reposición.

En último lugar, la pérdida de confianza, esto se refiere a los clientes que intentar comprar durante el periodo que el sistema de información no está disponible y ya no vuelven, para este cálculo se han calculado los clientes que intentan comprar mientras el sistema de información no está funcionando. Además, hemos buscado un estudio que dice que el 14% de los clientes que tienen un mal servicio en una empresa no vuelven, y el valor de las ventas de un cliente al año. Por lo tanto, se han multiplicado estos tres valores y de esta manera se obtiene el valor de la pérdida de confianza.

Cabe destacar que falta un valor que este activo no afecta, que son las sanciones, esto se refiere a las sanciones que puede acarrear un fallo o una avería en el activo, y en caso de que se diese alguna, el valor que tendrían cada una de ellas.

### 2.1.2 Amenazas

El siguiente paso consiste en determinar las amenazas que afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño. (Magerit, 2012b)

$$Amenaza = EF\ x\ ARO \tag{2.3}$$

La gravedad de una amenaza se calcula como EF x ARO donde:

- EF (Factor de exposición): Cuánto y/o cómo afecta al SI
- ARO (Tasa anual de ocurrencia): Cada cuánto ocurre, siendo 1 si se produce cada año y 0.1 si produce cada 10.

Una amenaza es tanto más grave cuanto más afecta al SI (EF) y cuánto más frecuentemente se dé (ARO).

Ambos se tratan de valores probabilísticos, por lo tanto, ambos tienen un valor mínimo de 0 y un valor máximo de 1.

Probabilidad de una amenaza (Magerit, 2012a)

$$P = \{0, \dots, p_{0,} p_1, \dots, p_i, \dots\} \tag{2.3}$$

Riesgo.

$$R = \{0, \dots, r_{0,}\ r_1, \dots, r_i, \dots\} \tag{2.3}$$

Hay una serie de amenazas típicas que las podemos clasificar en los siguientes grupos:

- De origen natural
- Del entorno (de origen industrial)
- Defectos de las aplicaciones
- Causadas por las personas de accidentalmente
- Causadas por las personas de deliberadamente

Por lo tanto, siguiendo está clasificación y la que realiza Magerit v3. en el "Libro 2. Catálogo de elementos", de todas las amenazas, se procede a describir de manera detallada las amenazas que pueden darse en cada activo junto con su EF y ARO. (Magerit, n.d.)

| **Amenazas** | | | |
|---|---|---|---|
| | | EF (1) | ARO (1) |
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | [I.5] Avería de origen físico o lógico | 0,1 | 0,0189 |
| | [I.6] Corte suministro eléctrico | 0,1 | 1 |
| | [I.10] Degradación de los soportes de almacenamiento de la información | 0,1 | 0,43 |
| **Errores y fallos no intencionados [E]** | [E.4] Errores de configuración | 0,3 | 1 |
| | [E.25] Pérdida de equipos | 0,4 | 0,04 |
| **Ataques intencionados [A]** | [A.11] Acceso no autorizado | 0,3 | 0,1 |
| | [A.25] Robo | 0,5 | 0,04 |

***Tabla 3. Amenazas AUX1***

| **Amenazas** | | | |
|---|---|---|---|
| | | EF | ARO |
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | - | | |
| **Errores y fallos no intencionados [E]** | [E.15] Alteración accidental de la información | 1 | 1 |
| | [E.18] Destrucción de información | 1 | 0,2 |
| | [E.19] Fugas de información | 1 | 0,2 |
| **Ataques intencionados [A]** | [A.5] Suplantación de la identidad del usuario | 1 | 0,1 |
| | [A.6] Abuso de privilegios de acceso | 1 | 0,5 |
| | [A.11] Acceso no autorizado | 1 | 0,5 |
| | [A.18] Destrucción de la información | 1 | 0,2 |
| | [A.19] Divulgación de la información | 1 | 0,2 |

*Tabla 4. Amenazas D1*

| Amenazas | | | |
|---|---|---|---|
| | | EF | ARO |
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | [I.5] Avería de origen físico o lógico | 1 | 1 |
| | [I.6] Corte del suministro eléctrico | 1 | 1 |
| **Errores y fallos no intencionados [E]** | - | | |
| **Ataques intencionados [A]** | [A.6] Abuso de privilegios de acceso | 1 | 0,1 |
| | [A.7] Uso no previsto | 1 | 0,1 |
| | [A.11] Acceso no autorizado | 1 | 0,1 |
| | [A.25] Robo | 1 | 0,04 |

*Tabla 5. Amenazas HW1*

| Amenazas | | | |
|---|---|---|---|
| | | EF (1) | ARO (1) |
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | [I.5] Avería de origen físico o lógico | 1 | 1 |
| **Errores y fallos no intencionados [E]** | [E.14] Escapes de información | 1 | 0,1 |
| | [E.19] Fugas de información | 1 | 0,2 |
| **Ataques intencionados [A]** | [A.5] Suplantación de la identidad del usuario | 1 | 0,1 |
| | [A.15] Modificación deliberada de la información | 1 | 0,1 |
| | [A.18] Destrucción de información | 0,7 | 0,1 |
| | [A.19] Divulgación de información | 0,7 | 0,1 |

*Tabla 6. Amenazas SW1*

| Amenazas | | | |
|---|---|---|---|
| | | EF | ARO |
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | [I.5] Avería de origen físico o lógico | 1 | 1 |
| | [I.6] Corte del suministro eléctrico | 1 | 1 |
| **Errores y fallos no intencionados [E]** | - | | |
| **Ataques intencionados [A]** | [A.6] Abuso de privilegios de acceso | 1 | 0,1 |
| | [A.7] Uso no previsto | 1 | 0,1 |
| | [A.11] Acceso no autorizado | 1 | 0,1 |
| | [A.25] Robo | 1 | 0,04 |

*Tabla 7. Amenazas SRVD1*

| Amenazas |
|---|

| | | EF | ARO |
|---|---|---|---|
| **Desastres naturales [N]** | - | | |
| **De origen industrial [I]** | [I.5] Avería de origen físico o lógico | 1 | 1 |
| | [I.6] Corte del suministro eléctrico | 0,2 | 1 |
| **Errores y fallos no intencionados [E]** | - | | |
| **Ataques intencionados [A]** | [A.6] Abuso de privilegios de acceso | 0,2 | 0,1 |
| | [A.7] Uso no previsto | 0,2 | 0,1 |
| | [A.11] Acceso no autorizado | 0,2 | 0,1 |
| | [A.25] Robo | 0,2 | 0,04 |

*Tabla 8. Amenazas T1*

### 2.1.3 Impacto

El siguiente paso consiste en determinar los impactos que afectan a los principales activos. Los impactos son la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. (Magerit, 2012b)

$$impacto = Activo\ x\ EF \tag{2.3}$$

Si el activo A depende del activo B, las amenazas sobre B repercuten sobre A. Si B sufre una degradación “d”, A pierde en la proporción en que dependa de B. Si el activo A tiene un valor propio “V”, el impacto es (Magerit, 2012a)

$$impacto = v\ x\ d\ x\ grado(A \rightarrow B) \tag{2.3}$$

Por lo tanto, teniendo en cuenta esta fórmula, hemos calculado todos los impactos de nuestros activos, acumulando el factor de exposición (EF) de unos activos sobre otros y teniendo en cuenta los grados de dependencia.

*Nota: Los valores están calculados con tabla automáticas de Excel correctamente. A continuación, en las tablas sólo añadimos el resumen del valor de los impactos, ya que si no la extensión es demasiada.*

| ACTIVO | VALOR | AMENAZA | | IMPACTO (€) |
|---|---|---|---|---|
| **S1** | 1819186,62 | AUX1 | [I.5] Avería de origen físico o lógico | 181918,66 |
| | | | [I.6] Corte suministro eléctrico | 181918,66 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 181918,66 |

| | | | | |
|---|---|---|---|---|
| | | | [E.4] Errores de configuración | 545755,99 |
| | | | [E.25] Pérdida de equipos | 727674,65 |
| | | | [A.11] Acceso no autorizado | 545755,99 |
| | | | [A.25] Robo | 909593,31 |
| | | D1 | [E.15] Alteración accidental de la información | 1819186,62 |
| | | | [E.18] Destrucción de información | 1819186,62 |
| | | | [E.19] Fugas de información | 1819186,62 |
| | | | [A.5] Suplantación de la identidad del usuario | 1819186,62 |
| | | | [A.6] Abuso de privilegios de acceso | 1819186,62 |
| | | | [A.11] Acceso no autorizado | 1819186,62 |
| | | | [A.18] Destrucción de la información | 1819186,62 |
| | | | [A.19] Divulgación de la información | 1819186,62 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [I.6] Corte del suministro eléctrico | 1819186,62 |
| | | | [A.6] Abuso de privilegios de acceso | 1819186,62 |
| | | | [A.7] Uso no previsto | 1819186,62 |
| | | | [A.11] Acceso no autorizado | 1819186,62 |
| | | | [A.25] Robo | 1819186,62 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [E.14] Escapes de información | 1819186,62 |
| | | | [E.19] Fugas de información | 1819186,62 |
| | | | [A.5] Suplantación de la identidad del usuario | 1819186,62 |
| | | | [A.15] Modificación deliberada de la información | 1819186,62 |
| | | | [A.18] Destrucción de información | 1273430,63 |
| | | | [A.19] Divulgación de información | 1273430,63 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [I.6] Corte del suministro eléctrico | 1819186,62 |
| | | | [A.6] Abuso de privilegios de acceso | 1819186,62 |
| | | | [A.7] Uso no previsto | 1819186,62 |
| | | | [A.11] Acceso no autorizado | 1819186,62 |
| | | | [A.25] Robo | 1819186,62 |
| | | T1 | [I.5] Avería de origen físico o lógico | 303197,77 |
| | | | [I.6] Corte del suministro eléctrico | 60639,55 |
| | | | [A.6] Abuso de privilegios de acceso | 60639,55 |
| | | | [A.7] Uso no previsto | 60639,55 |
| | | | [A.11] Acceso no autorizado | 60639,55 |
| | | | [A.25] Robo | 60639,55 |

***Tabla 9. Impactos sobre el activo S1***

| ACTIVO | VALOR | AMENAZA | | IMPACTO |
|---|---|---|---|---|
| **S2** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 121878,30 |

| | | | | |
|---|---|---|---|---|
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 121878,30 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 487513,19 |
| | | | [A.11] Acceso no autorizado | 365634,89 |
| | | | [A.25] Robo | 609391,49 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.18] Destrucción de la información | 1218782,98 |
| | | | [A.19] Divulgación de la información | 1218782,98 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.15] Modificación deliberada de la información | 1218782,98 |
| | | | [A.18] Destrucción de información | 853148,09 |
| | | | [A.19] Divulgación de información | 853148,09 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 40626,10 |
| | | | [A.7] Uso no previsto | 40626,10 |
| | | | [A.11] Acceso no autorizado | 40626,10 |
| | | | [A.25] Robo | 40626,10 |

***Tabla 10. Impactos sobre el activo S2***

| ACTIVO | VALOR | AMENAZA | | IMPACTO |
|---|---|---|---|---|
| **S3** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 121878,30 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 121878,30 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 487513,19 |
| | | | [A.11] Acceso no autorizado | 365634,89 |
| | | | [A.25] Robo | 609391,49 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.18] Destrucción de la información | 1218782,98 |
| | | | [A.19] Divulgación de la información | 1218782,98 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.15] Modificación deliberada de la información | 1218782,98 |
| | | | [A.18] Destrucción de información | 853148,09 |
| | | | [A.19] Divulgación de información | 853148,09 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 40626,10 |
| | | | [A.7] Uso no previsto | 40626,10 |
| | | | [A.11] Acceso no autorizado | 40626,10 |
| | | | [A.25] Robo | 40626,10 |

***Tabla 11. Impactos sobre el activo S3***

| ACTIVO | VALOR | AMENAZA | | IMPACTO |
|---|---|---|---|---|
| **S4** | 1218751,41 | AUX1 | [I.5] Avería de origen físico o lógico | 121875,14 |
| | | | [I.6] Corte suministro eléctrico | 121875,14 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 121875,14 |
| | | | [E.4] Errores de configuración | 365625,42 |
| | | | [E.25] Pérdida de equipos | 487500,56 |
| | | | [A.11] Acceso no autorizado | 365625,42 |
| | | | [A.25] Robo | 609375,71 |
| | | D1 | [E.15] Alteración accidental de la información | 1218751,41 |
| | | | [E.18] Destrucción de información | 1218751,41 |
| | | | [E.19] Fugas de información | 1218751,41 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218751,41 |
| | | | [A.6] Abuso de privilegios de acceso | 1218751,41 |
| | | | [A.11] Acceso no autorizado | 1218751,41 |
| | | | [A.18] Destrucción de la información | 1218751,41 |
| | | | [A.19] Divulgación de la información | 1218751,41 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [I.6] Corte del suministro eléctrico | 1218751,41 |
| | | | [A.6] Abuso de privilegios de acceso | 1218751,41 |
| | | | [A.7] Uso no previsto | 1218751,41 |
| | | | [A.11] Acceso no autorizado | 1218751,41 |
| | | | [A.25] Robo | 1218751,41 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [E.14] Escapes de información | 1218751,41 |
| | | | [E.19] Fugas de información | 1218751,41 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218751,41 |
| | | | [A.15] Modificación deliberada de la información | 1218751,41 |
| | | | [A.18] Destrucción de información | 853125,99 |
| | | | [A.19] Divulgación de información | 853125,99 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [I.6] Corte del suministro eléctrico | 1218751,41 |
| | | | [A.6] Abuso de privilegios de acceso | 1218751,41 |
| | | | [A.7] Uso no previsto | 1218751,41 |
| | | | [A.11] Acceso no autorizado | 1218751,41 |
| | | | [A.25] Robo | 1218751,41 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203125,24 |
| | | | [I.6] Corte del suministro eléctrico | 40625,05 |
| | | | [A.6] Abuso de privilegios de acceso | 40625,05 |
| | | | [A.7] Uso no previsto | 40625,05 |

| | | | | |
|---|---|---|---|---|
| | | | [A.11] Acceso no autorizado | 40625,05 |
| | | | [A.25] Robo | 40625,05 |

*Tabla 12. Impactos sobre el activo S4*

| ACTIVO | VALOR | AMENAZA | | IMPACTO |
|---|---|---|---|---|
| **S5** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 121878,30 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 121878,30 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 487513,19 |
| | | | [A.11] Acceso no autorizado | 365634,89 |
| | | | [A.25] Robo | 609391,49 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.18] Destrucción de la información | 1218782,98 |
| | | | [A.19] Divulgación de la información | 1218782,98 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.15] Modificación deliberada de la información | 1218782,98 |
| | | | [A.18] Destrucción de información | 853148,09 |
| | | | [A.19] Divulgación de información | 853148,09 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |

| | | | | |
|---|---|---|---|---|
| | | | [A.6] Abuso de privilegios de acceso | 40626,10 |
| | | | [A.7] Uso no previsto | 40626,10 |
| | | | [A.11] Acceso no autorizado | 40626,10 |
| | | | [A.25] Robo | 40626,10 |

***Tabla 13. Impactos sobre el activo S5***

| ACTIVO | VALOR | AMENAZA | | IMPACTO |
|---|---|---|---|---|
| **S6** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 121878,30 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 121878,30 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 487513,19 |
| | | | [A.11] Acceso no autorizado | 365634,89 |
| | | | [A.25] Robo | 609391,49 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.18] Destrucción de la información | 1218782,98 |
| | | | [A.19] Divulgación de la información | 1218782,98 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 1218782,98 |
| | | | [E.19] Fugas de información | 1218782,98 |
| | | | [A.5] Suplantación de la identidad del usuario | 1218782,98 |
| | | | [A.15] Modificación deliberada de la información | 1218782,98 |
| | | | [A.18] Destrucción de información | 853148,09 |
| | | | [A.19] Divulgación de información | 853148,09 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 1218782,98 |
| | | | [A.7] Uso no previsto | 1218782,98 |
| | | | [A.11] Acceso no autorizado | 1218782,98 |
| | | | [A.25] Robo | 1218782,98 |

| | | | | |
|---|---|---|---|---|
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 40626,10 |
| | | | [A.7] Uso no previsto | 40626,10 |
| | | | [A.11] Acceso no autorizado | 40626,10 |
| | | | [A.25] Robo | 40626,10 |

***Tabla 14. Impactos sobre el activo S6***

### 2.1.4 Riesgo potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

$$Riesgo\ potencial = Impacto\ x\ ARO \quad (2.3)$$

El riesgo crece con el impacto y con la probabilidad. El riesgo acumulado es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza. El riesgo acumulado se calculada para cada activo, por cada amenaza y en cada dimensión de valoración. (Magerit, 2012b)

Por lo tanto, teniendo en cuenta esta fórmula, hemos calculado todos los riesgos potenciales de nuestros activos, multiplicando los impactos acumulados obtenidos anteriormente por el factor anual de ocurrencia.

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S1** | 1819186,62 | AUX1 | [I.5] Avería de origen físico o lógico | 3438,26 |
| | | | [I.6] Corte suministro eléctrico | 181918,66 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 78225,02 |
| | | | [E.4] Errores de configuración | 545755,99 |
| | | | [E.25] Pérdida de equipos | 29106,99 |
| | | | [A.11] Acceso no autorizado | 54575,60 |
| | | | [A.25] Robo | 36383,73 |
| | | D1 | [E.15] Alteración accidental de la información | 1819186,62 |
| | | | [E.18] Destrucción de información | 363837,32 |
| | | | [E.19] Fugas de información | 363837,32 |
| | | | [A.5] Suplantación de la identidad del usuario | 181918,66 |
| | | | [A.6] Abuso de privilegios de acceso | 909593,31 |
| | | | [A.11] Acceso no autorizado | 909593,31 |
| | | | [A.18] Destrucción de la información | 363837,32 |

| | | | | |
|---|---|---|---|---|
| | | | [A.19] Divulgación de la información | 363837,32 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [I.6] Corte del suministro eléctrico | 1819186,62 |
| | | | [A.6] Abuso de privilegios de acceso | 181918,66 |
| | | | [A.7] Uso no previsto | 181918,66 |
| | | | [A.11] Acceso no autorizado | 181918,66 |
| | | | [A.25] Robo | 72767,46 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [E.14] Escapes de información | 181918,66 |
| | | | [E.19] Fugas de información | 363837,32 |
| | | | [A.5] Suplantación de la identidad del usuario | 181918,66 |
| | | | [A.15] Modificación deliberada de la información | 181918,66 |
| | | | [A.18] Destrucción de información | 127343,06 |
| | | | [A.19] Divulgación de información | 127343,06 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1819186,62 |
| | | | [I.6] Corte del suministro eléctrico | 1819186,62 |
| | | | [A.6] Abuso de privilegios de acceso | 181918,66 |
| | | | [A.7] Uso no previsto | 181918,66 |
| | | | [A.11] Acceso no autorizado | 181918,66 |
| | | | [A.25] Robo | 72767,46 |
| | | T1 | [I.5] Avería de origen físico o lógico | 303197,77 |
| | | | [I.6] Corte del suministro eléctrico | 60639,55 |
| | | | [A.6] Abuso de privilegios de acceso | 6063,96 |
| | | | [A.7] Uso no previsto | 6063,96 |
| | | | [A.11] Acceso no autorizado | 6063,96 |
| | | | [A.25] Robo | 2425,58 |

***Tabla 15. Riesgos potenciales sobre el activo S1***

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S2** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,50 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52407,67 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 19500,53 |
| | | | [A.11] Acceso no autorizado | 36563,49 |
| | | | [A.25] Robo | 24375,66 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 243756,60 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |

| | | | | |
|---|---|---|---|---|
| | | | [A.6] Abuso de privilegios de acceso | 609391,49 |
| | | | [A.11] Acceso no autorizado | 609391,49 |
| | | | [A.18] Destrucción de la información | 243756,60 |
| | | | [A.19] Divulgación de la información | 243756,60 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 121878,30 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.15] Modificación deliberada de la información | 121878,30 |
| | | | [A.18] Destrucción de información | 85314,81 |
| | | | [A.19] Divulgación de información | 85314,81 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,61 |
| | | | [A.7] Uso no previsto | 4062,61 |
| | | | [A.11] Acceso no autorizado | 4062,61 |
| | | | [A.25] Robo | 1625,04 |

***Tabla 16. Riesgos potenciales sobre el activo S2***

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S3** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,50 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52407,6682 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 19500,53 |
| | | | [A.11] Acceso no autorizado | 36563,49 |
| | | | [A.25] Robo | 24375,66 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |

| | | | | |
|---|---|---|---|---|
| | | | [E.18] Destrucción de información | 243756,60 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.6] Abuso de privilegios de acceso | 609391,49 |
| | | | [A.11] Acceso no autorizado | 609391,49 |
| | | | [A.18] Destrucción de la información | 243756,60 |
| | | | [A.19] Divulgación de la información | 243756,60 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 121878,30 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.15] Modificación deliberada de la información | 121878,30 |
| | | | [A.18] Destrucción de información | 85314,81 |
| | | | [A.19] Divulgación de información | 85314,81 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,61 |
| | | | [A.7] Uso no previsto | 4062,61 |
| | | | [A.11] Acceso no autorizado | 4062,61 |
| | | | [A.25] Robo | 1625,04 |

***Tabla 17. Riesgos potenciales sobre el activo S3***

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S4** | 1218751,41 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,44 |
| | | | [I.6] Corte suministro eléctrico | 121875,14 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52406,31 |
| | | | [E.4] Errores de configuración | 365625,42 |
| | | | [E.25] Pérdida de equipos | 19500,02 |

| | | | | |
|---|---|---|---|---|
| | | | [A.11] Acceso no autorizado | 36562,54 |
| | | | [A.25] Robo | 24375,03 |
| | | D1 | [E.15] Alteración accidental de la información | 1218751,41 |
| | | | [E.18] Destrucción de información | 243750,28 |
| | | | [E.19] Fugas de información | 243750,28 |
| | | | [A.5] Suplantación de la identidad del usuario | 121875,14 |
| | | | [A.6] Abuso de privilegios de acceso | 609375,71 |
| | | | [A.11] Acceso no autorizado | 609375,71 |
| | | | [A.18] Destrucción de la información | 243750,28 |
| | | | [A.19] Divulgación de la información | 243750,28 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [I.6] Corte del suministro eléctrico | 1218751,41 |
| | | | [A.6] Abuso de privilegios de acceso | 121875,14 |
| | | | [A.7] Uso no previsto | 121875,14 |
| | | | [A.11] Acceso no autorizado | 121875,14 |
| | | | [A.25] Robo | 48750,06 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [E.14] Escapes de información | 121875,14 |
| | | | [E.19] Fugas de información | 243750,28 |
| | | | [A.5] Suplantación de la identidad del usuario | 121875,14 |
| | | | [A.15] Modificación deliberada de la información | 121875,14 |
| | | | [A.18] Destrucción de información | 85312,60 |
| | | | [A.19] Divulgación de información | 85312,60 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218751,41 |
| | | | [I.6] Corte del suministro eléctrico | 1218751,41 |
| | | | [A.6] Abuso de privilegios de acceso | 121875,14 |
| | | | [A.7] Uso no previsto | 121875,14 |
| | | | [A.11] Acceso no autorizado | 121875,14 |
| | | | [A.25] Robo | 48750,06 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203125,24 |
| | | | [I.6] Corte del suministro eléctrico | 40625,05 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,50 |
| | | | [A.7] Uso no previsto | 4062,50 |
| | | | [A.11] Acceso no autorizado | 4062,50 |
| | | | [A.25] Robo | 1625,00 |

***Tabla 18. Riesgos potenciales sobre el activo S4***

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S5** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,50 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |

| | | | | |
|---|---|---|---|---|
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52407,67 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 19500,53 |
| | | | [A.11] Acceso no autorizado | 36563,49 |
| | | | [A.25] Robo | 24375,66 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 243756,60 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.6] Abuso de privilegios de acceso | 609391,49 |
| | | | [A.11] Acceso no autorizado | 609391,49 |
| | | | [A.18] Destrucción de la información | 243756,60 |
| | | | [A.19] Divulgación de la información | 243756,60 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 121878,30 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.15] Modificación deliberada de la información | 121878,30 |
| | | | [A.18] Destrucción de información | 85314,81 |
| | | | [A.19] Divulgación de información | 85314,81 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,61 |
| | | | [A.7] Uso no previsto | 4062,61 |
| | | | [A.11] Acceso no autorizado | 4062,61 |
| | | | [A.25] Robo | 1625,04 |

***Tabla 19. Riesgos potenciales sobre el activo S4***

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S5** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,50 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52407,67 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 19500,53 |
| | | | [A.11] Acceso no autorizado | 36563,49 |
| | | | [A.25] Robo | 24375,66 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 243756,60 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.6] Abuso de privilegios de acceso | 609391,49 |
| | | | [A.11] Acceso no autorizado | 609391,49 |
| | | | [A.18] Destrucción de la información | 243756,60 |
| | | | [A.19] Divulgación de la información | 243756,60 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 121878,30 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.15] Modificación deliberada de la información | 121878,30 |
| | | | [A.18] Destrucción de información | 85314,81 |
| | | | [A.19] Divulgación de información | 85314,81 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,61 |
| | | | [A.7] Uso no previsto | 4062,61 |
| | | | [A.11] Acceso no autorizado | 4062,61 |

| | | | | |
|---|---|---|---|---|
| | | | [A.25] Robo | 1625,04 |

*Tabla 20. Riesgos potenciales sobre el activo S5*

| ACTIVO | VALOR | AMENAZA | | RIESGO POTENCIAL |
|---|---|---|---|---|
| **S6** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 2303,50 |
| | | | [I.6] Corte suministro eléctrico | 121878,30 |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 52407,67 |
| | | | [E.4] Errores de configuración | 365634,89 |
| | | | [E.25] Pérdida de equipos | 19500,53 |
| | | | [A.11] Acceso no autorizado | 36563,49 |
| | | | [A.25] Robo | 24375,66 |
| | | D1 | [E.15] Alteración accidental de la información | 1218782,98 |
| | | | [E.18] Destrucción de información | 243756,60 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.6] Abuso de privilegios de acceso | 609391,49 |
| | | | [A.11] Acceso no autorizado | 609391,49 |
| | | | [A.18] Destrucción de la información | 243756,60 |
| | | | [A.19] Divulgación de la información | 243756,60 |
| | | HW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | SW1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [E.14] Escapes de información | 121878,30 |
| | | | [E.19] Fugas de información | 243756,60 |
| | | | [A.5] Suplantación de la identidad del usuario | 121878,30 |
| | | | [A.15] Modificación deliberada de la información | 121878,30 |
| | | | [A.18] Destrucción de información | 85314,81 |
| | | | [A.19] Divulgación de información | 85314,81 |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 1218782,98 |
| | | | [I.6] Corte del suministro eléctrico | 1218782,98 |
| | | | [A.6] Abuso de privilegios de acceso | 121878,30 |
| | | | [A.7] Uso no previsto | 121878,30 |
| | | | [A.11] Acceso no autorizado | 121878,30 |
| | | | [A.25] Robo | 48751,32 |
| | | T1 | [I.5] Avería de origen físico o lógico | 203130,50 |

| | | | | |
|---|---|---|---|---|
| | | | [I.6] Corte del suministro eléctrico | 40626,10 |
| | | | [A.6] Abuso de privilegios de acceso | 4062,61 |
| | | | [A.7] Uso no previsto | 4062,61 |
| | | | [A.11] Acceso no autorizado | 4062,61 |
| | | | [A.25] Robo | 1625,04 |

***Tabla 21. Riesgos potenciales sobre el activo S6***

### 2.1.5 Salvaguardas o controles internos

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por lo tanto, los impactos y los riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

Se definen las salvaguardas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se mitigan simplemente organizándose adecuadamente, otras requieren elementos técnicos, seguridad física y la política del personal.

Con respecto a la definición de las salvaguardas, estas se deben realizar de forma que no quede ningún riesgo potencial sin cubrir con alguna salvaguarda, no son excluyentes, es decir, puede haber una salvaguarda que afecta a varios riesgos potenciales.

Las salvaguardas entran en el cálculo del riesgo de dos formas: reduciendo la probabilidad de las amenazas o limitando el daño causado. Además, se pueden distinguir entre muchos tipos de protección de los mismos: prevención, disuasión, eliminación, minimización del impacto, corrección, recuperación, monitorización, detección, concienciación y administración.

En cuanto a la eficacia de las salvaguardas, una salvaguarda ideal es 100% eficaz, combina dos factores: desde el punto de vista técnico y desde el punto de vista de operación de salvaguarda. Cabe destacar que casi nunca se da el 100% de eficacia en un control.

Con respecto a la madurez de una salvaguarda, esta mide lo bien gestionada y documentada que está. (Magerit, 2012b)

| Factor | Nivel | Significado |
|---|---|---|
| 0 % | L0 | Inexistente |
| | L1 | Inicial / ad hoc |
| | L2 | Reproducible, pero intuitivo |
| | L3 | Proceso definido |
| | L4 | Gestionado y medible |
| 100 % | L5 | Optimizado |

*Tabla 22. Madurez de las salvaguardas*

Además, cabe destacar las partes de las que se compone un/a control o salvaguarda:

- Título, con el que llamamos a nuestra salvaguarda
- Finalidad, cual es el fin con el que desarrollamos dicha salvaguarda
- Empresa, es aquella en la que se debe aplicar la salvaguarda
- Leyes aplicables, es un listado de todas las leyes en vigor que determinan en todo o en parte cómo debe definirse el presente control
- Normas aplicables, es un listado de todas las normas o estándares internacionales que se hayan seguido a la hora de redactar el presente control
- Descripción del control, es una descripción precisa y detallada que explique en qué consiste la salvaguarda; responsables, es una lista de todos aquellos empleados que tienen alguna responsabilidad en la aplicación del control
- Dispositivos, es una lista de todos los dispositivos necesarios para la puesta en marca de la salvaguarda
- Costes del control, que están divididos en tres partes, implantación, son los costes que se derivan del diseño e instalación del control, coste de ejecución y mantenimiento, son costes periódicos necesarios para mantener activo el control y, coste de búsqueda de irregularidades, son los que se producen cuando la amenaza realmente se materializa en el sistema de información
- Rentabilidad del control, un estudio de como de rentable es el control en nuestro sistema de información.

Por último, la fórmula que se usa para calcular el riesgo residual después de la implantación de los controles es la siguiente:

$$Riesgo\ residual = Riesgo\ potencia\ x\ (1 - Efectividad) \quad (2.3)$$

Siendo la efectividad $e^f$ =0 si la salvaguarda es absolutamente ineficaz y $e^f$ =1 siendo la salvaguarda plenamente eficaz.

Por lo tanto, siguiendo toda esta serie de recomendaciones se han desarrollado los controles necesarios para cubrir todos los riesgos potenciales existentes.

#### 2.1.5.1 Primer control

##### 2.1.5.1.1 Titulo

Control de cortes de suministro eléctrico.

##### 2.1.5.1.2 Finalidad

Una amenaza a la que nos enfrentamos en cualquier Sistemas de información son los cortes de suministro eléctrico, por lo tanto, debemos protegernos de ellos con los dispositivos que tenemos disponibles, en este caso vamos a usar un dispositivo SAI.

##### 2.1.5.1.3 Empresa

“Sanitaria AMS SL”

##### 2.1.5.1.4 Leyes aplicables

No hay referencias de leyes para este control.

##### 2.1.5.1.5 Normas aplicables

UNE-EN 62040-1:2008/A1:2013. Sistemas de alimentación ininterrumpida (SAI). Parte 1: Requisitos generales y de seguridad para los SAI.

UNE-EN IEC 62040-1:2019/AC:2019-11. Sistemas de alimentación ininterrumpida (SAI). Parte 1: Requisitos de seguridad

UNE-EN IEC 62040-1:2019. Sistemas de alimentación ininterrumpida (SAI). Parte 1: Requisitos de seguridad.

UNE-EN IEC 62040-2:2018. Sistemas de alimentación ininterrumpida (SAI). Parte 2: Requisitos de compatibilidad electromagnética (CEM)
UNE-EN 62040-5-3:2017. Sistemas de alimentación ininterrumpida (SAI). Parte 5-3: SAI de salida en corriente continua. Funcionamiento y requisitos de ensayo
UNE-EN 62040-4:2013. Sistemas de alimentación ininterrumpida (SAI) Parte 4: Aspectos ambientales. Requisitos e informes.
UNE-EN 62040-1:2008. Sistemas de alimentación ininterrumpida (SAI) Parte 1: Requisitos generales y de seguridad para los SAI.
UNE-EN 62040-2:2006. Sistemas de alimentación ininterrumpida (SAI). Parte 2: Requisitos de compatibilidad electromagnética (CEM).
UNE-EN 62040-3:2011. Sistemas de alimentación ininterrumpida (SAI). Parte 3: Método para especificar las prestaciones y los requisitos de ensayo.

#### 2.1.5.1.6 Descripción del control

A continuación, vamos a separar las zonas para saber cuántos dispositivos SAI debemos instalar en nuestro SI. En primer lugar, vamos a instar un SAI para el servidor en el que sólo conectaremos a este. En segundo lugar, vamos a instalar otro SAI para el ordenador de sobremesa que hay en el mostrador. En tercer lugar, vamos a instalar un SAI para los dos ordenadores todo en uno de los puestos de venta. Por último, instalaremos un SAI en el ordenador de sobremesa que se encuentra en el gabinete de optometría.

En cuanto al portátil del taller no vamos a instalarle ningún dispositivo SAI, ya que este terminal está solo encendido cuando la empresa está abierta y al ser un portátil, en caso de que haya un corte de suministro eléctrico podemos apagarlo correctamente antes de que se quede sin batería.

A continuación, vamos a detallar cada uno de los dispositivos SAI que mejor se ajustan y hacen falta instalar para cada una de las zonas que hemos definido anteriormente.

En primer lugar, el servidor, debido a que es el terminal que más necesita estar protegido y del que depende todo el funcionamiento del SI usaremos un SAI Online, este tipo de SAI son los que más protegen con respecto a los problemas que puede haber en el suministro eléctrico, el modelo es “SAI 1000VA Online SoHo Lapara”, el cual tiene dos baterías de 12 V 9 Ah, con un precio de 250 €. En caso de no poder

conseguir este dispositivo se recomienda que el dispositivo de reemplazo sea uno de iguales o similares características.

En segundo lugar, vamos a usar el mismo modelo de SAI para las demás zonas, ya que son ordenadores que no tienen una carga de trabajo tan grande como el terminal del servidor, así que usaremos un SAI Off-line, más concreto el modelo "SAI – Woxter UPS 800 VA", tiene una autonomía de 8-15 minutos, que será suficiente para desconectar los equipos de forma segura, tienen un precio cada uno de 77.99 €.

Ahora vamos a describir de manera detallada como se debe realizar la instalación de los dispositivos SAI para que estos queden funcionando de manera correcta.

En primer lugar, debemos **ubicar el SAI**, los ubicaremos en el suelo, ya que no deberemos tocar a menudo las conexiones, en un sitio cercano a los terminales que se conectarán en él. Cabe destacar que no los instalaremos en un sito en el que haya una mala ventilación para que estos no se calienten fácilmente, además, no pondremos nada encima de ellos y no taparemos sus ranuras de ventilación.

En segundo lugar, **conectaremos los equipos y corriente eléctrica**, conectaremos todos los equipos a los SAI primero, después conectaremos los SAI a la corriente con los cables que incluyen las cajas de los dispositivos para hacer llegar la corriente hasta la máquina/monitor. En caso de que no sea así, o precisásemos conectar una regleta, tendremos que acudir a una tienda de material eléctrico para encontrar lo que necesitamos. Por último, conectaremos el cable de datos que va hasta el PC vía USB.

En tercer lugar, **encender el SAI**, cuando ya hayamos conectado todos los cables conectados, procederemos a encender el SAI. Según el modelo, es posible que se enciendan múltiples luces o alarmas sonoras. Probablemente se trate de avisos de que la batería esta baja (lógico, pues vendrá con poca o nula carga de fábrica). En todo caso, en unos segundos todo se normalizará y podremos empezar a trabajar normalmente con nuestro PC. Eso sí, las baterías tardarán 4 horas en cargarse en caso del servidor, por lo que no podremos exigir las máximas prestaciones hasta no haber realizado uno o varios ciclos completos de carga/descarga.

En cuarto lugar, **conectar el SAI al PC**, lo primero que tendremos que hacer será conectar el SAI a nuestro PC gracias al puerto USB, utilizando para ello un cable específico que nos entrega el fabricante. Hecho esto, nuestra máquina detectará automáticamente el nuevo componente. Aun así, tendremos que insertar el CD-ROM

de instalación y optar por instalar el programa del SAI. Una vez instalado el programa, usaremos el libro de instrucciones para saber cómo podemos obtener la información deseada en el programa de nuestro SAI.

En quinto lugar, instalamos el software WinPower (SI, 2017) y realizamos los ajustes que se van a describir a continuación: al abrir el programa, lo primero es entrar en modo administrador (contraseña por defecto: Administrador)

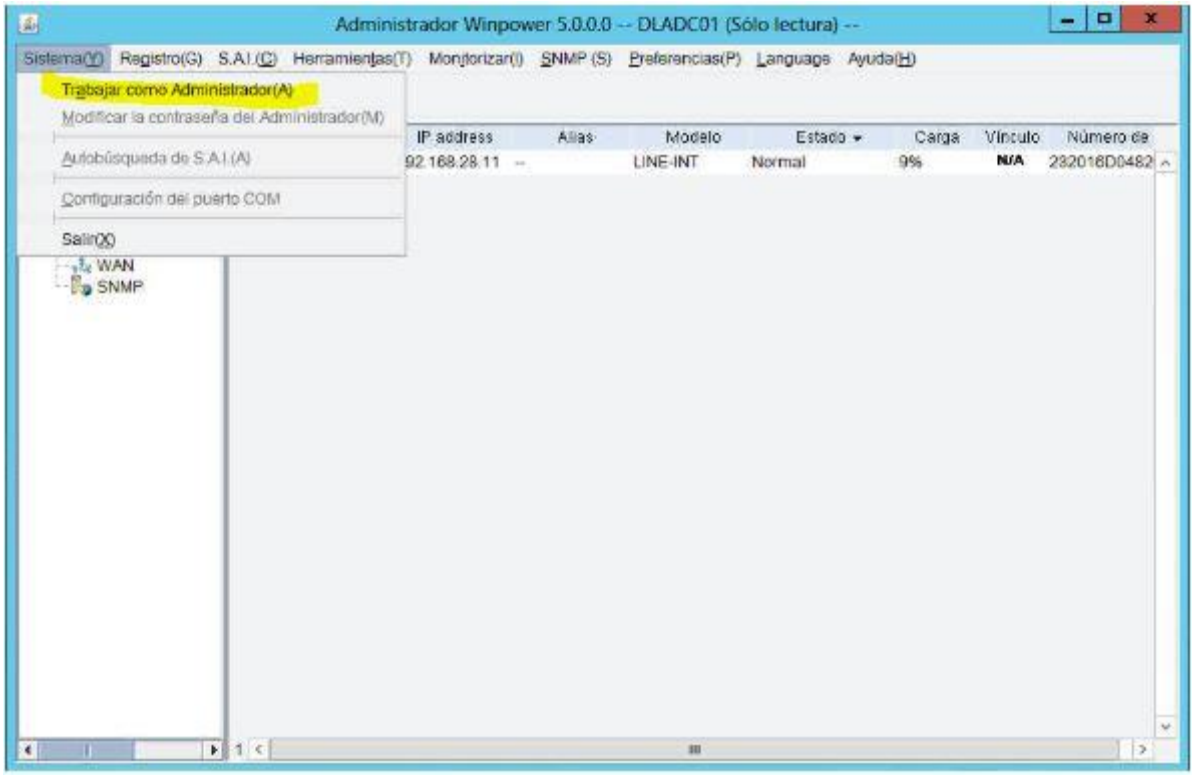



***Ilustración 3. Instalación WinPower 1***

A continuación, vamos a la pestaña >> Herramientas >> Configuración de email. Aquí configuramos los parámetros de nuestro servidor de correo y tantas cuentas como queramos que reciban los eventos, y los tipos de eventos que queremos que nos notifique.

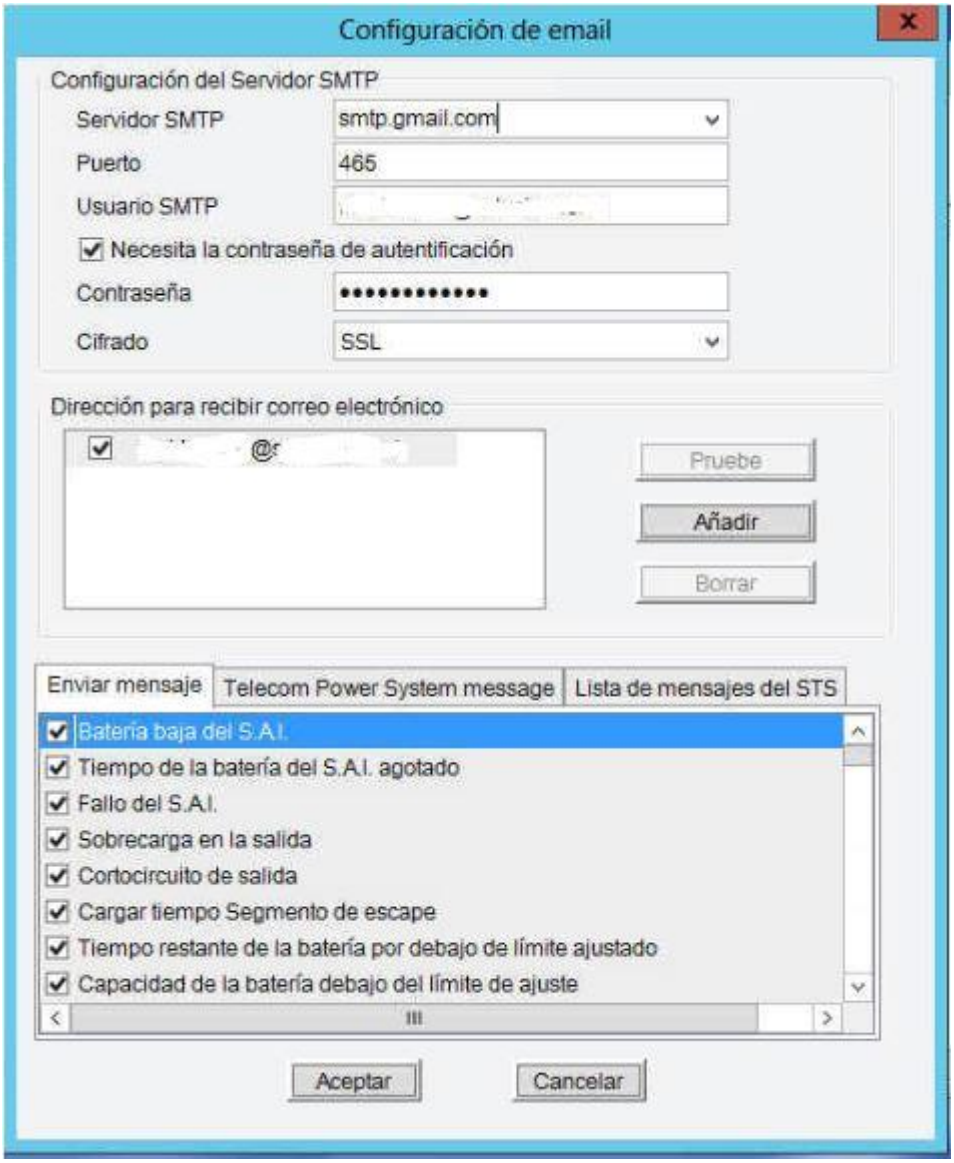



***Ilustración 4. Instalación WinPower 2***

También podemos añadir los eventos en la pestaña S.A.I >> Eventos

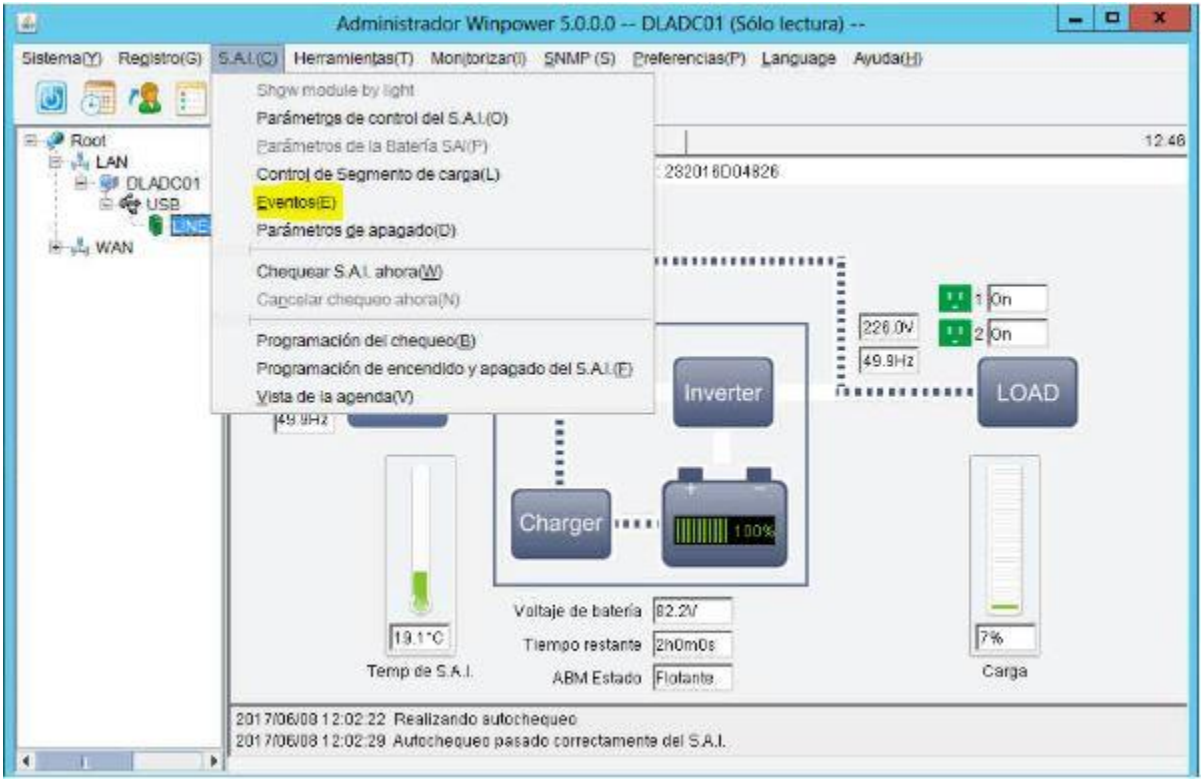



***Ilustración 5. Instalación WinPower 3***

Aquí marcando el evento deseado, en el menú derecho vemos si está incluido en las notificaciones por correo.

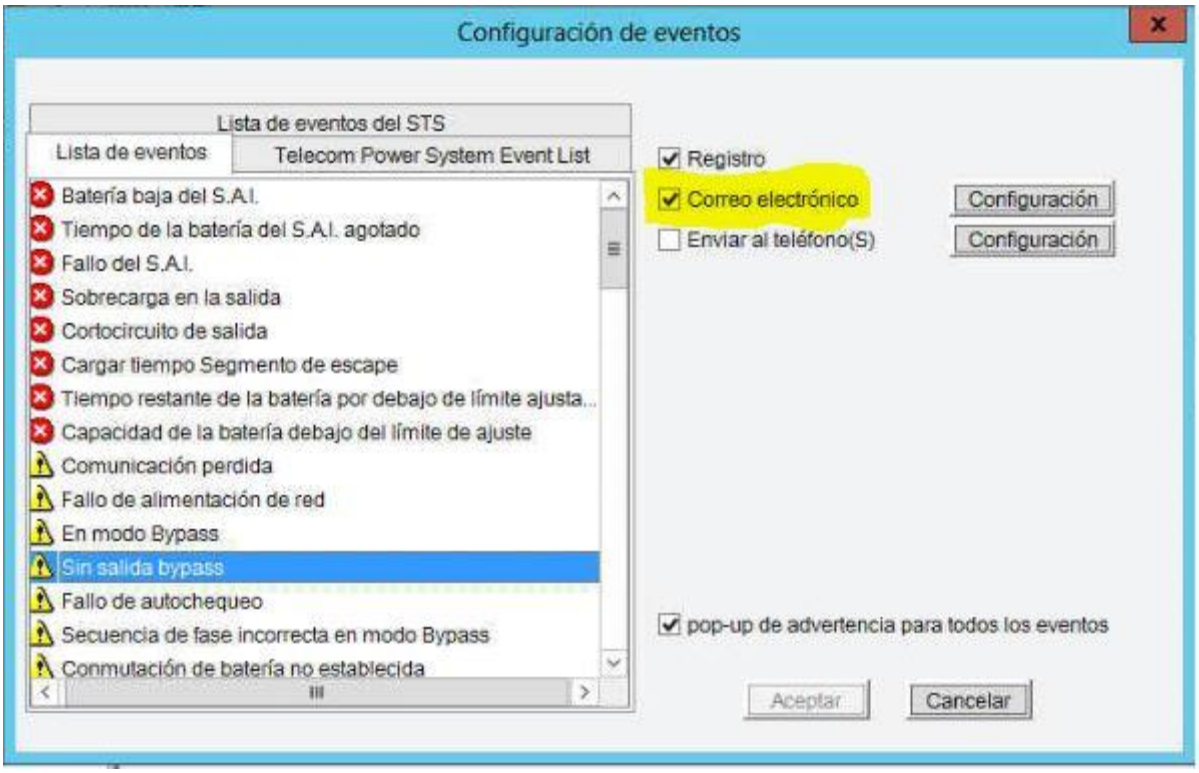



***Ilustración 6. Instalación WinPower 4***

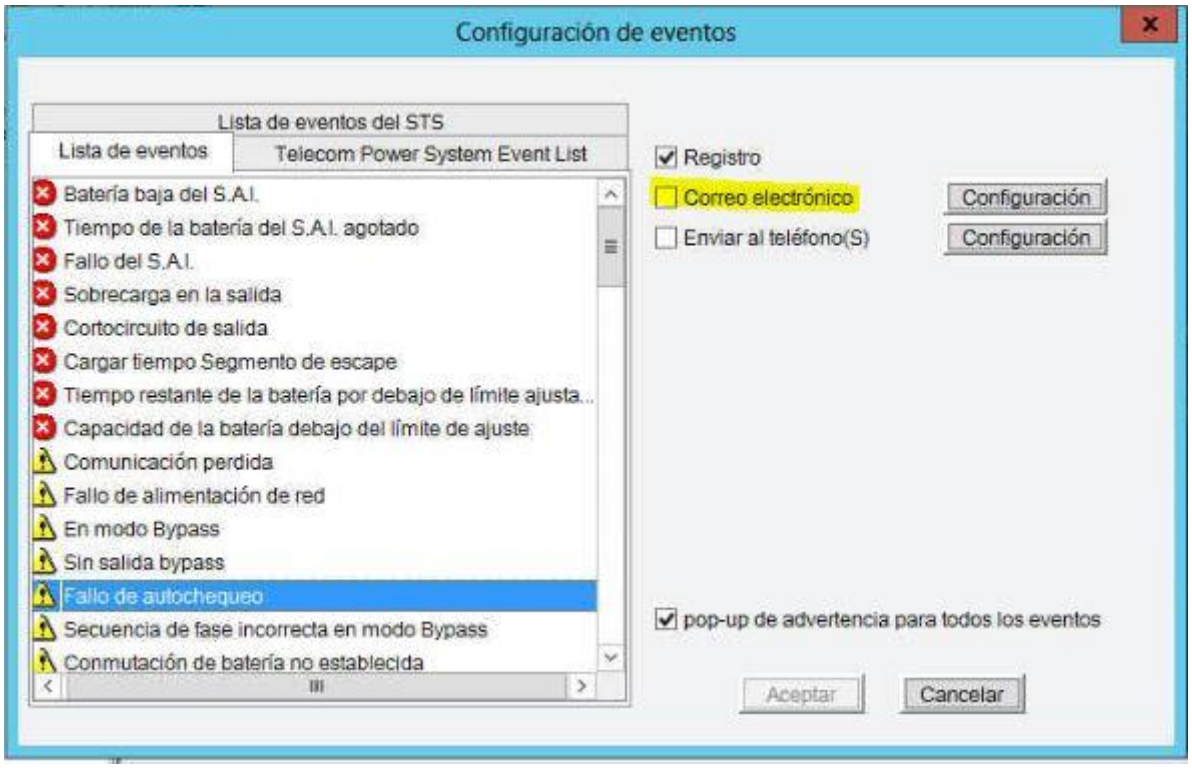



*Ilustración 7. Instalación WinPower 5*

Adicionalmente podemos programar el apagado de equipos dentro de nuestra LAN cuando se produzca algún evento concreto.

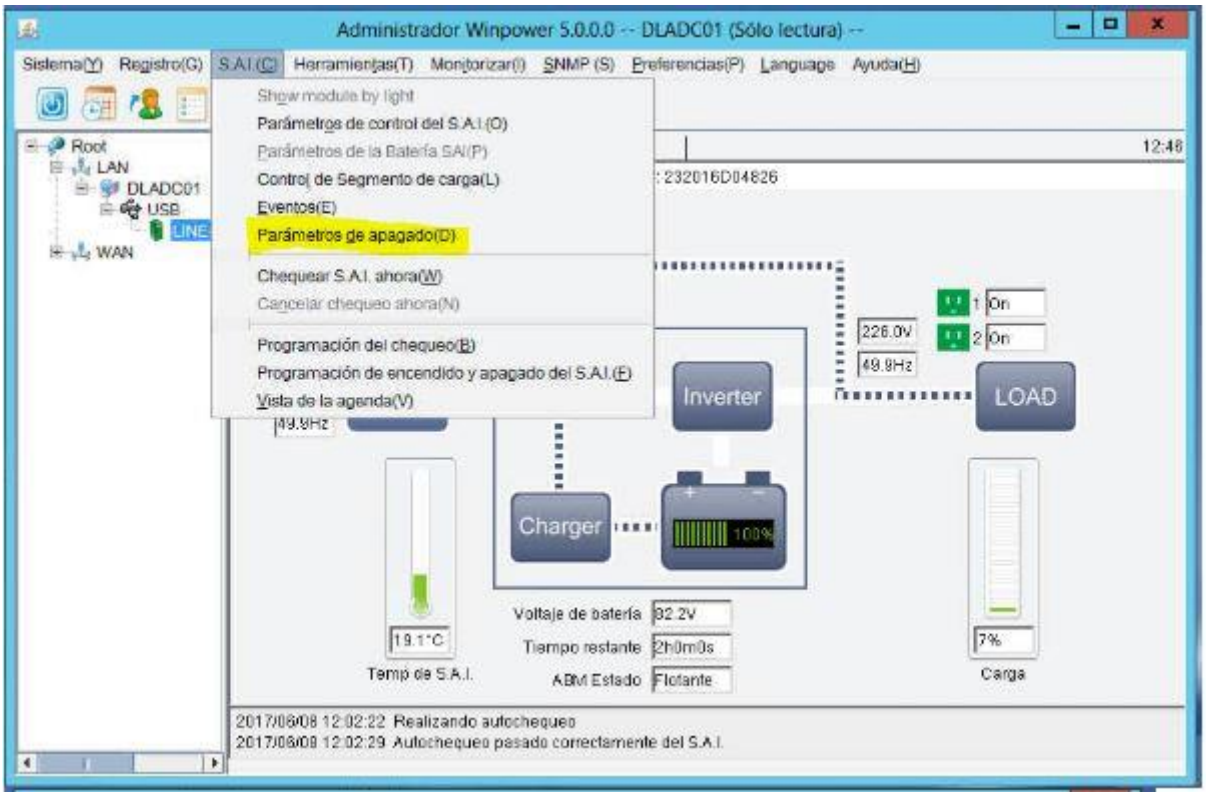



*Ilustración 8. Instalación WinPower 6*

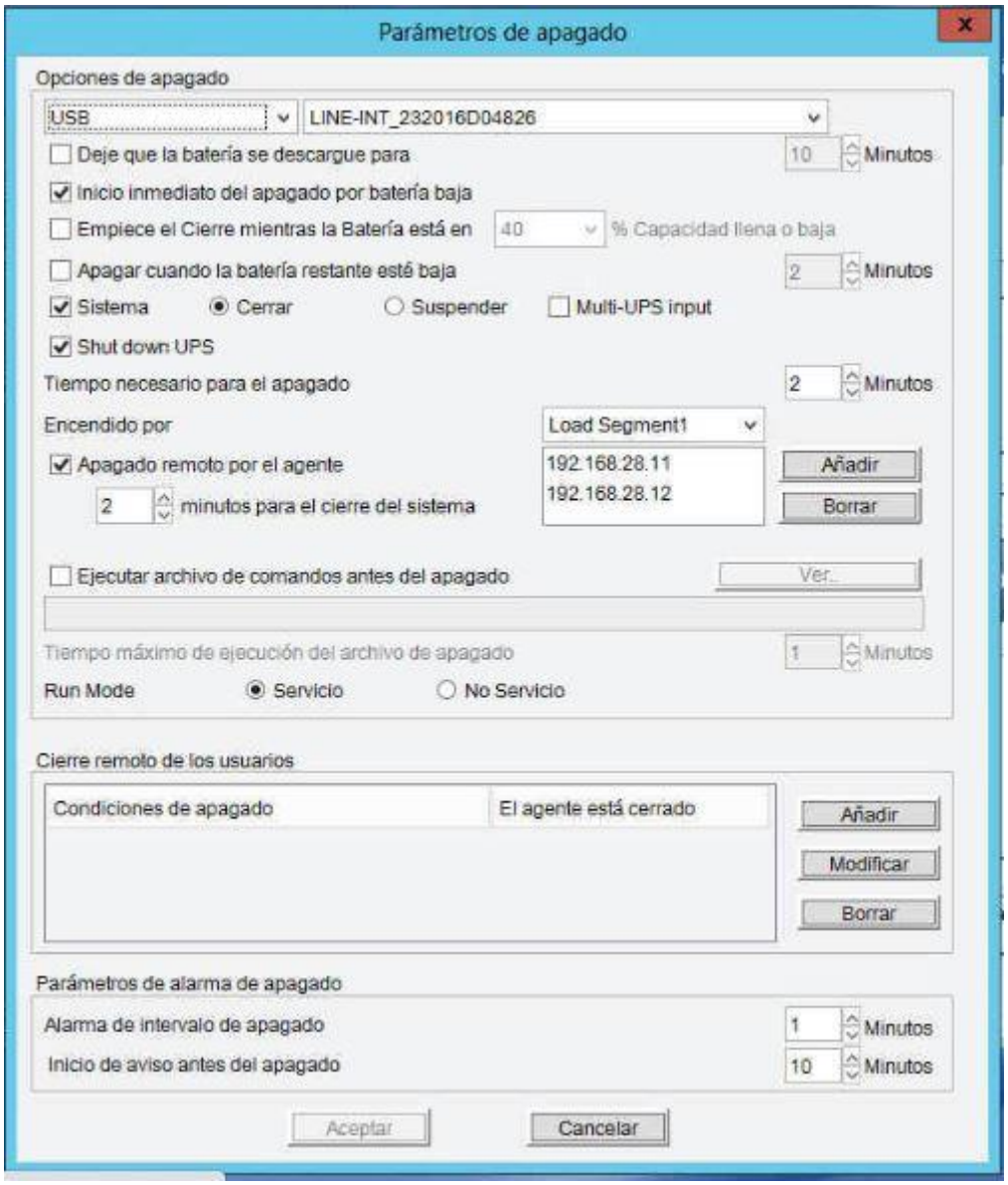



*Ilustración 9. Instalación WinPOwer 7*

#### 2.1.5.1.7 Responsables

Administrador del SI, será el encargado de comprar e instalar los dispositivos SAI en cada una de las zonas descritas anteriormente, debe comprobar que su funcionamiento es correcto. Por último y no menos importante, deberá comprobar que funcionan correctamente una vez cada dos semanas, dentro de estas comprobaciones estaría incluida la comprobación de que las baterías se cargan de manera adecuada, el rendimiento de las baterías es el adecuado, todo eso se debe hacer con los auto test que incluyen los propios SAI.

#### 2.1.5.1.8 Dispositivos

- 1 x SAI 1000VA Online Soho Lapara
- 3 x SAI – Woxter UPS 800 VA

#### 2.1.5.1.9 Costes

- **Implantación**: 250 + (3 x 77.99) = 483.97 €, este es el precio que cuesta comprar todos los SAI. Por otro lado, la instalación la hará el administrador del SI, que en este caso es uno de los dueños de la empresa, por lo tanto, no tendrá costes adicionales.
- **Ejecución y mantenimiento**: 0 €, no cuesta nada ejecutar ni mantener los SAI, sólo energía eléctrica que es prácticamente irrelevante.
- **Búsqueda de irregularidades**: si en algún momento se detecta algún fallo en el funcionamiento de algún SAI, habrá que sustituirlo por otro. Además, hay que tener en cuenta que si el dispositivo está aún en garantía no habrá que pagar ningún coste adicional, sino habrá que comprar otro dispositivo completamente igual al que se haya estropeado.

#### 2.1.5.1.10 Rentabilidad

El corte de luz o corte de suministro eléctrico puede conllevar pérdida de datos, y como ya hemos estudiado es un problema muy grave, por lo que realizar este control sería muy importante. Además, los picos de tensión también son bastante graves y pueden producir daños en los equipos, por eso debemos conectar todos los terminales a un dispositivo SAI, ya que es más económico cambiar un SAI que un ordenador.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar estos controles en nuestro SI. Vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 80 % ya que:

- Puede fallar por un error de conexión del SAI a la red eléctrica.
- Puede fallar por un error de conexión del PC al SAI.
- Puede fallar por una mala configuración.
- Puede fallar por olvido de revisión del responsable.

Se va a hacer una pequeña descripción para ver el significado de la tabla que utilizamos para el cálculo de la rentabilidad del control. La primera fila representa los valores que tendríamos sin tener el control implantado y la segunda fila con el control implantado. Con respecto a la primera columna, se trata del riesgo residual sin el control y con el control. En cuanto a la segunda columna, se trata del coste que tiene la implantación, en la primera fila siempre es 0, porque no está el control implantado y en la segunda fila, es el coste de implantación del control. En la tercera columna, tenemos en la primera fila un 0 porque al no estar el control implantado el valor es cero, y en la segunda fila el coste de estar ejecutando el control.

Por último, tenemos las siguientes 5 columnas que se corresponden con el valor en los 5 años, en la primera fila es el riesgo residual sin ejecutar el control y en la segunda fila tendremos el valor de cada año con el control puesto. Debemos destacar que en la segunda fila del primer año debemos sumar los valores del coste de implantación y en la de la segunda columna, debemos sumar el valor de ejecución. El valor de los años se va sumando con el anterior para de esta manera poder estudiar cómo evoluciona la rentabilidad del control.

Para estudiar la rentabilidad, comparamos en la gráfica los valores que tenemos sin control y con otros, y de esta manera queda representado de manera gráfica como de rentable es el control.

Activo: Información pacientes (S1)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 36383,73 | 483,97 | 0 | 36867,7 | 73251,43 | 109635,16 | 146018,89 | 182402,62 |

***Tabla 23. Rentabilidad amenaza AUX1 - [I.6] activo S1***

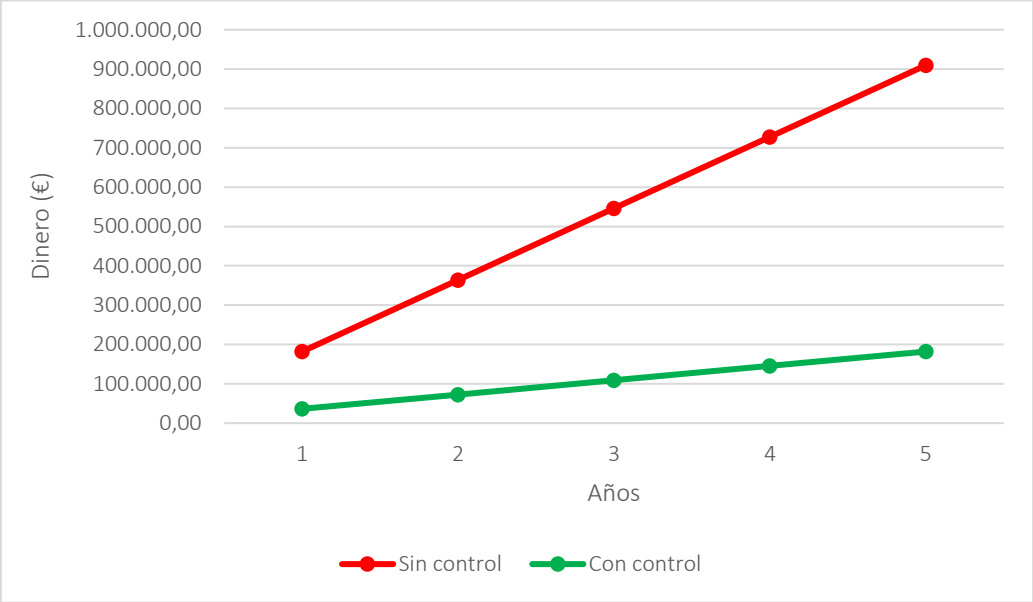



*Ilustración 10. Rentabilidad amenaza AUX - [I.6] activo S1*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,6 | 3638373,24 | 5457559,86 | 7276746,48 | 9095933,1 |
| 363837,32 | 483,97 | 0 | 364321,29 | 728158,61 | 1091995,93 | 1455833,25 | 1819670,57 |

*Tabla 24. Rentabilidad amenaza HW1 - [I.5] activo S1*

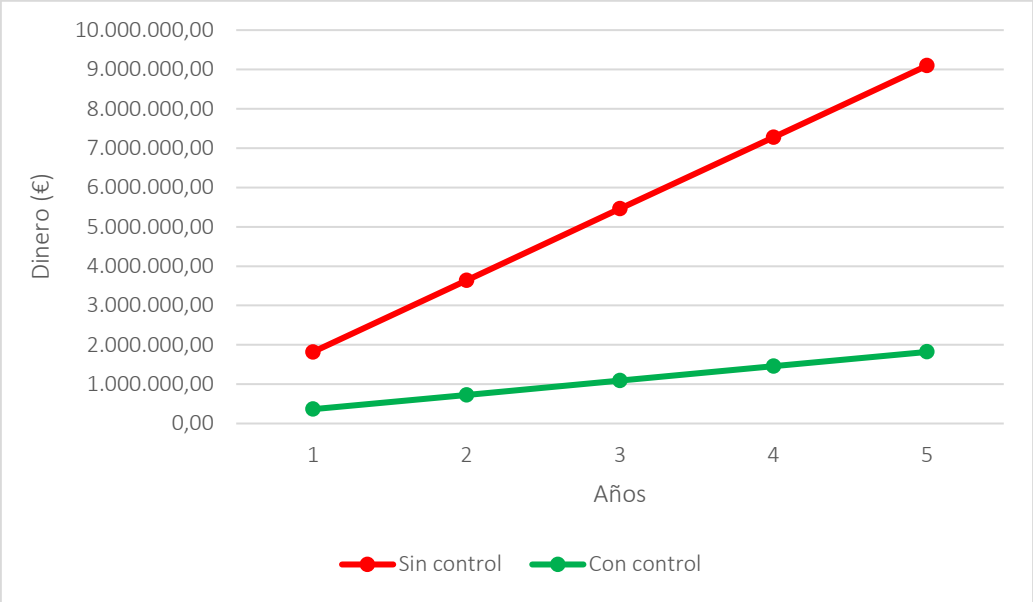



*Ilustración 11. Rentabilidad amenaza HW1 - [I.5] activo S1*

Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,6 | 3638373,24 | 5457559,86 | 7276746,48 | 9095933,1 |
| 363837,32 | 483,97 | 0 | 364321,29 | 728158,61 | 1091995,93 | 1455833,25 | 1819670,57 |

*Tabla 25. Rentabilidad amenaza HW1 - [I.6] activo S1*

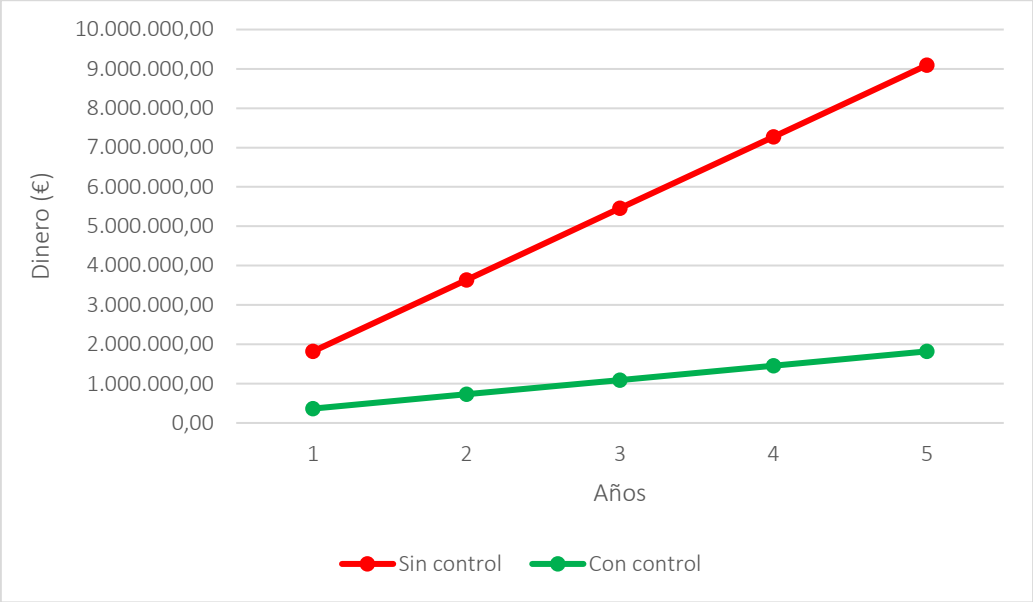



*Ilustración 12. Rentabilidad amenaza HW1 - [I.6] activo S1*

## Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,6 | 3638373,24 | 5457559,86 | 7276746,48 | 9095933,1 |
| 363837,32 | 483,97 | 0 | 364321,29 | 728158,61 | 1091995,93 | 1455833,25 | 1819670,57 |

*Tabla 26. Rentabilidad amenaza SW1 - [I.5] activo S1*

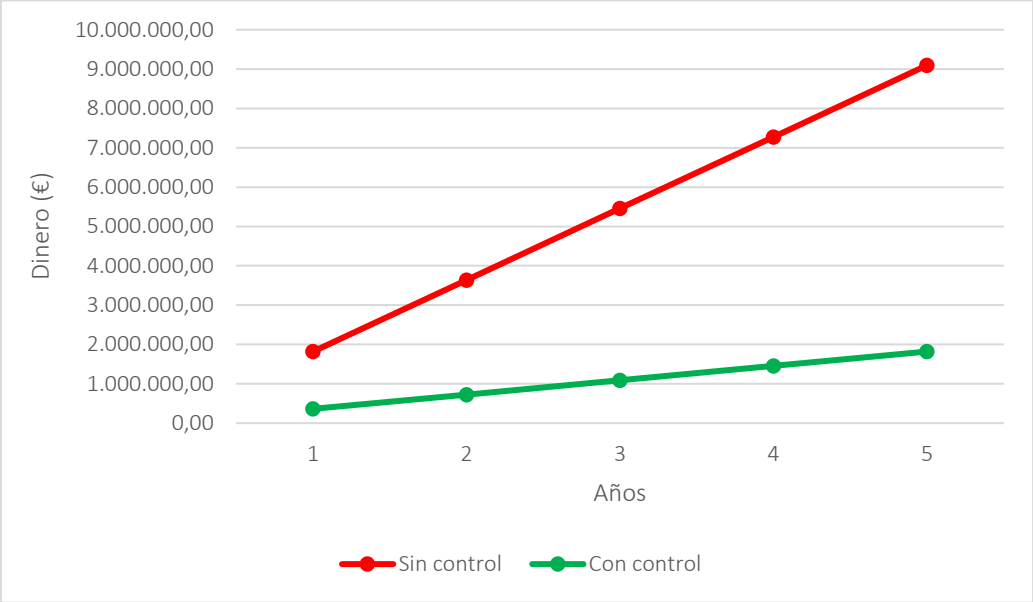



*Ilustración 13. Rentabilidad amenaza SW1 - [I.5] activo S1*

Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,6 | 3638373,24 | 5457559,86 | 7276746,48 | 9095933,1 |
| 363837,32 | 483,97 | 0 | 364321,29 | 728158,61 | 1091995,93 | 1455833,25 | 1819670,57 |

*Tabla 27. Rentabilidad amenaza SRVD1 - [I.5] activo S1*

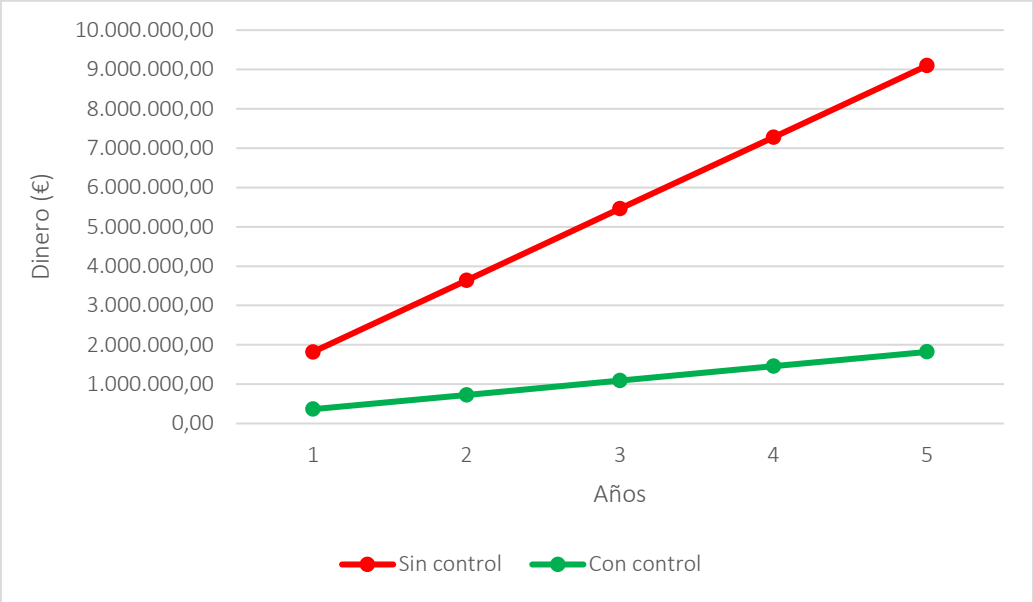



*Ilustración 14. Rentabilidad amenaza SRVD1 - [I.5] activo S1*

Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,6 | 3638373,24 | 5457559,86 | 7276746,48 | 9095933,1 |
| 363837,32 | 483,97 | 0 | 364321,29 | 728158,61 | 1091995,93 | 1455833,25 | 1819670,57 |

***Tabla 28. Rentabilidad amenaza SRVD1 - [I.6] activo S1***

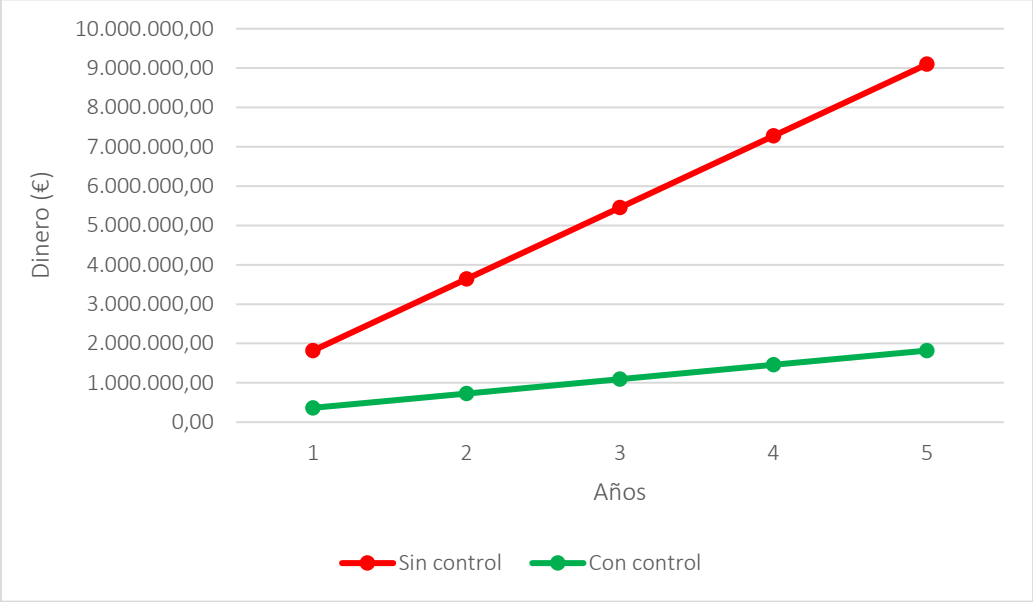



***Ilustración 15. Rentabilidad amenaza SRVD1 - [I.6] activo S1***

Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 303197,77 | 0 | 0 | 303197,77 | 606395,54 | 909593,31 | 1212791,08 | 1515988,85 |
| 60639,55 | 483,97 | 0 | 61123,52 | 121763,07 | 182402,62 | 243042,17 | 303681,72 |

***Tabla 29. Rentabilidad amenaza T1 - [I.5] activo S1***

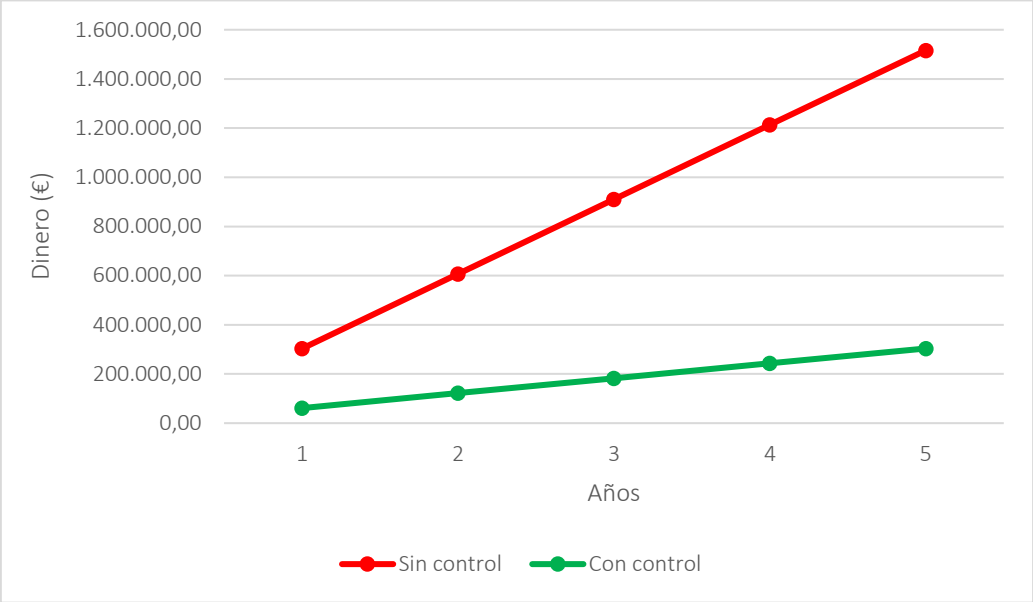



*Ilustración 16. Rentabilidad amenaza T1 - [I.5] activo S1*

Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 60639,55 | 0 | 0 | 60639,55 | 121279,1 | 181918,65 | 242558,2 | 303197,75 |
| 12127,91 | 483,97 | 0 | 12611,88 | 24739,79 | 36867,7 | 48995,61 | 61123,52 |

*Tabla 30. Rentabilidad amenaza T1 - [I.6] activo S1*

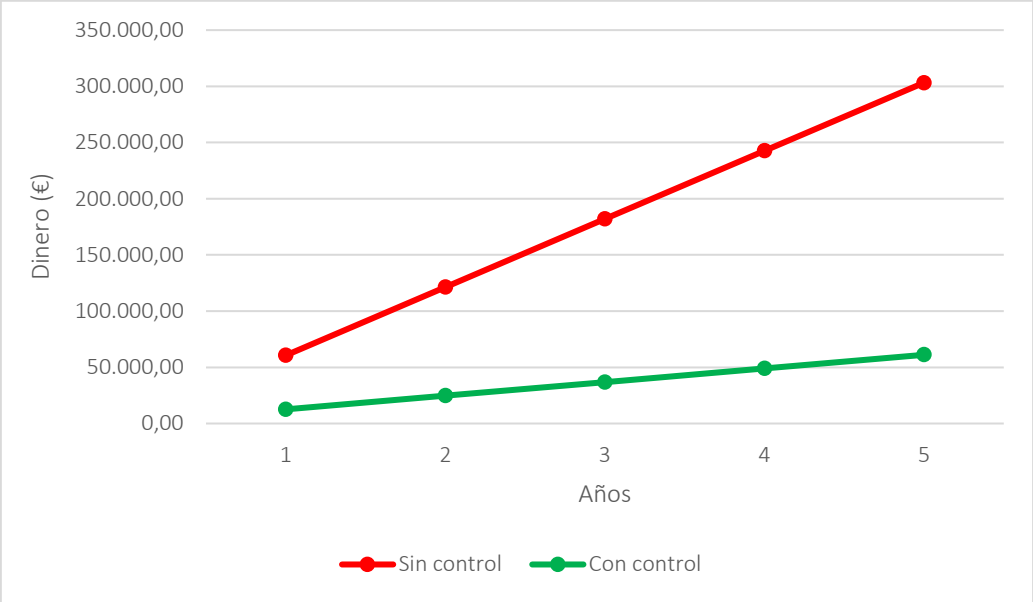



*Ilustración 17. Rentabilidad amenaza T1- [I.6] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 24375,66 | 483,97 | 0 | 24859,63 | 49235,29 | 73610,95 | 97986,61 | 122362,27 |

*Tabla 31. Rentabilidad amenaza AUX1 - [I.6] activo S2*

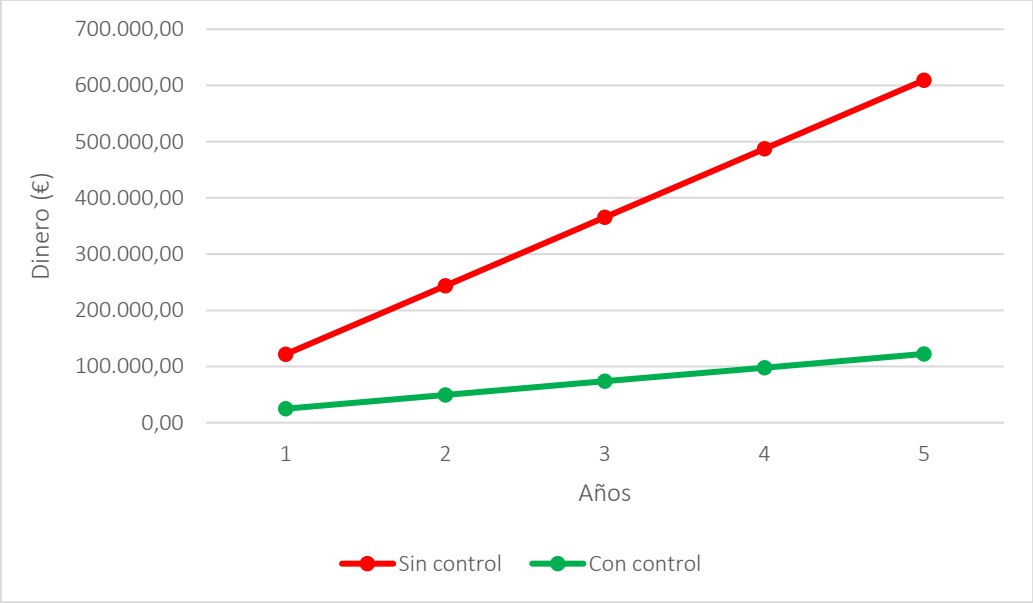



*Ilustración 18. Rentabilidad amenaza AUX1 - [I.6] activo S2*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 32. Rentabilidad amenaza HW1 - [I.5] activo S2*

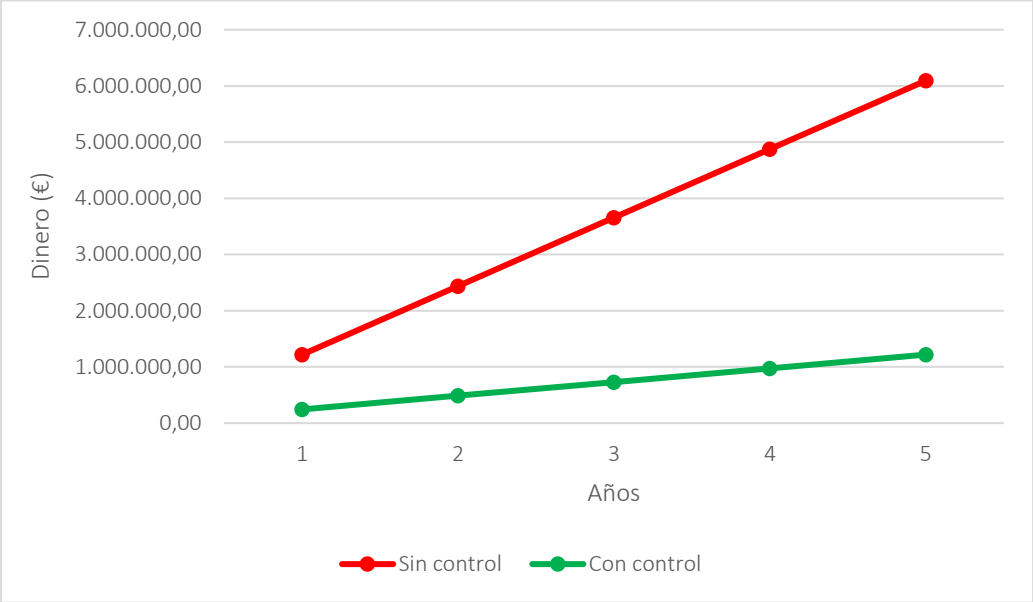



*Ilustración 19. Rentabilidad amenaza HW1 - [I.5] activo S2*

Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 33. Rentabilidad amenaza HW1 - [I.6] activo S2*

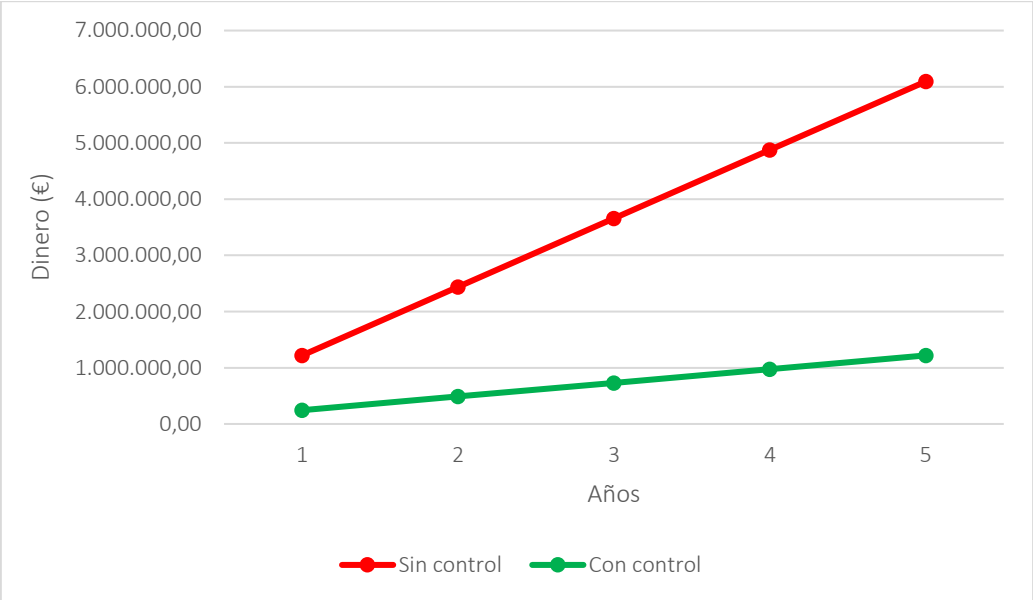



*Ilustración 20. Rentabilidad amenaza HW1 - [I.6] activo S2*

## Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 34. Rentabilidad amenaza SW1 - [I.5] activo S2*

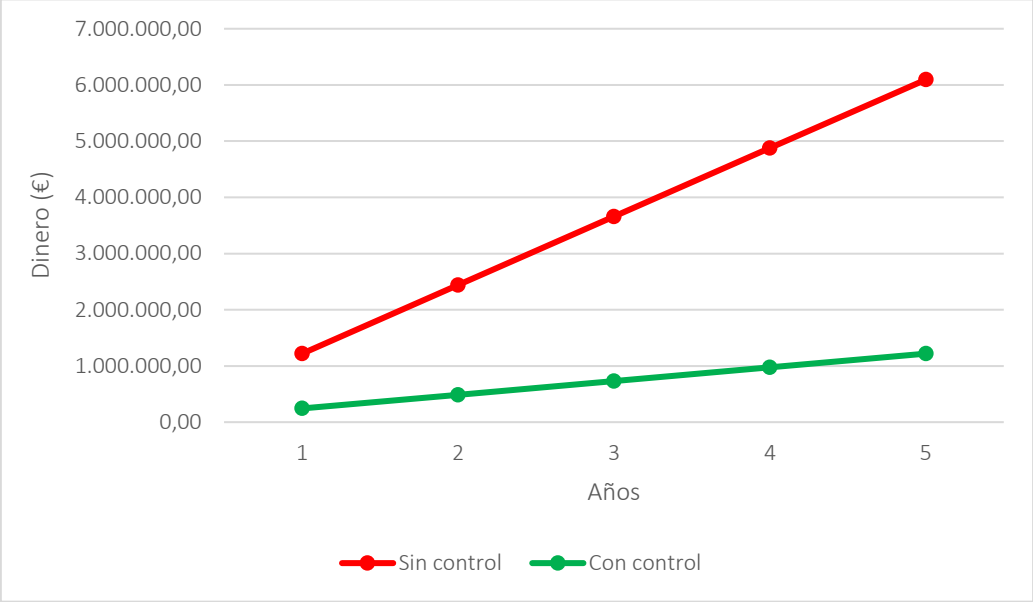



*Ilustración 21. Rentabilidad amenaza SW1 - [I.5] activo S2*

## Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 35. Rentabilidad amenaza SRVD1 - [I.5] activo S2*

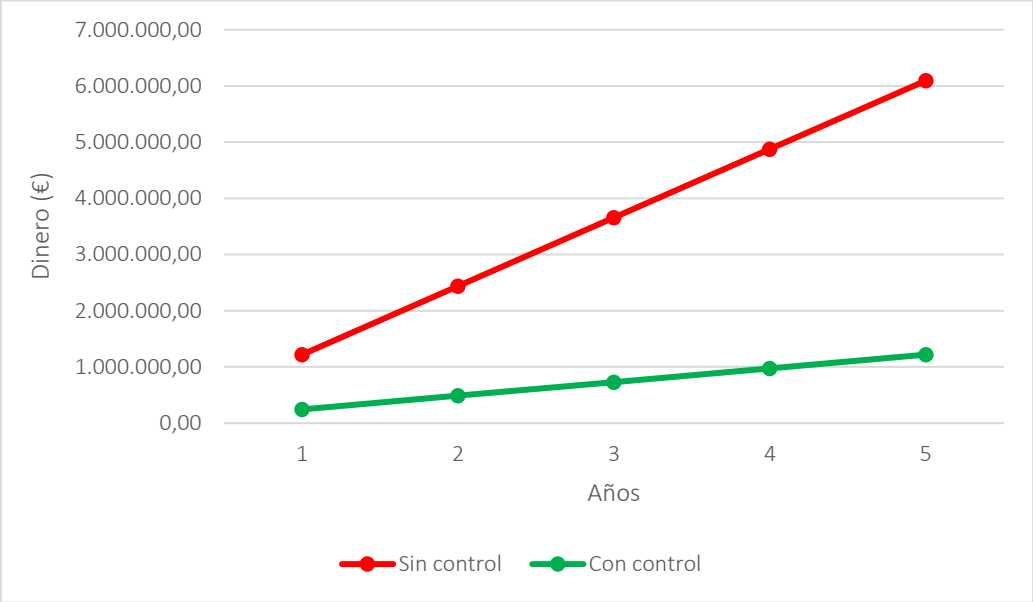



*Ilustración 22. Rentabilidad amenaza SRVD1 - [I.5] activo S2*

## Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 36. Rentabilidad amenaza SRVD1 - [I.6] activo S2*

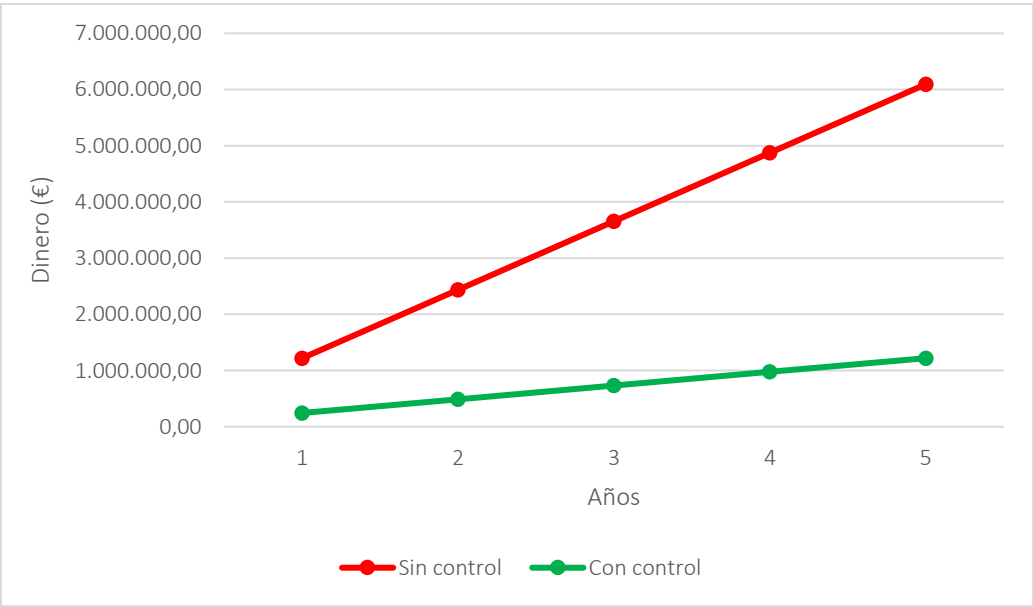



*Ilustración 23. Rentabilidad amenaza SRVD1 - [I.6] activo S2*

## Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 203130,5 | 0 | 0 | 203130,5 | 406261 | 609391,5 | 812522 | 1015652,5 |
| 40626,1 | 483,97 | 0 | 41110,07 | 81736,17 | 122362,27 | 162988,37 | 203614,47 |

*Tabla 37. Rentabilidad amenaza T1 - [I.5] activo S2*

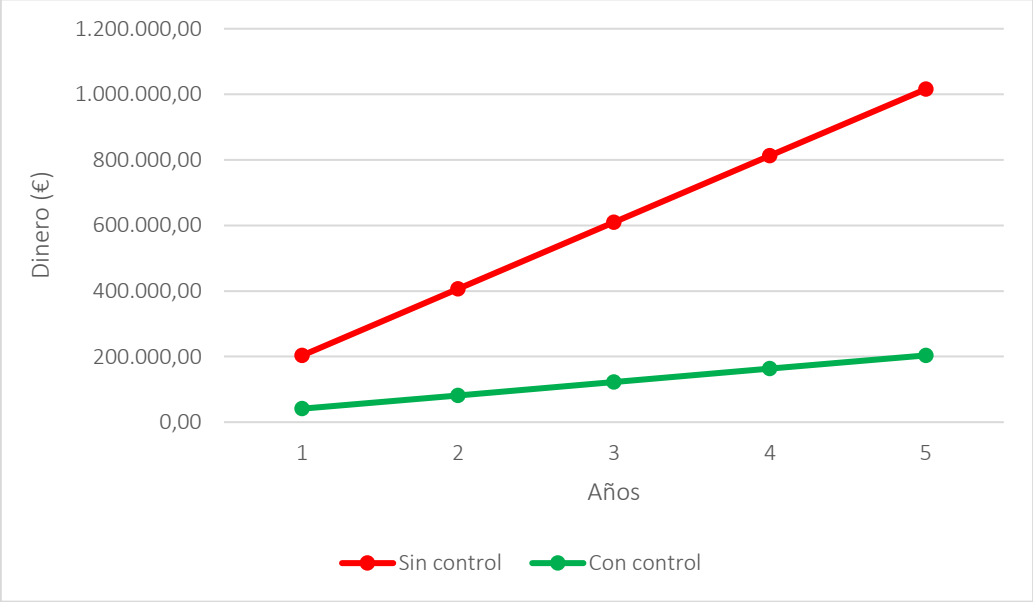



*Ilustración 24. Rentabilidad amenaza T1 - [I.5] activo S2*

## Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 40626,1 | 0 | 0 | 40626,1 | 81252,2 | 121878,3 | 162504,4 | 203130,5 |
| 8125,22 | 483,97 | 0 | 8609,19 | 16734,41 | 24859,63 | 32984,85 | 41110,07 |

*Tabla 38. Rentabilidad amenaza T1 - [I.6] activo S2*

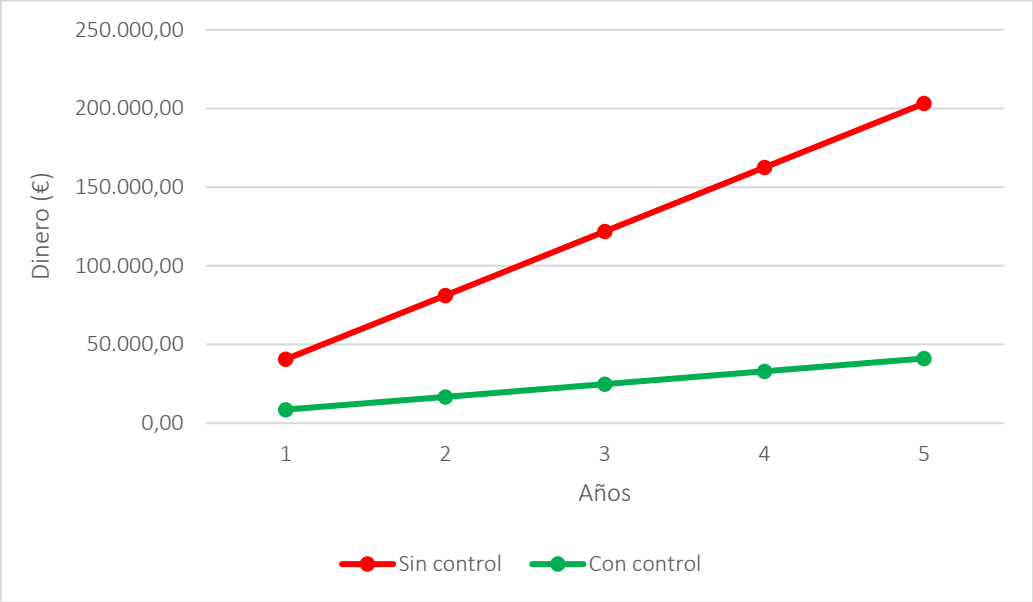



*Ilustración 25. Rentabilidad amenaza T1 - [I.6] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 24375,66 | 483,97 | 0 | 24859,63 | 49235,29 | 73610,95 | 97986,61 | 122362,27 |

*Tabla 39. Rentabilidad amenaza AUX1 - [I.6] activo S3*

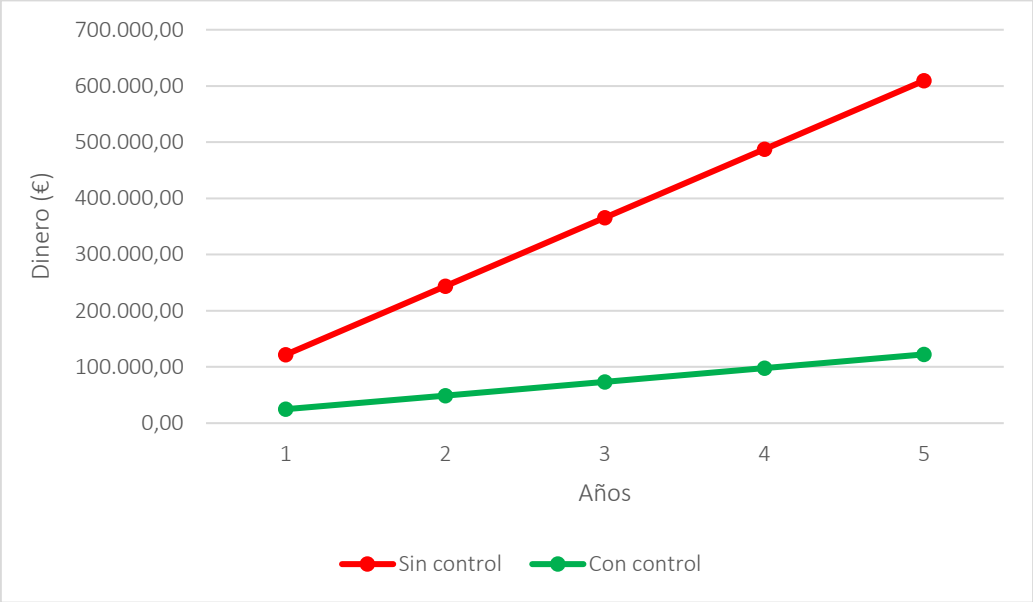



*Ilustración 26. Rentabilidad amenaza AUX1 - [I.6] activo S3*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 40. Rentabilidad amenaza HW1 - [I.5] activo S3*

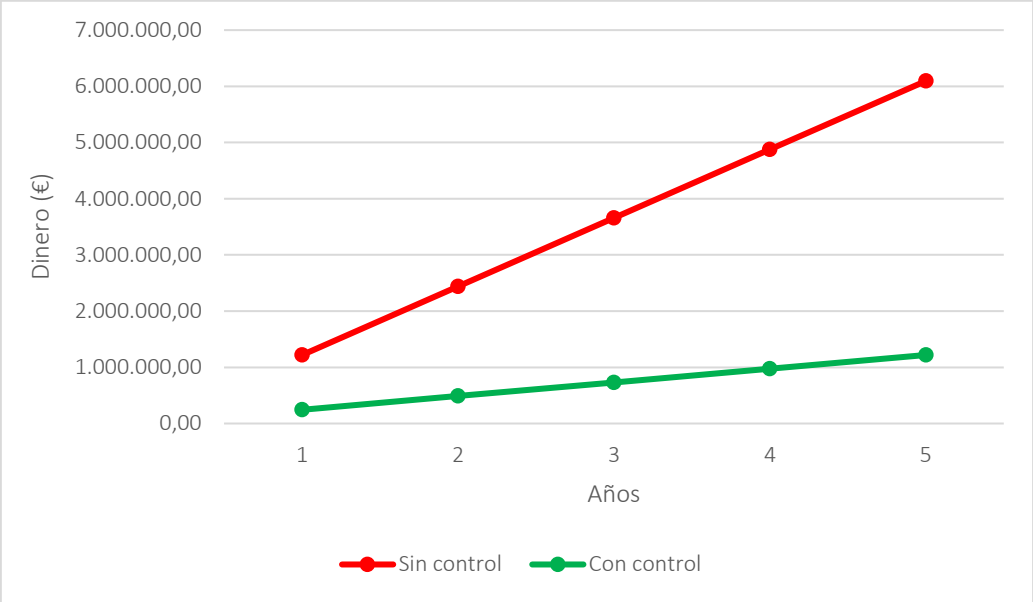



*Ilustración 27. Rentabilidad amenaza HW1 - [I.5] activo S3*

Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 41. Rentabilidad amenaza HW1 - [I.6] activo S3*

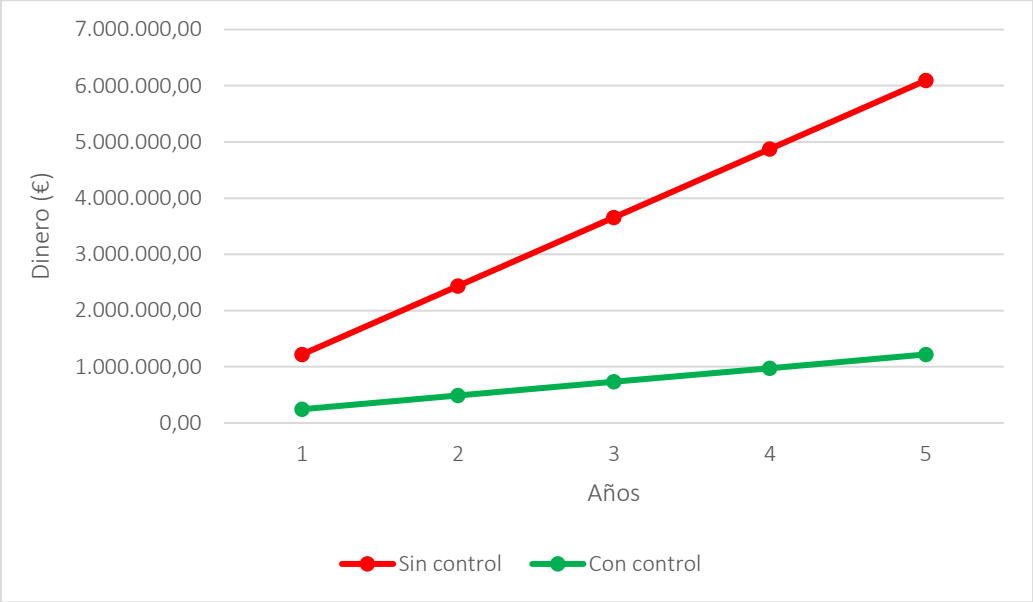



*Ilustración 28. Rentabilidad amenaza HW1 - [I.6] activo S3*

## Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 42. Rentabilidad amenaza SW1 - [I.5] activo S3*

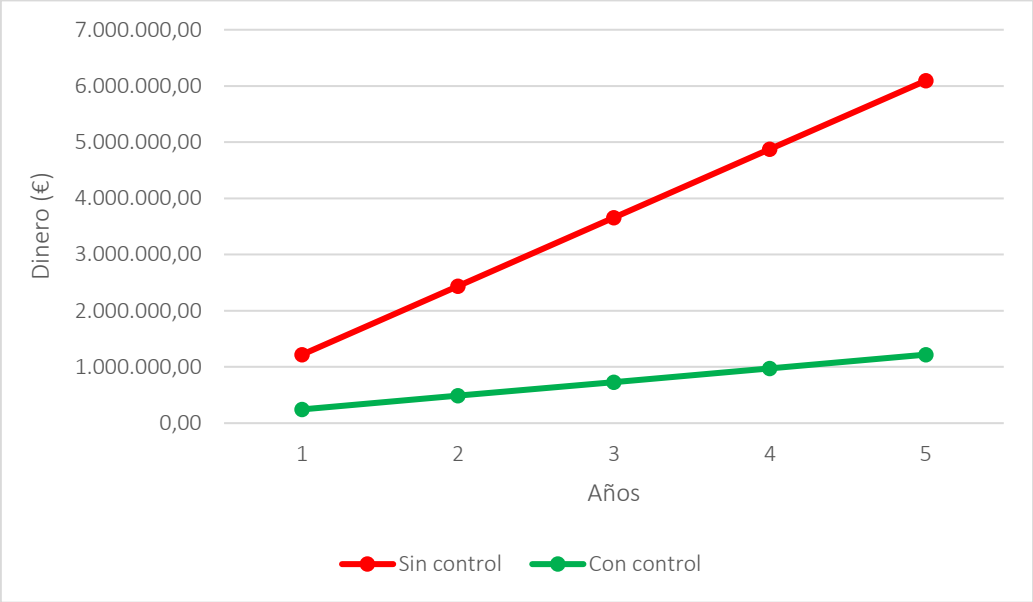



*Ilustración 29. Rentabilidad amenaza SW1 - [I.5] activo S3*

Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 43. Rentabilidad amenaza SRVD1 - [I.5] activo S3*

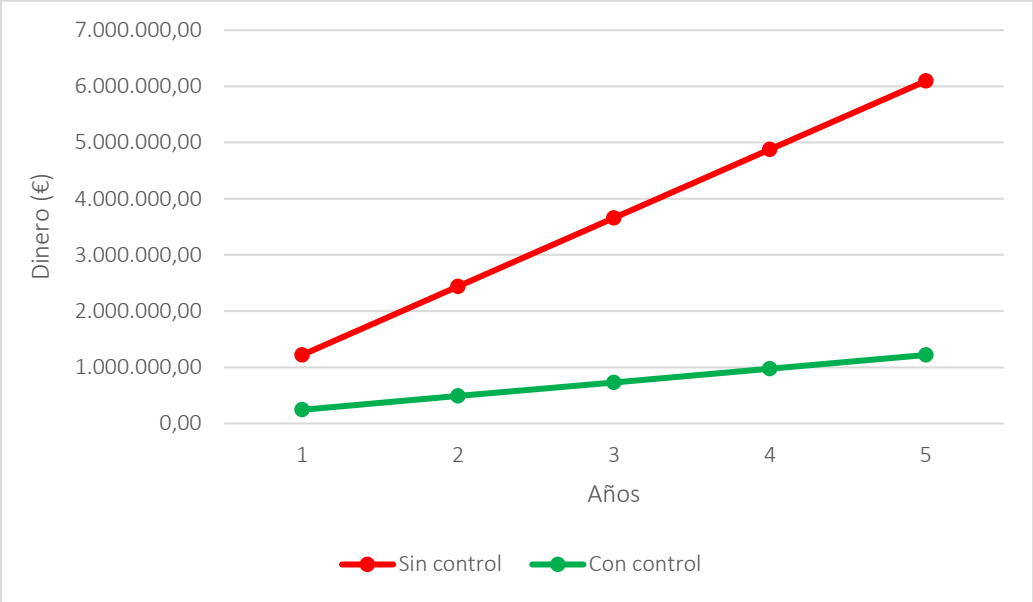



*Ilustración 30. Rentabilidad amenaza SRVD1 - [I.5] activo S3*

Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 44. Rentabilidad amenaza SRVD1 - [I.6] activo S3*

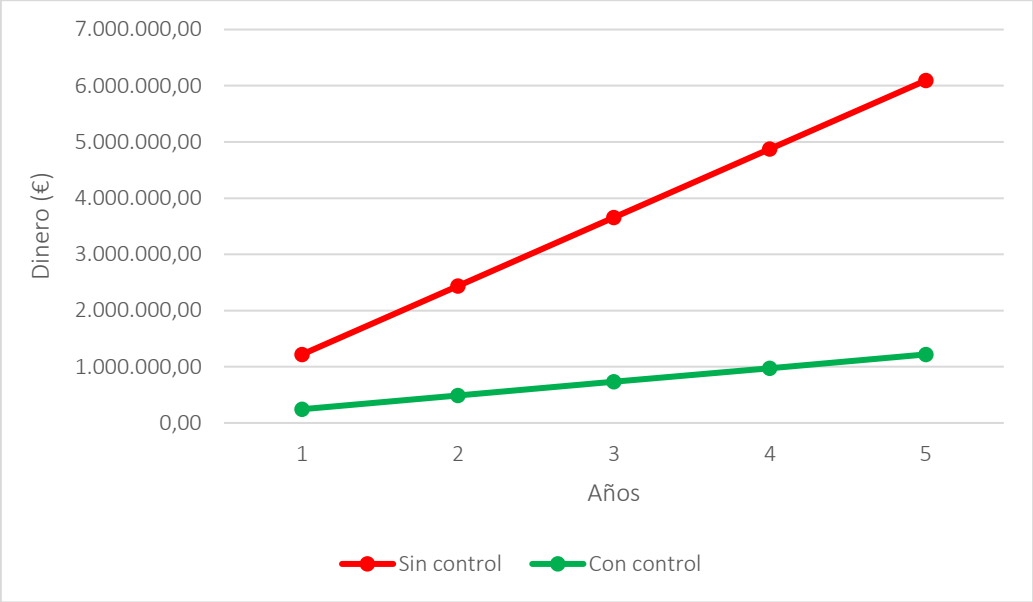



*Ilustración 31. Rentabilidad amenaza SRVD1 - [I.6] activo S3*

## Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 203130,5 | 0 | 0 | 203130,5 | 406261 | 609391,5 | 812522 | 1015652,5 |
| 40626,1 | 483,97 | 0 | 41110,07 | 81736,17 | 122362,27 | 162988,37 | 203614,47 |

*Tabla 45. Rentabilidad amenaza T1 - [I.5] activo S3*

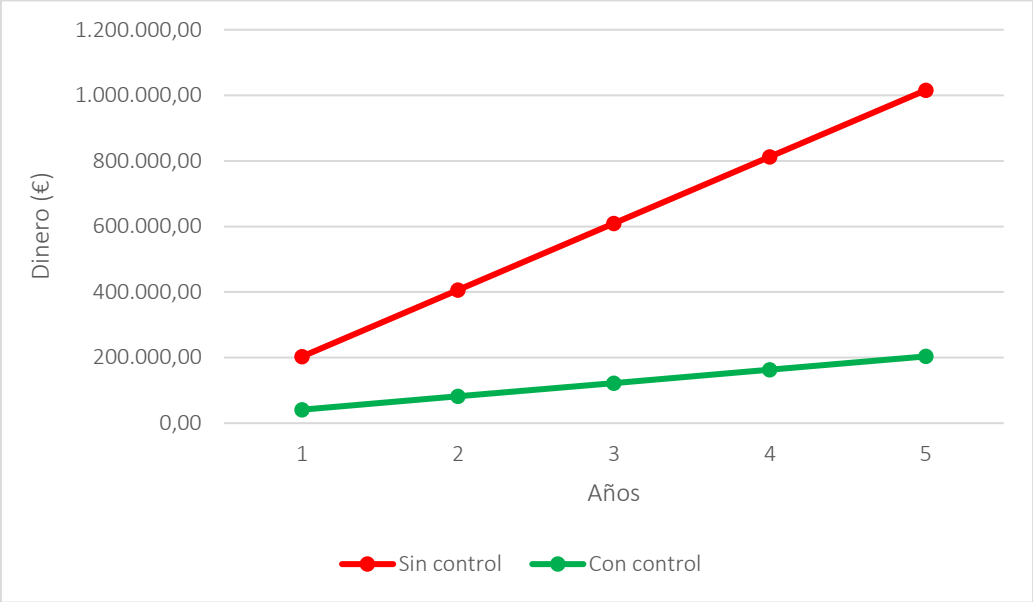



*Ilustración 32. Rentabilidad amenaza T1 - [I.5] activo S3*

Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 40626,1 | 0 | 0 | 40626,1 | 81252,2 | 121878,3 | 162504,4 | 203130,5 |
| 8125,22 | 483,97 | 0 | 8609,19 | 16734,41 | 24859,63 | 32984,85 | 41110,07 |

*Tabla 46. Rentabilidad amenaza T1 - [I.6] activo S3*

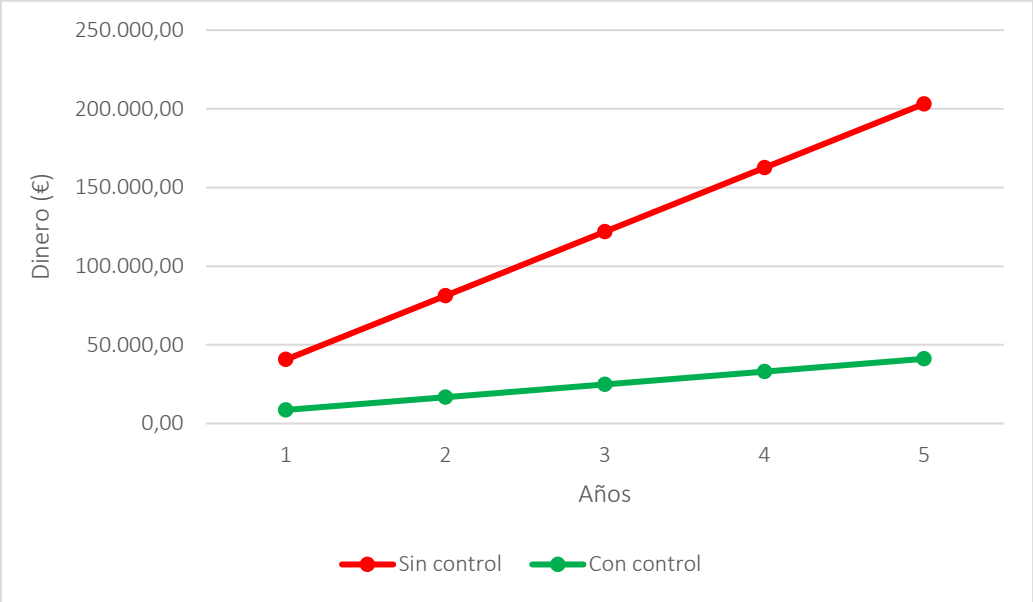



*Ilustración 33. Rentabilidad amenaza T1 - [I.6] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 24375,03 | 483,97 | 0 | 24859 | 49234,03 | 73609,06 | 97984,09 | 122359,12 |

*Tabla 47. Rentabilidad amenaza AUX1 - [I.6] activo S4*

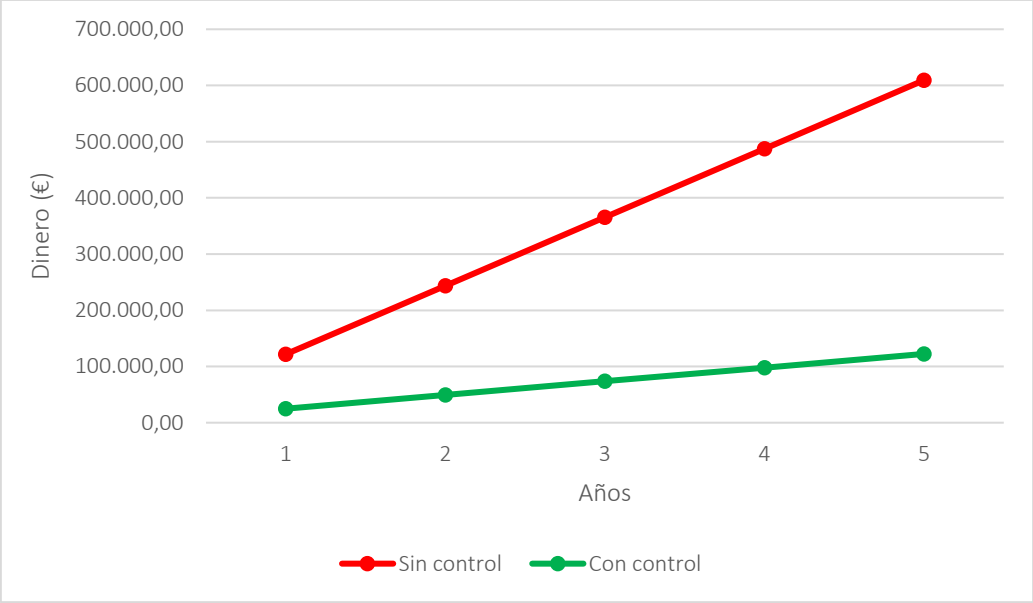



*Ilustración 34. Rentabilidad amenaza AUX1 - [I.6] activo S4*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 243750,28 | 483,97 | 0 | 244234,25 | 487984,53 | 731734,81 | 975485,09 | 1219235,37 |

*Tabla 48. Rentabilidad amenaza HW1 - [I.5] activo S4*

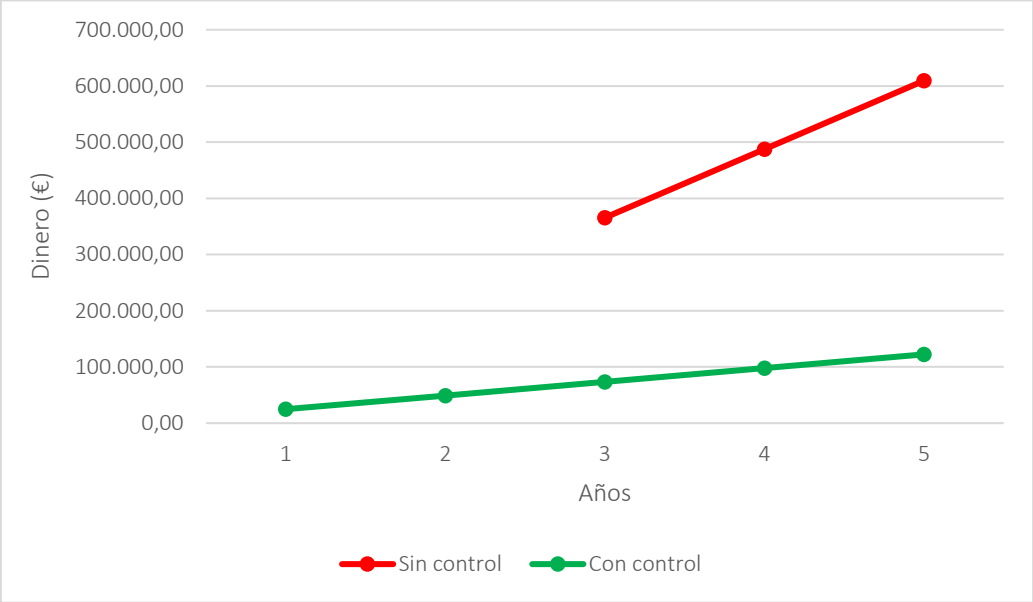



*Ilustración 35. Rentabilidad amenaza HW1 - [I.5] activo S4*

## Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 243750,28 | 483,97 | 0 | 244234,25 | 487984,53 | 731734,81 | 975485,09 | 1219235,37 |

*Tabla 49. Rentabilidad amenaza HW1 - [I.6] activo S4*

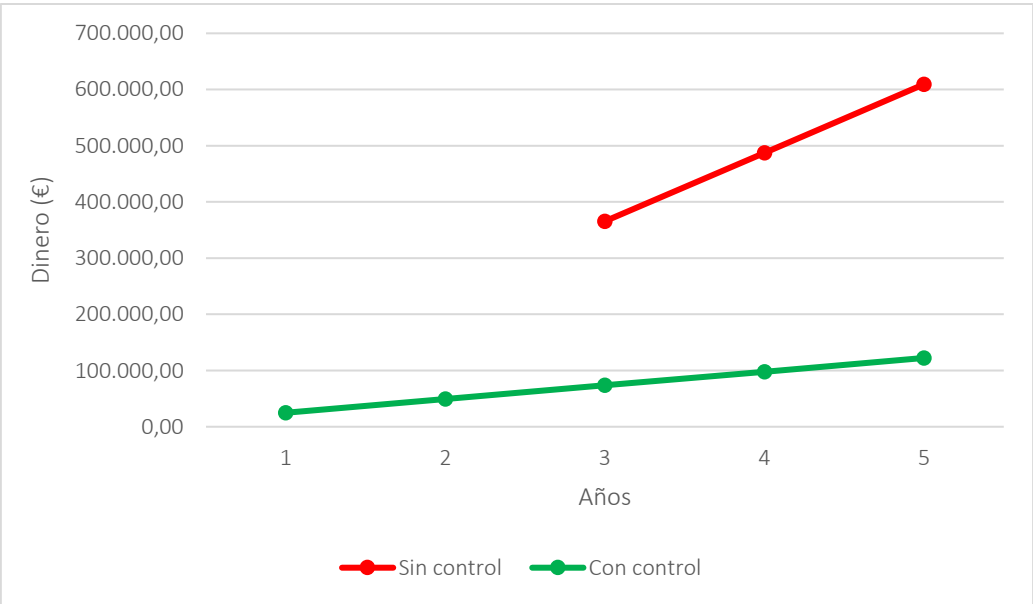



*Ilustración 36. Rentabilidad amenaza HW1 - [I.6] activo S4*

Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 243750,28 | 483,97 | 0 | 244234,25 | 487984,53 | 731734,81 | 975485,09 | 1219235,37 |

*Tabla 50. Rentabilidad amenaza SW1 - [I.5] activo S4*

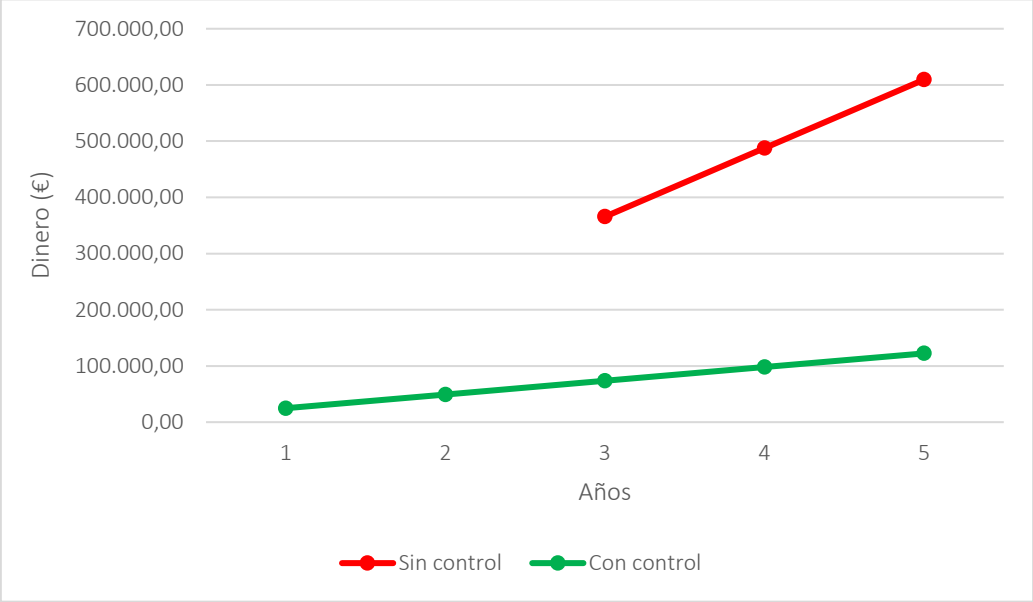



*Ilustración 37. Rentabilidad amenaza SW1 - [I.5] activo S4*

Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 243750,28 | 483,97 | 0 | 244234,25 | 487984,53 | 731734,81 | 975485,09 | 1219235,37 |

*Tabla 51. Rentabilidad amenaza SRVD1 - [I.5] activo S4*

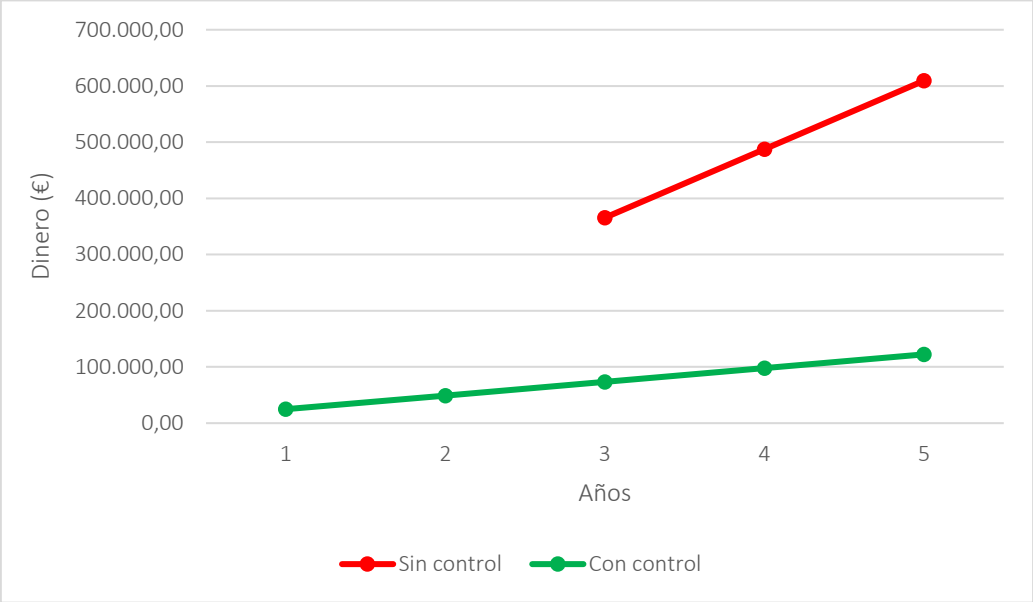



*Ilustración 38. Rentabilidad amenaza SRVD1 - [I.5] activo S4*

## Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 243750,28 | 483,97 | 0 | 244234,25 | 487984,53 | 731734,81 | 975485,09 | 1219235,37 |

*Tabla 52. Rentabilidad amenaza SRVD1 - [I.6] activo S4*

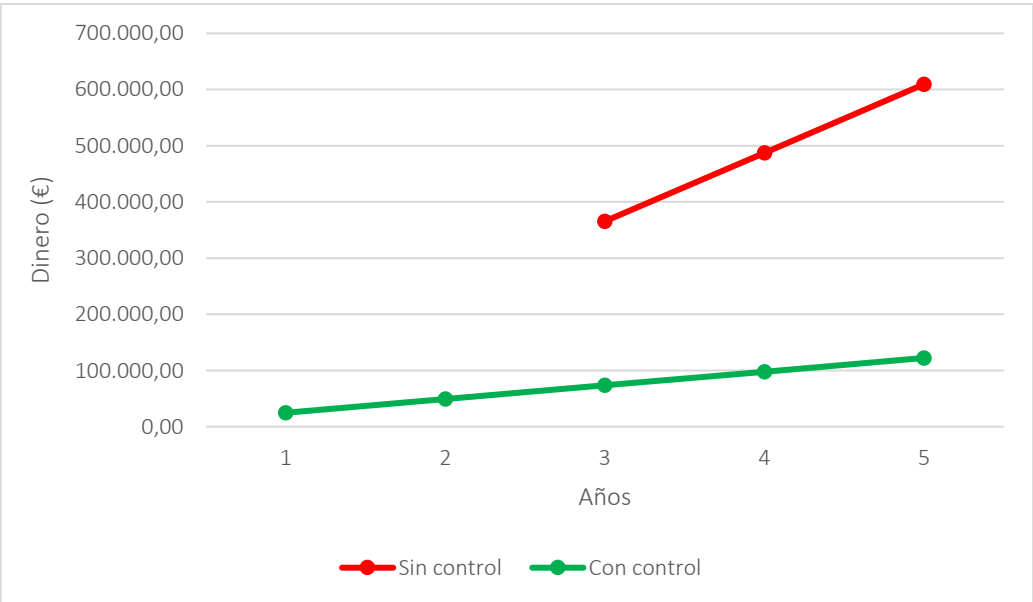



*Ilustración 39. Rentabilidad amenaza SRVD1 - [I.6] activo S4*

## Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 203125,24 | 0 | 0 | 203125,24 | 406250,48 | 609375,72 | 812500,96 | 1015626,2 |
| 40625,05 | 483,97 | 0 | 41109,02 | 81734,07 | 122359,12 | 162984,17 | 203609,22 |

*Tabla 53. Rentabilidad amenaza T1 - [I.5] activo S4*

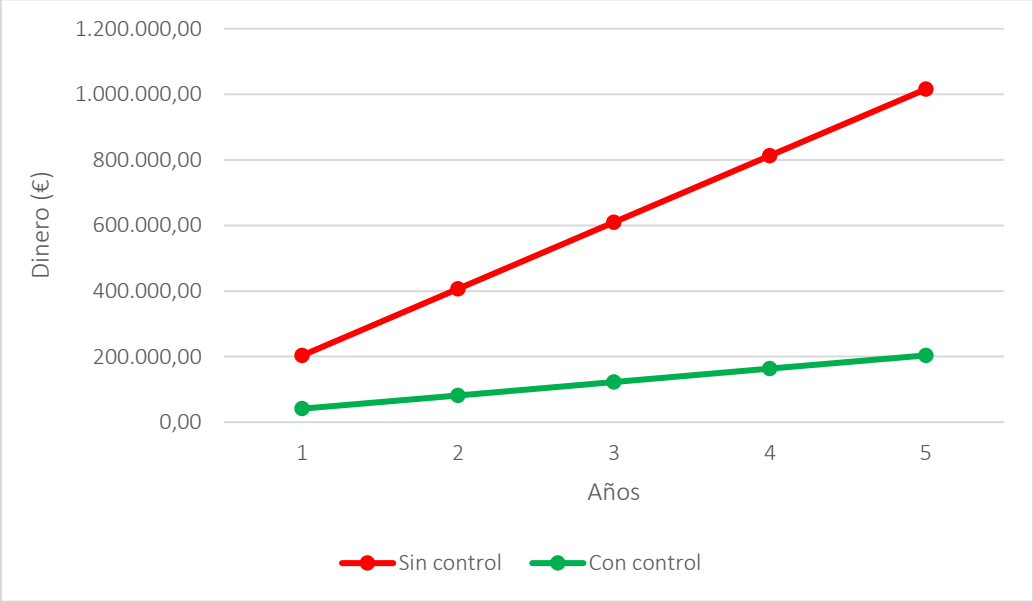



*Ilustración 40. Rentabilidad amenaza T1 - [I.5] activo S4*

## Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 40625,05 | 0 | 0 | 40625,05 | 81250,1 | 121875,15 | 162500,2 | 203125,25 |
| 8125,01 | 483,97 | 0 | 8608,98 | 16733,99 | 24859 | 32984,01 | 41109,02 |

*Tabla 54. Rentabilidad amenaza T1 - [I.6] activo S4*

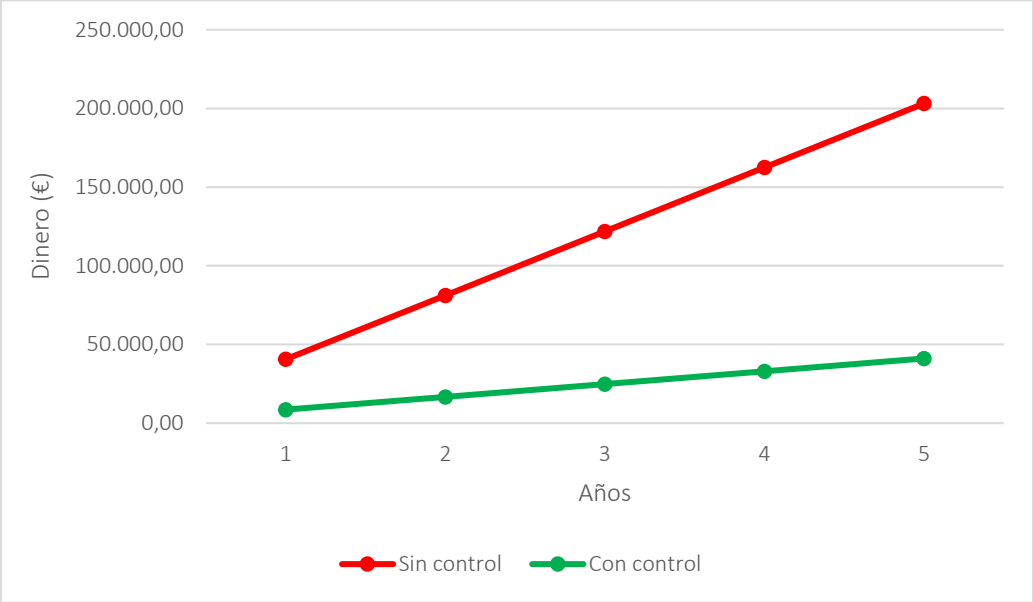



*Ilustración 41. Rentabilidad amenaza T1 - [I.6] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 24375,66 | 483,97 | 0 | 24859,63 | 49235,29 | 73610,95 | 97986,61 | 122362,27 |

*Tabla 55. Rentabilidad amenaza AUX1 - [I.6] activo S5*

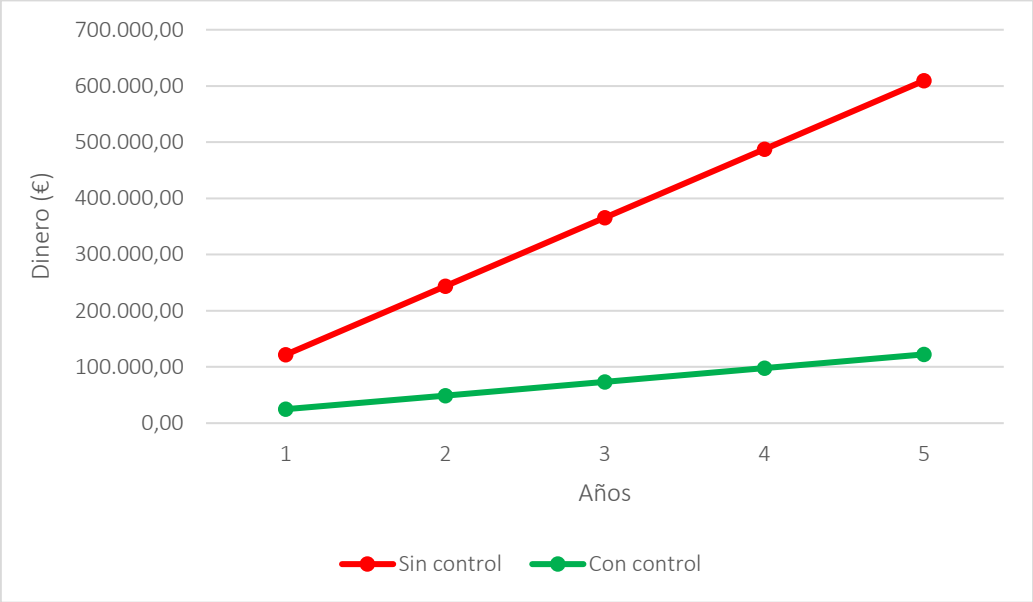



*Ilustración 42. Rentabilidad amenaza AUX1 - [I.6] activo S5*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 56. Rentabilidad amenaza HW1 - [I.5] activo S5*

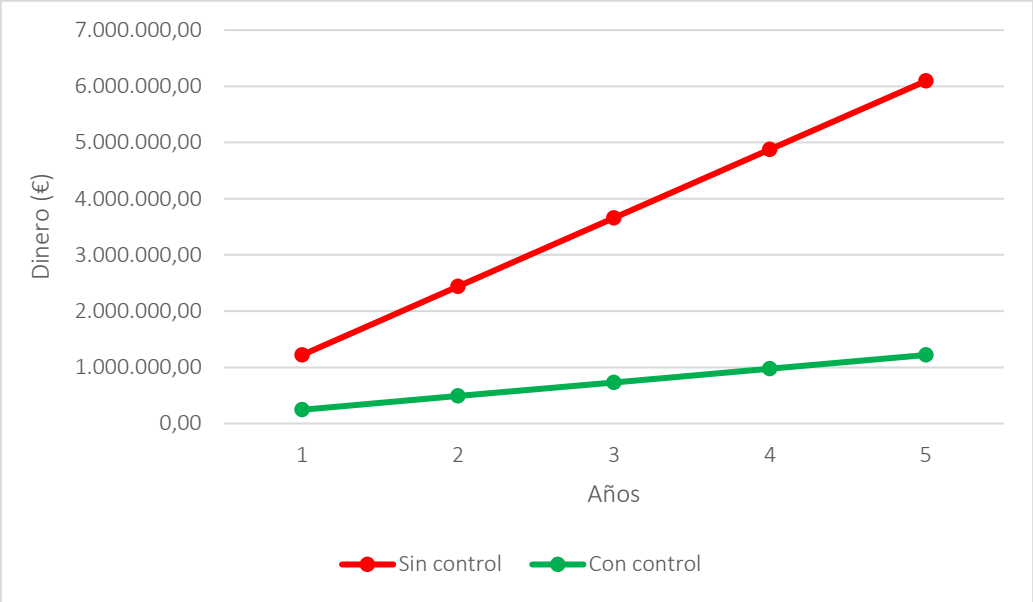



*Ilustración 43. Rentabilidad amenaza HW1 - [I.5] activo S5*

Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 57. Rentabilidad amenaza HW1 - [I.6] activo S5*

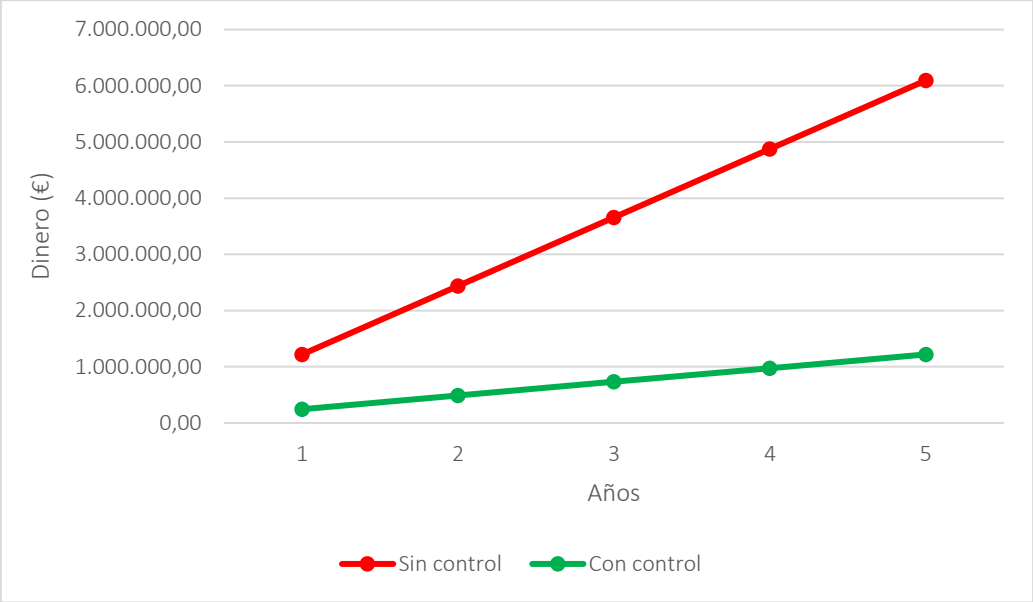



*Ilustración 44. Rentabilidad amenaza HW1 - [I.6] activo S5*

## Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 58. Rentabilidad amenaza SW1 - [I.5] activo S5*

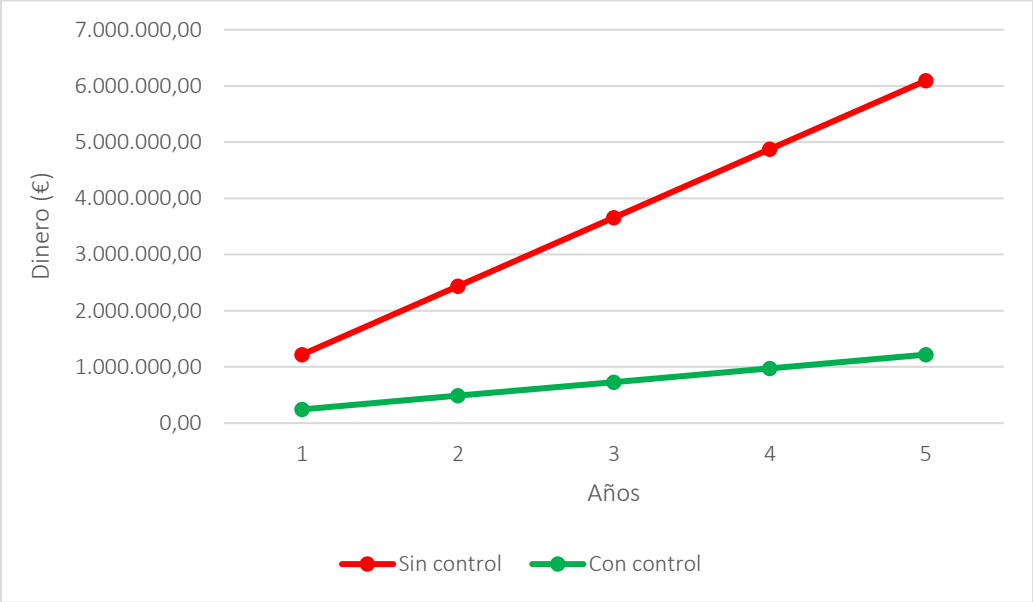



*Ilustración 45. Rentabilidad amenaza SW1 - [I.5] activo S5*

Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 59. Rentabilidad amenaza SRVD1 - [I.5] activo S5*

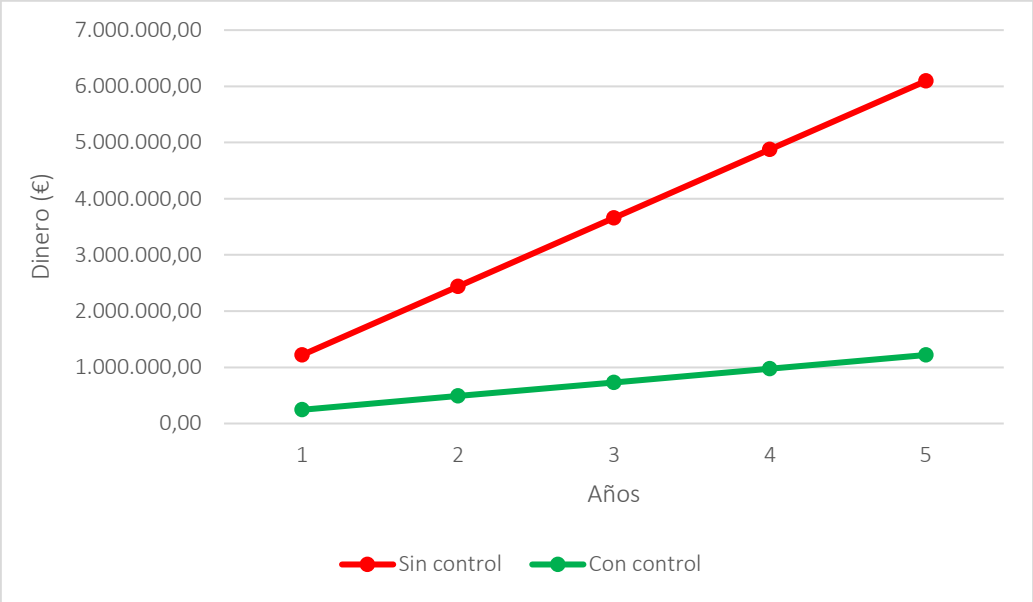



*Ilustración 46. Rentabilidad amenaza SRVD1 - [I.5] activo S5*

Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 60. Rentabilidad amenaza SRVD1 - [I.6] activo S5*

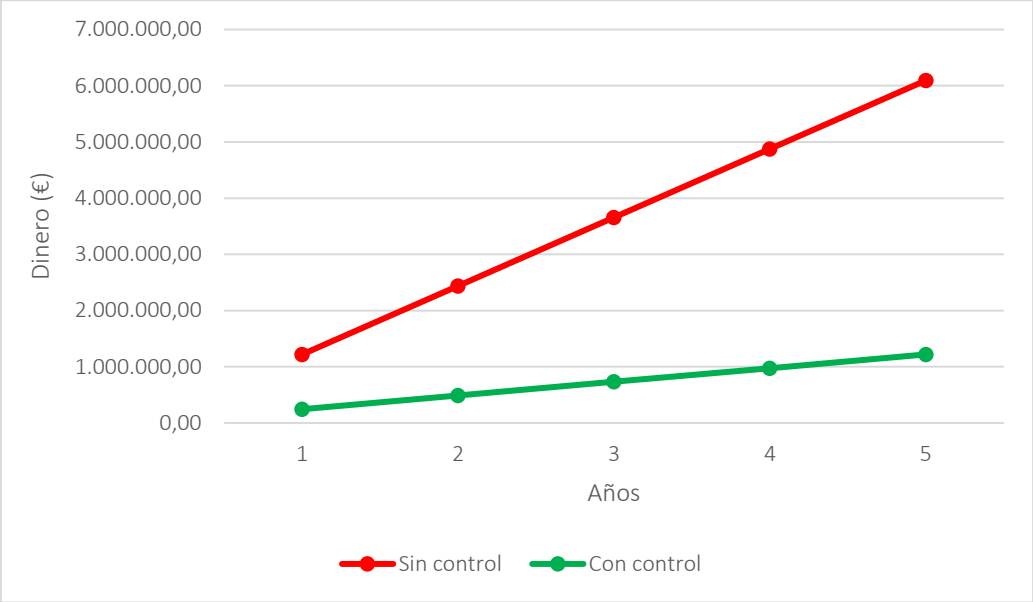



*Ilustración 47. Rentabilidad amenaza SRVD1 - [I.6] activo S5*

Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 203130,5 | 0 | 0 | 203130,5 | 406261 | 609391,5 | 812522 | 1015652,5 |
| 40626,1 | 483,97 | 0 | 41110,07 | 81736,17 | 122362,27 | 162988,37 | 203614,47 |

*Tabla 61. Rentabilidad amenaza T1 - [I.5] activo S5*

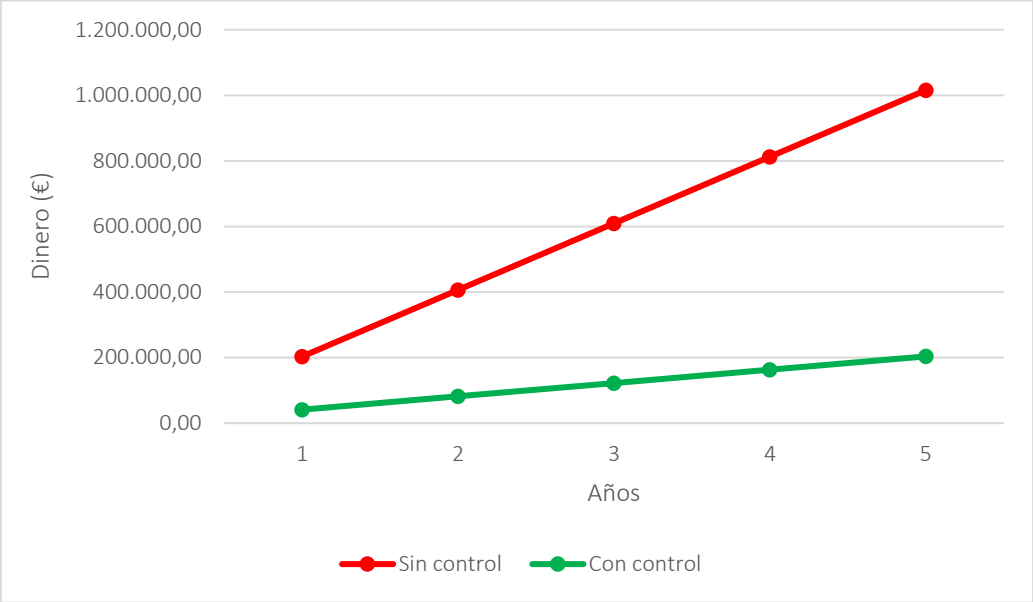



*Ilustración 48. Rentabilidad amenaza T1 - [I.5] activo S5*

## Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 40626,1 | 0 | 0 | 40626,1 | 81252,2 | 121878,3 | 162504,4 | 203130,5 |
| 8125,22 | 483,97 | 0 | 8609,19 | 16734,41 | 24859,63 | 32984,85 | 41110,07 |

*Tabla 62. Rentabilidad amenaza T1 - [I.6] activo S5*

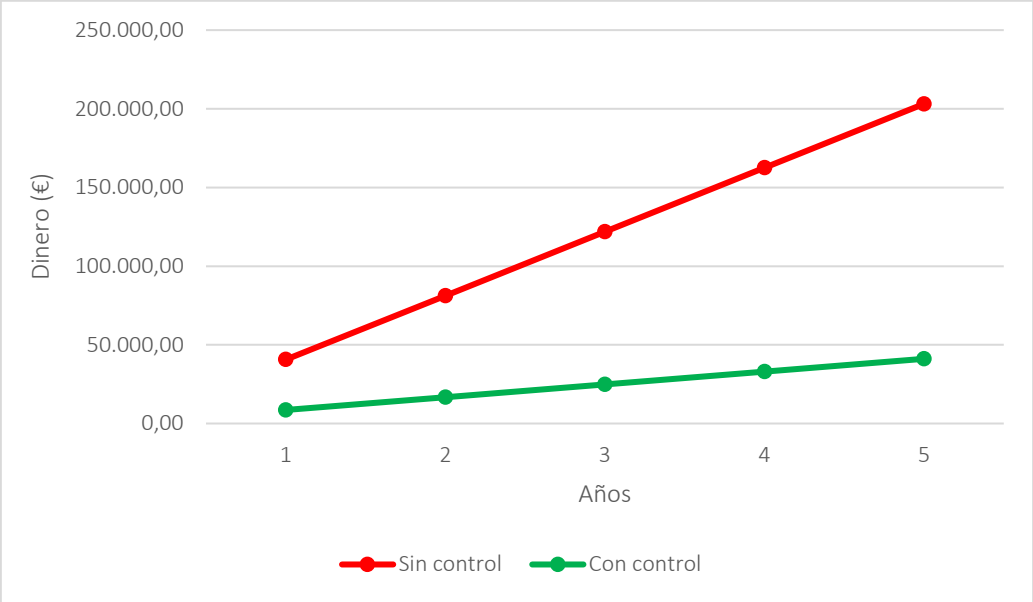



*Ilustración 49. Rentabilidad amenaza T1 - [I.6] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: AUX1 – [I.6] Corte suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 24375,66 | 483,97 | 0 | 24859,63 | 49235,29 | 73610,95 | 97986,61 | 122362,27 |

*Tabla 63. Rentabilidad amenaza AUX1 - [I.6] activo S6*

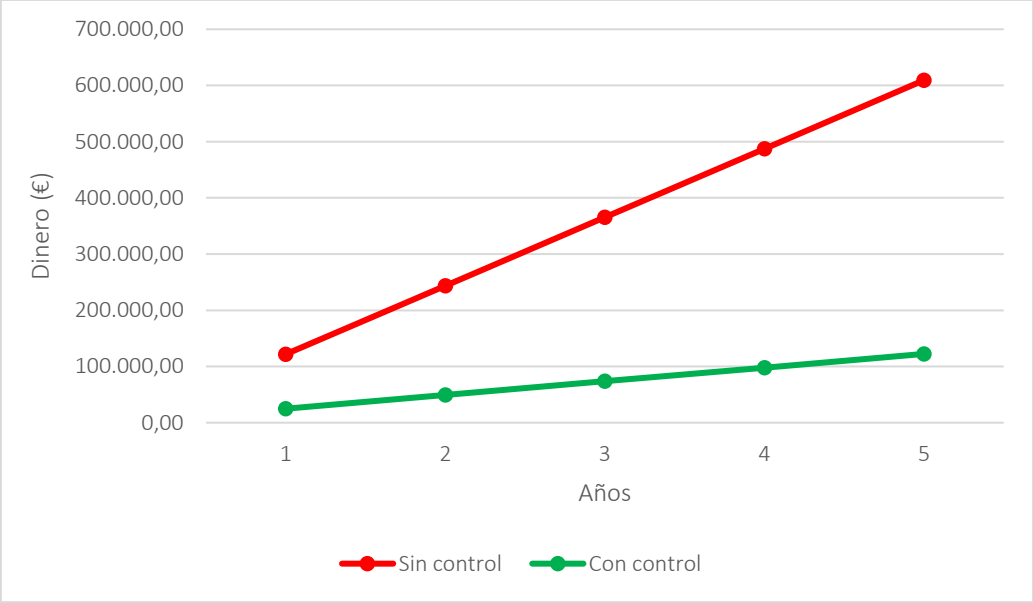



*Ilustración 50. Rentabilidad amenaza AUX1 - [I.6] activo S6*

Amenaza: HW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 64. Rentabilidad amenaza HW1 - [I.5] activo S6*

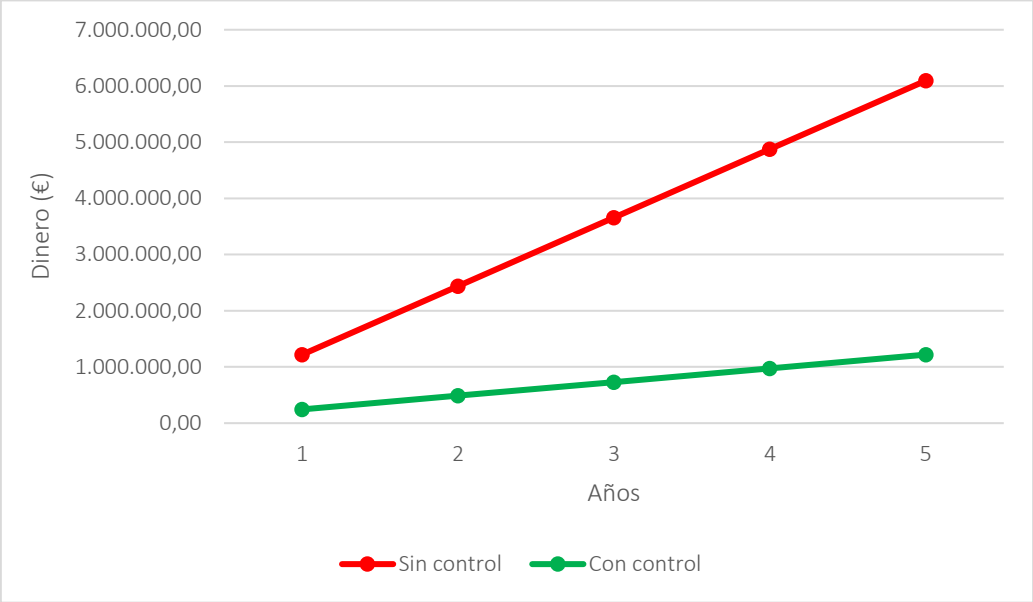



*Ilustración 51. Rentabilidad amenaza HW1 - [I.5] activo S6*

Amenaza: HW1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 65. Rentabilidad amenaza HW1 - [I.6] activo S6*

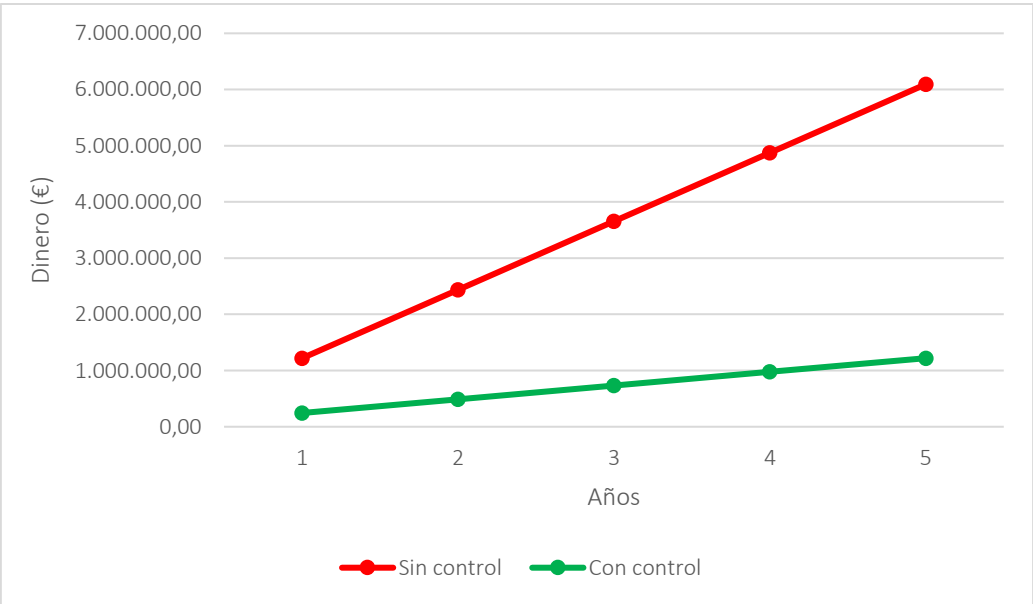



*Ilustración 52. Rentabilidad amenaza HW1 - [I.6] activo S6*

## Amenaza: SW1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 66. Rentabilidad amenaza SW1 - [I.5] activo S6*

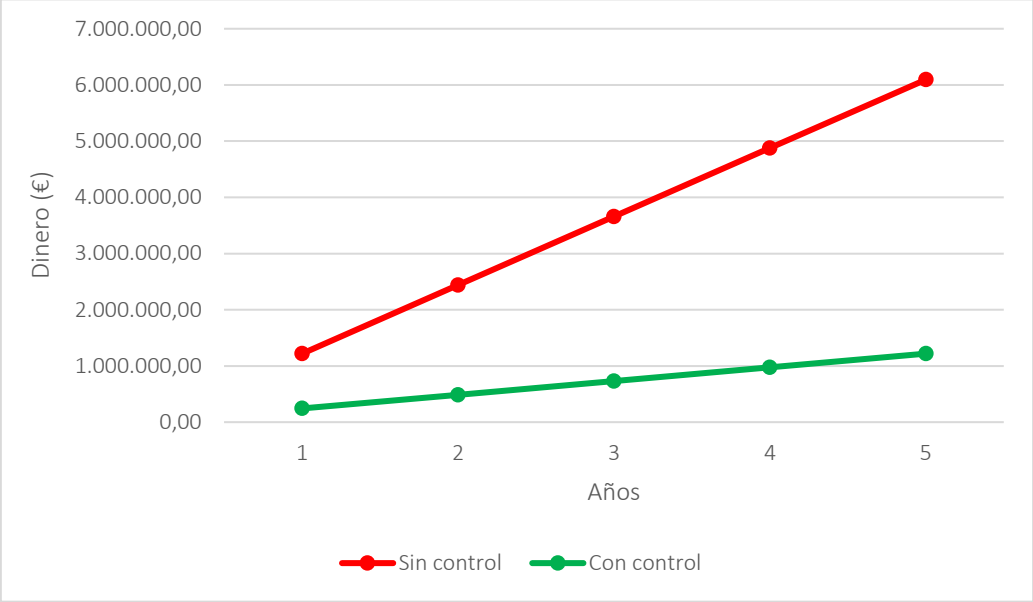



*Ilustración 53. Rentabilidad amenaza SW1 - [I.5] activo S6*

## Amenaza: SRVD1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 67. Rentabilidad amenaza SRVD1 - [I.5] activo S6*

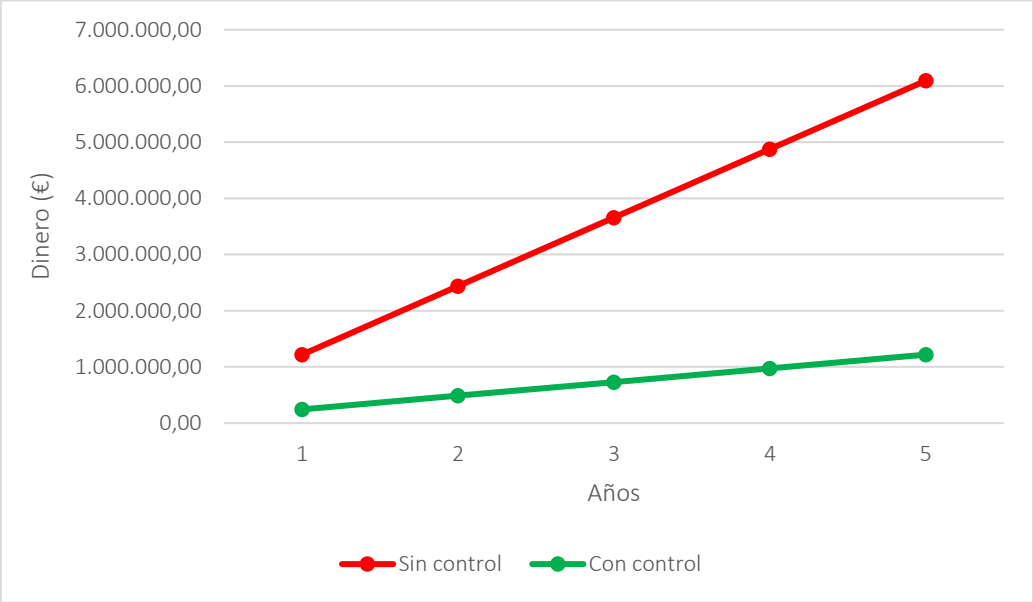



*Ilustración 54. Rentabilidad amenaza SRVD1 - [I.5] activo S6*

## Amenaza: SRVD1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 243756,6 | 483,97 | 0 | 244240,57 | 487997,17 | 731753,77 | 975510,37 | 1219266,97 |

*Tabla 68. Rentabilidad amenaza SRVD1 - [I.6] activo S6*

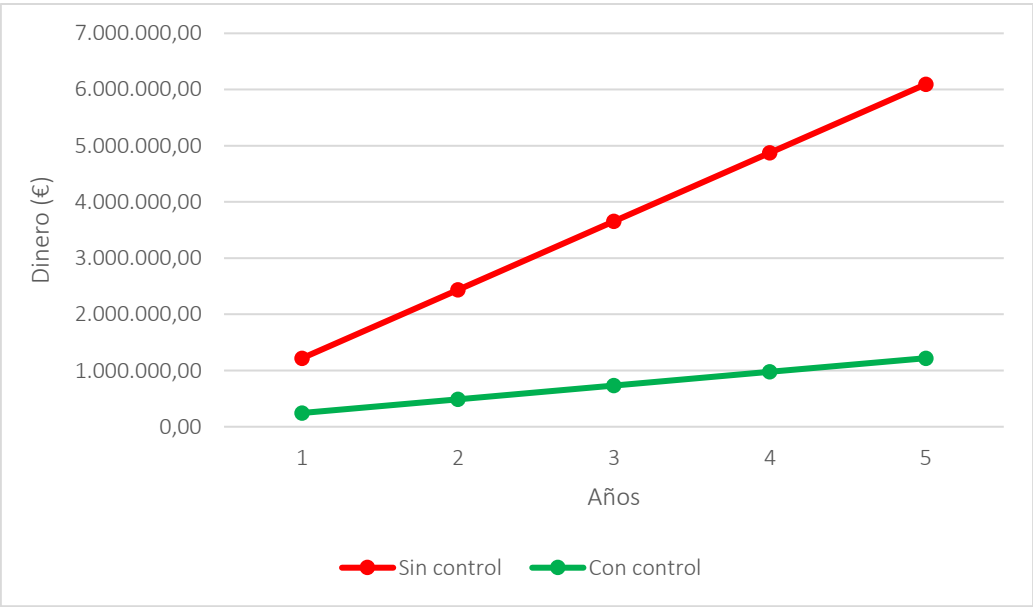



*Ilustración 55. Rentabilidad amenaza SRVD1 - [I.6] activo S6*

## Amenaza: T1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 203130,5 | 0 | 0 | 203130,5 | 406261 | 609391,5 | 812522 | 1015652,5 |
| 40626,1 | 483,97 | 0 | 41110,07 | 81736,17 | 122362,27 | 162988,37 | 203614,47 |

***Tabla 69. Rentabilidad amenaza T1 - [I.5] activo S6***

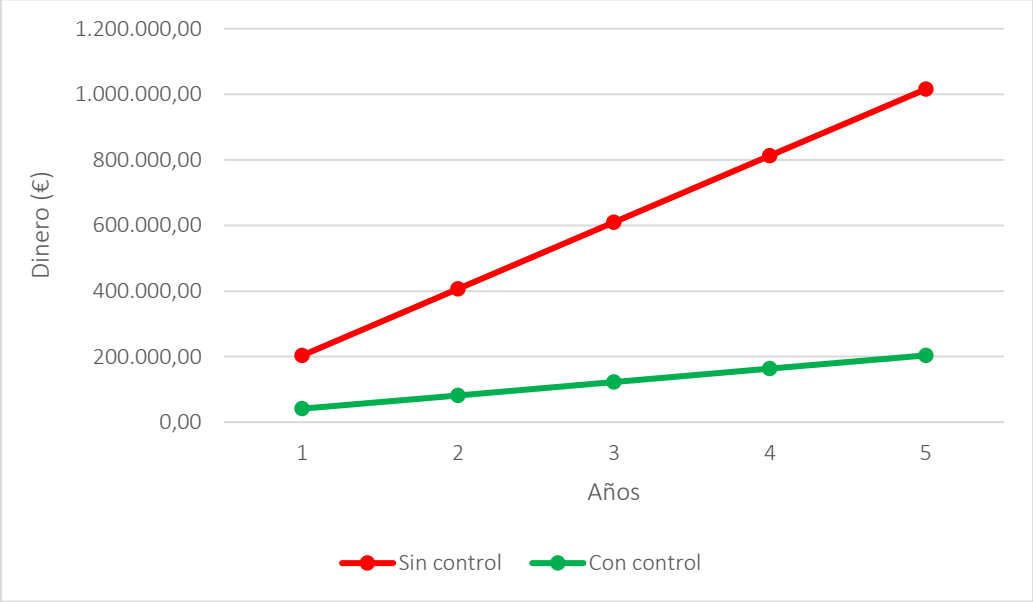



***Ilustración 56. Rentabilidad amenaza T1 - [I.5] activo S6***

## Amenaza: T1 – [I.6] Corte de suministro eléctrico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 40626,1 | 0 | 0 | 40626,1 | 81252,2 | 121878,3 | 162504,4 | 203130,5 |
| 8125,22 | 483,97 | 0 | 8609,19 | 16734,41 | 24859,63 | 32984,85 | 41110,07 |

***Tabla 70. Rentabilidad amenaza T1 - [I.6] activo S6***

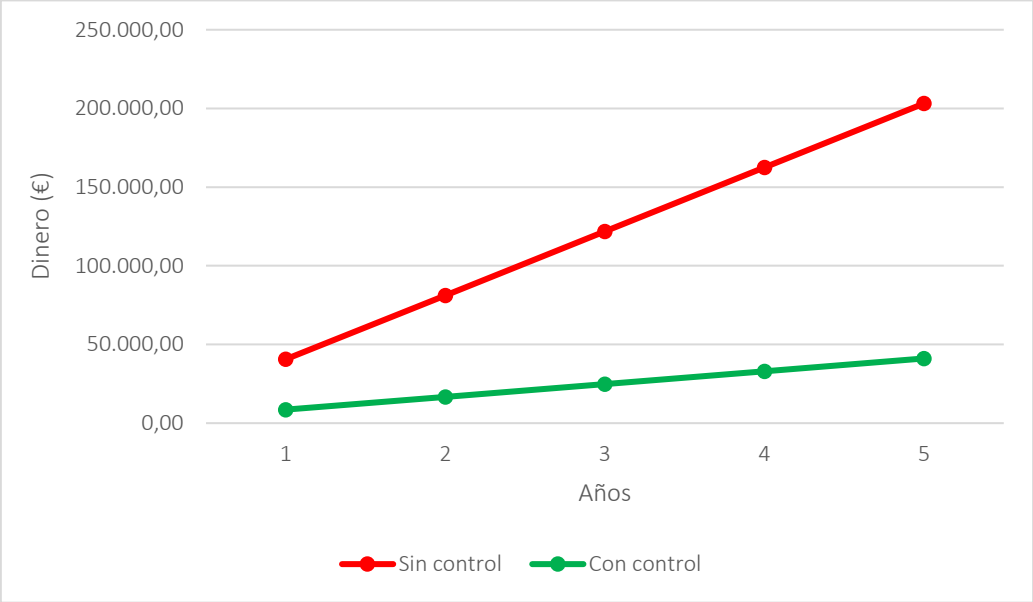



*Ilustración 57. Rentabilidad amenaza T1 - [I.6] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.2 Segundo control

##### 2.1.5.2.1 Título

Control de seguridad de red Wifi.

##### 2.1.5.2.2 Finalidad

Una de las mayores vulnerabilidades de las empresas es su conexión a internet, especialmente su red Wifi. Actualmente, la gran mayoría de personas disponen de un dispositivo con capacidad para conectarse a una red Wifi, por lo tanto, debemos tener especial cuidado en quien se conecta a la red de nuestra empresa. En consecuencia, debemos protegernos de estas vulnerabilidades y amenazas mediante las pautas y dispositivos que tenemos a nuestra disposición. En este caso, vamos a basarnos en una serie de recomendaciones elaboradas por el Instituto Nacional de Seguridad.

#### 2.1.5.2.3 Empresa

"Sanitaria AMS S.L."

#### 2.1.5.2.4 Leyes aplicables

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

#### 2.1.5.2.5 Normas aplicables

No hay referencias de normas para este control.

#### 2.1.5.2.6 Descripción del control

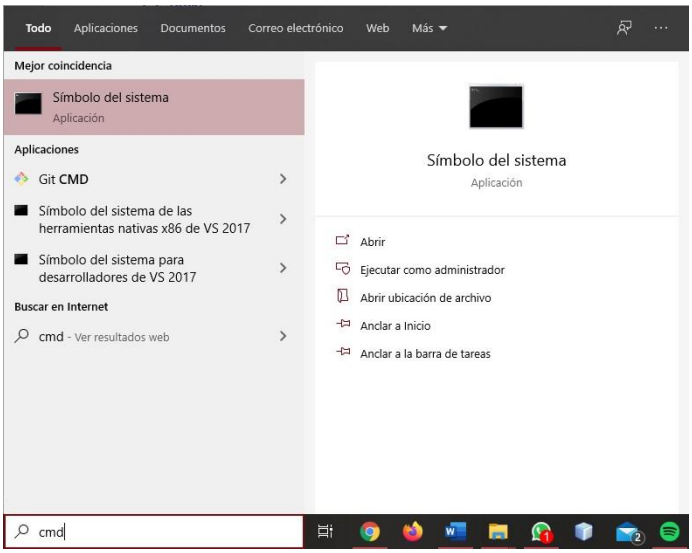
Como ya hemos comentado anteriormente, cualquier empresa puede ser atacada por medio de su conexión Wifi, por lo tanto, a continuación, vamos a desarrollar de manera detallada todos los pasos que son necesarios para llevar a cabo este control de manera adecuada y así protegernos de las amenazas. Para esto nos hemos basado en una guía proporcionada por el Instituto Nacional de Ciberseguridad, "Seguridad en redes Wifi". (INCIBE, 2019)

*Nota: Solo se especificarán como se realizan las diferentes acciones para el sistema operativo Windows ya que todos los terminales de la empresa auditada tienen dicho Sistema Operativo.*

##### 2.1.5.2.6.1 ¿Cómo acceder a la configuración del router?

Para llevar a la práctica esta acción será necesario, en primer lugar, conocer la dirección IP[1] que nos da acceso al *router.* Se puede saber de varias formas, pero nosotros recomendamos seguir los siguientes pasos para el caso de ordenadores Windows:

[1] Una dirección IP (del acrónimo inglés IP para *Internet Protocol*), es un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.




Botón de **Inicio** >> (en el cuadro donde dice "Buscar programas y archivos") escribir <<**cmd**>> Pinchar en el resultado >> Escribir <<**ipconfig**>> >> buscar la <<**Puerta de enlace**>>

***Ilustración 58. Consola sistema control Wifi***

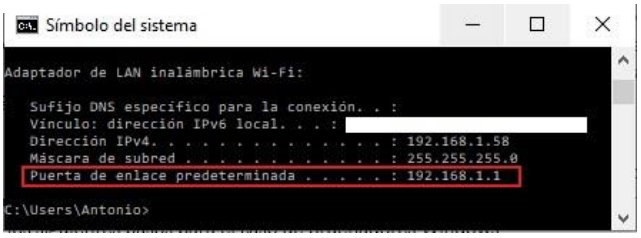



***Ilustración 59. Consola sistema 2 control Wifi***

Una vez que contamos con la dirección IP del *router,* necesitaremos de un navegador web para poder acceder al dispositivo, así como las credenciales de acceso que se puede encontrar bien en el manual del *router* o bien, en la pegatina que viene en su base o parte trasera. Una última opción sería consultar directamente al fabricante cuál es dicha contraseña.

Ahora que ya estamos dentro de la configuración de nuestro *router* vamos a describir detalladamente cada uno de los pasos que tenemos que seguir para mejorar la seguridad de nuestra red Wifi.

#### 2.1.5.2.6.2 Cambiar el nombre y contraseña de acceso al router.

Se deberá cambiar el nombre y la contraseña que nos ha proporcionado por defecto nuestro Proveedor de Servicios de Internet (ISP[2]). La nueva contraseña debe tener un mínimo de 8 caracteres que combinen minúsculas, mayúsculas, números y caracteres especiales.

[2] Por sus siglas en inglés *Internet Service Provider,* es la empresa que confiere conexión a Internet a sus clientes.

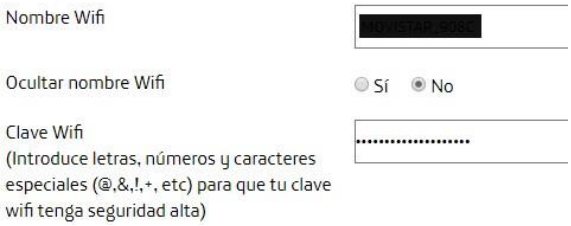



***Ilustración 60. Credenciales acceso router***

#### 2.1.5.2.6.3 Actualización de Firmware.

Se tendrá que actualizar el firmware[3] del *router* cada vez que haya una nueva versión disponible. Al usar la última versión del software nos aseguramos de tener todos los parches de seguridad disponibles.

#### 2.1.5.2.6.4 Configurar red wifi con cifrado WPA2 o WPA3.

WPA viene de las siglas *Wi-Fi Protected Access.* Se trata de una estándar dirigido a la protección de los dispositivos, como los *routers*, de tal manera que nadie ajeno pueda acceder a los datos de manera inalámbrica. De esta forma WPA3 irá reemplazando progresivamente al WPA2.

En caso de que nuestro *router* tenga disponible el cifrado WPA3 usaremos este, sino lo haremos con el cifrado WPA2-PSK (AES).


***Ilustración 61. Cifrado red wifi***

#### 2.1.5.2.6.5 Desactivar WPS.

Se trata de un mecanismo que facilita la conexión de dispositivos con nuestro *router* a través de un código PIN[4] de 8 dígitos. El dispositivo que se quiere conectar a la wifi debe transmitir el código numérico al *router* y éste a cambio le enviará los datos para acceder a la red.

Tener activada esta opción implica una nueva forma de conexión que podría ser utilizada por un atacante para acceder a nuestra red wifi, ya que el tiempo que se

[3] Se trata de un programa informático o software que controla las funcionalidades de un dispositivo físico o un hardware concreto como un *router*, un *Smartphone*, etc.
[4] Por sus siglas en inglés *Personal Identification Number,* compuesto por al menos 4 cifras, es un número de identificación personal que funciona como sistema de seguridad de acceso.

necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesitaría averiguar una contraseña WPA2-PSK(AES) configurada en la red.

Por lo tanto, si queremos mantener la red wifi segura, deberemos renunciar a este tipo de utilidad, desactivando el WPS.

#### 2.1.5.2.6.6 Habilitar el filtrado por dirección MAC.

Mediante este mecanismo se pretende que únicamente las direcciones MAC que se encuentren incluidas en el *router* puedan conectarse a la red. Esta dirección es un identificador único asociado a un dispositivo concreto como un portátil o un *smartphone.*

Por lo tanto, activaremos esta función en nuestro *router* y habrá que incluir las direcciones que entendamos como oportunas en nuestro *router* y para ello deberemos acceder a las opciones en el dispositivo para establecer este control de acceso.

Como paso previo, hemos de conocer la dirección MAC de los diferentes dispositivos que queramos añadir, bien sean ordenadores, teléfonos móviles, tabletas, etc.

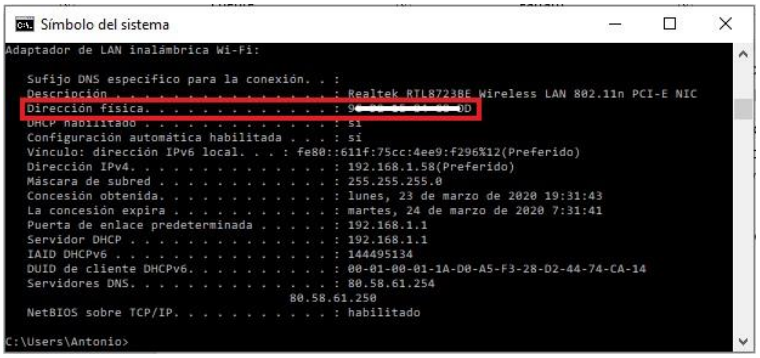



***Ilustración 62. Dirección MAC red wifi***

En el caso de los dispositivos con sistema operativo Windows obtendremos la dirección MAC a través de la consola de MS-DOS haciendo uso del comando <<ipconfig/all>>. En este caso, deberemos buscar el campo <<dirección física>>.

Los pasos necesarios para saber la dirección MAC en un móvil **Android** son los siguientes:

**Menú** >> **Ajustes Sistemas** >> **Información del Teléfono** >> **Estado** >> **Dirección Mac de la red Wifi:**

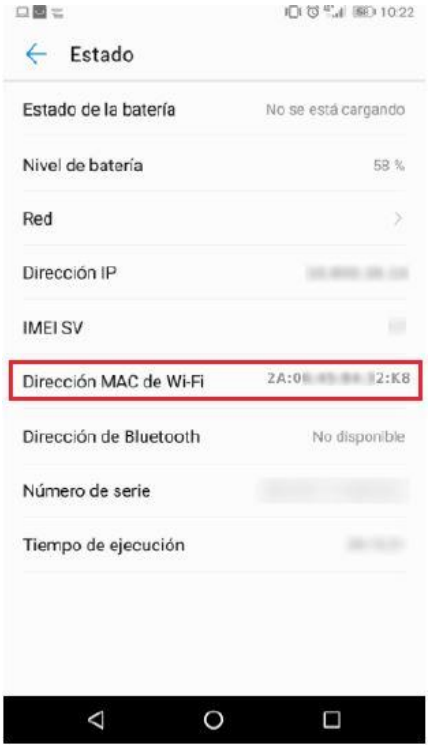



*Ilustración 63. Ajustes dirección MAC Android*

Los pasos necesarios para saber la dirección MAC en un móvil con sistema operativo IOS son los siguientes:

**Ajustes** >> **General** >> **Información** >> ver el apartado **"Dirección wifi"**:


*Ilustración 64. Ajustes dirección MAC IOS*

#### 2.1.5.2.6.7 Red wifi para invitados

Si nuestro modelo de *router* lo permite, podemos crear una red inalámbrica separada de la red local y conocida como red de invitados.

De esta manera, mediante la creación de una red de invitados, a través de una red inalámbrica evitaremos que se tenga acceso a la red local, así como a los datos que aquí se albergan, evitando potenciales infecciones mediante la propagación de virus, *malware* o una fuga de información.

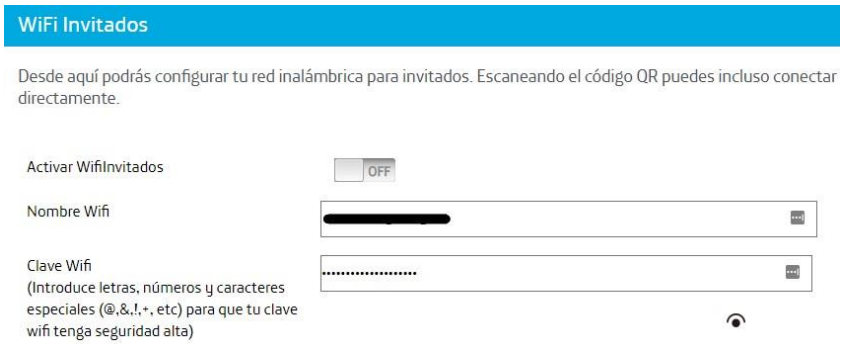




***Ilustración 65. Credenciales red wifi invitados***

***Ilustración 66. Red wifi invitados***

Se deberá configurar una red wifi de invitados con un nombre y una contraseña diferente a la que usamos en nuestra red wifi principal.

#### 2.1.5.2.6.8 Deshabilita UPnP.

También habrá un ajuste en el panel de administración para UPnP siglas en inglés de *Universal Pulg and Play.* Esto les permite a los dispositivos en la red como ordenadores, impresoras, y otros dispositivos a descubrirse entre ellos mismos dentro de la red. Esto puede introducir riesgos de seguridad, y debe deshabilitarse si la opción está presente.

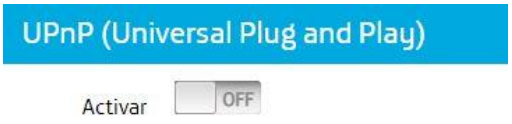



***Ilustración 67. Deshabilitar UPnP***

#### 2.1.5.2.7 Responsables

Administrador del SI, será el encargado de configurar cada una de las acciones necesarias descritas anteriormente, debe comprobar que su funcionamiento es correcto. Además, deberá comprobar que funciona correctamente una vez cada dos semanas.

#### 2.1.5.2.8 Dispositivos

Para la implantación de este control no es necesario ningún dispositivo, ya que todas configuraciones realizadas se llevarán a cabo en el *router* que nos proporciona nuestra compañía con la cual tengamos contratada nuestra tarifa de Internet.

#### 2.1.5.2.9 Costes

- **Implantación:** 0 €, como ya hemos especificado anteriormente, no necesitamos ningún dispositivo extra. Por otro lado, la instalación la hará el administrador del SI, que en este caso es uno de los dueños de la empresa, por lo tanto, no tendrá costes adicionales.
- **Ejecución y mantenimiento:** 0 €, no cuesta nada ejecutar ni mantener las medidas, ya que las hacemos sobre nuestro propio *router.*
- **Búsqueda de irregularidades:** si en algún momento se detecta algún fallo en alguna de las medidas configuradas, se deberán volver a seguir todos los pasos de la misma manera, para que vuelva a funcionar correctamente.

#### 2.1.5.2.10 Rentabilidad

Las amenazas que se dan a través de la red wifi de una empresa pueden conllevar pérdida de datos, el cual ya hemos visto que es un problema muy grave para la empresa debido a las sanciones que puede provocar. Además, podemos tener intrusiones no deseadas dentro del Sistema de información de nuestra empresa, que también pueden provocar una gran cantidad de problemas en nuestra empresa.

Por lo tanto, después de haber visto el gran número de amenazas que tiene nuestra empresa a través de la red wifi, podemos decir que es muy importante la implantación de este control en nuestro Sistema de información.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar dicho control en nuestro SI. Vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 90 % ya que:

- Puede fallar por una mala configuración.
- Puede fallar por olvido de revisión del responsable.

Activo: Información de pacientes (S1)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 54575,6 | 0 | 0 | 54575,6 | 109151,2 | 163726,8 | 218302,4 | 272878 |
| 5457,56 | 0 | 0 | 5457,56 | 10915,12 | 16372,68 | 21830,24 | 27287,8 |

*Tabla 71. Rentabilidad amenaza AUX1 - [A.11] activo S1*

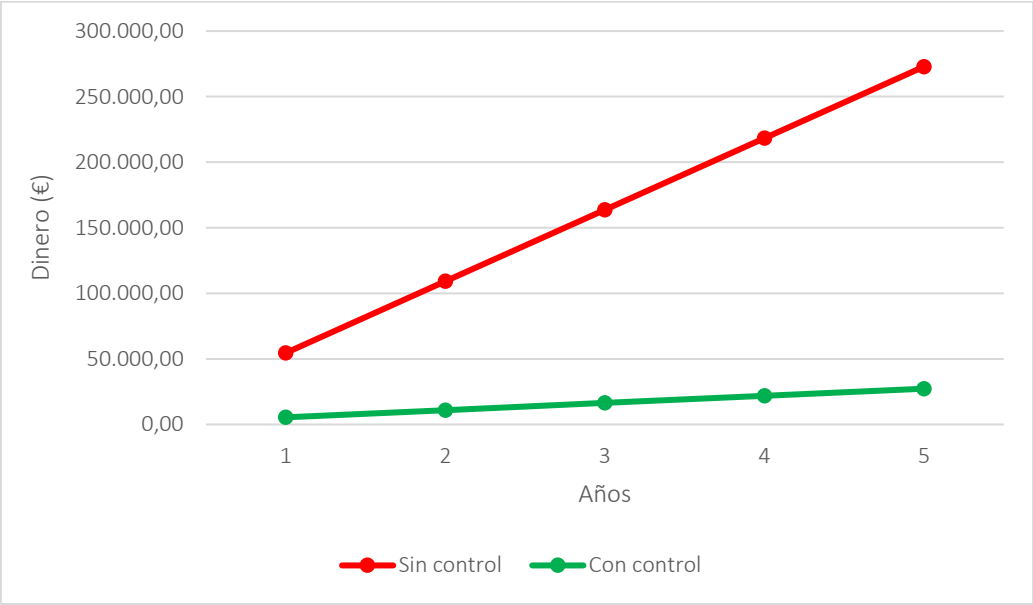



*Ilustración 68. Rentabilidad amenaza AUX1 - [A.11] activo S1*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 72. Rentabilidad amenaza D1 - [A.5] activo S1*

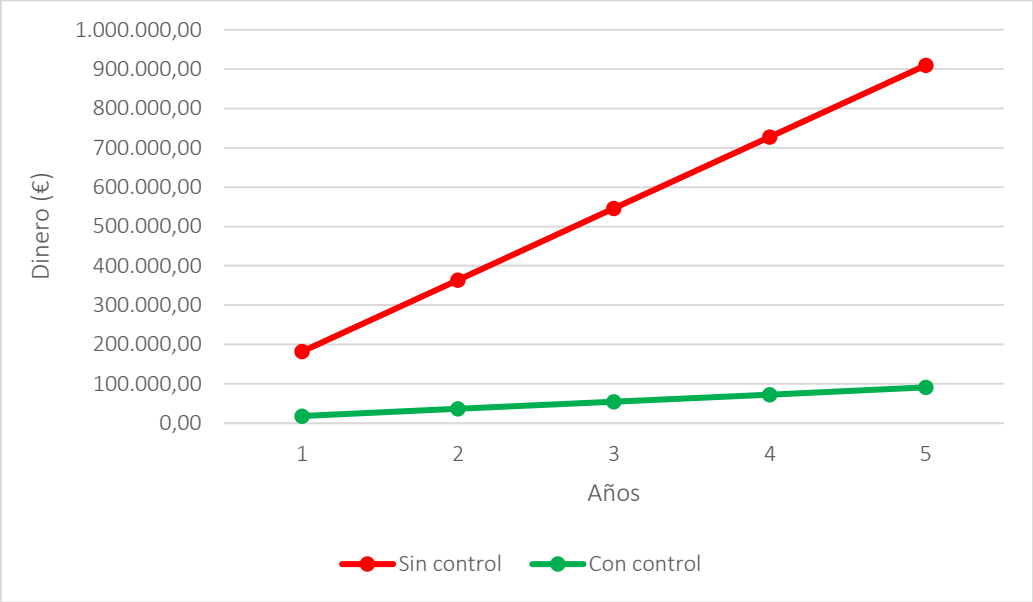



*Ilustración 69. Rentabilidad amenaza D1 - [A.5] activo S1*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 909593,31 | 0 | 0 | 909593,31 | 1819186,6 | 2728779,93 | 3638373,24 | 4547966,55 |
| 90959,33 | 0 | 0 | 90959,33 | 181918,66 | 272877,99 | 363837,32 | 454796,65 |

*Tabla 73. Rentabilidad amenaza D1 - [A.11] activo S1*

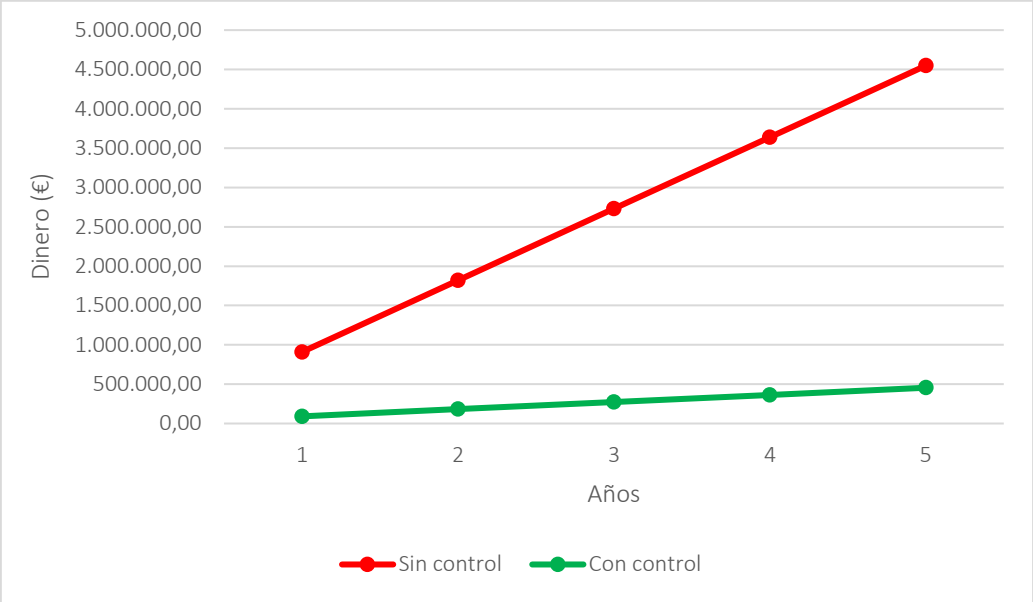



*Ilustración 70. Rentabilidad amenaza D1 - [A.11] activo S1*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

*Tabla 74. Rentabilidad amenaza D1 - [A.18] activo S1*

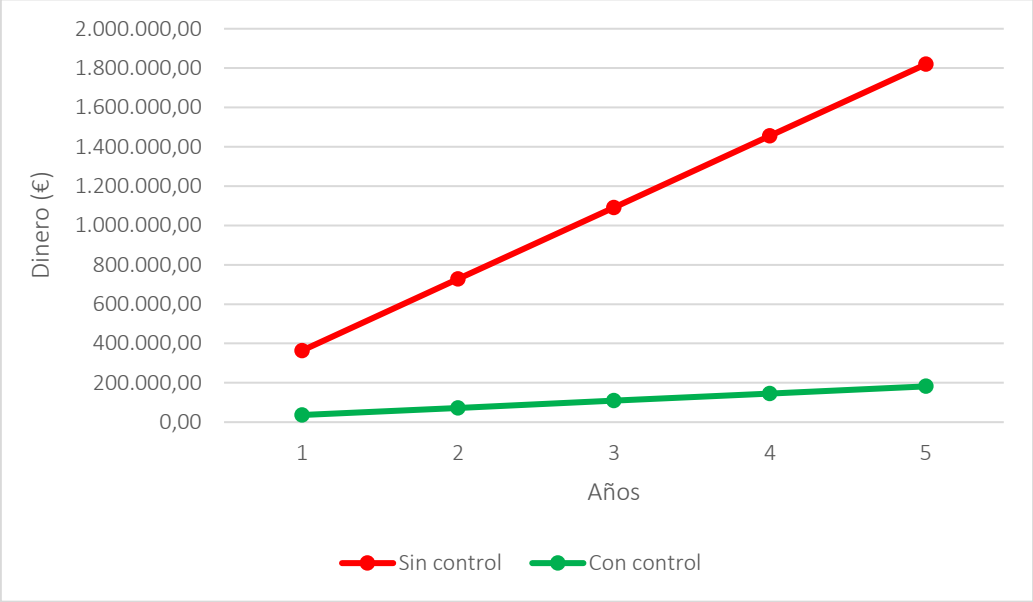



*Ilustración 71. Rentabilidad amenaza D1 - [A.18] activo S1*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

*Tabla 75. Rentabilidad amenaza D1 - [A.18] activo S1*

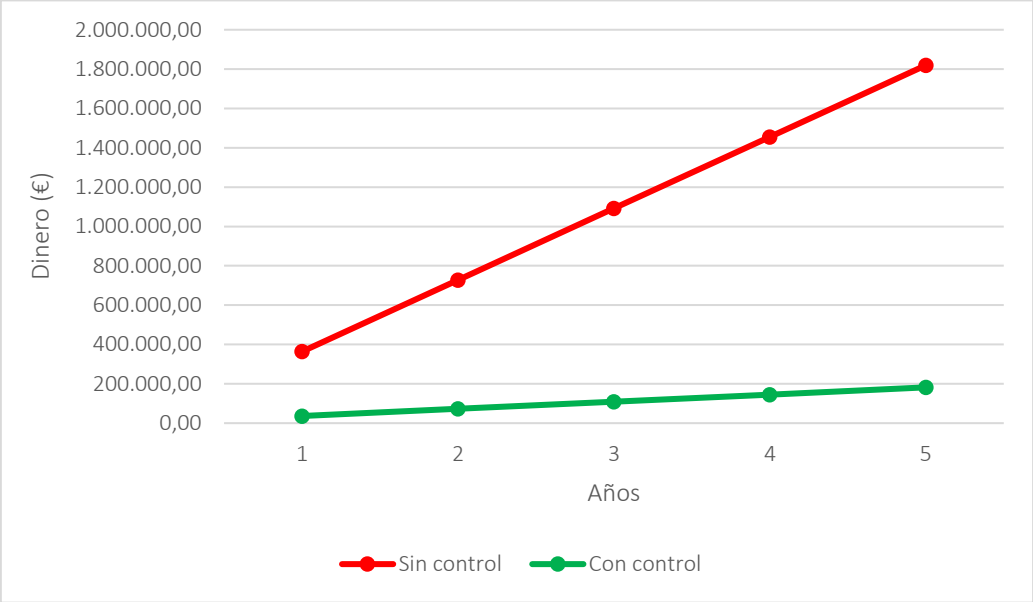



*Ilustración 72. Rentabilidad amenaza D1 - [A.18] activo S1*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 76. Rentabilidad amenaza HW1 - [A.11] activo S1*

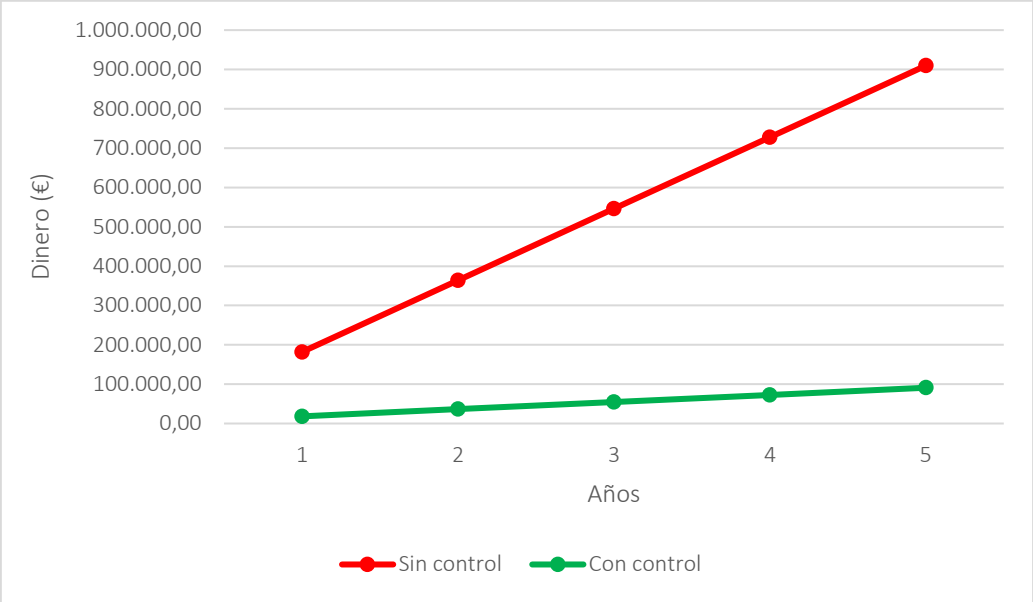



*Ilustración 73. Rentabilidad amenaza HW1 - [A.11] activo S1*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 77. Rentabilidad amenaza SW1 - [A.5] activo S1*

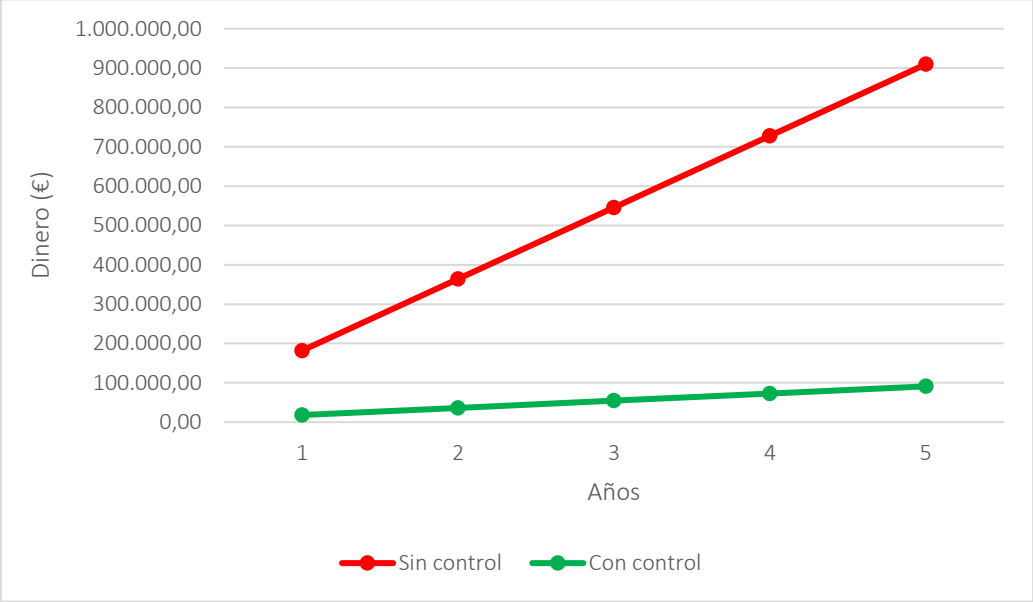



*Tabla 78. Rentabilidad amenaza SW1 - [A.5] activo S1*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 79. Rentabilidad amenaza SW1 - [A.15] activo S1*

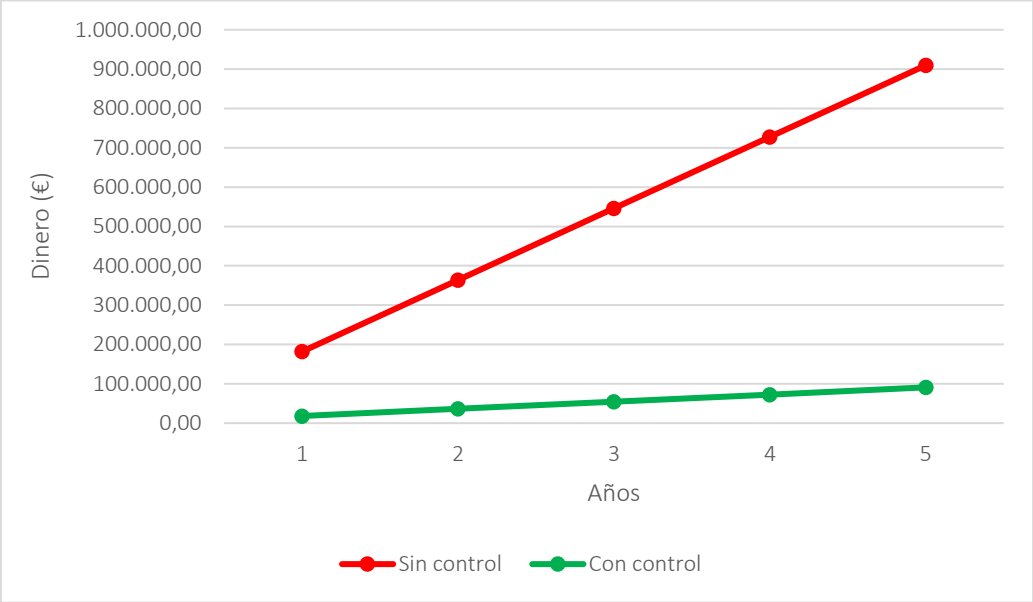



*Ilustración 74. Rentabilidad amenaza SW1 - [A.15] activo S1*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 127343,06 | 0 | 0 | 127343,06 | 254686,12 | 382029,18 | 509372,24 | 636715,3 |
| 12734,31 | 0 | 0 | 12734,31 | 25468,62 | 38202,93 | 50937,24 | 63671,55 |

*Tabla 80. Rentabilidad amenaza SW1 - [A.18] activo S1*

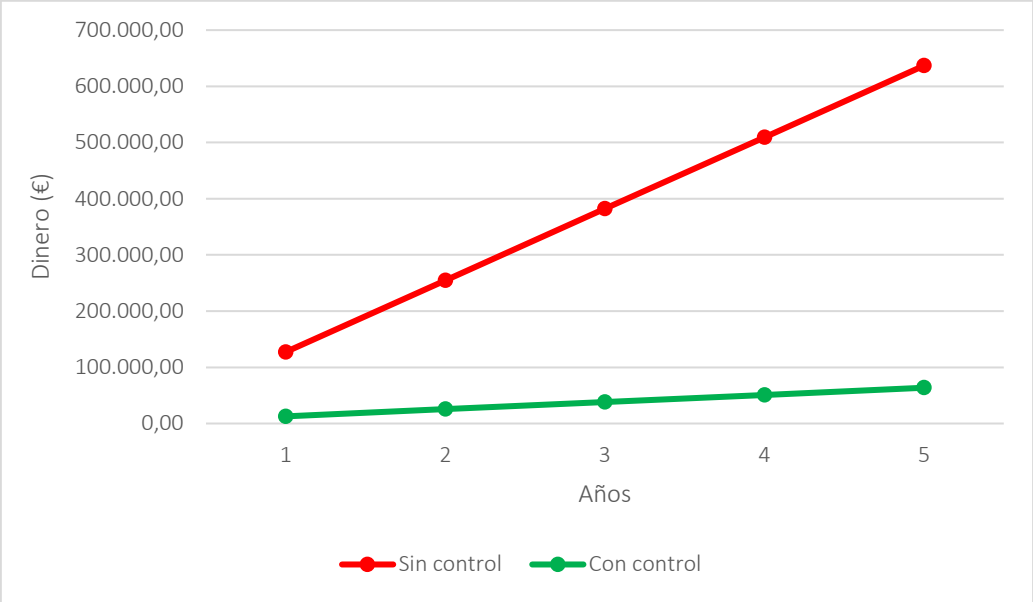



*Ilustración 75. Rentabilidad amenaza SW1 - [A.18] activo S1*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 127343,06 | 0 | 0 | 127343,06 | 254686,12 | 382029,18 | 509372,24 | 636715,3 |
| 12734,31 | 0 | 0 | 12734,31 | 25468,62 | 38202,93 | 50937,24 | 63671,55 |

***Tabla 81. Rentabilidad amenaza SW1 - [A.19] activo S1***

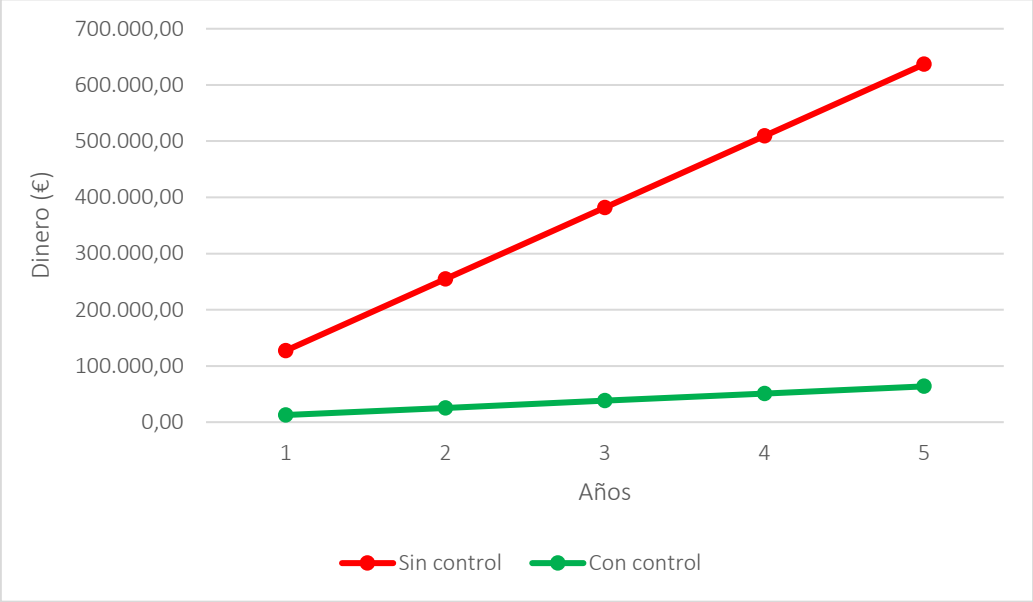



***Ilustración 76. Rentabilidad amenaza SW1 - [A.19] activo S1***

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

***Tabla 82. Rentabilidad amenaza SRVD1 - [A.11] activo S1***

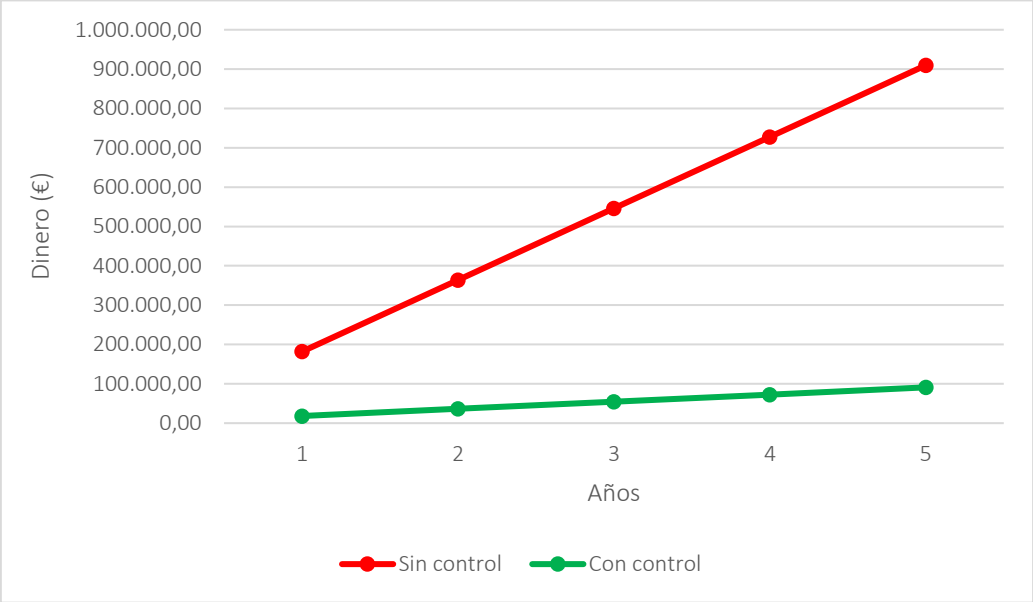



*Ilustración 77. Rentabilidad amenaza SRVD1 - [A.11] activo S1*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 6063,96 | 0 | 0 | 6063,96 | 12127,92 | 18191,88 | 24255,84 | 30319,8 |
| 606,4 | 0 | 0 | 606,4 | 1212,8 | 1819,2 | 2425,6 | 3032 |

*Tabla 83. Rentabilidad amenaza T1 - [A.11] activo S1*

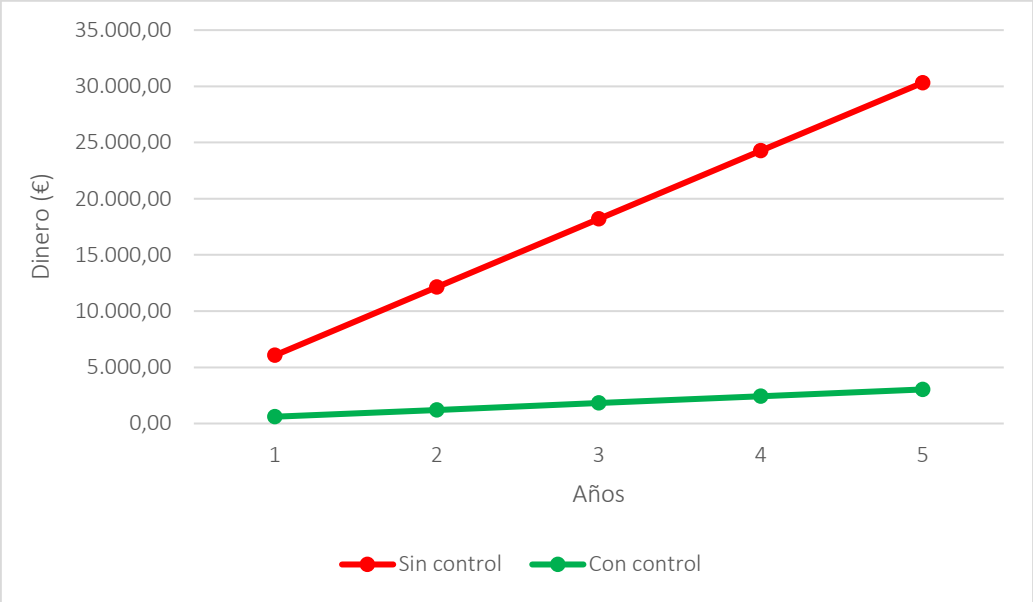



*Ilustración 78. Rentabilidad amenaza T1 - [A.11] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 84. Rentabilidad amenaza AUX1 - [A.11] activo S2*

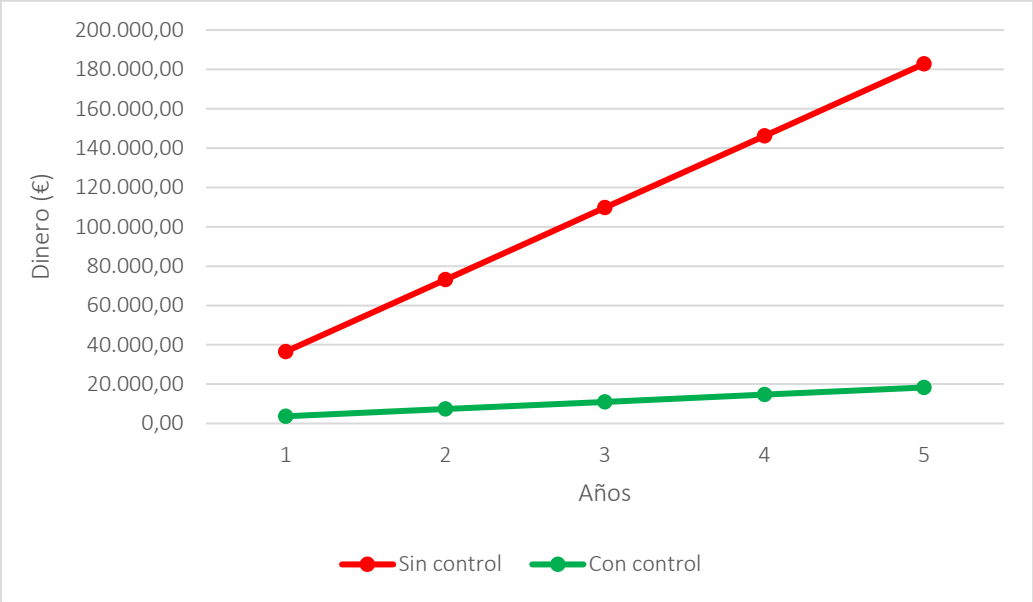



*Ilustración 79. Rentabilidad amenaza AUX1 - [A.11] activo S2*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 85. Rentabilidad amenaza D1 - [A.5] activo S2*

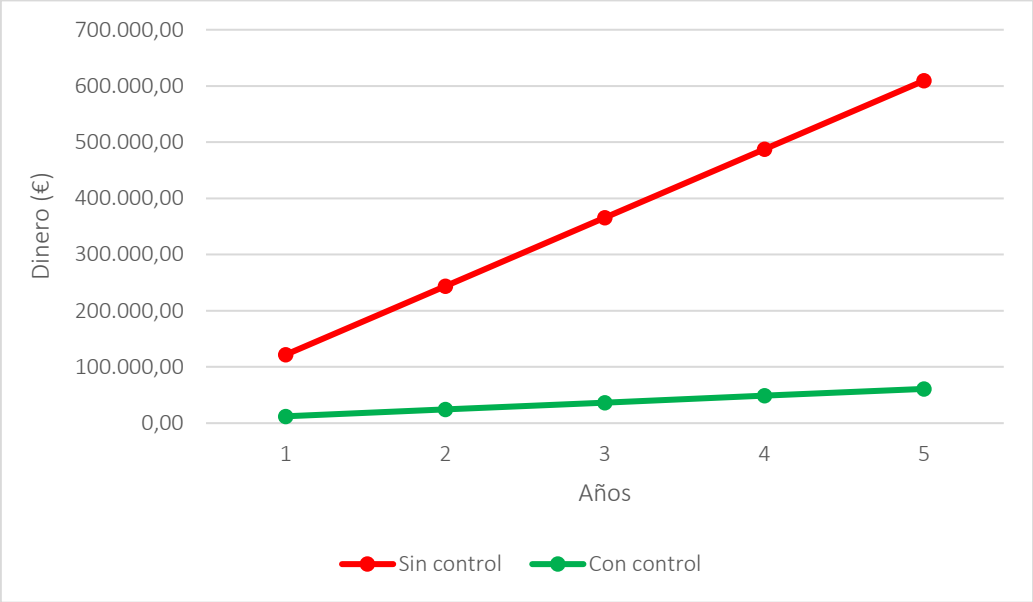



*Ilustración 80. Rentabilidad amenaza D1 - [A.5] activo S2*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 86. Rentabilidad amenaza D1 - [A.11] activo S2*

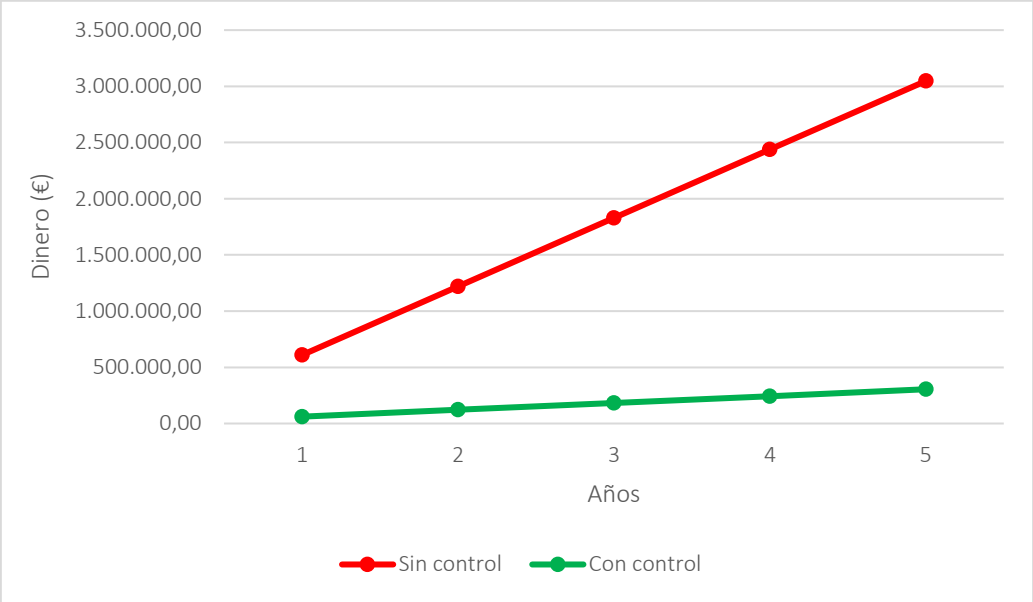



*Ilustración 81. Rentabilidad amenaza D1 - [A.11] activo S2*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 87. Rentabilidad amenaza D1 - [A.18] activo S2*

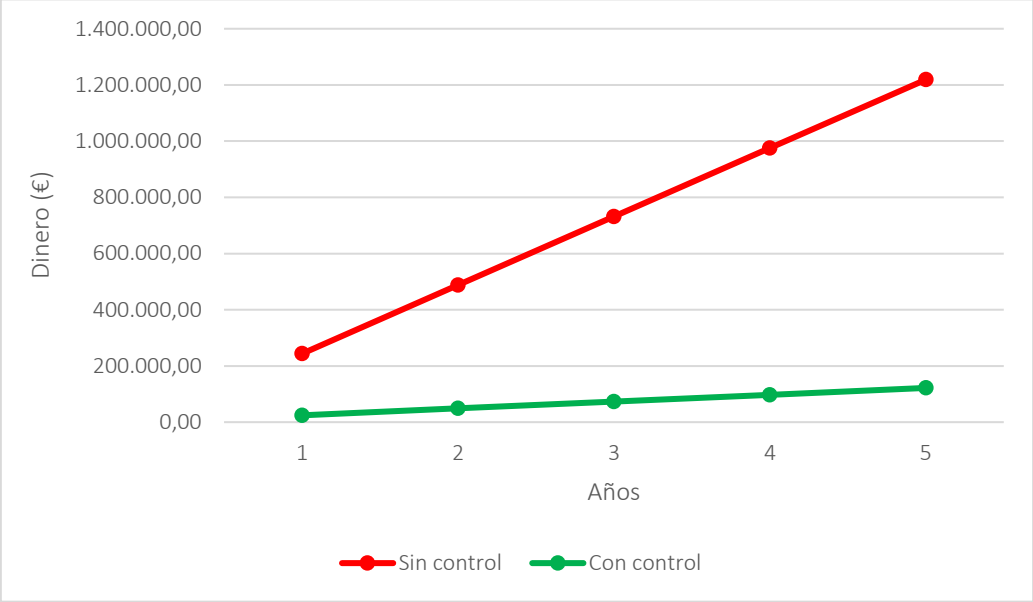



*Ilustración 82. Rentabilidad amenaza D1 - [A.18] activo S2*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 88. Rentabilidad amenaza D1 - [A.19] activo S2*

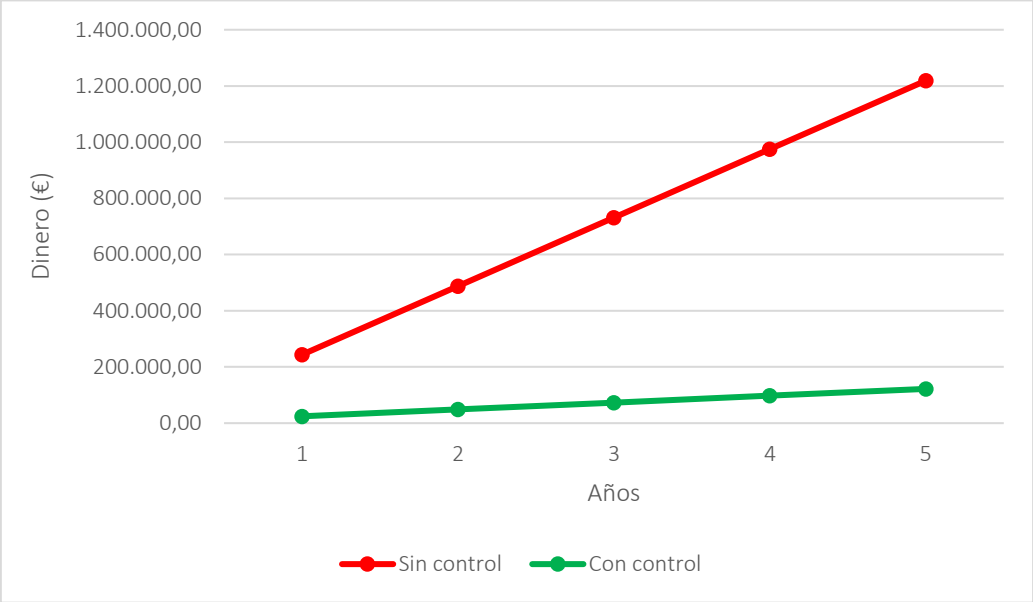



*Ilustración 83. Rentabilidad amenaza D1 - [A.19] activo S2*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 89. Rentabilidad amenaza HW1 - [A.11] activo S2*

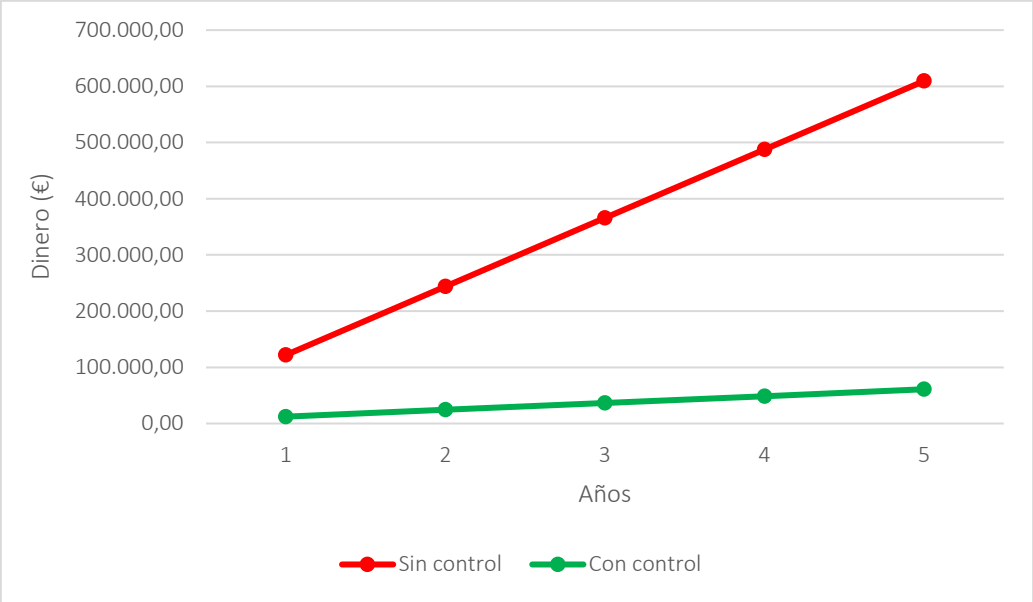



*Ilustración 84. Rentabilidad amenaza HW1 - [A.11] activo S2*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 90. Rentabilidad amenaza SW1 - [A.5] activo S2*

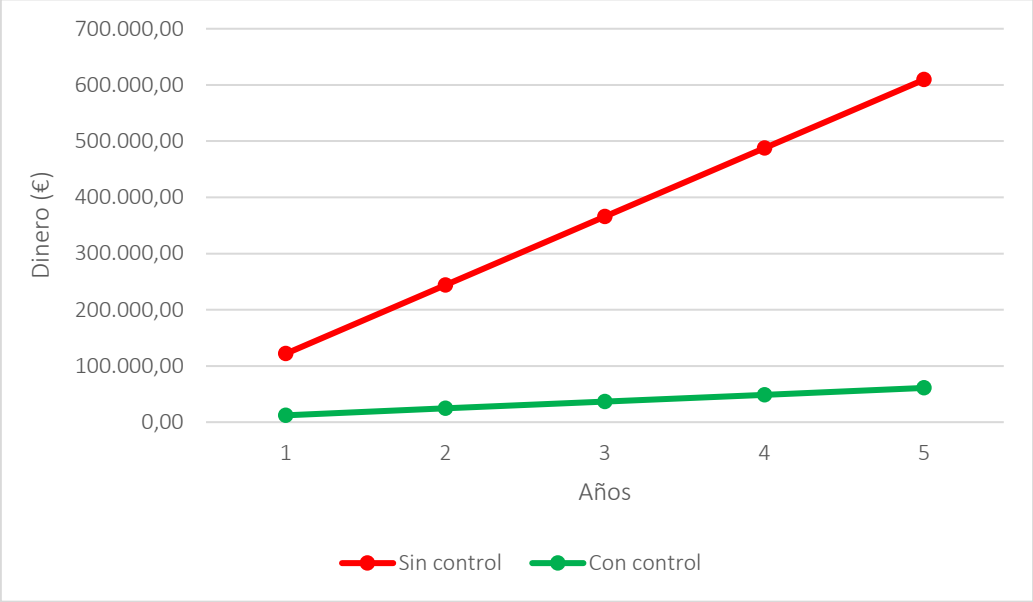



*Ilustración 85. Rentabilidad amenaza SW1 - [A.5] activo S2*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 91. Rentabilidad amenaza SW1 - [A.15] activo S2*

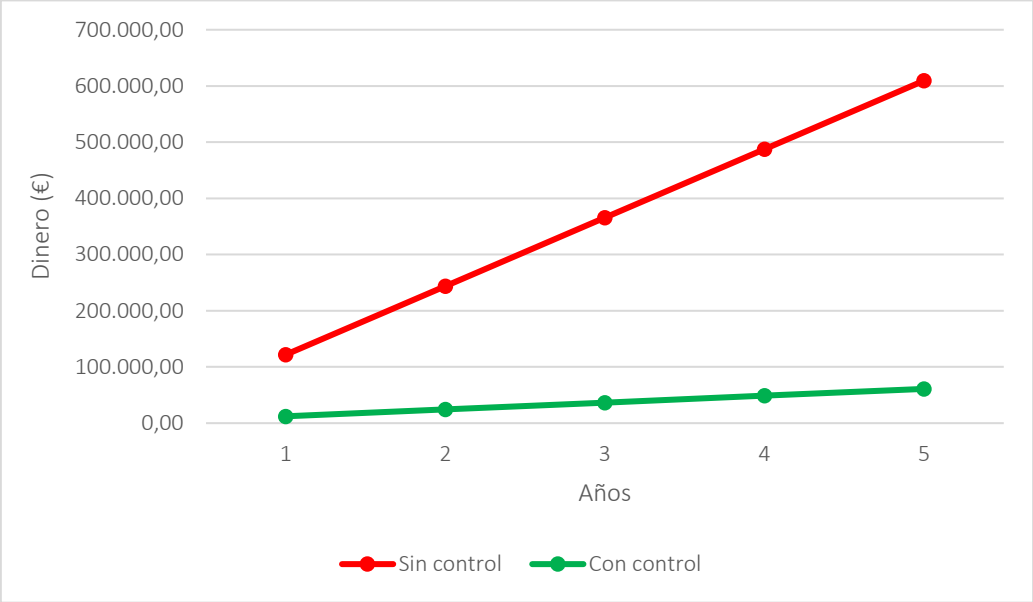



*Ilustración 86. Rentabilidad amenaza SW1 - [A.15] activo S2*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 92. Rentabilidad amenaza SW1 - [A.18] activo S2*

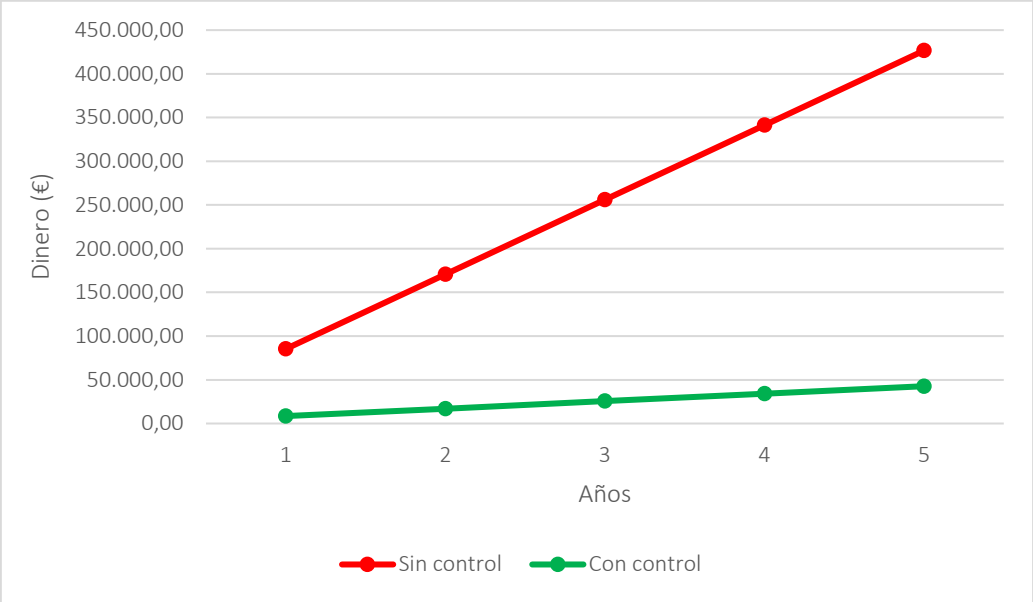



*Ilustración 87. Rentabilidad amenaza SW1 - [A.18] activo S2*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 93. Rentabilidad amenaza SW1 - [A.19] activo S2*

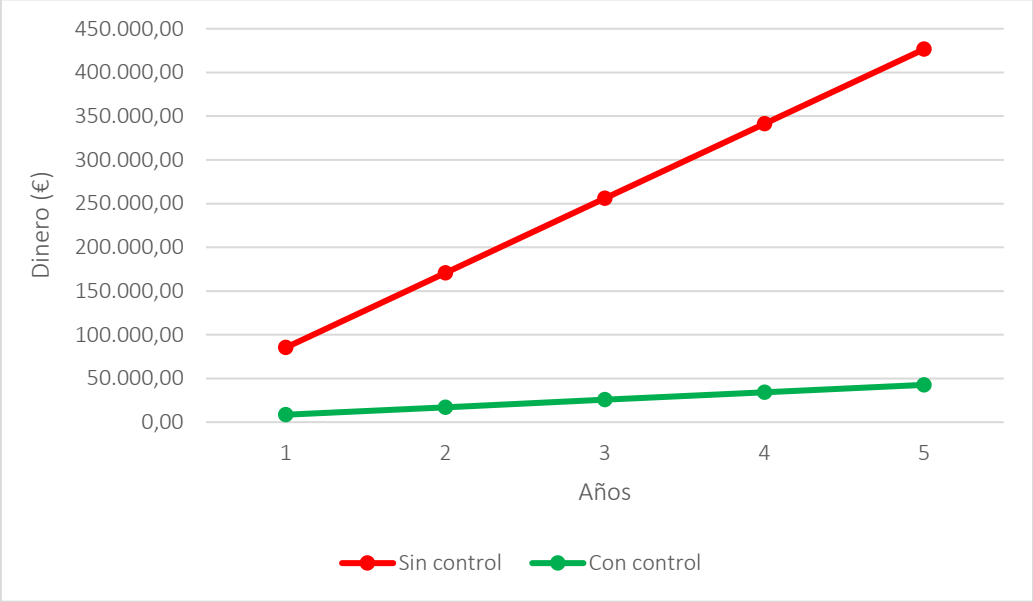



*Ilustración 88. Rentabilidad amenaza SW1 - [A.19] activo S2*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 94. Rentabilidad amenaza SRVD1 - [A.11] activo S2*

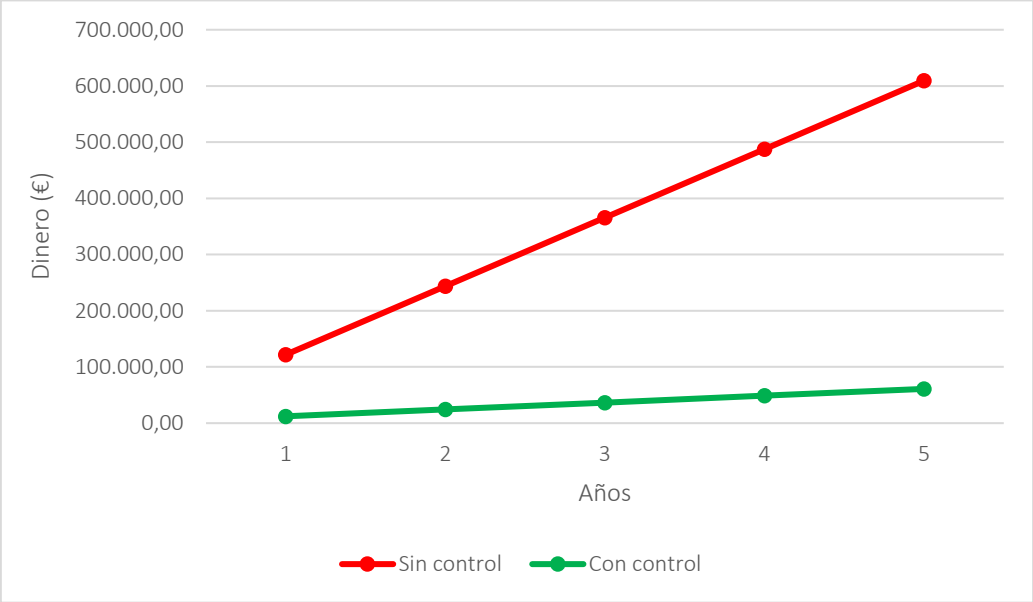



*Ilustración 89. Rentabilidad amenaza SRVD1 - [A.11] activo S2*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 95. Rentabilidad amenaza T1 - [A.11] activo S2*

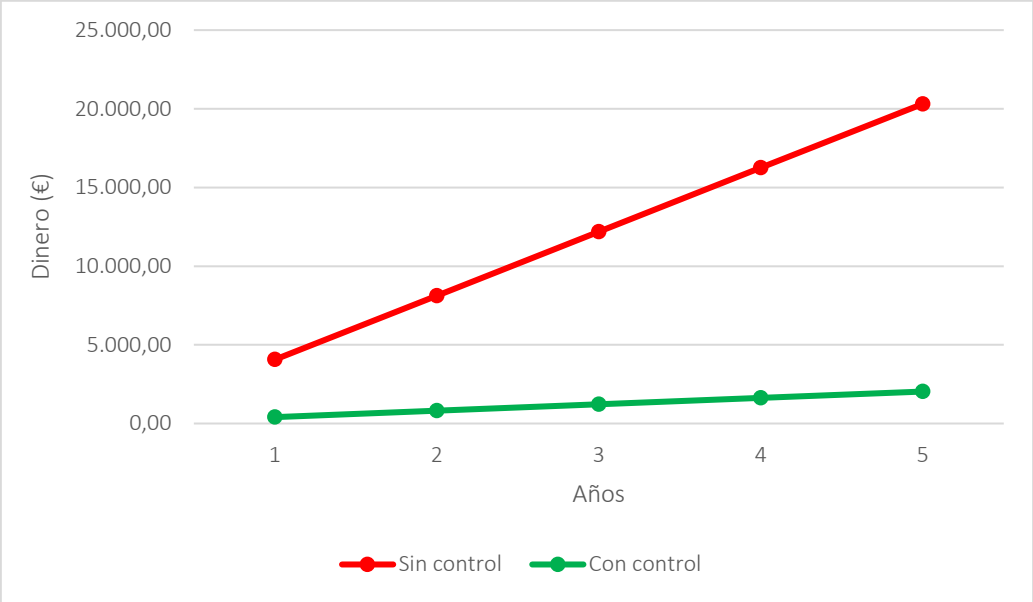



*Ilustración 90. Rentabilidad amenaza T1 - [A.11] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 96. Rentabilidad amenaza AUX1 - [A.11] activo S3*

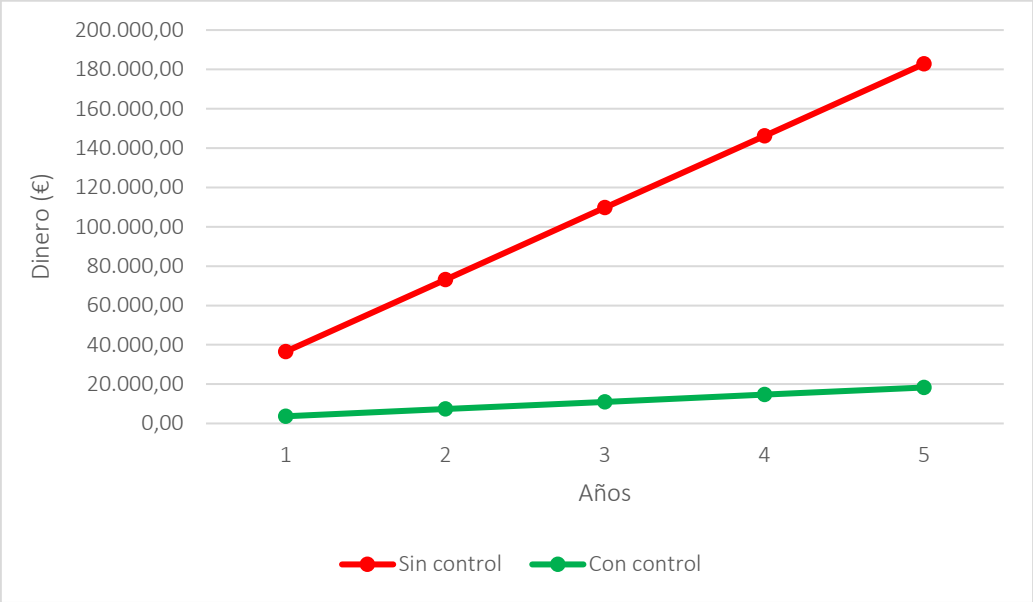



*Ilustración 91. Rentabilidad amenaza AUX1 - [A.11] activo S3*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 97. Rentabilidad amenaza D1 - [A.5] activo S3*

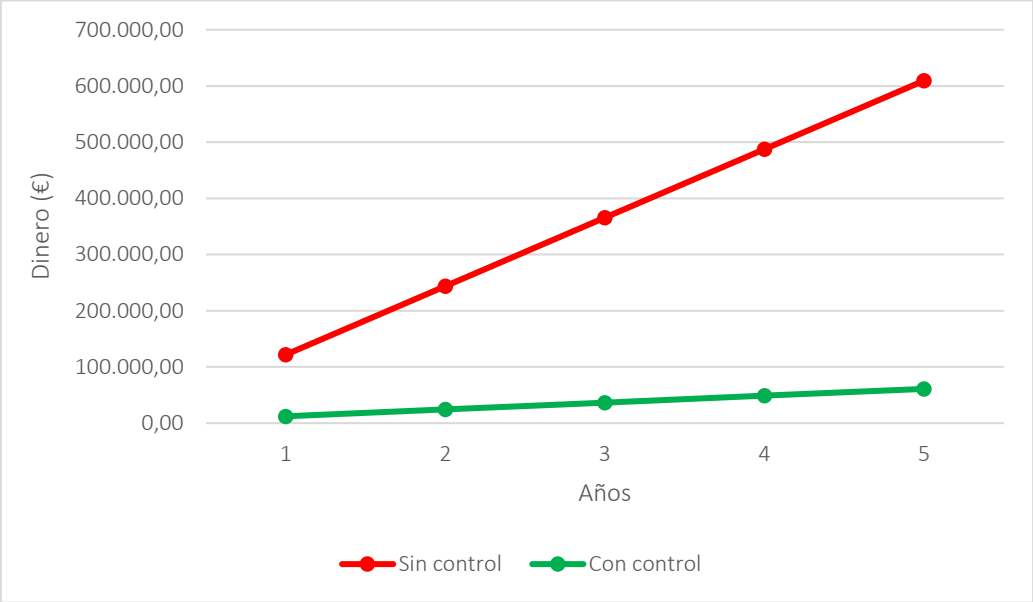



*Ilustración 92. Rentabilidad amenaza D1 - [A.5] activo S3*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 98. Rentabilidad amenaza D1 - [A.11] activo S3*

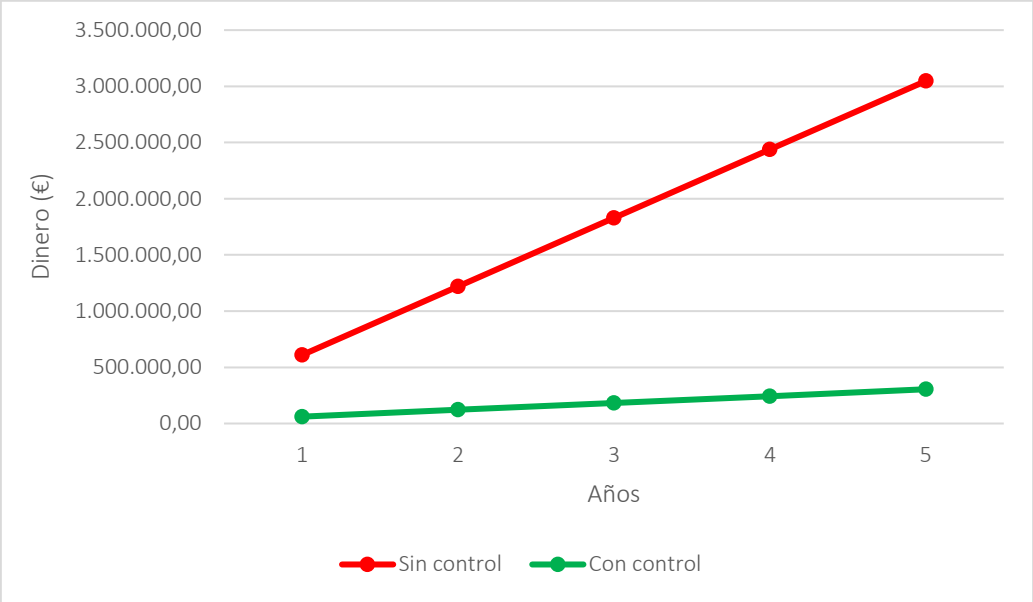



*Ilustración 93. Rentabilidad amenaza D1 - [A.11] activo S3*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 99. Rentabilidad amenaza D1 - [A.18] activo S3*

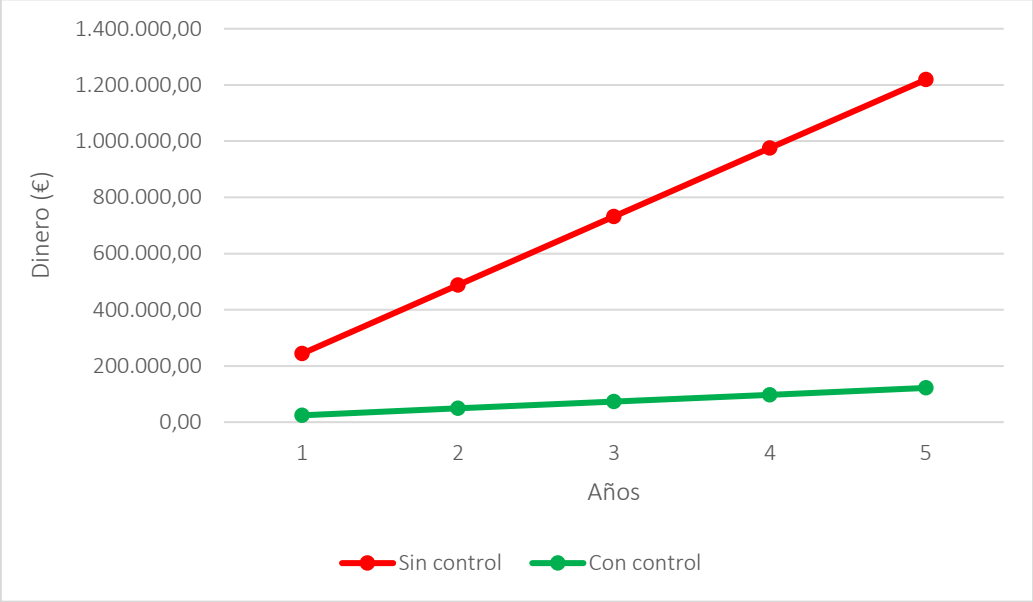



*Ilustración 94. Rentabilidad amenaza D1 - [A.18] activo S3*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 100. Rentabilidad amenaza D1 - [A.19] activo S3*

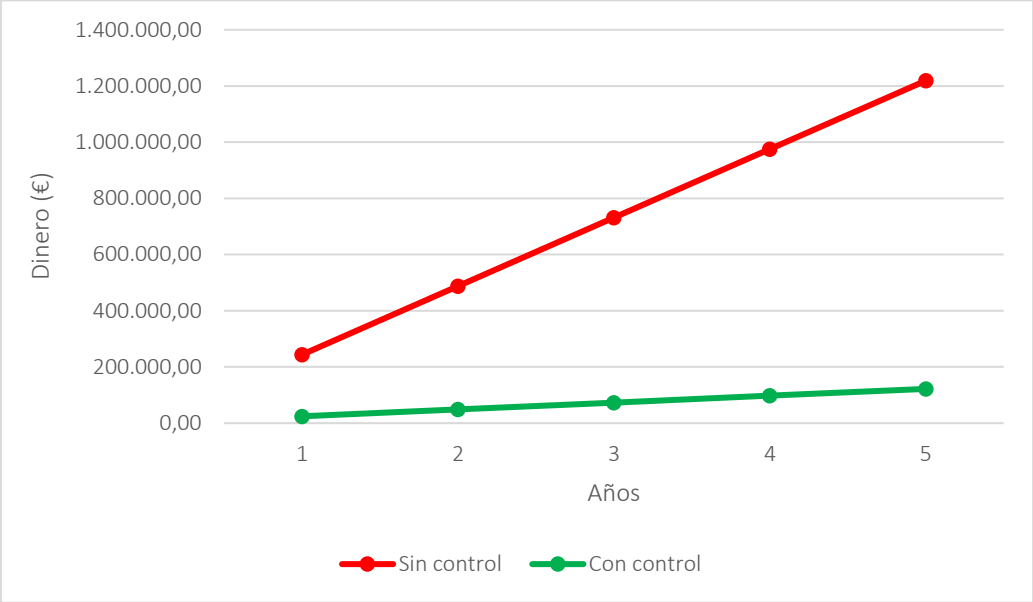



*Ilustración 95. Rentabilidad amenaza D1 - [A.19] activo S3*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 101. Rentabilidad amenaza HW1 - [A.11] activo S3*

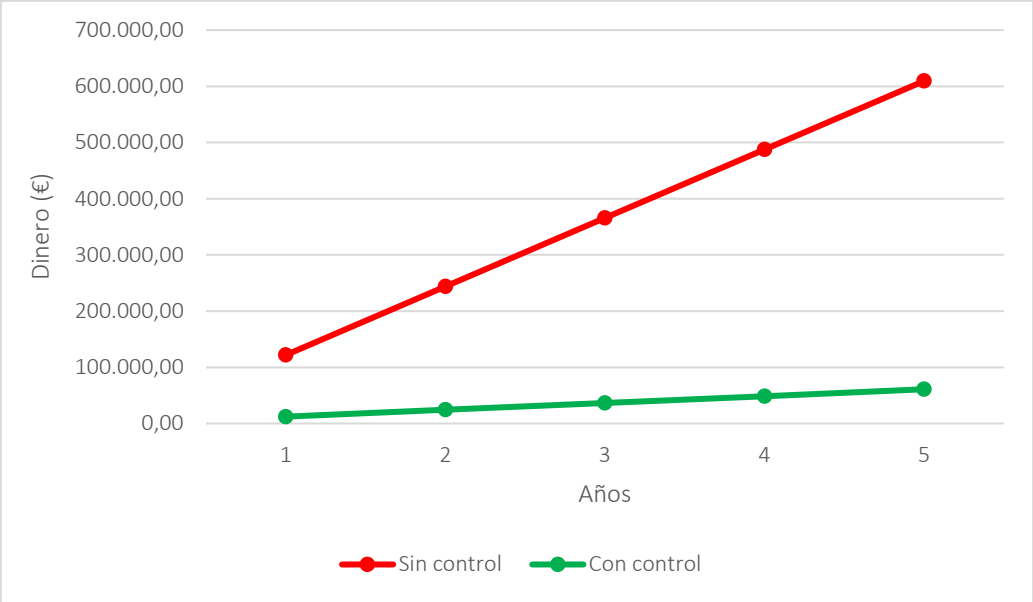



*Ilustración 96. Rentabilidad amenaza HW1 - [A.11] activo S3*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 102. Rentabilidad amenaza SW1 - [A.5] activo S3*

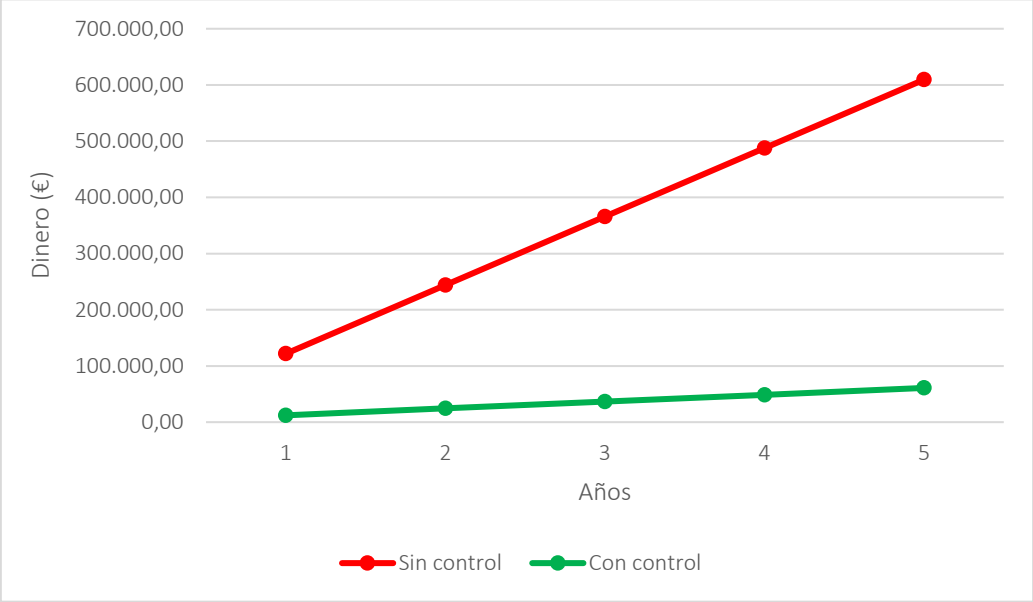



*Ilustración 97. Rentabilidad amenaza SW1 - [A.5] activo S3*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 103. Rentabilidad amenaza SW1 - [A.15] activo S3*

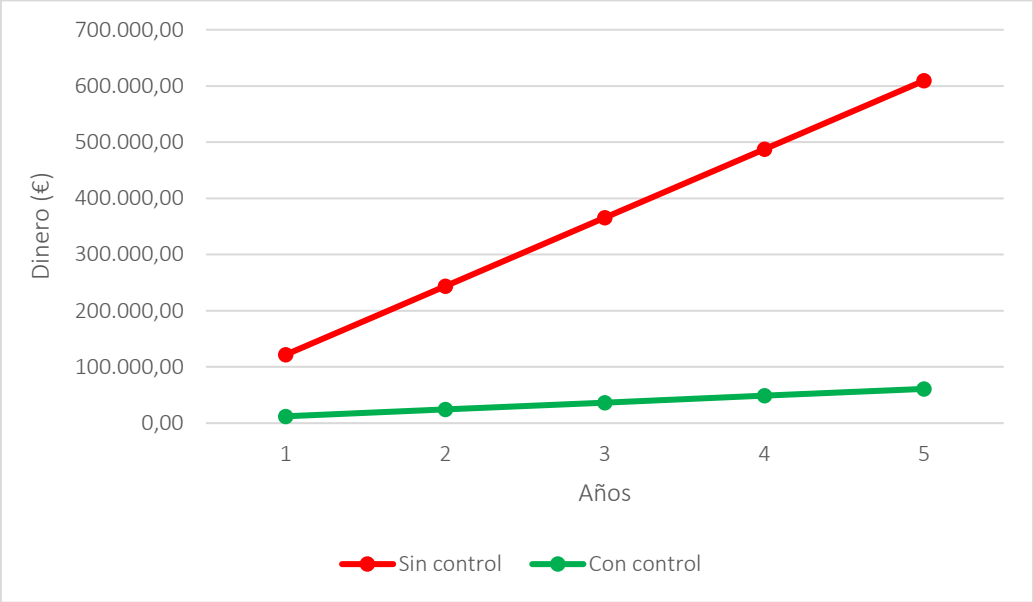



*Ilustración 98. Rentabilidad amenaza SW1 - [A.15] activo S3*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 104. Rentabilidad amenaza SW1 - [A.18] activo S3*

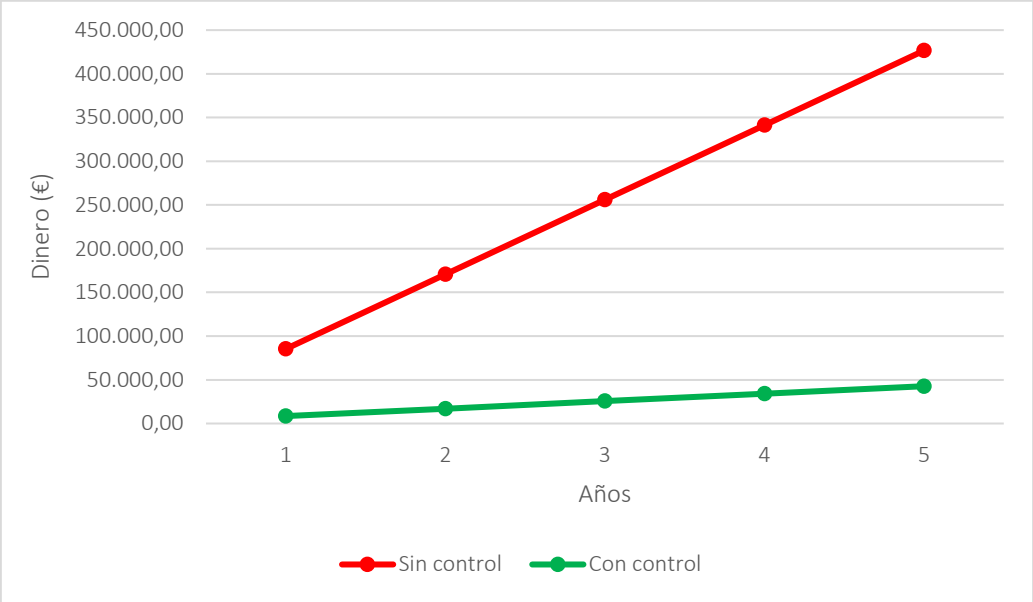



*Ilustración 99. Rentabilidad amenaza SW1 - [A.18] activo S3*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 105. Rentabilidad amenaza SW1 - [A.19] activo S3*

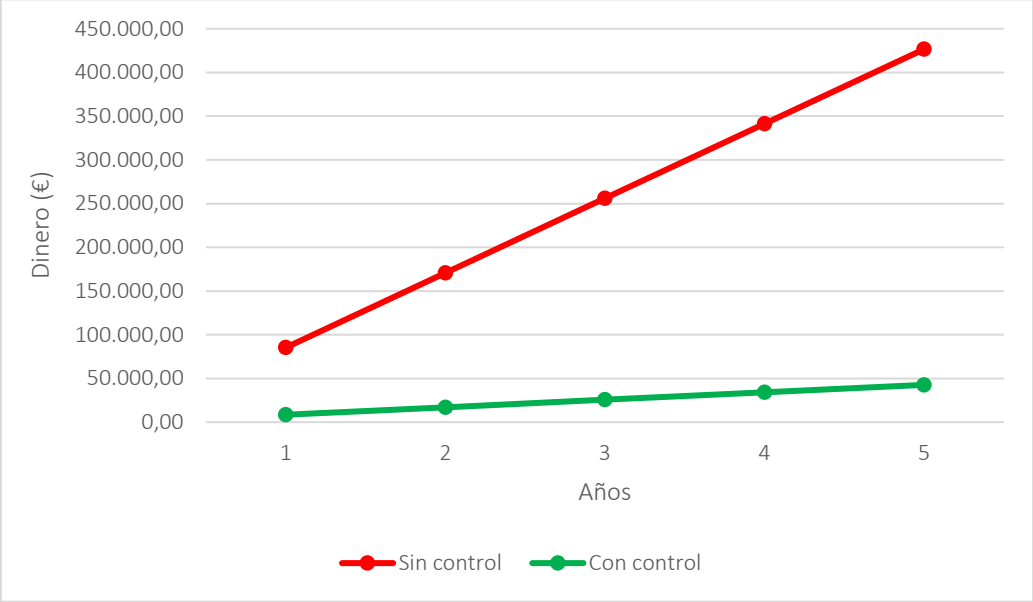



*Ilustración 100. Rentabilidad amenaza SW1 - [A.19] activo S3*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 106. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

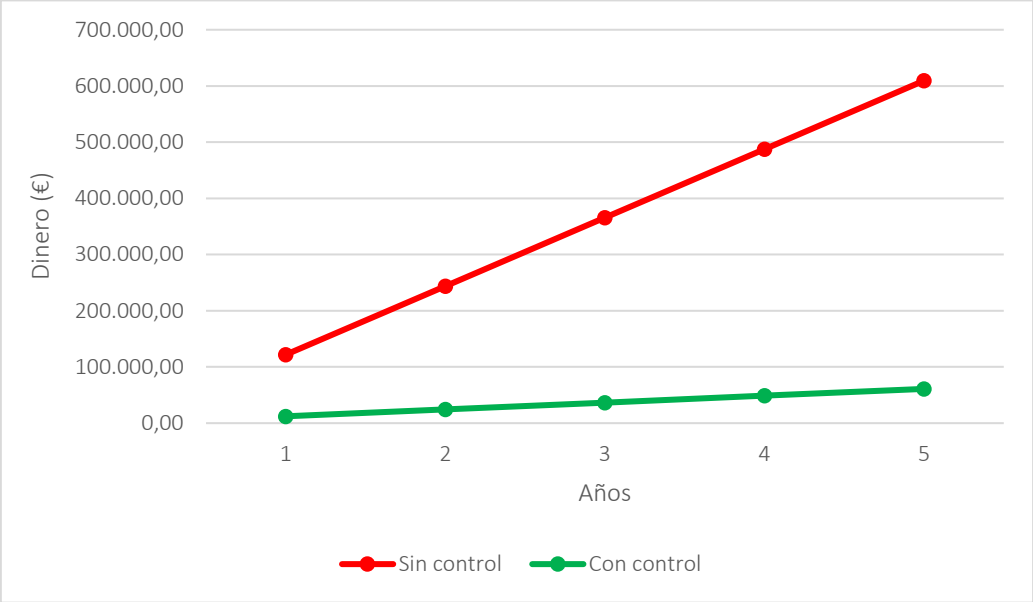



*Ilustración 101. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 107. Rentabilidad amenaza T1 - [A.11] activo S3*

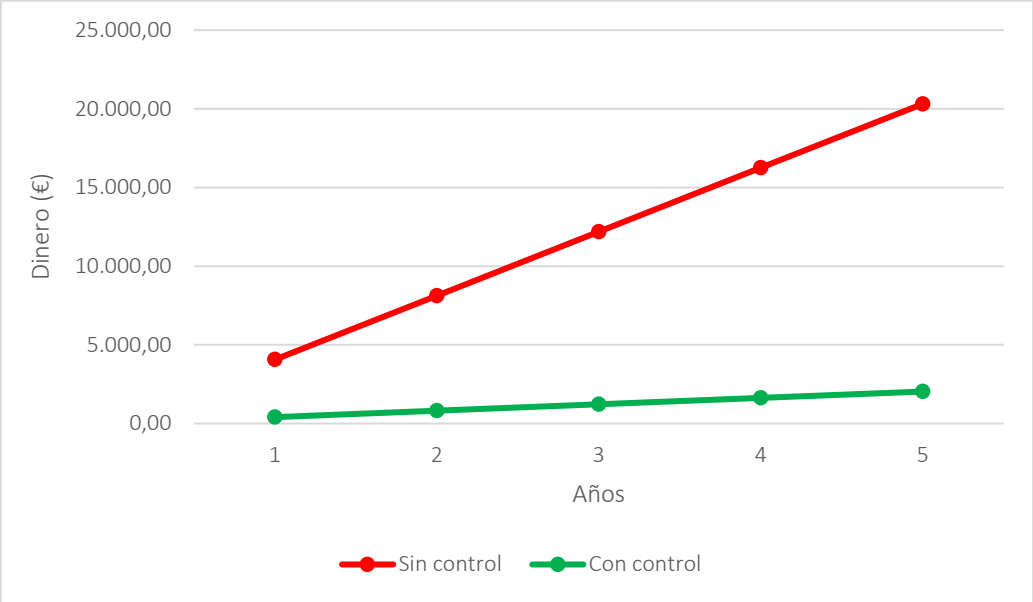



*Ilustración 102. Rentabilidad amenaza T1 - [A.11] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36562,54 | 0 | 0 | 36562,54 | 73125,08 | 109687,62 | 146250,16 | 182812,7 |
| 3656,25 | 0 | 0 | 3656,25 | 7312,5 | 10968,75 | 14625 | 18281,25 |

*Tabla 108. Rentabilidad amenaza AUX1 - [A.11] activo S4*

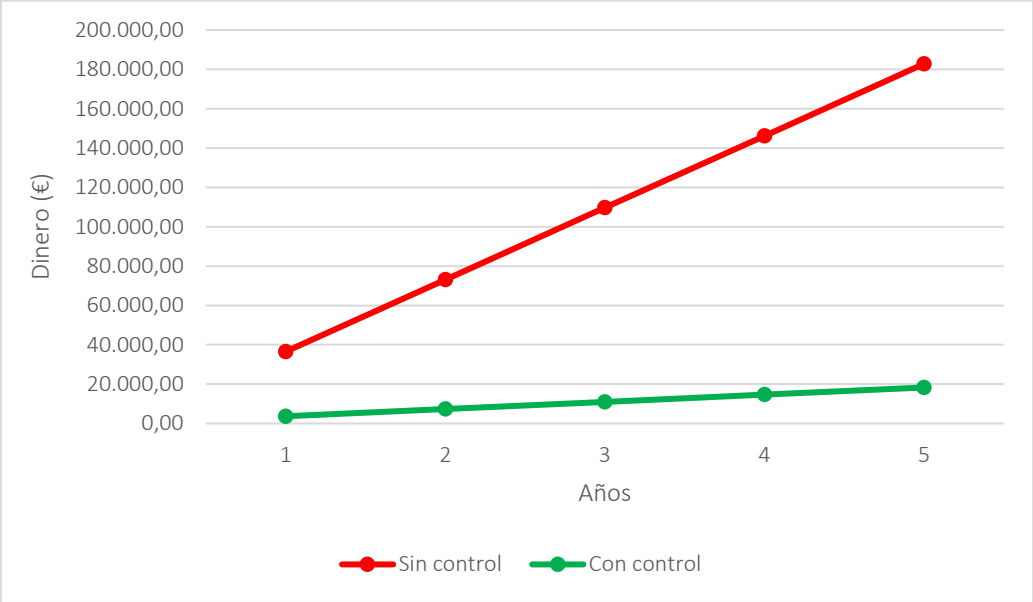



*Ilustración 103. Rentabilidad amenaza AUX1 - [A.11] activo S4*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 109. Rentabilidad amenaza D1 - [A.5] activo S4*

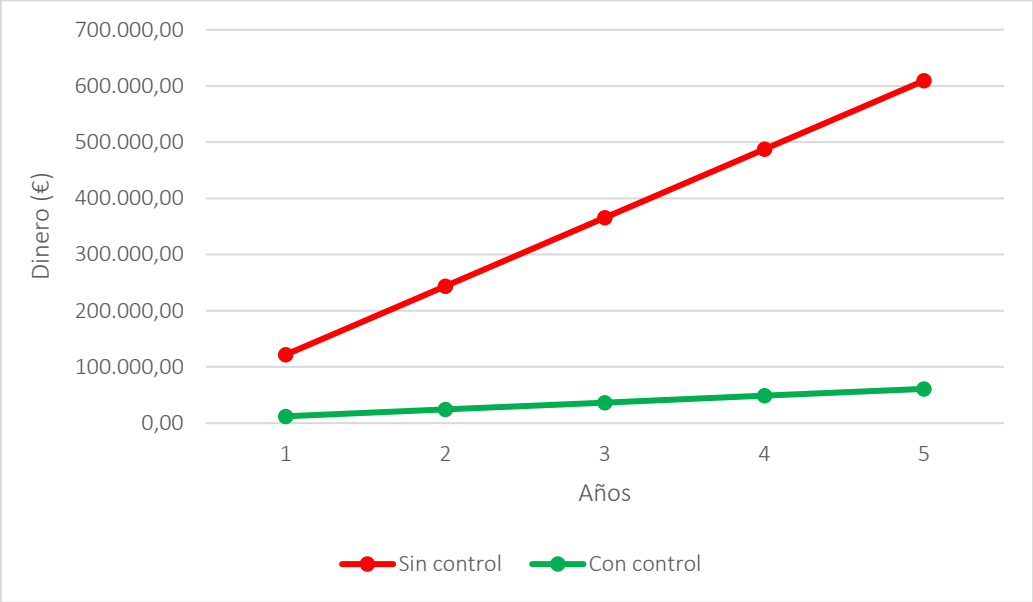



*Ilustración 104. Rentabilidad amenaza D1 - [A.5] activo S4*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609375,71 | 0 | 0 | 609375,71 | 1218751,4 | 1828127,13 | 2437502,84 | 3046878,55 |
| 60937,57 | 0 | 0 | 60937,57 | 121875,14 | 182812,71 | 243750,28 | 304687,85 |

*Tabla 110. Rentabilidad amenaza D1 - [A.5] activo S4*

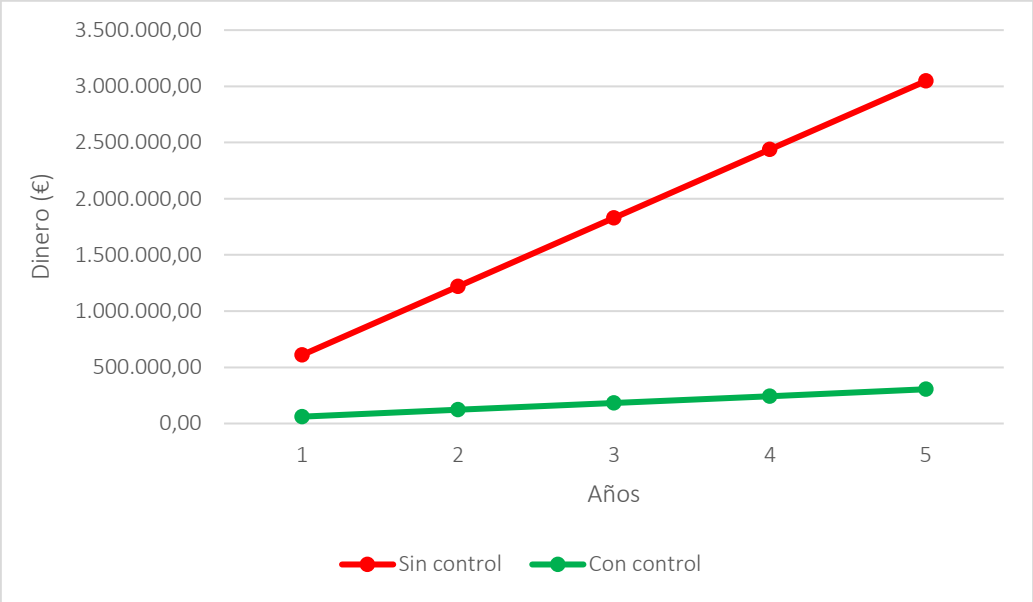



*Ilustración 105. Rentabilidad amenaza D1 - [A.5] activo S4*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

***Tabla 111. Rentabilidad amenaza D1 - [A.5] activo S4***

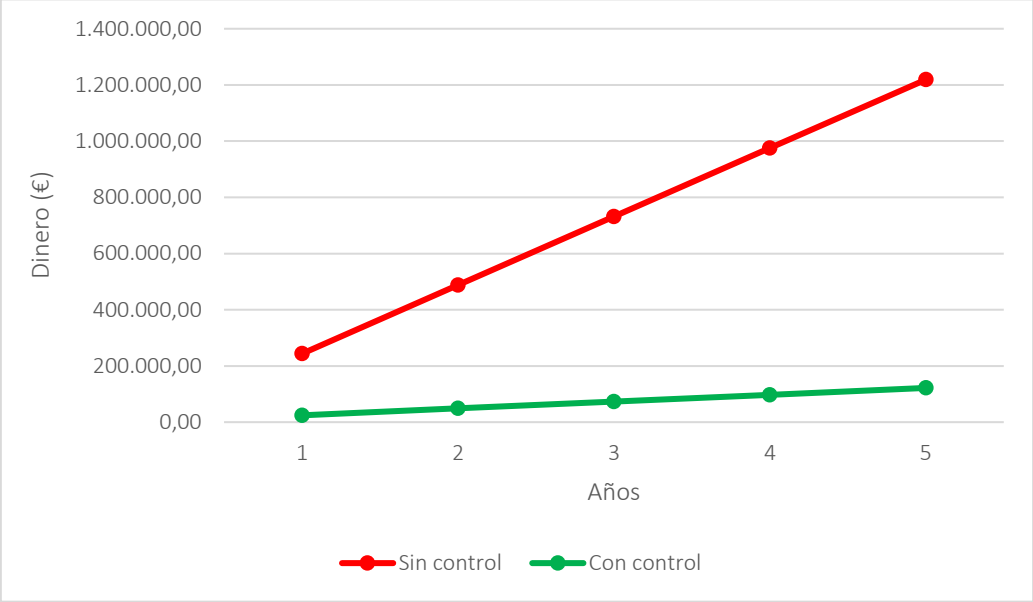



***Ilustración 106. Rentabilidad amenaza D1 - [A.5] activo S4***

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

***Tabla 112. Rentabilidad amenaza D1 - [A.19] activo S4***

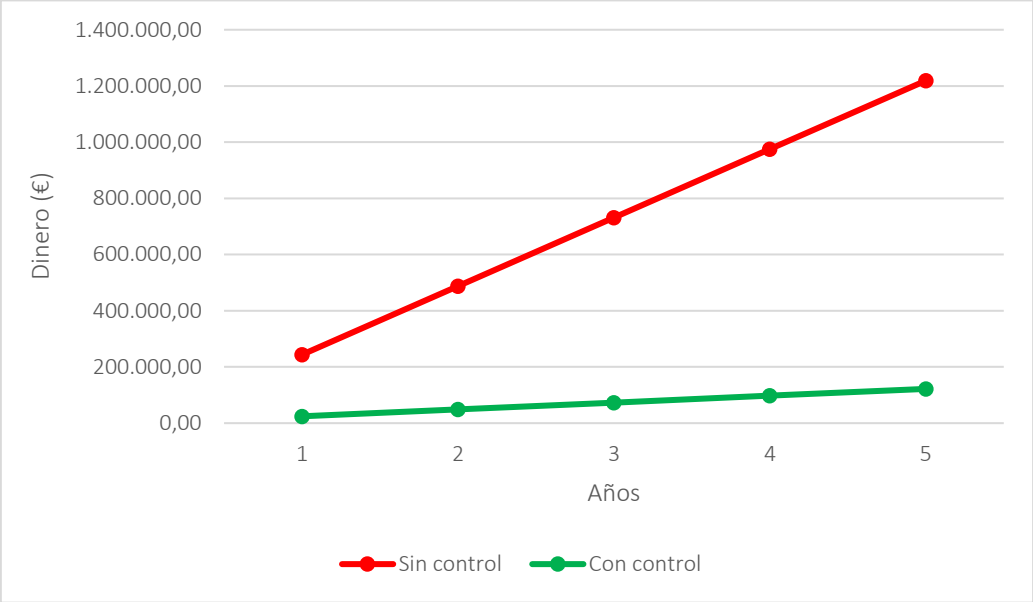



*Ilustración 107. Rentabilidad amenaza D1 - [A.19] activo S4*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 113. Rentabilidad amenaza HW1 - [A.19] activo S4*

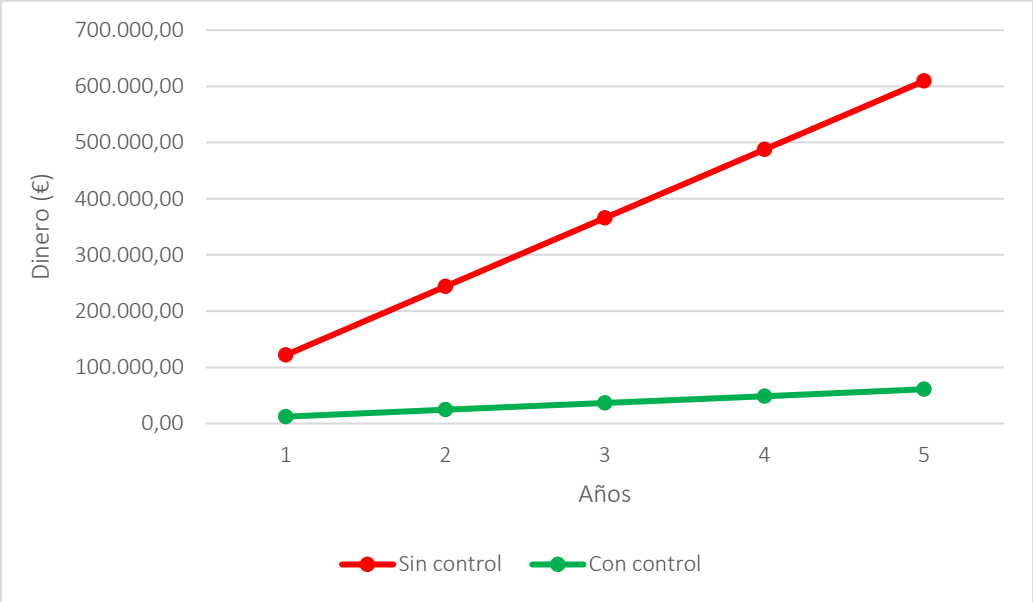



*Ilustración 108. Rentabilidad amenaza HW1 - [A.19] activo S4*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 114. Rentabilidad amenaza SW1 - [A.5] activo S4*

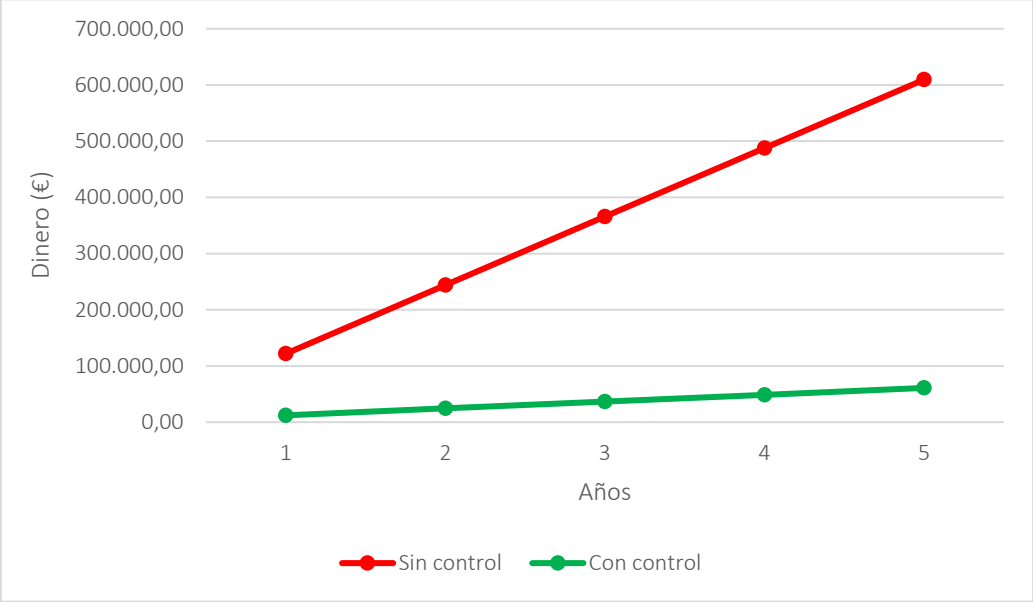



*Ilustración 109. Rentabilidad amenaza SW1 - [A.5] activo S4*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 115. Rentabilidad amenaza SW1 - [A.15] activo S4*

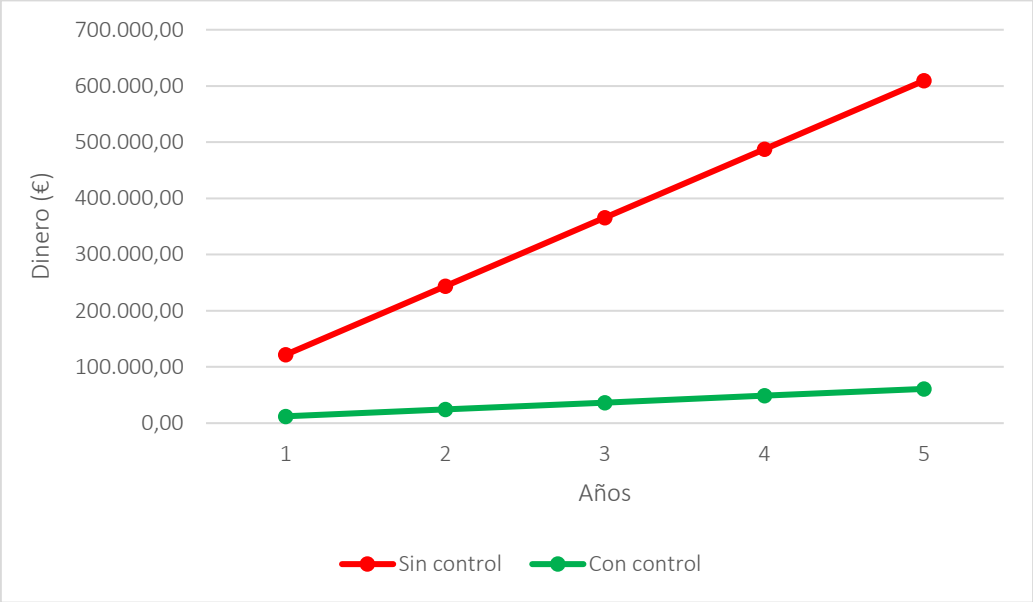



*Ilustración 110. Rentabilidad amenaza SW1 - [A.15] activo S4*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85312,6 | 0 | 0 | 85312,6 | 170625,2 | 255937,8 | 341250,4 | 426563 |
| 8531,26 | 0 | 0 | 8531,26 | 17062,52 | 25593,78 | 34125,04 | 42656,3 |

*Tabla 116. Rentabilidad amenaza SW1 - [A.18] activo S4*

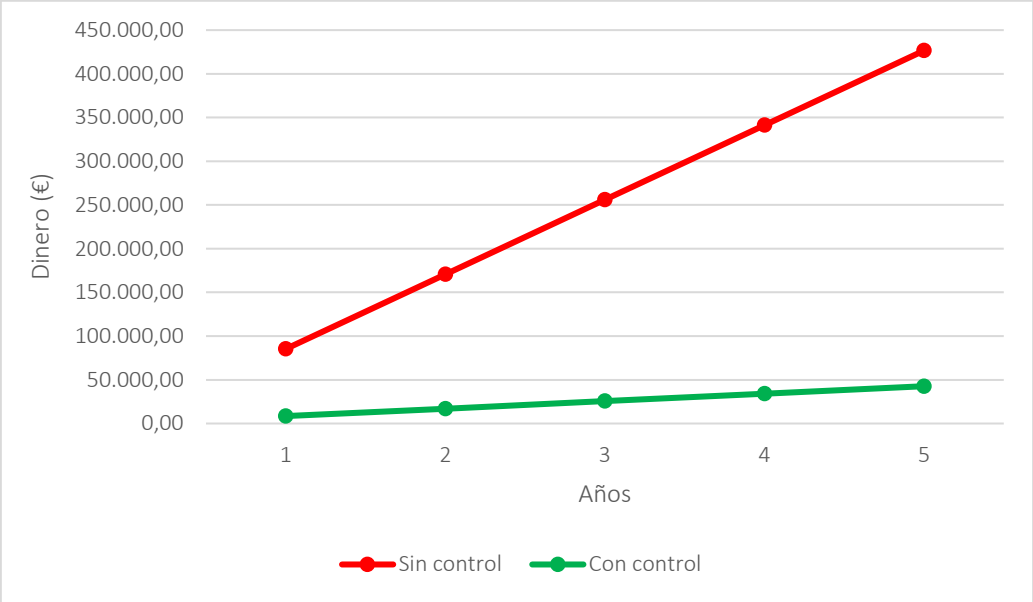



*Ilustración 111. Rentabilidad amenaza SW1 - [A.18] activo S4*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85312,6 | 0 | 0 | 85312,6 | 170625,2 | 255937,8 | 341250,4 | 426563 |
| 8531,26 | 0 | 0 | 8531,26 | 17062,52 | 25593,78 | 34125,04 | 42656,3 |

*Tabla 117. Rentabilidad amenaza SW1 - [A.19] activo S4*

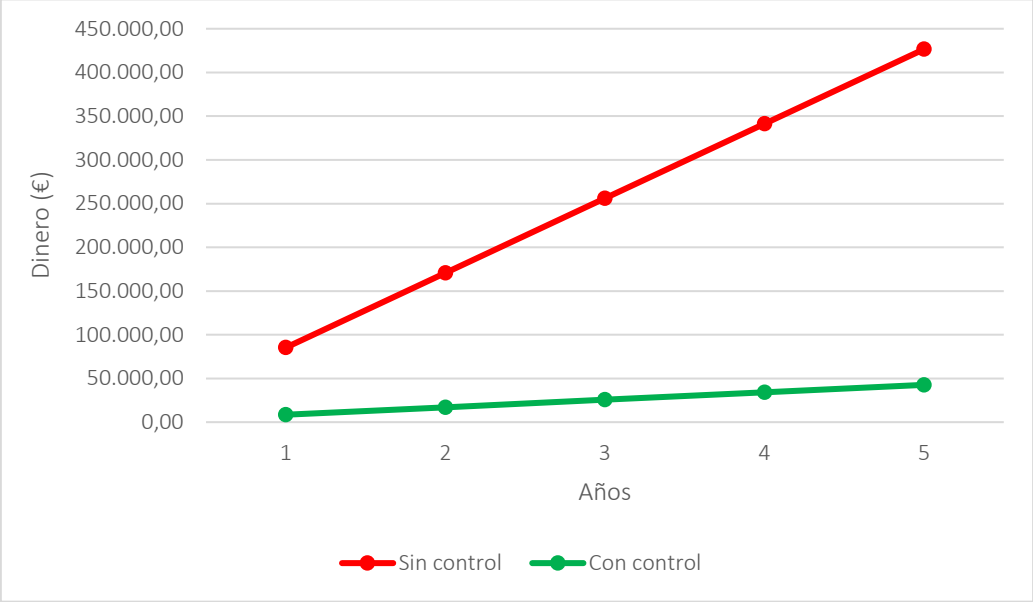



*Ilustración 112. Rentabilidad amenaza SW1 - [A.19] activo S4*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 118. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

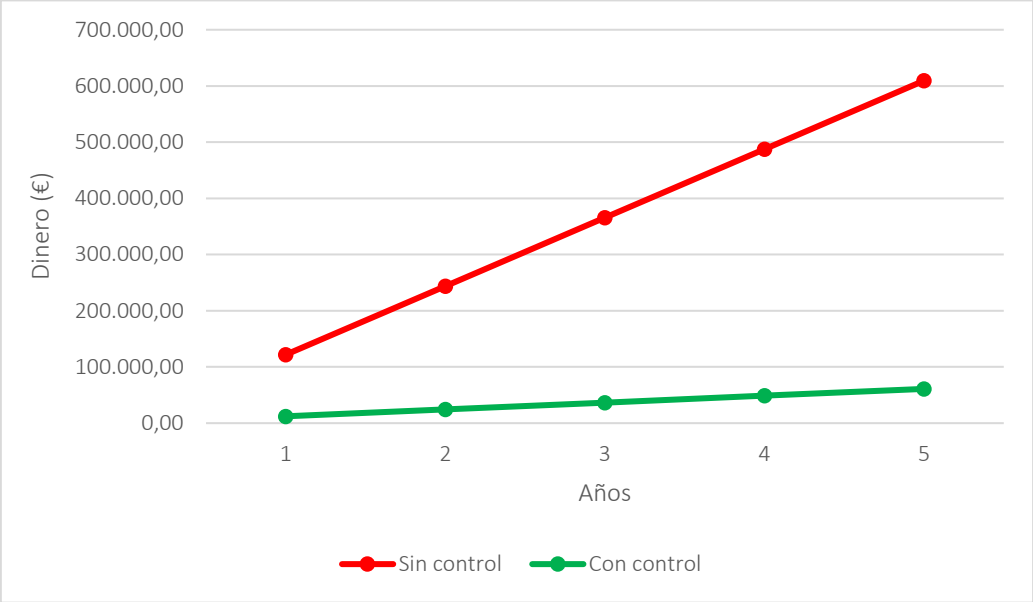



*Ilustración 113. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,5 | 0 | 0 | 4062,5 | 8125 | 12187,5 | 16250 | 20312,5 |
| 406,25 | 0 | 0 | 406,25 | 812,5 | 1218,75 | 1625 | 2031,25 |

*Tabla 119. Rentabilidad amenaza T1 - [A.11] activo S4*

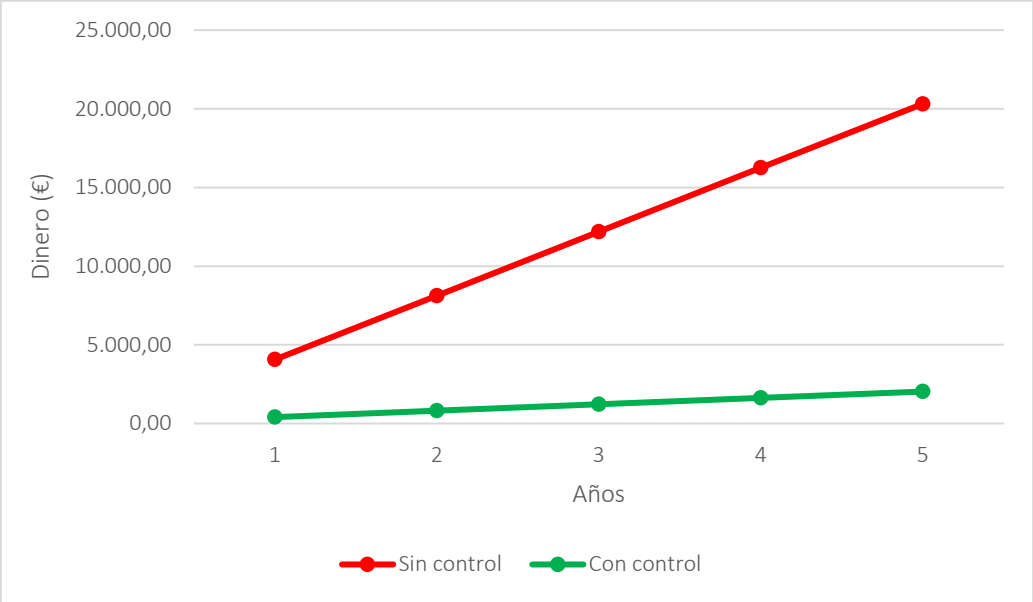



*Ilustración 114. Rentabilidad amenaza T1 - [A.11] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 120. Rentabilidad amenaza AUX1 - [A.11] - activo S5*

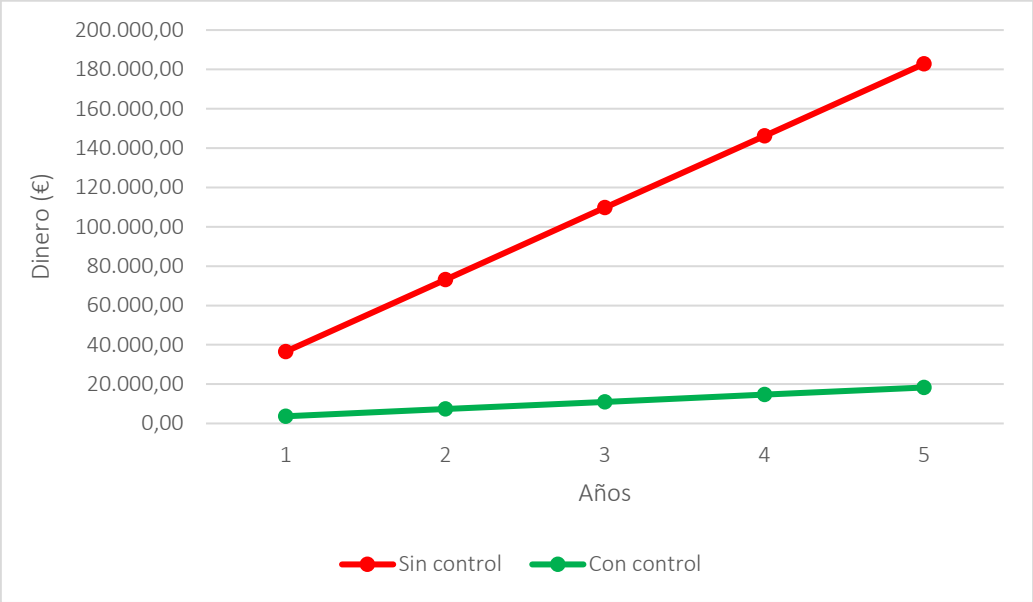



*Ilustración 115. Rentabilidad amenaza AUX1 - [A.11] - activo S5*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 121. Rentabilidad amenaza D1 - [A.5] - activo S5*

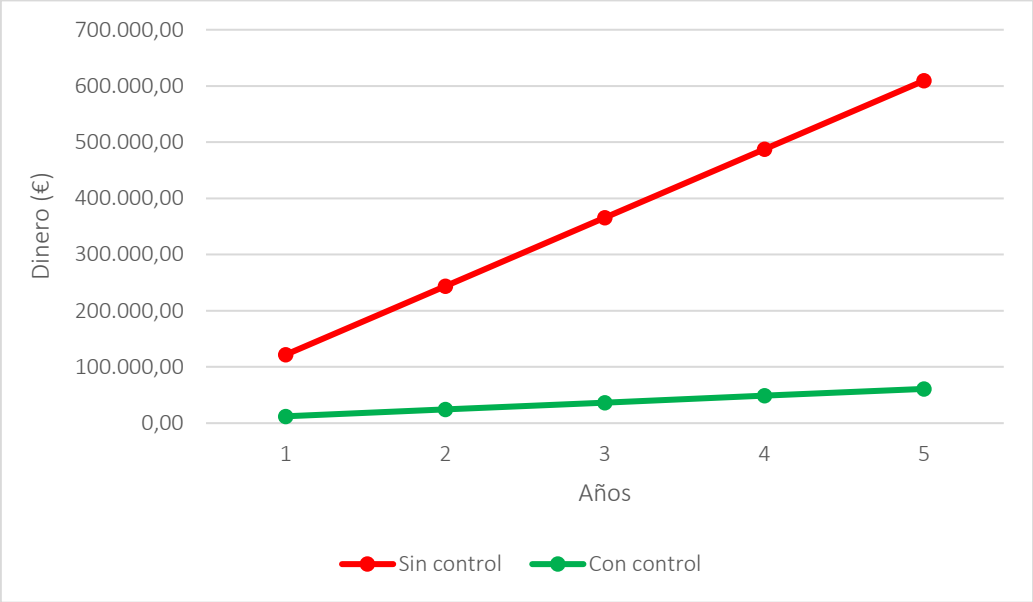



*Ilustración 116. Rentabilidad amenaza D1 - [A.5] - activo S5*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 122. Rentabilidad amenaza D1 - [A.11] - activo S5*

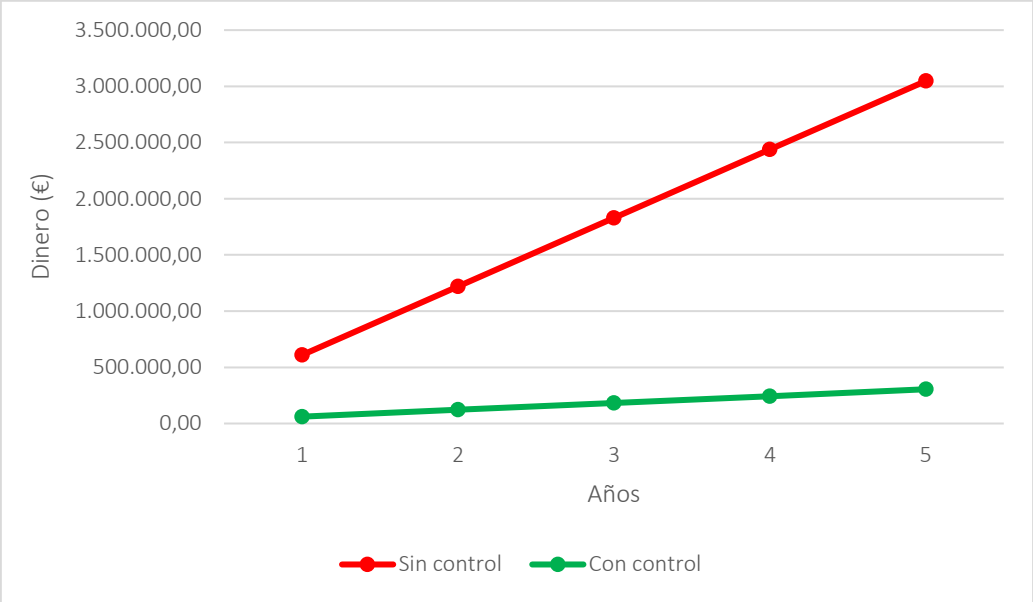



*Ilustración 117. Rentabilidad amenaza D1 - [A.11] - activo S5*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 123. Rentabilidad amenaza D1 - [A.18] - activo S5***

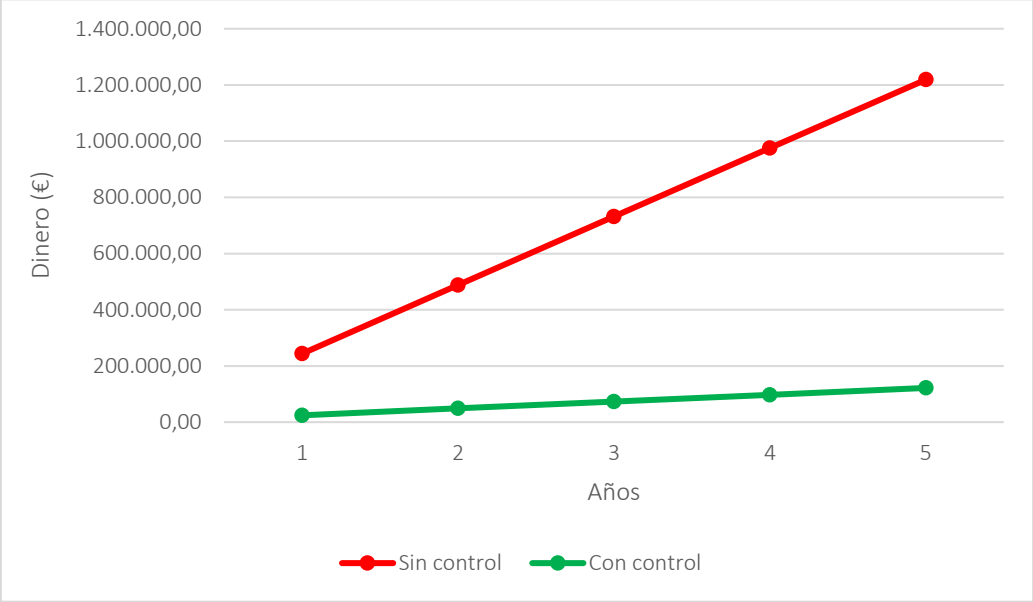



***Ilustración 118. Rentabilidad amenaza D1 - [A.18] - activo S5***

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 124. Rentabilidad amenaza D1 - [A.19] - activo S5***

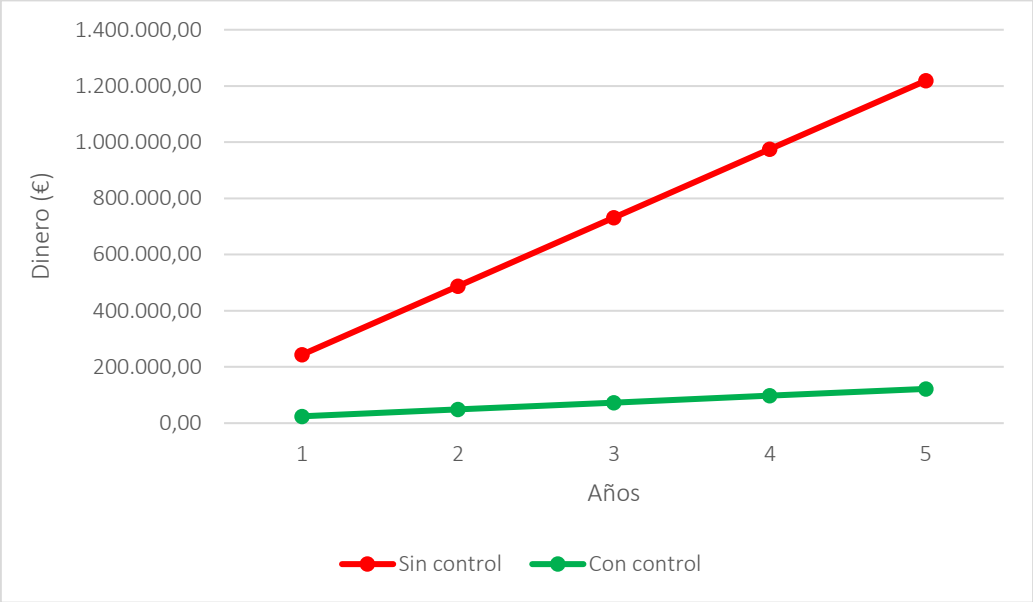



*Ilustración 119. Rentabilidad amenaza D1 - [A.19] - activo S5*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 125. Rentabilidad amenaza HW1 - [A.11] - activo S5*

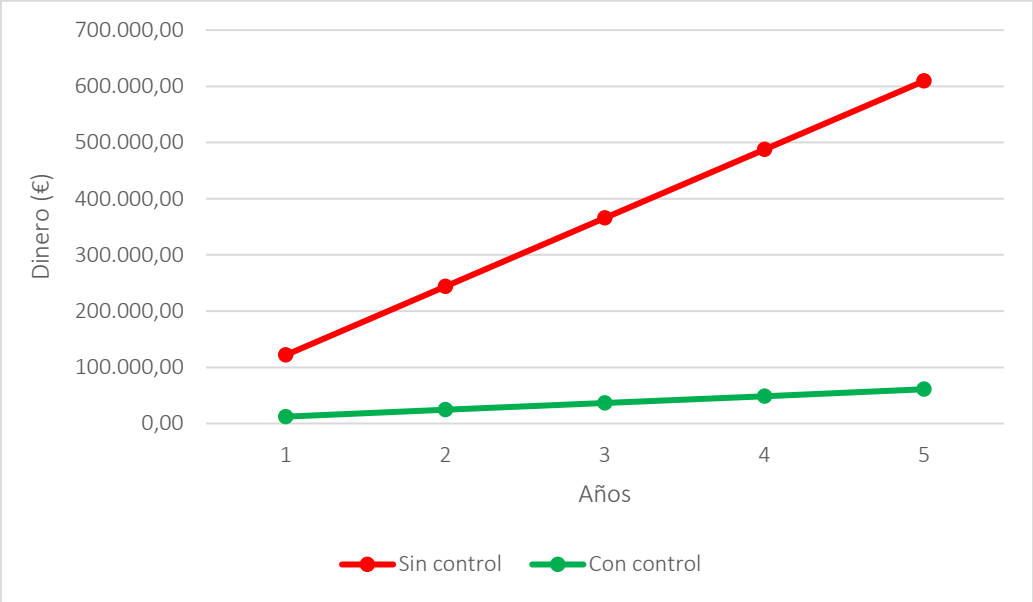



*Ilustración 120. Rentabilidad amenaza HW1 - [A.11] - activo S5*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 126. Rentabilidad amenaza SW1 - [A.5] - activo S5*

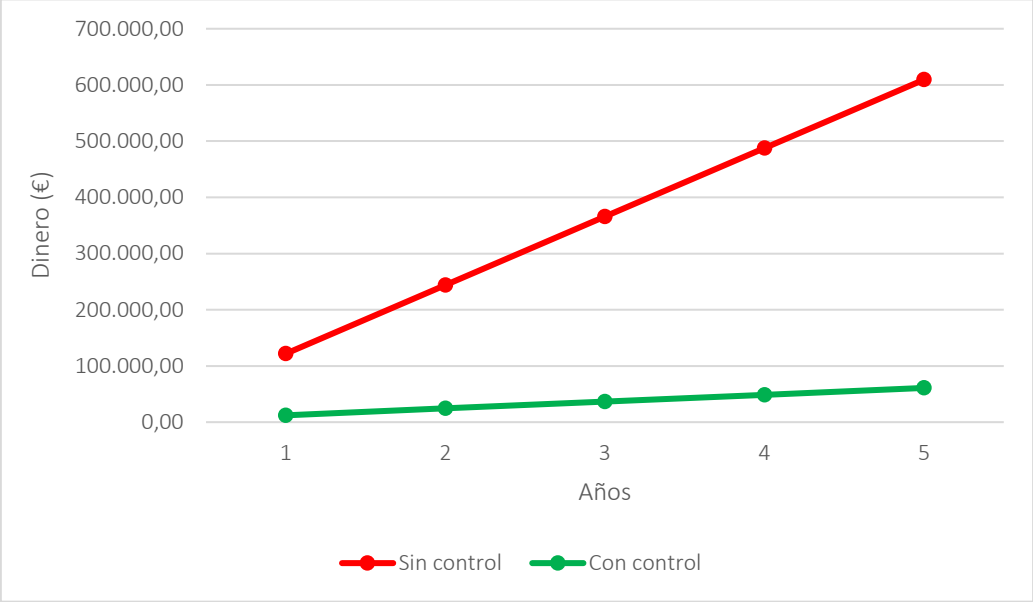



*Ilustración 121. Rentabilidad amenaza SW1 - [A.5] - activo S5*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 127. Rentabilidad amenaza SW1 - [A.15] - activo S5*

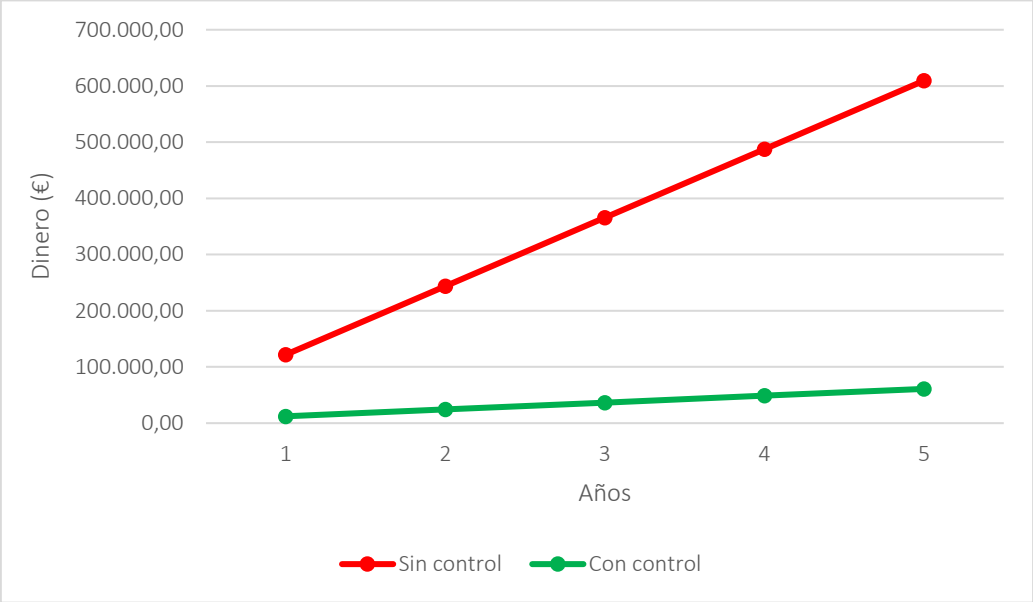



*Ilustración 122. Rentabilidad amenaza SW1 - [A.15] - activo S5*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 128. Rentabilidad amenaza SW1 - [A.18] - activo S5*

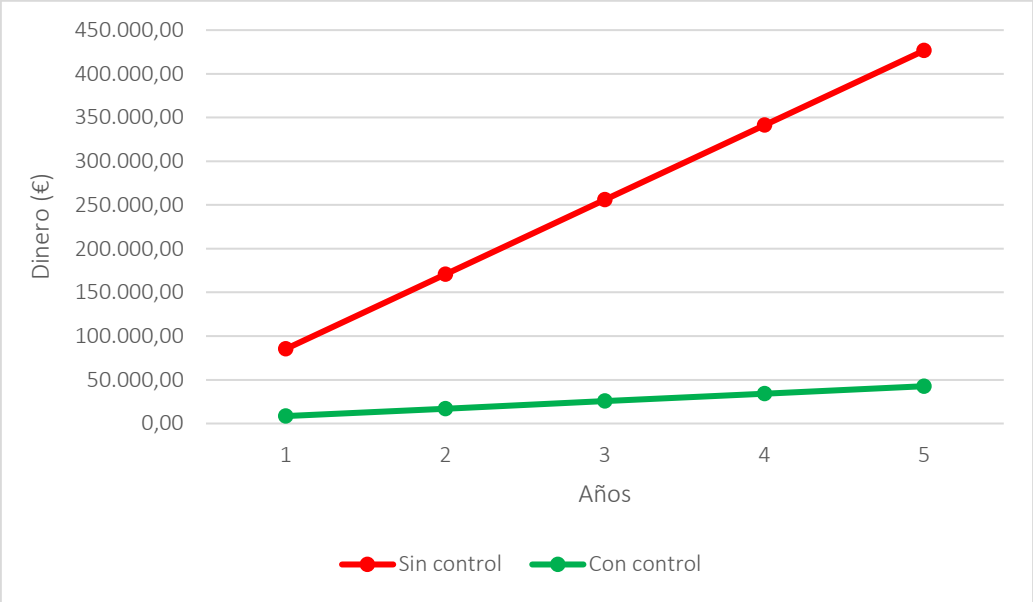



*Ilustración 123. Rentabilidad amenaza SW1 - [A.18] - activo S5*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 129. Rentabilidad amenaza SW1 - [A.19] - activo S5*

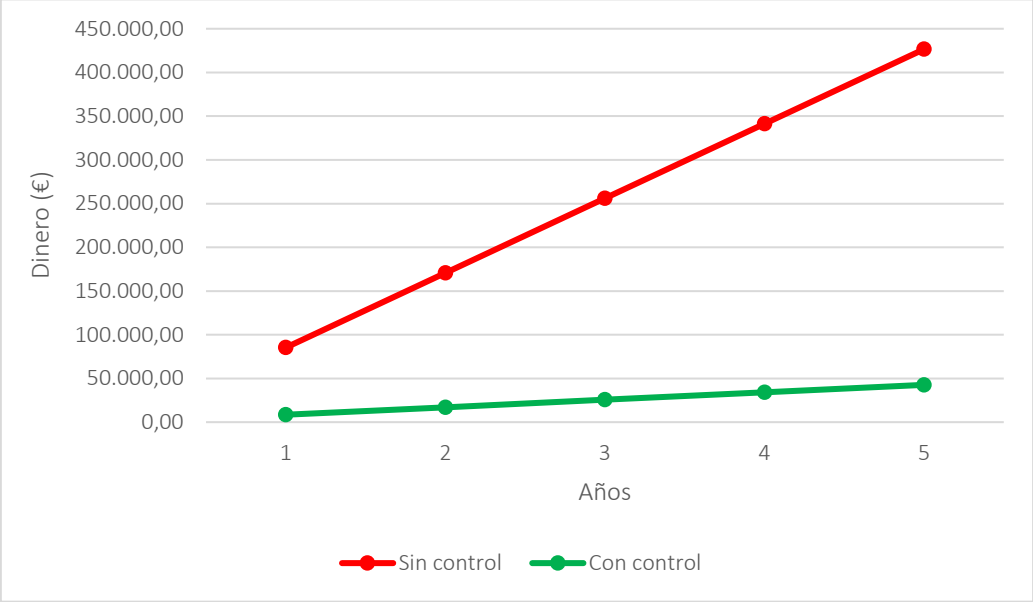



*Ilustración 124. Rentabilidad amenaza SW1 - [A.19] - activo S5*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 130. Rentabilidad amenaza SRVD1 - [A.11] - activo S5*

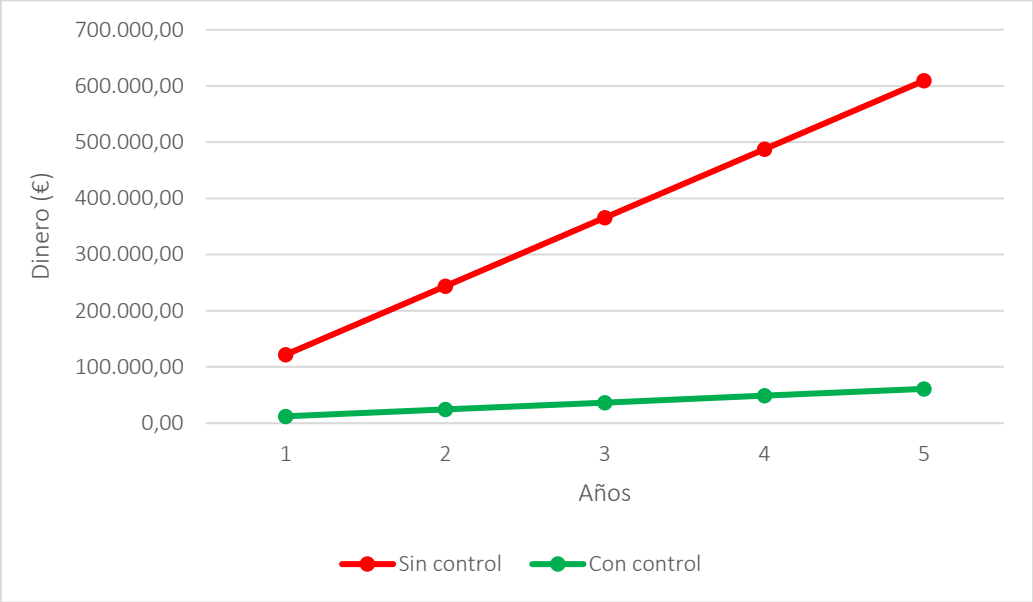



*Ilustración 125. Rentabilidad amenaza SRVD1 - [A.11] - activo S5*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 131. Rentabilidad amenaza T1 - [A.11] - activo S5*

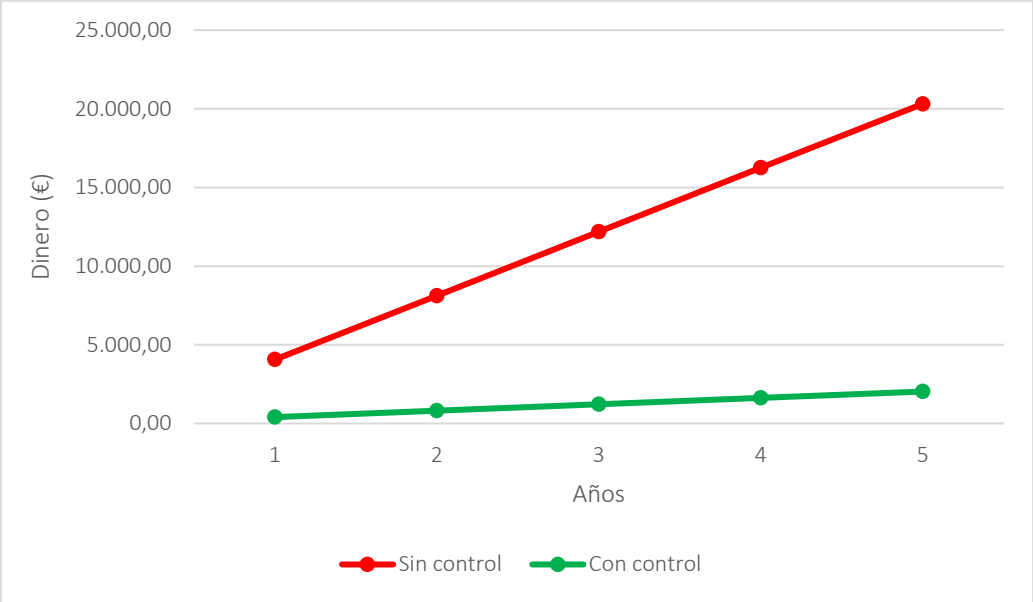



*Ilustración 126. Rentabilidad amenaza T1 - [A.11] - activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 132. Rentabilidad amenaza AUX1 - [A.11] activo S6*

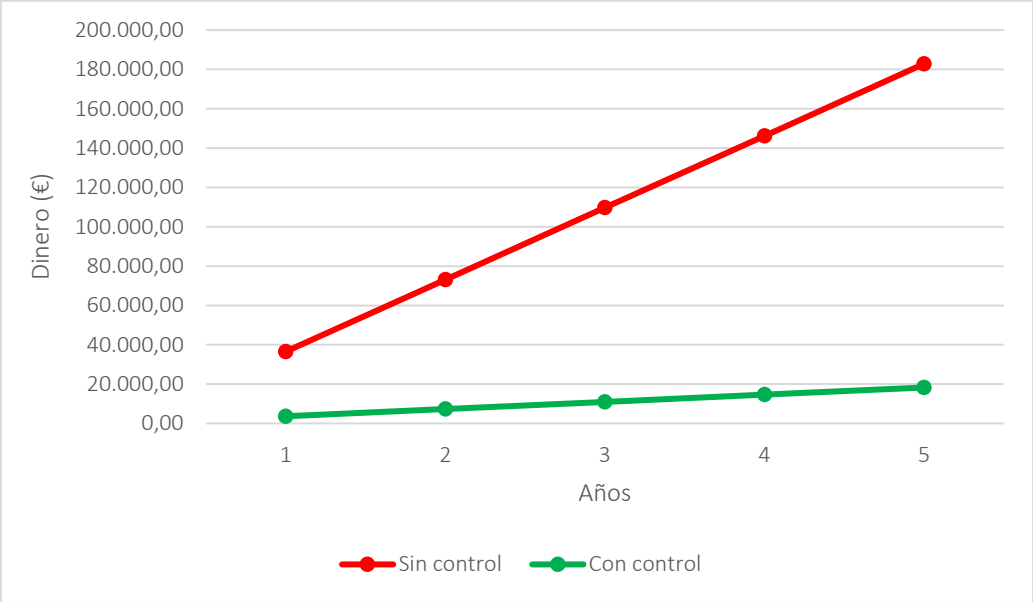



*Ilustración 127. Rentabilidad amenaza AUX1 - [A.11] activo S6*

Amenaza: D1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 133. Rentabilidad amenaza D1 - [A.5] activo S6*

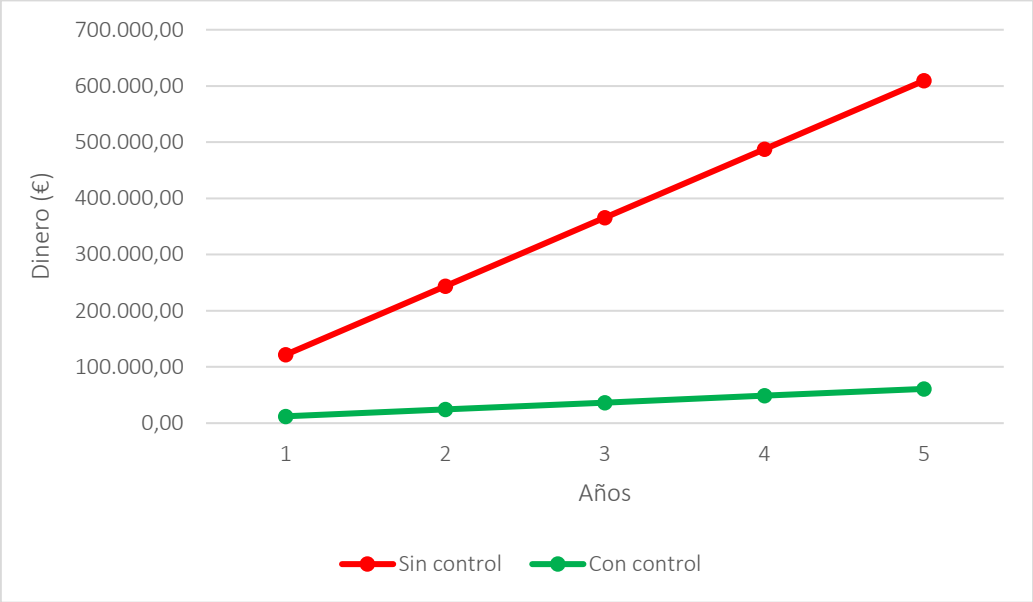



*Ilustración 128. Rentabilidad amenaza D1 - [A.5] activo S6*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 134. Rentabilidad amenaza D1 - [A.11] activo S6*

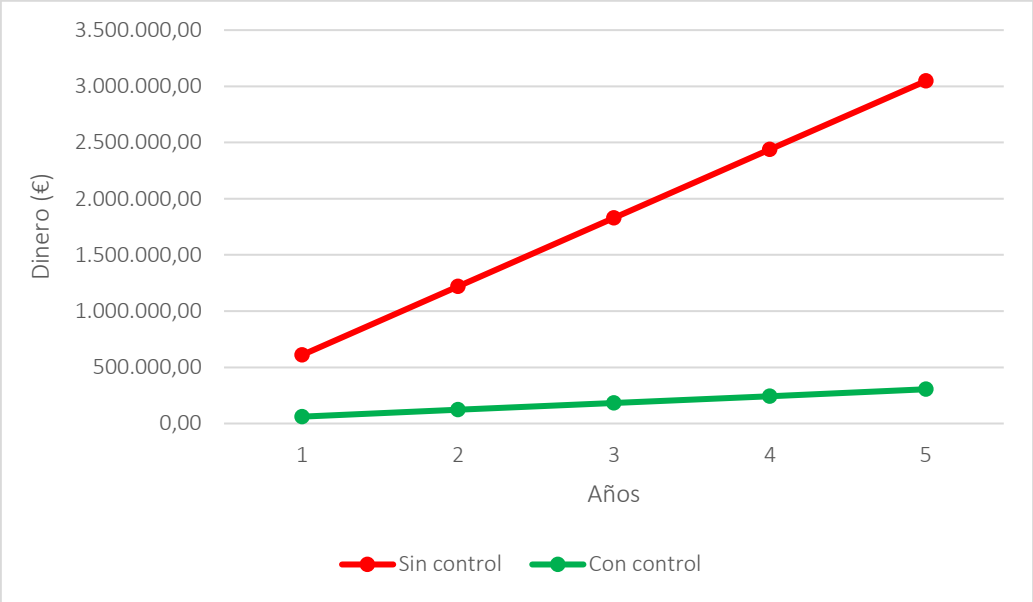



*Ilustración 129. Rentabilidad amenaza D1 - [A.11] activo S6*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 135. Rentabilidad amenaza D1 - [A.18] activo S6***

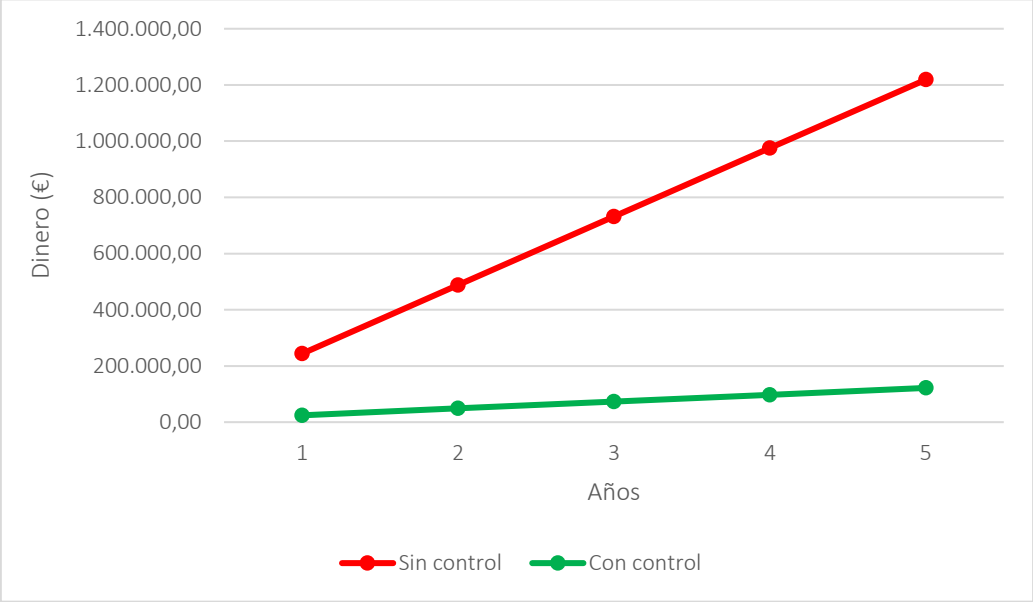



***Ilustración 130. Rentabilidad amenaza D1 - [A.18] activo S6***

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 136. Rentabilidad amenaza D1 - [A.19] activo S6***

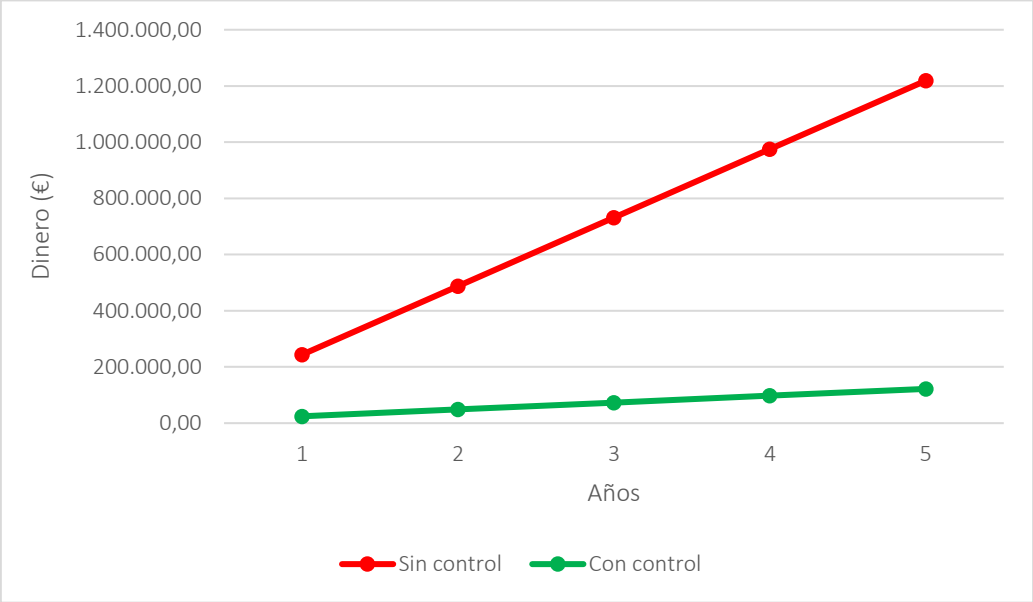



*Ilustración 131. Rentabilidad amenaza D1 - [A.18] activo S6*

Amenaza: HW1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 137. Rentabilidad amenaza HW1 - [A.11] activo S6*

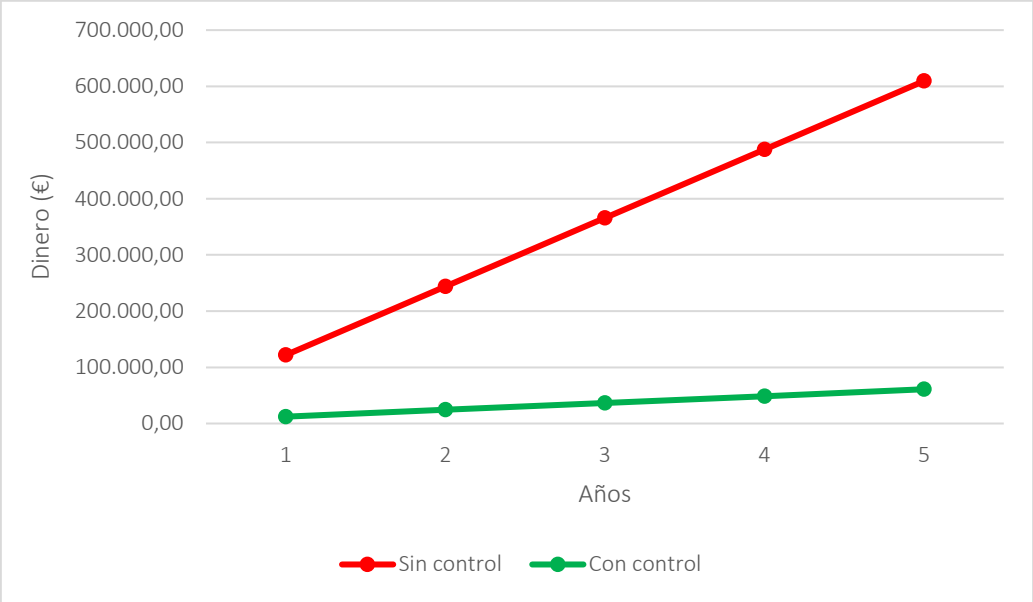



*Ilustración 132. Rentabilidad amenaza HW1 - [A.11] activo S6*

## Amenaza: SW1 – [A.5] Suplantación de la identidad del usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 138. Rentabilidad amenaza SW1 - [A.5] activo S6*

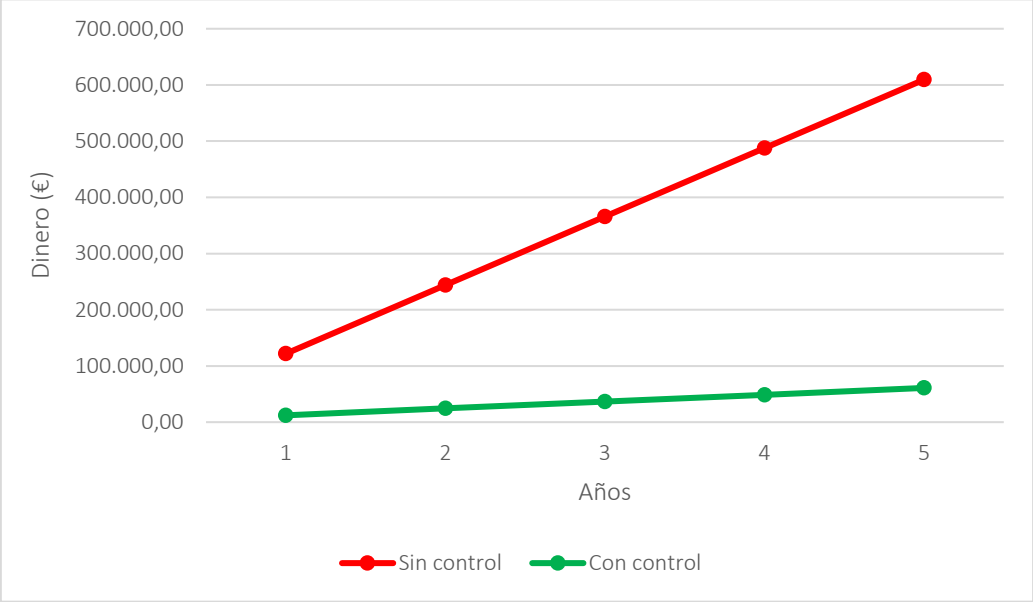



*Ilustración 133. Rentabilidad amenaza SW1 - [A.5] activo S6*

## Amenaza: SW1 – [A.15] Modificación deliberada de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 139. Rentabilidad amenaza SW1 - [A.15] activo S6*

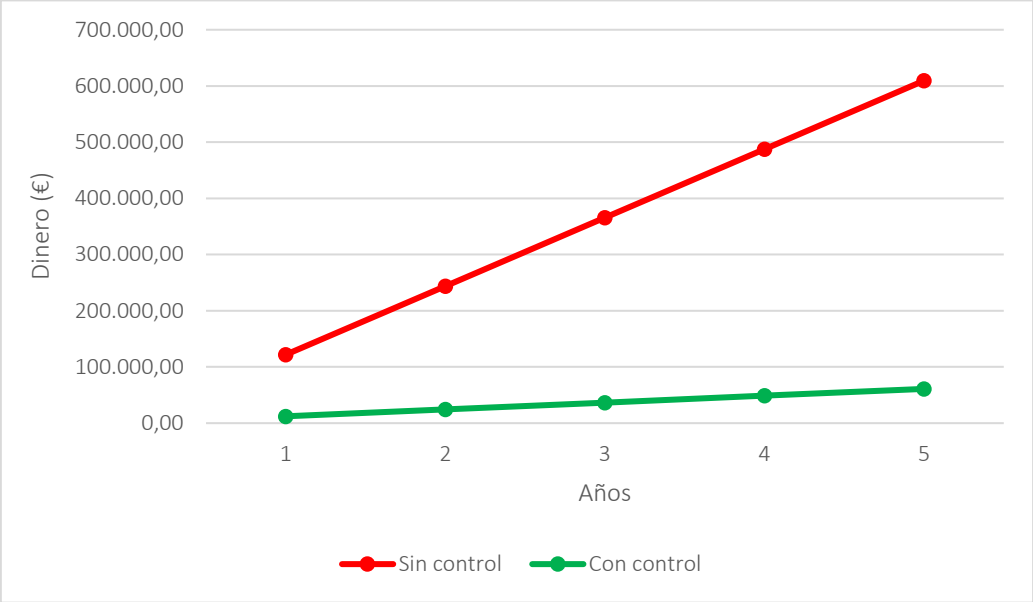



*Ilustración 134. Rentabilidad amenaza SW1 - [A.15] activo S6*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 140. Rentabilidad amenaza SW1 - [A.18] activo S6*

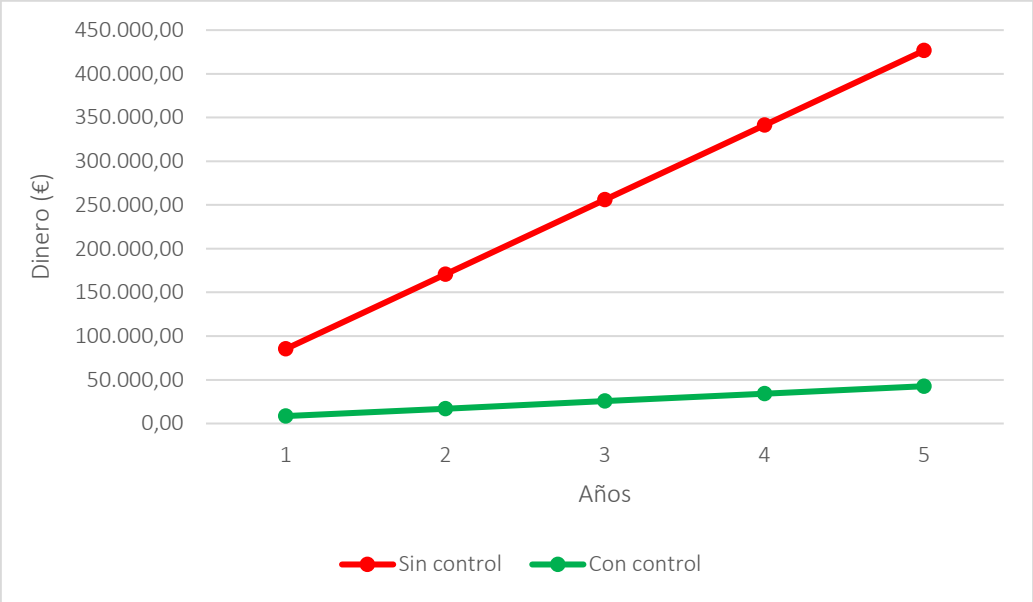



*Ilustración 135. Rentabilidad amenaza SW1 - [A.18] activo S6*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 141. Rentabilidad amenaza SW1 - [A.19] activo S6*

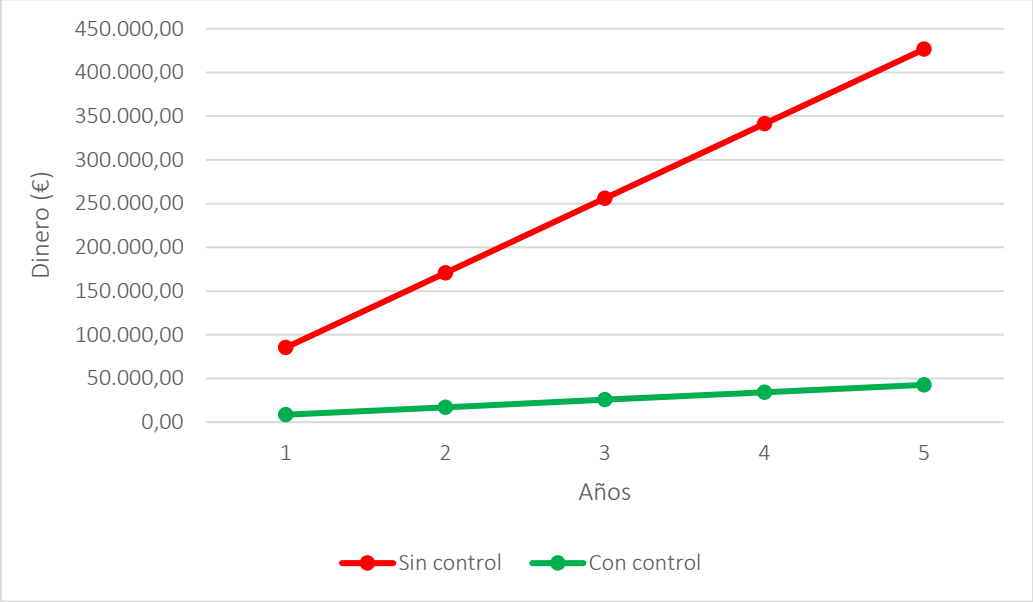



*Ilustración 136. Rentabilidad amenaza SW1 - [A.19] activo S6*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 142. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

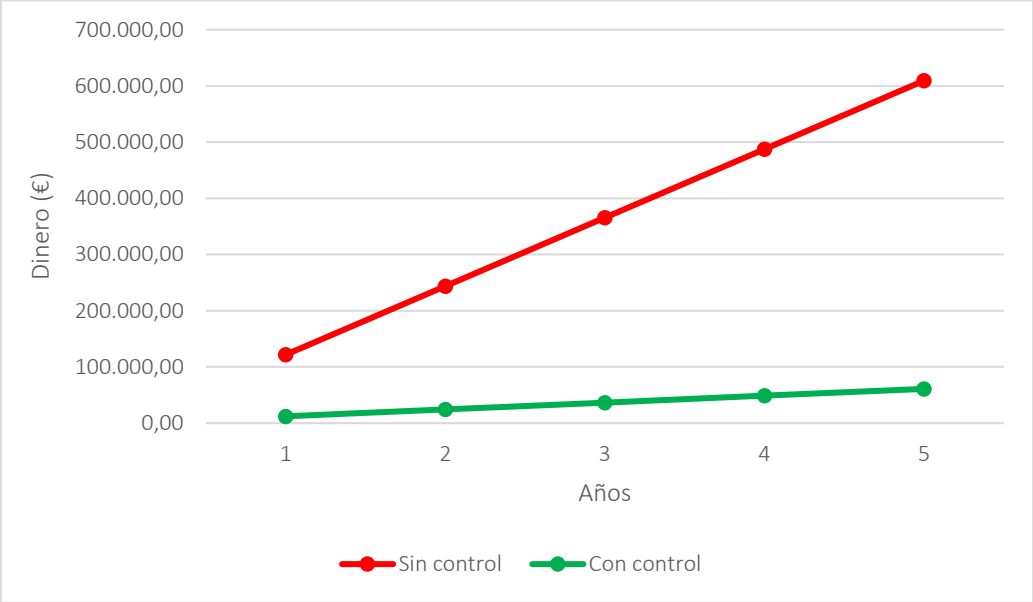



*Ilustración 137. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 143. Rentabilidad amenaza T1 - [A.11] activo S6*

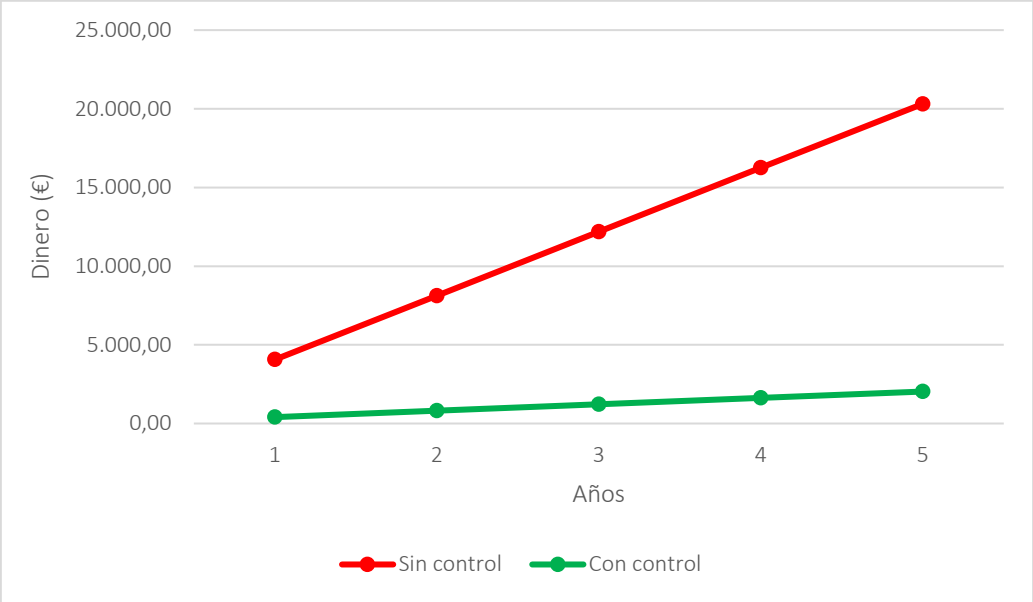



*Ilustración 138. Rentabilidad amenaza T1 - [A.11] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.3 Tercer control

##### 2.1.5.3.1 Título

Control de robo

##### 2.1.5.3.2 Finalidad

Una amenaza a la que se enfrenta cualquier empresa y, por lo tanto, su Sistema de información, son los robos, así que debemos protegernos contra ellos. Nosotros vamos a instalar una alarma, para ello, hay empresas que se dedican a la instalación y mantenimiento de estos sistemas.

##### 2.1.5.3.3 Empresa

“Sanitaria AMS S.L.”

##### 2.1.5.3.4 Leyes aplicables

Ley de Seguridad Privada. 23/1992, de 30 de Julio. BOE n º 186, de 4 de agosto de 1992.

Reglamento de Seguridad Privada. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.

##### 2.1.5.3.5 Normas aplicables

UNE-EN 50136-1:2012. Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 1: Requisitos generales para los sistemas de transmisión de alarmas.

UNE-EN 50518-1:2014. Centro de supervisión y recepción de alarmas. Parte 1: Requisitos de ubicación y construcción.

UNE-EN 50518-2:2014. Centro de supervisión y recepción de alarmas. Parte 2: Requisitos técnicos.

UNE-EN 50518-3:2013. Centro de supervisión y recepción de alarmas. Parte 3: Procedimientos y requisitos de operación.
UNE-EN 50136-2:2013. Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 2: Requisitos para los transceptores de instalaciones vigiladas (SPT).
UNE-EN 54-5:2017+A1:2019. Sistemas de detección y alarmas de incendios. Parte 5: Detectores de calor. Detectores de calor puntuales.
UNE-EN 50136-1:2012/A1:2019. Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 1: Requisitos generales para los sistemas de transmisión de alarmas.
UNE-EN 303406 V1.1.1. Dispositivo de corto alcance (SRD); Equipos de alarmas de teleasistencia operando en la gama de frecuencias de 25 MHz to 1000 MHz; Norma armonizada que cubre los requisitos esenciales según el artículo 3.2 de la Directiva 2014/53/UE (Ratificada por la Asociación Española de Normalización en abril de 2017).
UNE-EN 62541-9:2015. Arquitectura unificada OPC. Parte 9: Alarmas y estados (Ratificada por AENOR en junio de 2015).
UNE-CLC/TS 50131-9:2015. Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 9: Verificación de alarmas. Principios y métodos.
UNE-EN 50136-3:2014. Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 3: Requisitos para los transceptores del centro de recepción (RCT).

#### 2.1.5.3.6 Descripción del control

Sabemos que, aunque la probabilidad de que se dé la amenaza de robo es muy pequeña, no podemos dejarla pasar por alto, en caso de que la empresa sufra un robo podemos llegar a tener daños irreparables en nuestro SI.

Por lo tanto, debemos contratar un servicio de alarma con alguna de las empresas disponibles para nuestra empresa. En este control vamos a hacerlo con la empresa “Securitas Direct”. En caso de que se encuentre otra empresa que de un servicio mejor o a mejor precio, podrá ser contratada.

Debido a que el servicio lo vamos a contratar a terceros y es una empresa dedicada específicamente a ello, estos se encargarán expresamente de la instalación, mantenimiento y reparación en el sistema de alarma.

Con respecto a los servicios que debe prestar el sistema de alarma, son los siguientes: atención al cliente 24 horas, protección frente a inhibición y sabotaje,

conexión directa con la central de policía, cámara de vigilancia y sensores para los puntos de acceso, ya sean puertas o ventanas.

#### 2.1.5.3.7 Responsables

Los dueños de la empresa serán los encargados de buscar la empresa adecuada y contratar el sistema de alarma que mejor se adapte. Además, deberán comprobar su correcto funcionamiento cada semana y en caso de encontrar cualquier anomalía, avisar inmediatamente a la empresa prestadora del servicio.

#### 2.1.5.3.8 Dispositivos

Los dispositivos serán todos los necesarios que necesite la empresa para instalar correctamente el sistema de alarma dentro del establecimiento.

#### 2.1.5.3.9 Costes

- **Implantación:** En cuanto al coste de implantación e instalación del sistema va incluido en la cuota mensual que se pagará por el servicio de alarma.
- **Ejecución y mantenimiento:** Precio por mes: 54.99 €. Precio anual: Precio mes x 12; Precio anual = 54.99 x 12 = 659.88 €, este es el precio que costaría el sistema de alarma por un año. En este precio van incluidos todos los costes de mantenimiento, ya sean revisiones o cualquier anomalía que tenga el sistema.
- **Búsqueda de irregularidad:** Si en algún momento se detecta algún fallo en el funcionamiento del sistema de alarma, habrá que ponerse en contacto con la empresa la cual tenemos contratado el servicio para qué ellos se encarguen de solucionarlo. Esto no supondrá ningún coste extra debido a que el mantenimiento y los fallos van incluidos dentro de la cuota mensual.

#### 2.1.5.3.10 Rentabilidad

Un robo puede conllevar la pérdida de cualquier parte de nuestro SI, ya sean datos, sistemas hardware, software, entre otros. Por lo tanto, ya hemos estudiado que esto puede ser un problema muy grave, por lo que realizar este control sería muy importante.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar este control en nuestro SI. Vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 96 %, ya que:

- Puede fallar por una mala conexión de algún elemento del sistema de alarma.
- Puede fallar por una mala configuración
- Puede fallar por olvido de revisión del responsable.
- Puede fallar porque el responsable no la conecte.

Activo: Información pacientes (S1)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 29106,99 | 0 | 0 | 29106,99 | 58213,98 | 87320,97 | 116427,96 | 145534,95 |
| 873,21 | 0 | 659,88 | 1533,09 | 3066,18 | 4599,27 | 6132,36 | 7665,45 |

*Tabla 144. Rentabilidad amenaza AUX1 - [E.25] activo S1*

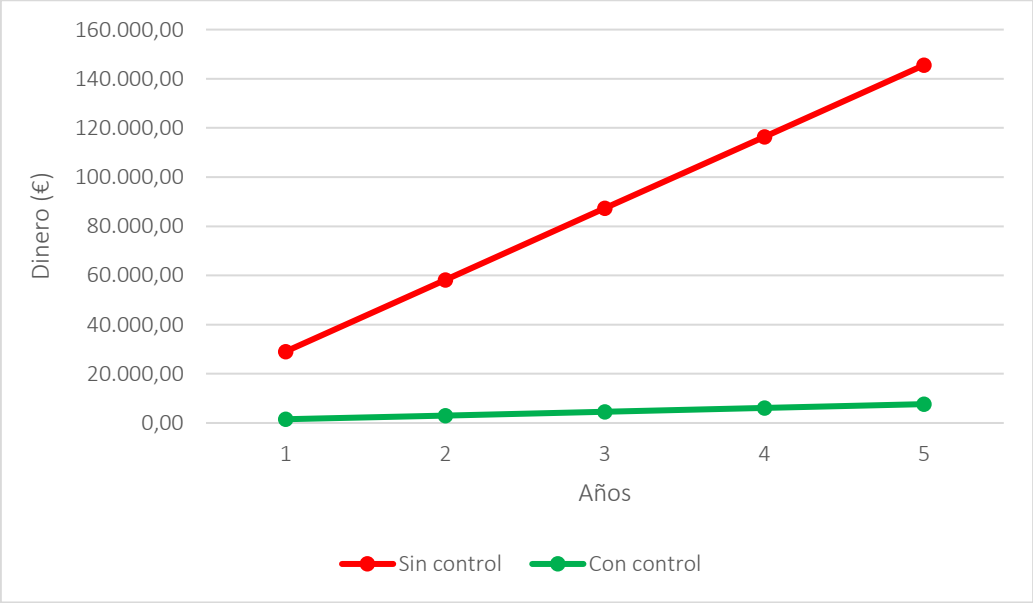



*Ilustración 139. Rentabilidad amenaza AUX1 - [E.25] activo S1*

## Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |
| 1091,51 | 0 | 659,88 | 1751,39 | 3502,78 | 5254,17 | 7005,56 | 8756,95 |

*Tabla 145. Rentabilidad amenaza AUX1 - [A.25] activo S1*

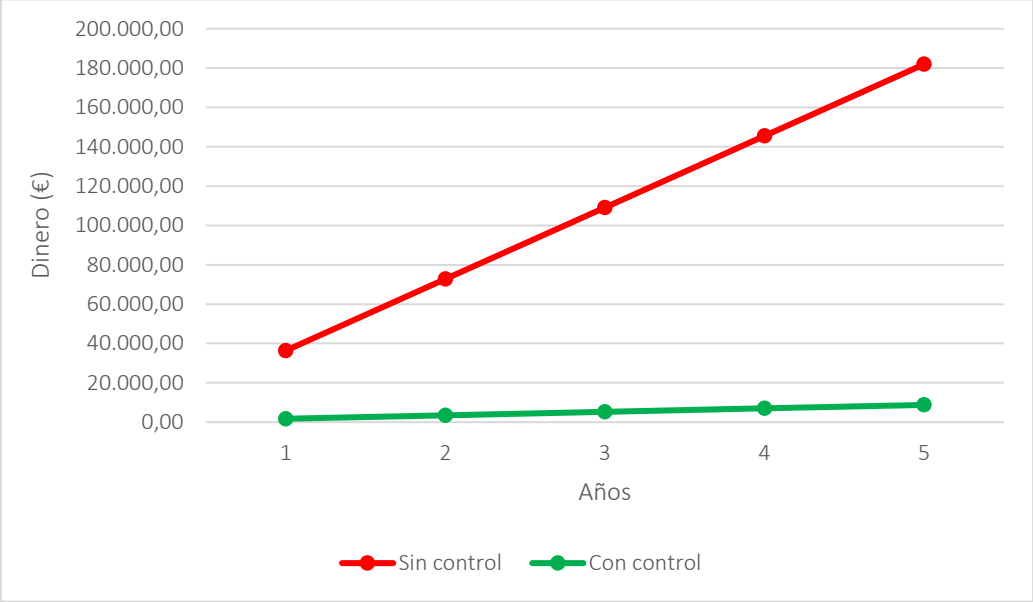



*Ilustración 140. Rentabilidad amenaza AUX1 - [A.25] activo S1*

## Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 72767,46 | 0 | 0 | 72767,46 | 145534,92 | 218302,38 | 291069,84 | 363837,3 |
| 2183,02 | 0 | 659,88 | 2842,9 | 5685,8 | 8528,7 | 11371,6 | 14214,5 |

*Tabla 146. Rentabilidad amenaza HW1 - [A.25] activo S1*

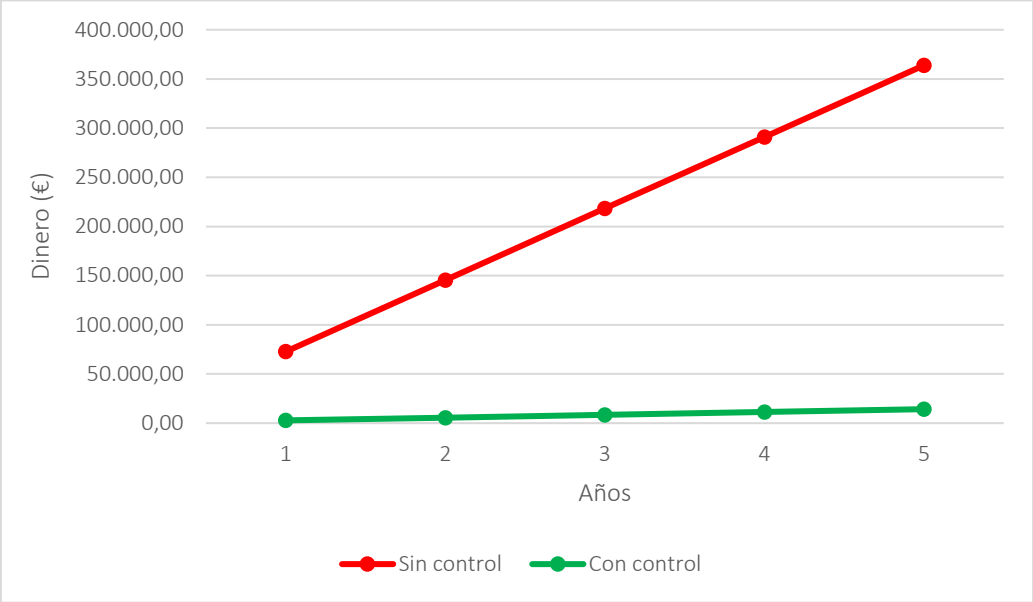



*Ilustración 141. Rentabilidad amenaza HW1 - [A.25] activo S1*

## Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 72767,46 | 0 | 0 | 72767,46 | 145534,92 | 218302,38 | 291069,84 | 363837,3 |
| 2183,02 | 0 | 659,88 | 2842,9 | 5685,8 | 8528,7 | 11371,6 | 14214,5 |

*Tabla 147. Rentabilidad amenaza SRVD1 - [A.25] activo S1*

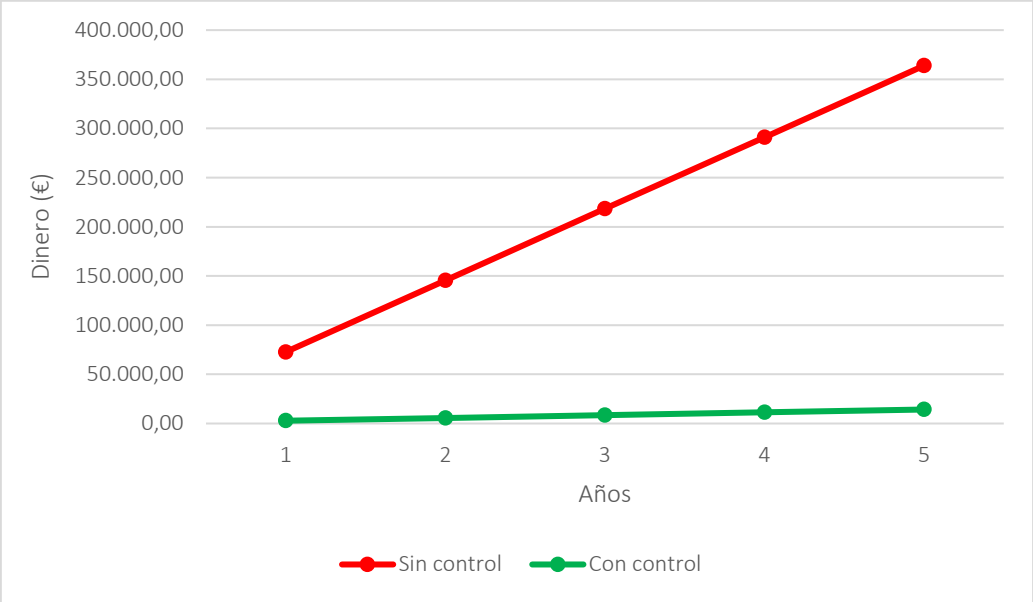



*Ilustración 142. Rentabilidad amenaza SRVD1 - [A.25] activo S1*

Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2425,58 | 0 | 0 | 2425,58 | 4851,16 | 7276,74 | 9702,32 | 12127,9 |
| 72,77 | 0 | 659,88 | 732,65 | 1465,3 | 2197,95 | 2930,6 | 3663,25 |

*Tabla 148. Rentabilidad amenaza T1 - [A.25] activo S1*

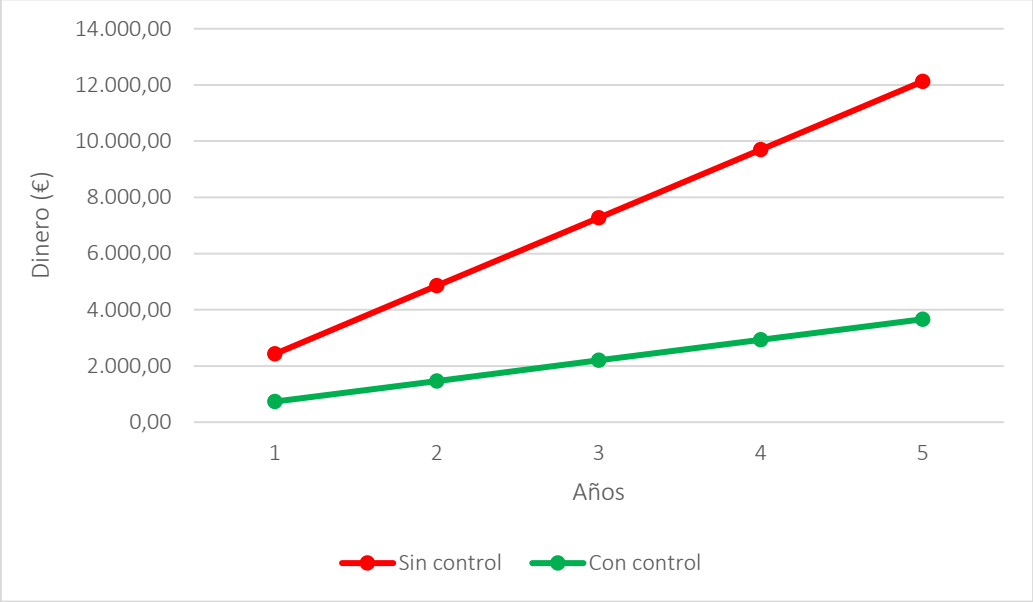



*Ilustración 143. Rentabilidad amenaza T1 - [A.25] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 19500,53 | 0 | 0 | 19500,53 | 39001,06 | 58501,59 | 78002,12 | 97502,65 |
| 585,02 | 0 | 659,88 | 1244,9 | 2489,8 | 3734,7 | 4979,6 | 6224,5 |

*Tabla 149. Rentabilidad amenaza AUX1 - [E.25] activo S2*

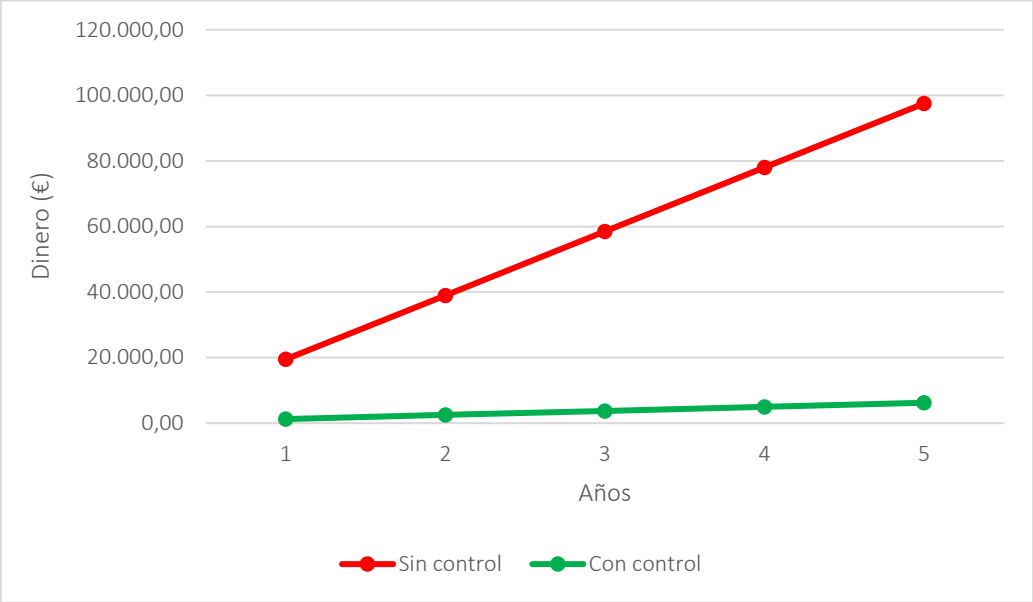



*Ilustración 144. Rentabilidad amenaza AUX1 - [E.25] activo S2*

Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |
| 731,27 | 0 | 659,88 | 1391,15 | 2782,3 | 4173,45 | 5564,6 | 6955,75 |

*Tabla 150. Rentabilidad amenaza AUX1 - [A.25] activo S2*

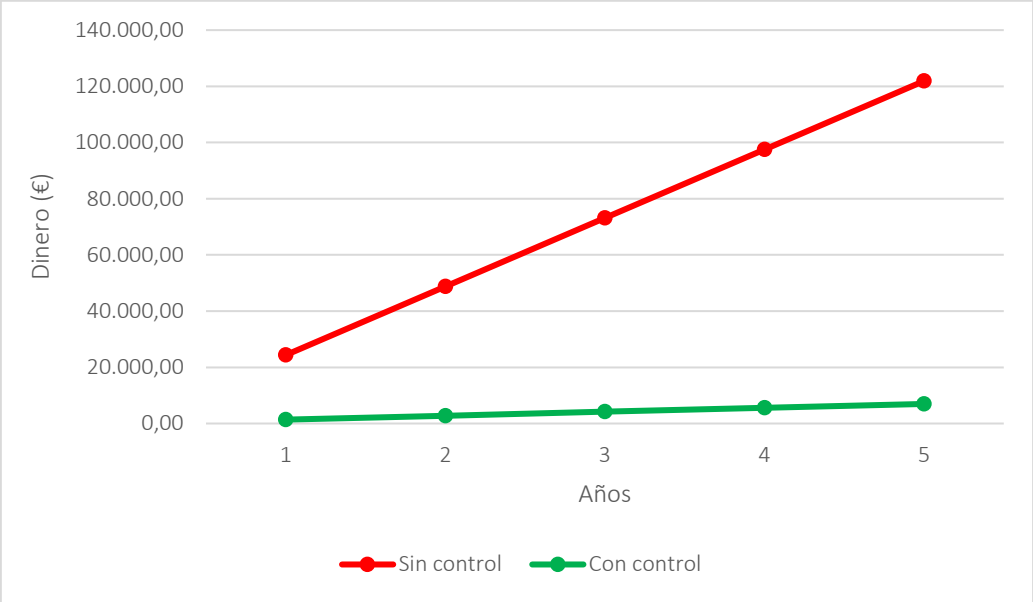



*Ilustración 145. Rentabilidad amenaza AUX1 - [A.25] activo S2*

Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 151. Rentabilidad amenaza HW1 - [A.25] activo S2*

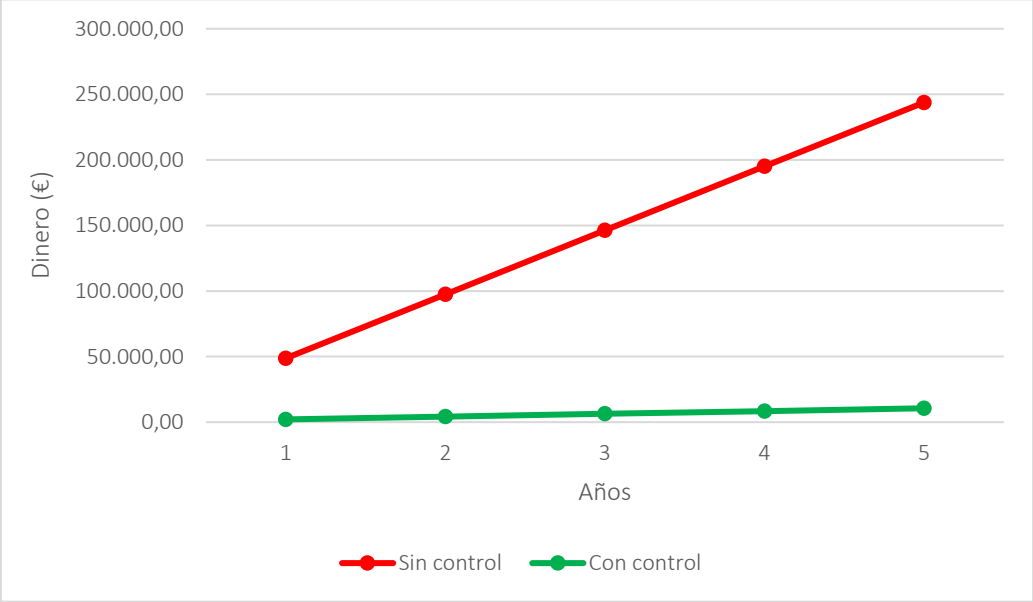



*Ilustración 146. Rentabilidad amenaza HW1 - [A.25] activo S2*

Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 152. Rentabilidad amenaza SRVD1 - [A.25] activo S2*

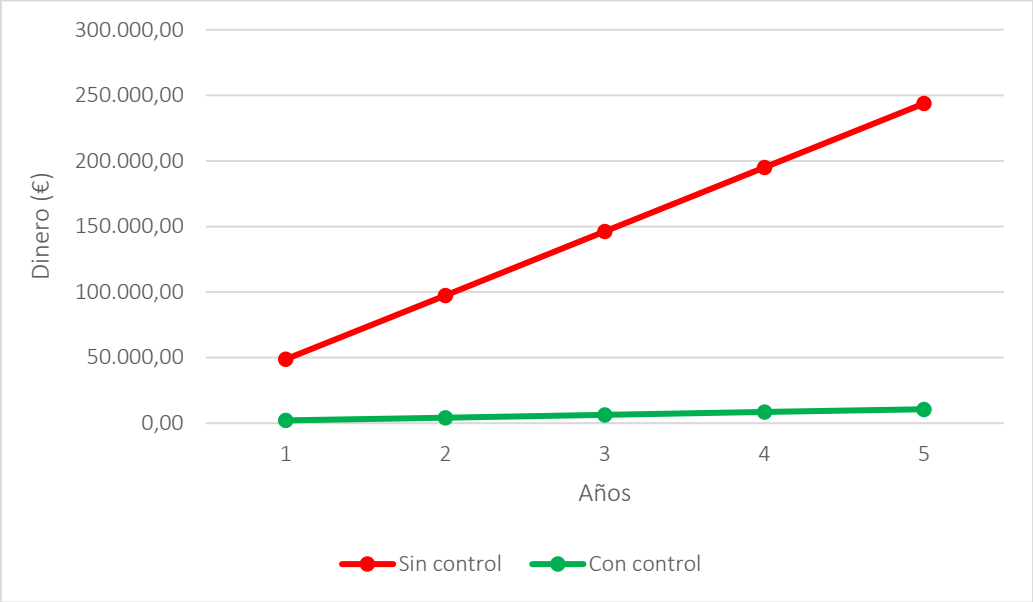



*Ilustración 147. Rentabilidad amenaza SRVD1 - [A.25] activo S2*

## Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1625,04 | 0 | 0 | 1625,04 | 3250,08 | 4875,12 | 6500,16 | 8125,2 |
| 48,75 | 0 | 659,88 | 708,63 | 1417,26 | 2125,89 | 2834,52 | 3543,15 |

*Tabla 153. Rentabilidad amenaza T1 - [A.25] activo S2*

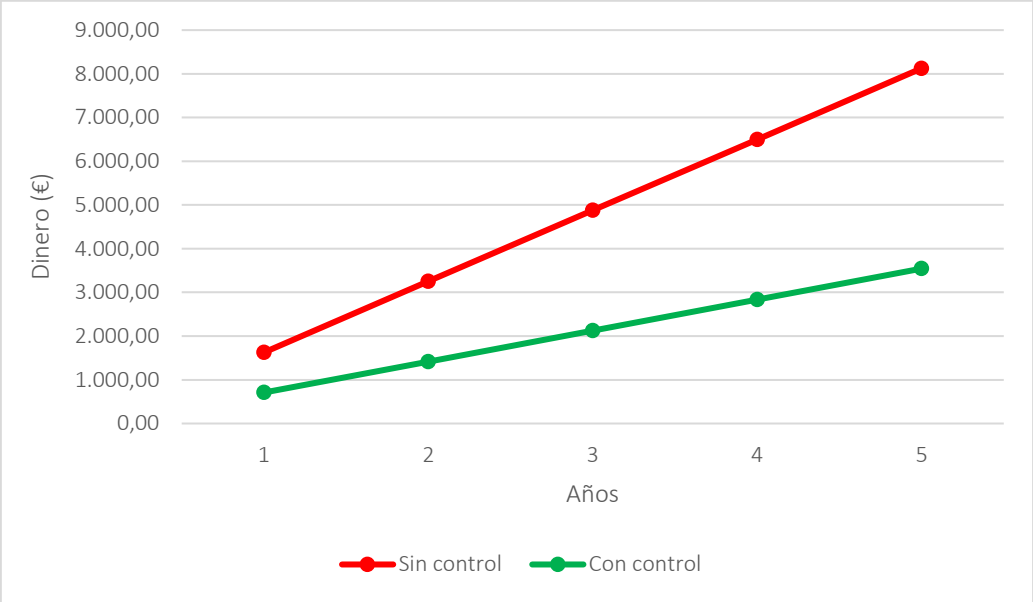



*Ilustración 148. Rentabilidad amenaza T1 - [A.25] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 19500,53 | 0 | 0 | 19500,53 | 39001,06 | 58501,59 | 78002,12 | 97502,65 |
| 585,02 | 0 | 659,88 | 1244,9 | 2489,8 | 3734,7 | 4979,6 | 6224,5 |

*Tabla 154. Rentabilidad amenaza AUX1 - [E.25] activo S3*

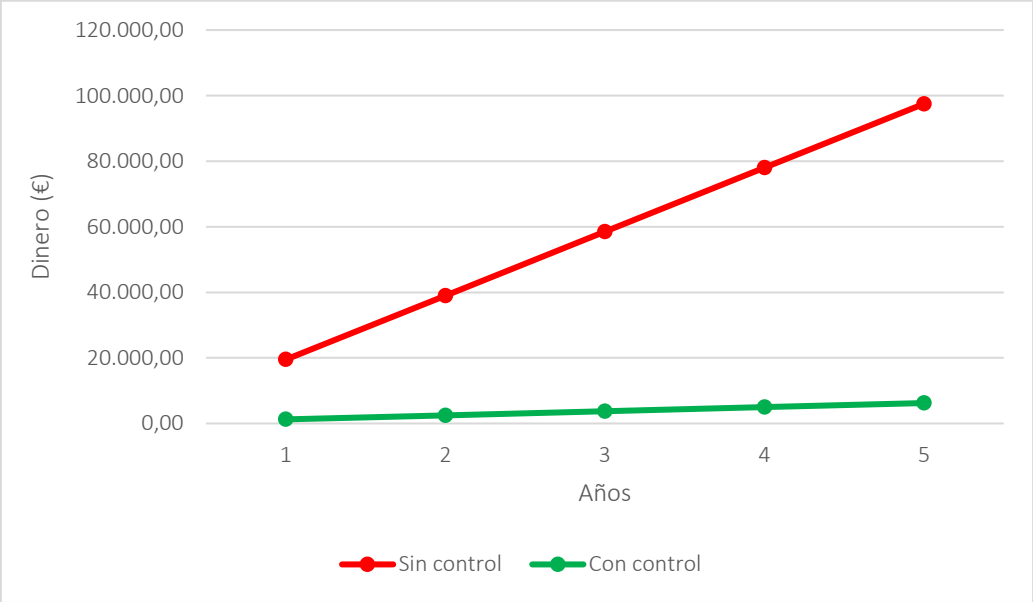



*Ilustración 149. Rentabilidad amenaza AUX1 - [E.25] activo S3*

Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |
| 731,27 | 0 | 659,88 | 1391,15 | 2782,3 | 4173,45 | 5564,6 | 6955,75 |

*Tabla 155. Rentabilidad amenaza AUX1 - [A.25] activo S3*

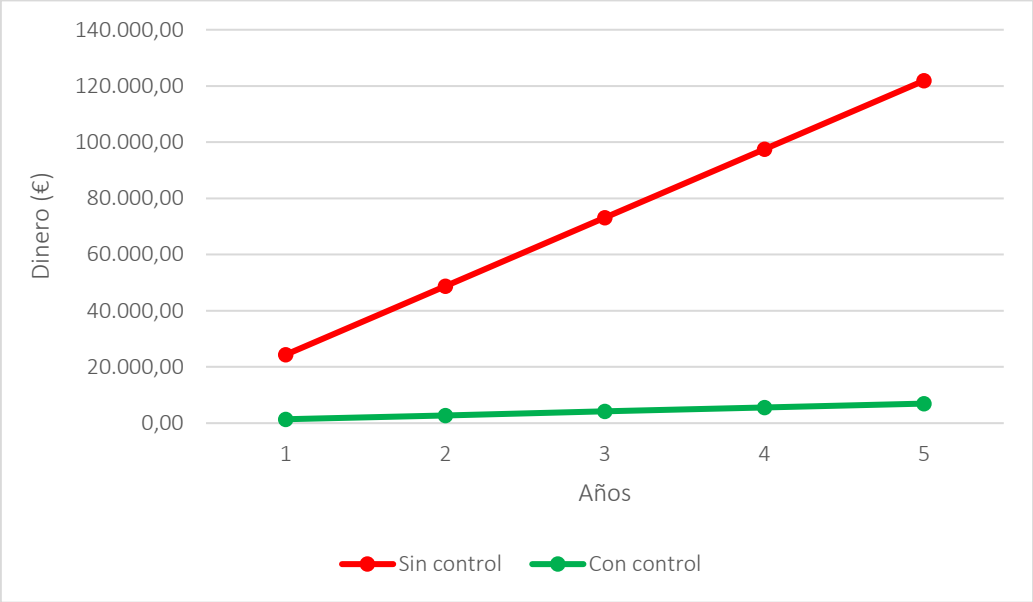



*Ilustración 150. Rentabilidad amenaza AUX1 - [A.25] activo S3*

Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 156. Rentabilidad amenaza HW1 - [A.25] activo S3*

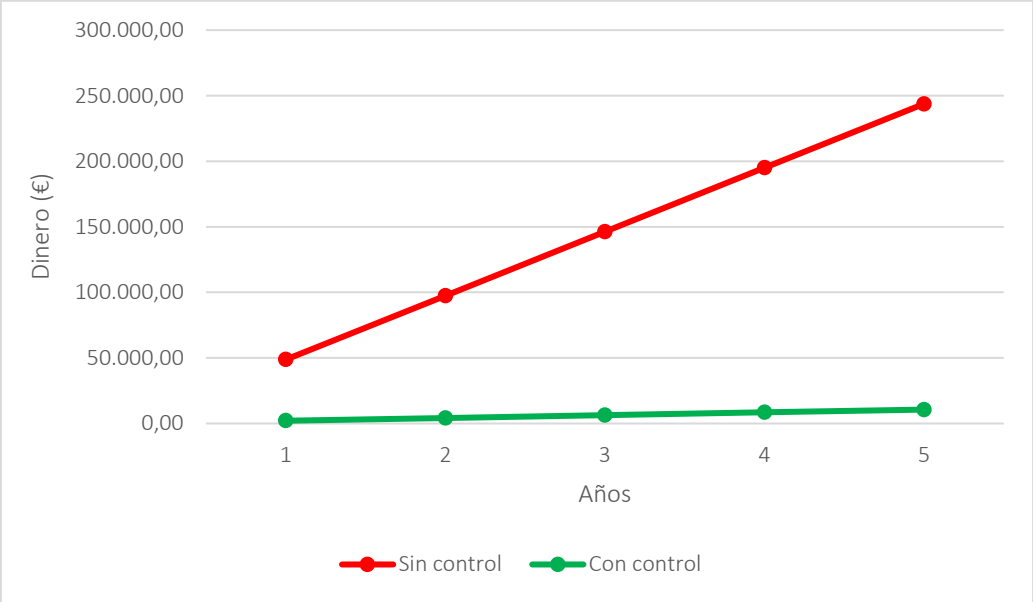



*Ilustración 151. Rentabilidad amenaza HW1 - [A.25] activo S3*

## Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 157. Rentabilidad amenaza SRVD1 - [A.25] activo S3*

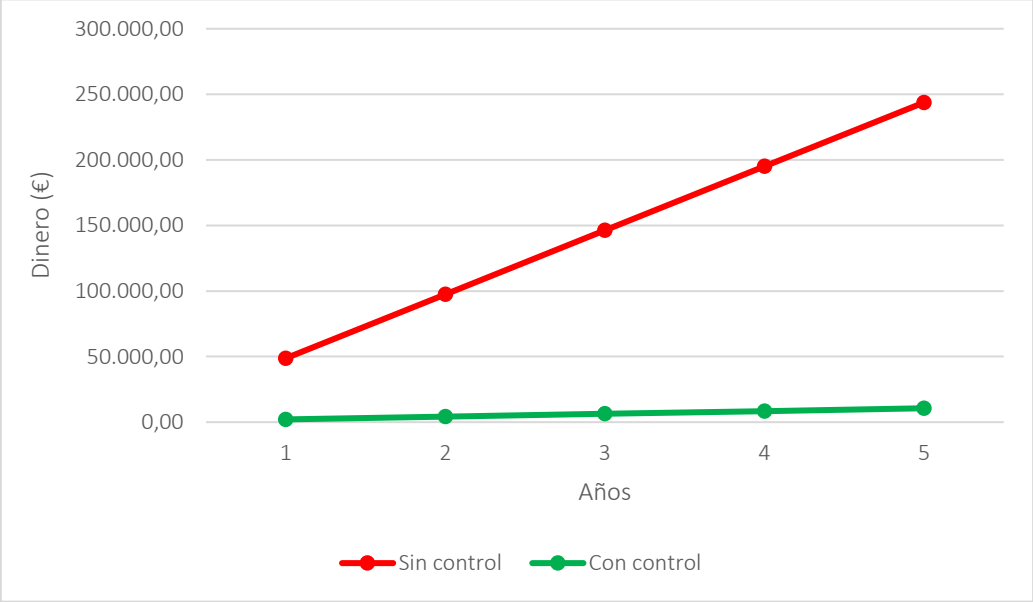



*Ilustración 152. Rentabilidad amenaza SRVD1 - [A.25] activo S3*

## Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1625,04 | 0 | 0 | 1625,04 | 3250,08 | 4875,12 | 6500,16 | 8125,2 |
| 48,75 | 0 | 659,88 | 708,63 | 1417,26 | 2125,89 | 2834,52 | 3543,15 |

*Tabla 158. Rentabilidad amenaza T1 - [A.25] activo S3*

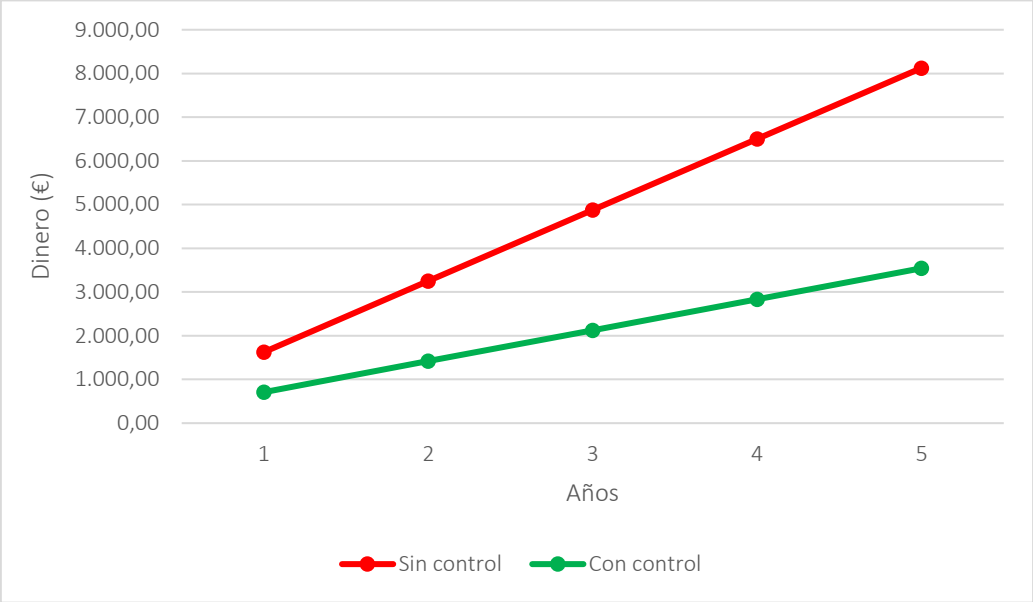



*Ilustración 153. Rentabilidad amenaza T1 - [A.25] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 19500,02 | 0 | 0 | 19500,02 | 39000,04 | 58500,06 | 78000,08 | 97500,1 |
| 585 | 0 | 659,88 | 1244,88 | 2489,76 | 3734,64 | 4979,52 | 6224,4 |

*Tabla 159. Rentabilidad amenaza AUX1 - [E.25] activo S4*

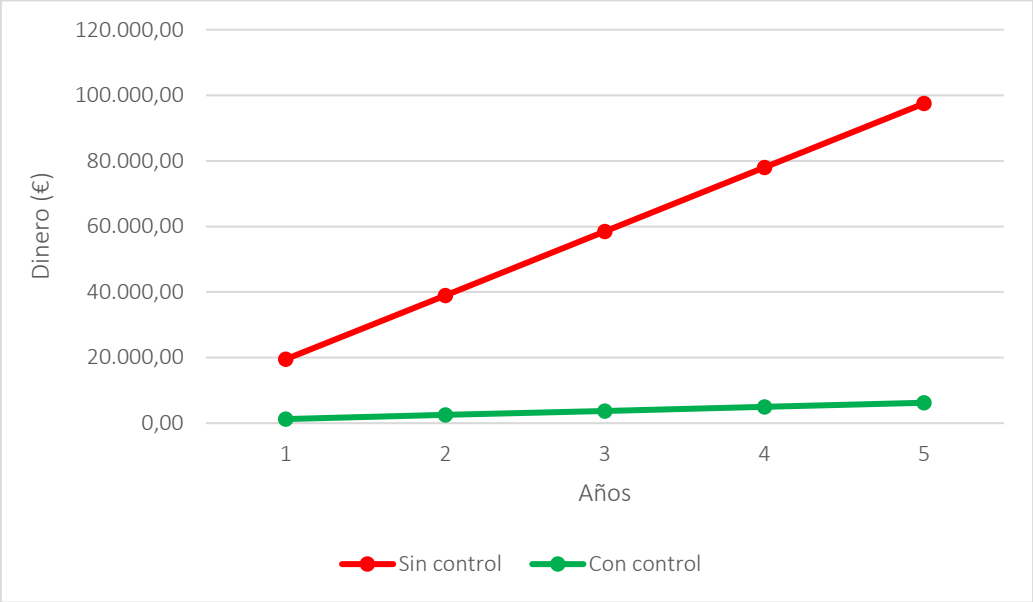



*Ilustración 154. Rentabilidad amenaza AUX1 - [E.25] activo S4*

Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |
| 731,25 | 0 | 659,88 | 1391,13 | 2782,26 | 4173,39 | 5564,52 | 6955,65 |

*Tabla 160. Rentabilidad amenaza AUX1 - [A.25] activo S4*

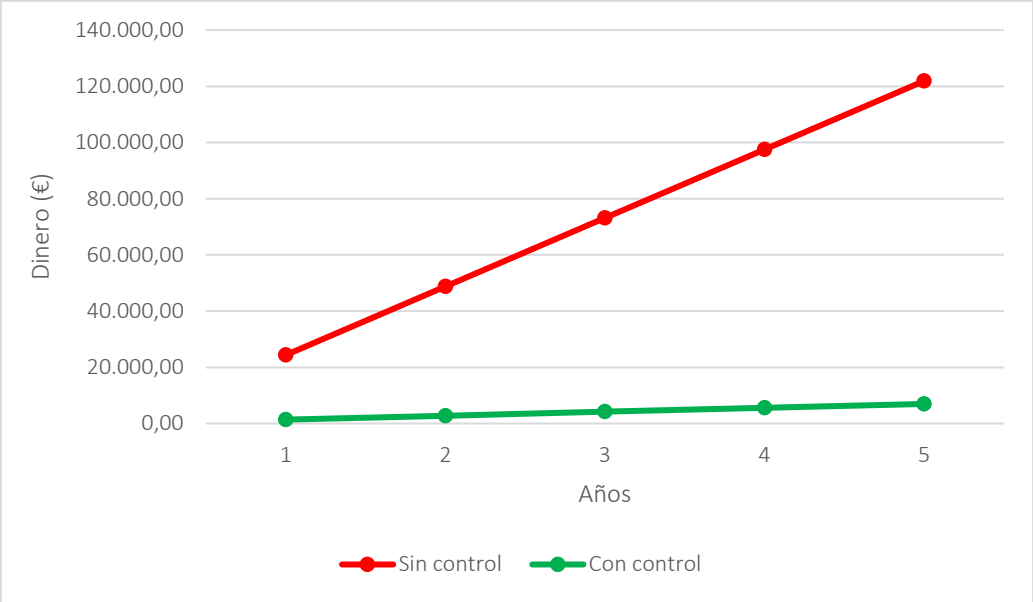



*Ilustración 155. Rentabilidad amenaza AUX1 - [A.25] activo S4*

Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48750,06 | 0 | 0 | 48750,06 | 97500,12 | 146250,18 | 195000,24 | 243750,3 |
| 1462,5 | 0 | 659,88 | 2122,38 | 4244,76 | 6367,14 | 8489,52 | 10611,9 |

*Tabla 161. Rentabilidad amenaza HW1 - [A.25] activo S4*

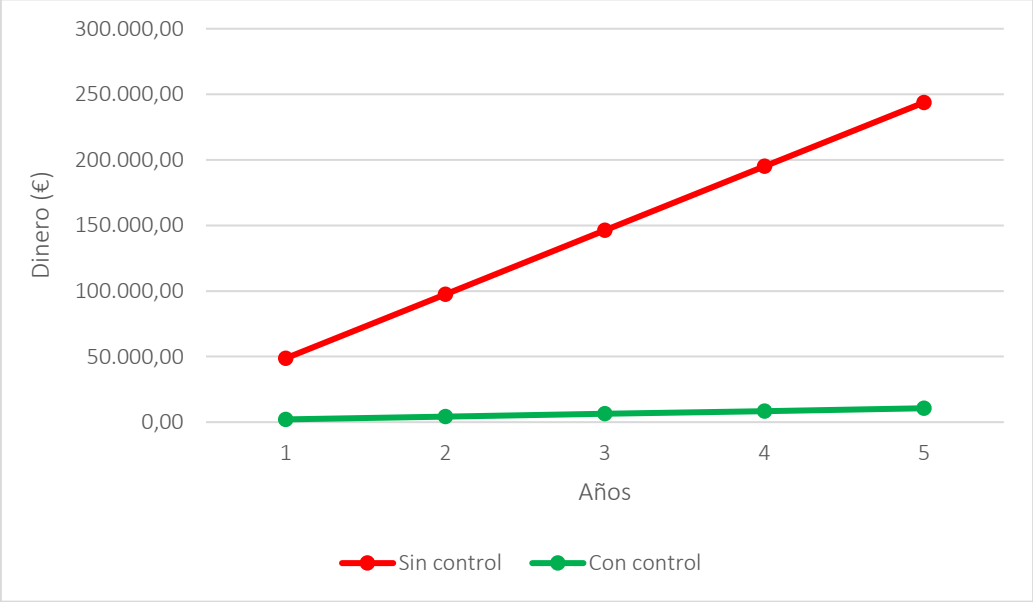



*Ilustración 156. Rentabilidad amenaza HW1 - [A.25] activo S4*

Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48750,06 | 0 | 0 | 48750,06 | 97500,12 | 146250,18 | 195000,24 | 243750,3 |
| 1462,5 | 0 | 659,88 | 2122,38 | 4244,76 | 6367,14 | 8489,52 | 10611,9 |

*Tabla 162. Rentabilidad amenaza SRVD1 - [A.25] activo S4*

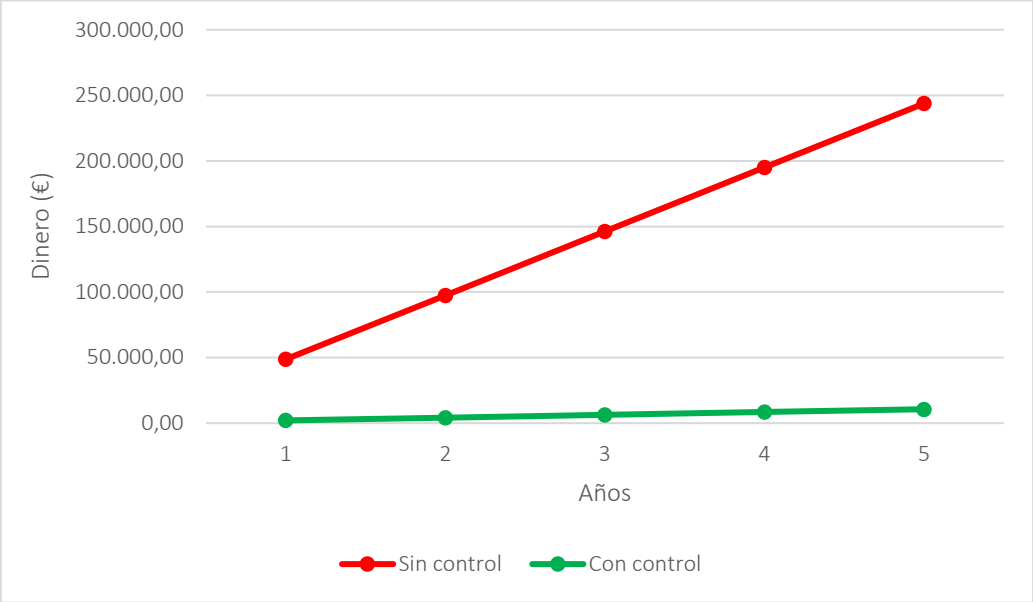



*Ilustración 157. Rentabilidad amenaza SRVD1 - [A.25] activo S4*

## Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1625 | 0 | 0 | 1625 | 3250 | 4875 | 6500 | 8125 |
| 48,75 | 0 | 659,88 | 708,63 | 1417,26 | 2125,89 | 2834,52 | 3543,15 |

*Tabla 163. Rentabilidad amenaza T1 - [A.25] activo S4*

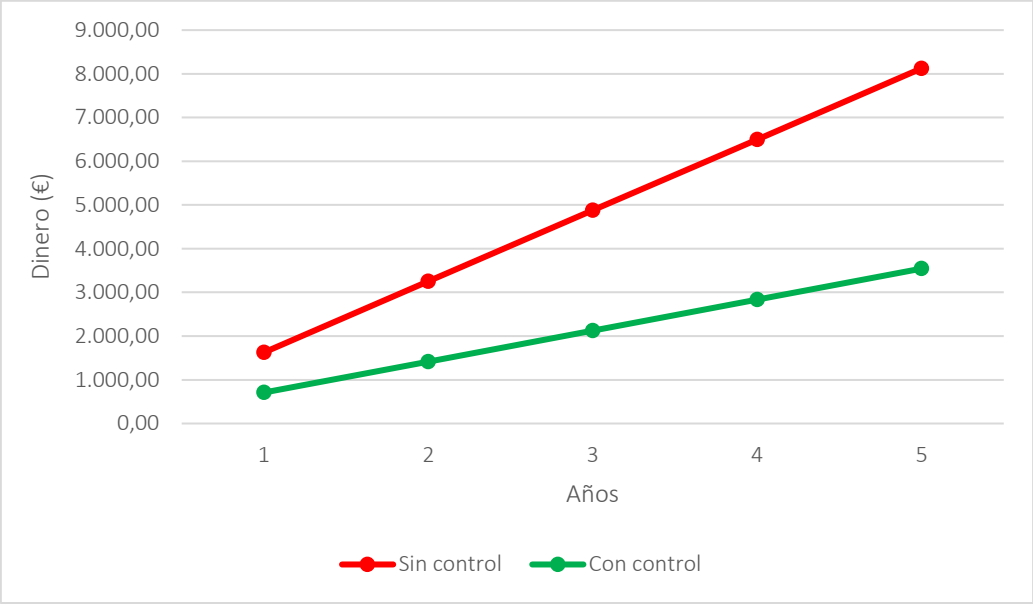



*Ilustración 158. Rentabilidad amenaza T1 - [A.25] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 19500,53 | 0 | 0 | 19500,53 | 39001,06 | 58501,59 | 78002,12 | 97502,65 |
| 585,02 | 0 | 659,88 | 1244,9 | 2489,8 | 3734,7 | 4979,6 | 6224,5 |

*Tabla 164. Rentabilidad amenaza AUX1 - [E.25] activo S5*

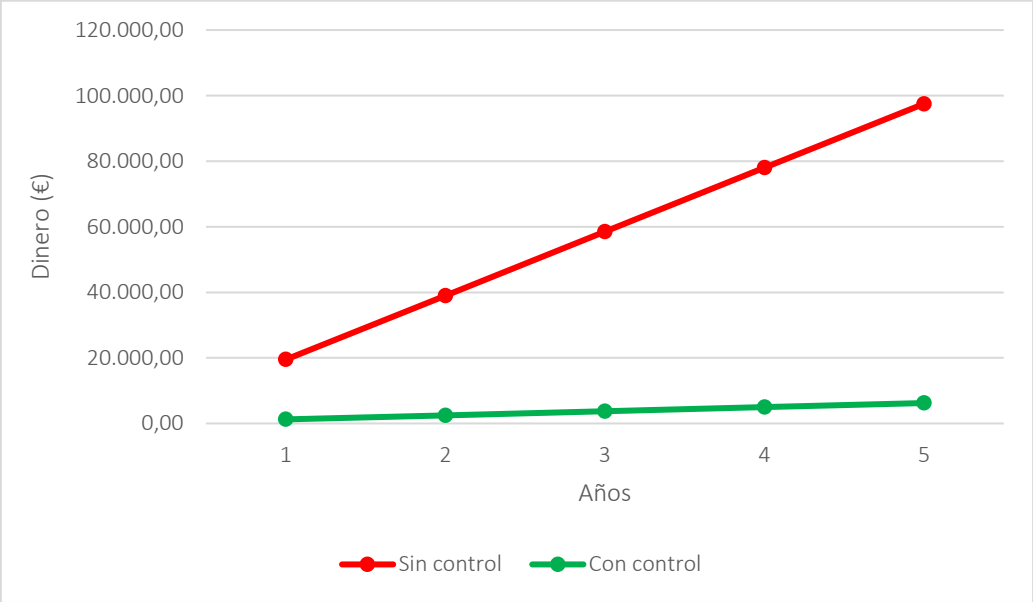



*Ilustración 159. Rentabilidad amenaza AUX1 - [E.25] activo S5*

Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |
| 731,27 | 0 | 659,88 | 1391,15 | 2782,3 | 4173,45 | 5564,6 | 6955,75 |

*Tabla 165. Rentabilidad amenaza AUX1 - [A.25] activo S5*

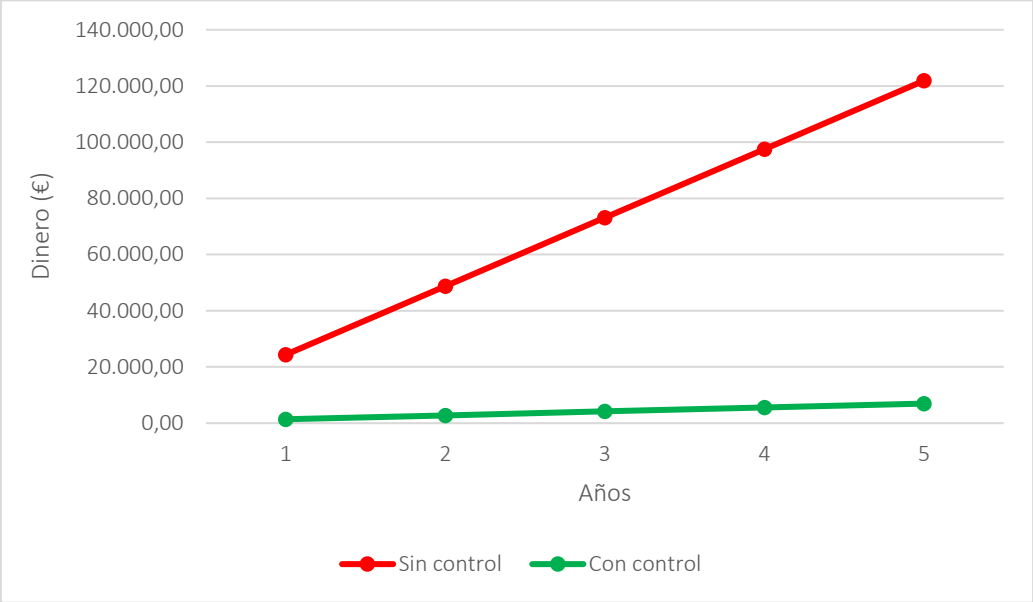



*Ilustración 160. Rentabilidad amenaza AUX1 - [A.25] activo S5*

Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 166. Rentabilidad amenaza HW1 - [A.25] activo S5*

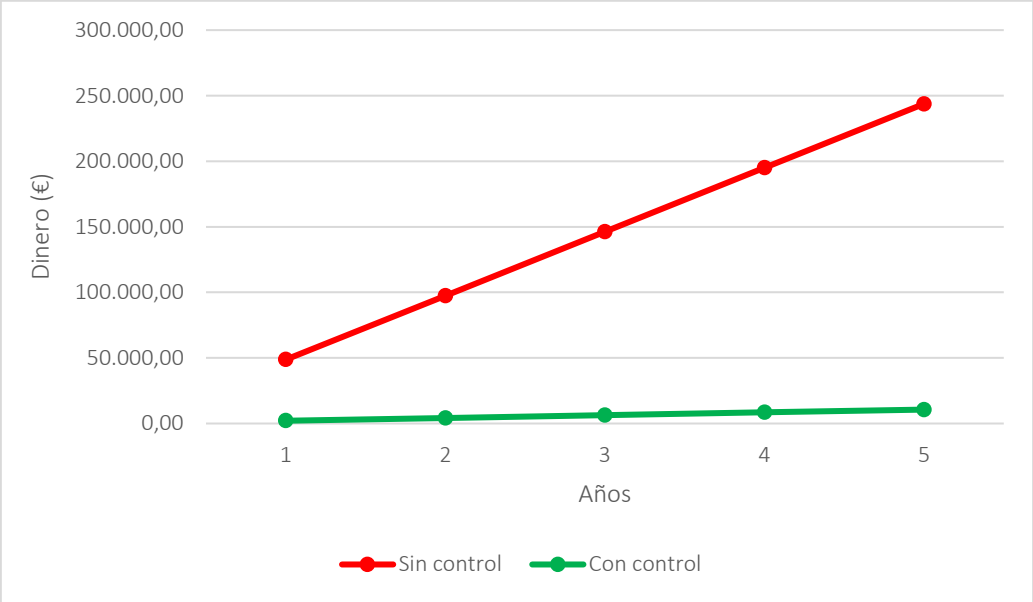



*Ilustración 161. Rentabilidad amenaza HW1 - [A.25] activo S5*

## Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 167. Rentabilidad amenaza SRVD1 - [A.25] activo S5*

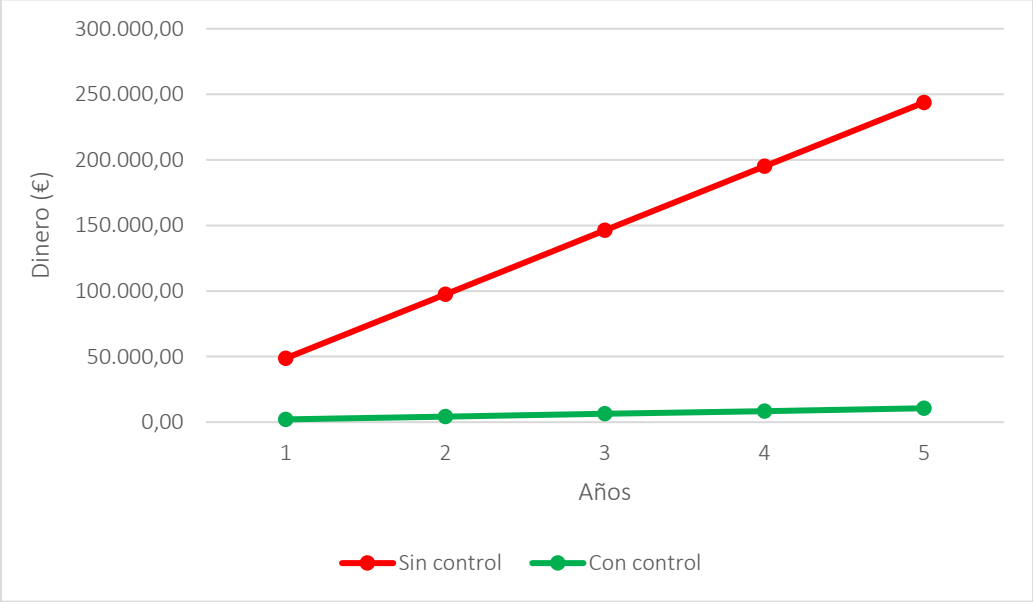



*Ilustración 162. Rentabilidad amenaza SRVD1 - [A.25] activo S5*

## Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1625,04 | 0 | 0 | 1625,04 | 3250,08 | 4875,12 | 6500,16 | 8125,2 |
| 48,75 | 0 | 659,88 | 708,63 | 1417,26 | 2125,89 | 2834,52 | 3543,15 |

*Tabla 168. Rentabilidad amenaza T1 - [A.25] activo S5*

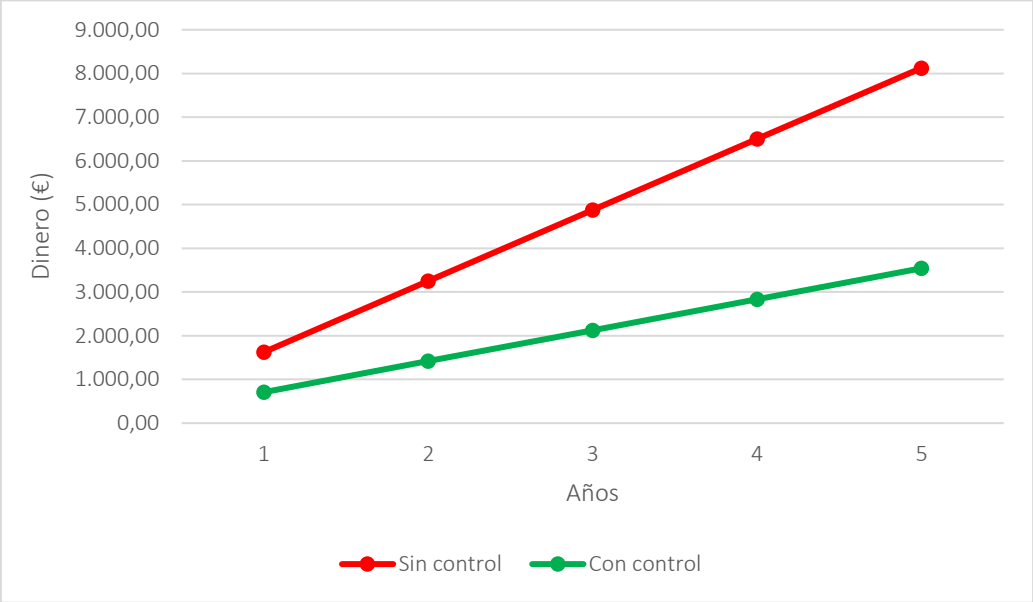



*Ilustración 163. Rentabilidad amenaza T1 - [A.25] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: AUX1 - [E.25] Pérdida de equipos

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 19500,53 | 0 | 0 | 19500,53 | 39001,06 | 58501,59 | 78002,12 | 97502,65 |
| 585,02 | 0 | 659,88 | 1244,9 | 2489,8 | 3734,7 | 4979,6 | 6224,5 |

*Tabla 169. Rentabilidad amenaza AUX1 - [E.25] activo S6*

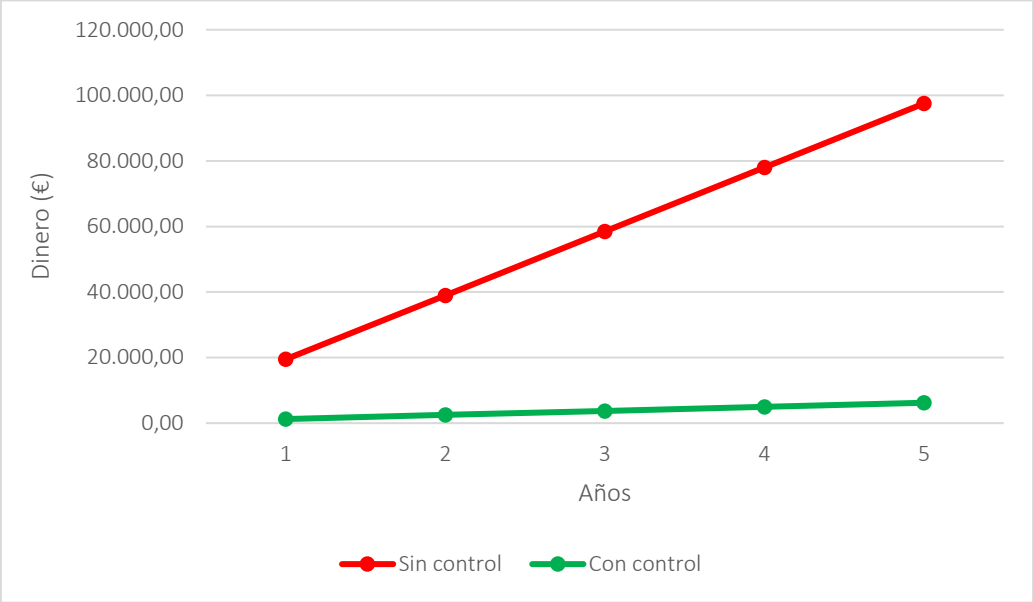



*Ilustración 164. Rentabilidad amenaza AUX1 - [E.25] activo S6*

Amenaza: AUX1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |
| 731,27 | 0 | 659,88 | 1391,15 | 2782,3 | 4173,45 | 5564,6 | 6955,75 |

*Tabla 170. Rentabilidad amenaza AUX1 - [A.25] activo S6*

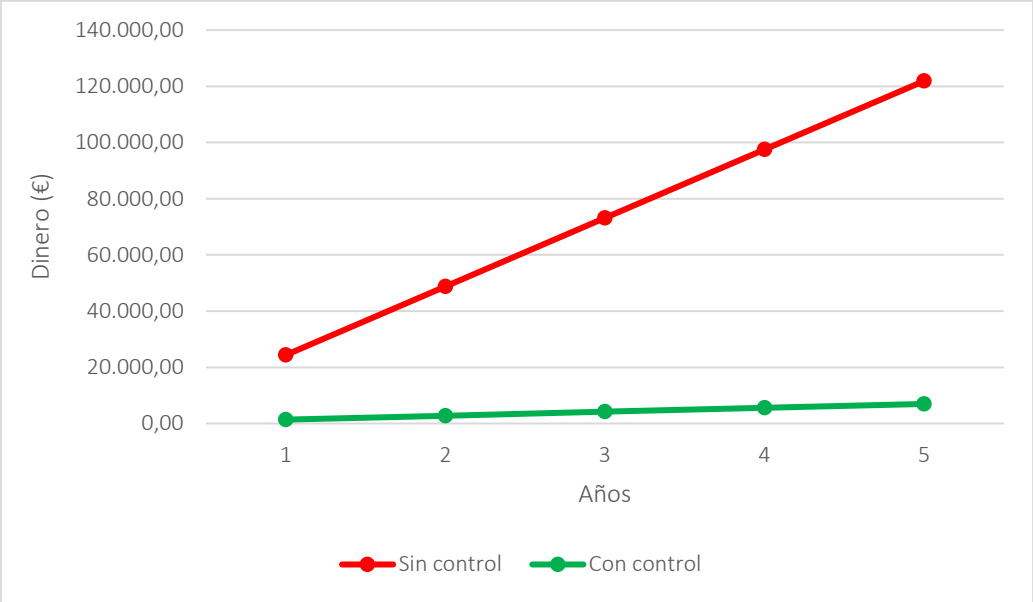



*Ilustración 165. Rentabilidad amenaza AUX1 - [A.25] activo S6*

Amenaza: HW1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 171. Rentabilidad amenaza HW1 - [A.25] activo S6*

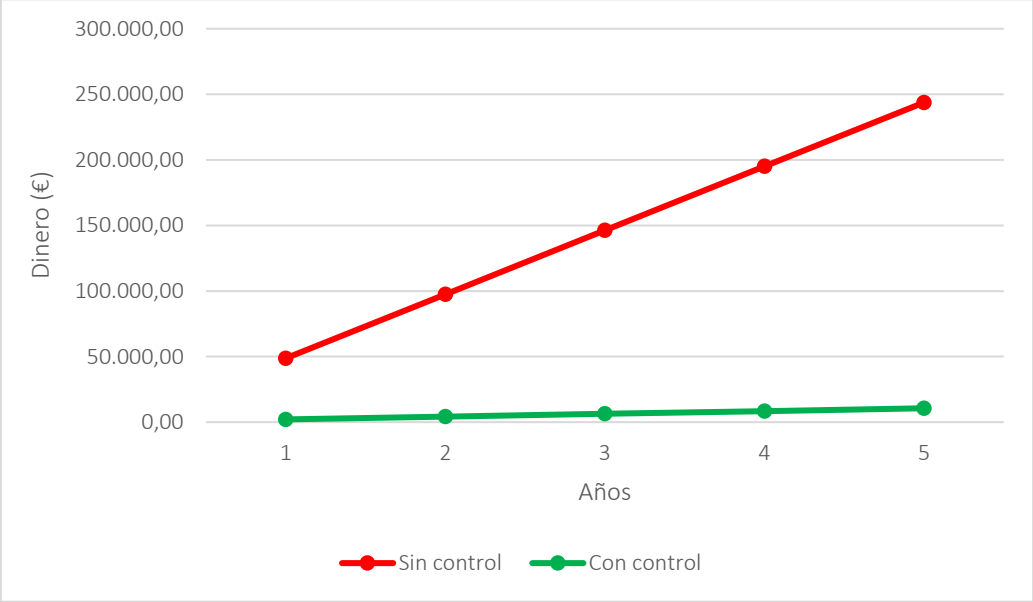



*Ilustración 166. Rentabilidad amenaza HW1 - [A.25] activo S6*

Amenaza: SRVD1 - [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 48751,32 | 0 | 0 | 48751,32 | 97502,64 | 146253,96 | 195005,28 | 243756,6 |
| 1462,54 | 0 | 659,88 | 2122,42 | 4244,84 | 6367,26 | 8489,68 | 10612,1 |

*Tabla 172. Rentabilidad amenaza SRVD1 - [A.25] activo S6*

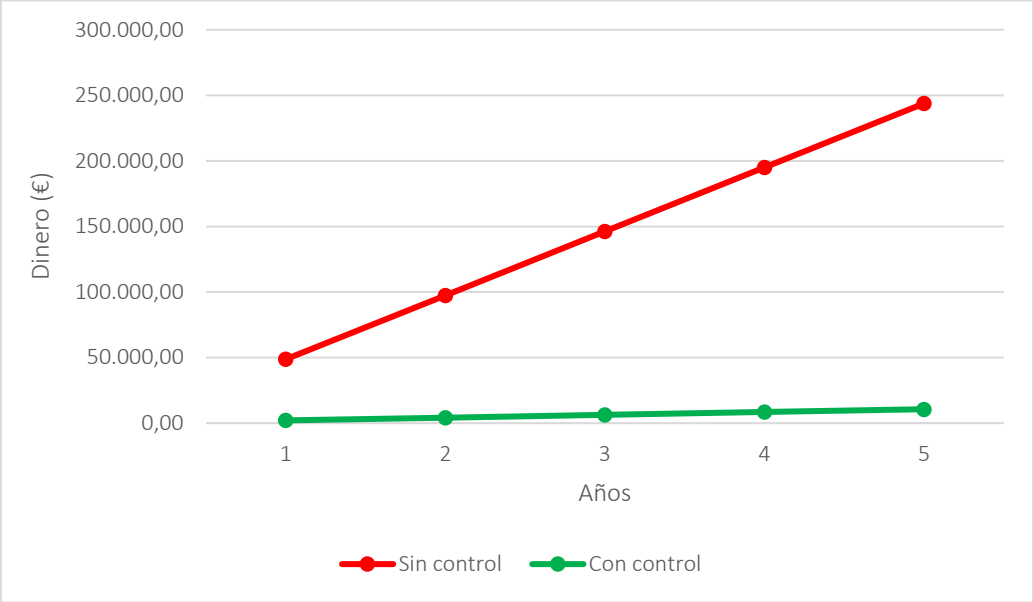



*Ilustración 167. Rentabilidad amenaza SRVD1 - [A.25] activo S6*

## Amenaza: T1 – [A.25] Robo

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1625,04 | 0 | 0 | 1625,04 | 3250,08 | 4875,12 | 6500,16 | 8125,2 |
| 48,75 | 0 | 659,88 | 708,63 | 1417,26 | 2125,89 | 2834,52 | 3543,15 |

*Tabla 173. Rentabilidad amenaza T1 - [A.25] activo S6*

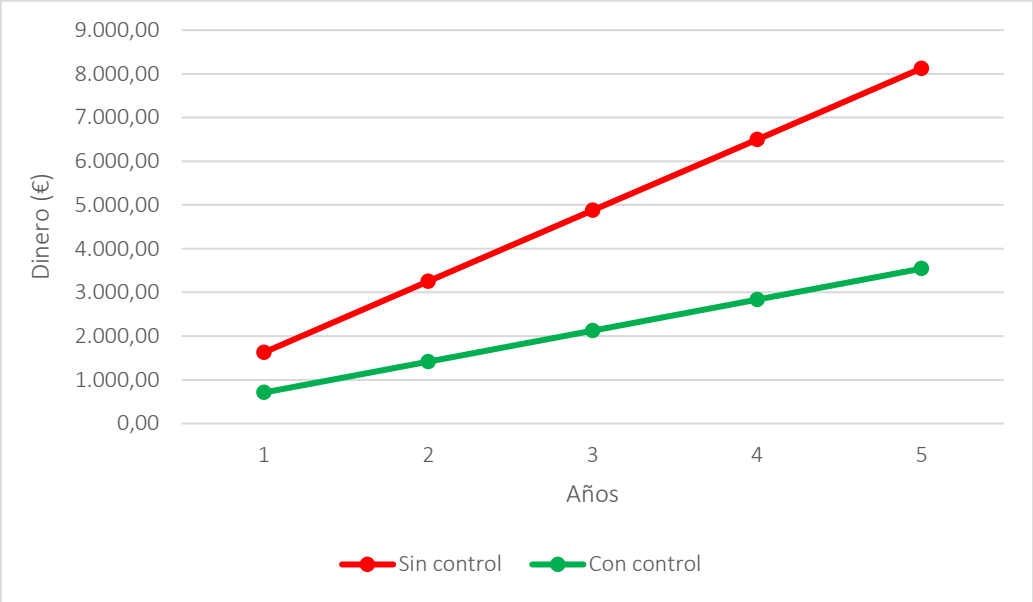



*Ilustración 168. Rentabilidad amenaza T1 - [A.25] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.4 Cuarto control

##### 2.1.5.4.1 Título

Control de contraseñas

##### 2.1.5.4.2 Finalidad

Una amenaza a la que podemos enfrentarnos en un Sistema de información son los robos de contraseñas, por lo tanto, debemos protegernos de ellos con las medidas que tenemos disponibles, en este caso vamos a usar una serie de medidas y de recomendaciones que hacen que nuestras contraseñas sean más seguras y robustas.

##### 2.1.5.4.3 Empresa

“Sanitaria AMS S.L.”

##### 2.1.5.4.4 Leyes aplicables

No hay referencias de leyes para este control.

##### 2.1.5.4.5 Normas aplicables

No hay referencias de normas para este control.

##### 2.1.5.4.6 Descripción del control

A continuación, vamos a detallar los pasos que debemos seguir y las características que deben cumplir nuestras contraseñas, para ello nos vamos a basar en un guía que ha elaborado el Instituto Nacional de Ciberseguridad.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir unas buenas prácticas: actualizarlas periódicamente, garantizar su fortaleza

(dificultad para adivinarla o craquearla), no utilizar contraseñas por defecto o cómo custodiarlas.

Vamos a incluir una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a las contraseñas. Vamos a definir una "Checklist", la cual debemos utilizar para comprobar que nuestra contraseña cumple con los requisitos necesarios.

| CONTROL | |
|---|---|
| **No utilizar las contraseñas por defecto**<br>*Cambias las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones y sistemas* | ☐ |
| **No compartir las contraseñas con nadie**<br>*Mantienes en secreto tus claves y evitas compartirlas* | ☐ |
| **Las contraseñas deben ser robustas**<br>*Genera tus contraseñas teniendo en cuenta su fortaleza. Deben tener un mínimo de 8 caracteres y ser una combinación de letras mayúsculas y minúsculas con números y caracteres especiales* | ☐ |
| **No utilizar la misma contraseña para servicios diferentes**<br>*Te aseguras de elegir distintas contraseñas para cada uno de los servicios que utilizas* | ☐ |
| **Cambiar las contraseñas periódicamente**<br>*Haces que se modifiquen las contraseñas una vez al mes* | ☐ |
| **No hacer uso del recordatorio de contraseñas**<br>*No utilizas nunca las opciones de recordatorio de contraseñas de navegadores y aplicaciones* | ☐ |
| **Utilizar gestores de contraseñas**<br>*Usas gestores de contraseñas seguros para poderlas recordar* | ☐ |

***Tabla 174. Checklist contraseñas***

- **No utilizar las contraseñas por defecto:** Debemos cambiar las claves por defecto, las que traen los equipos y sistemas al adquirirlos, por otras elegidas por nosotros mismo. Con esta medida evitamos el acceso no permitido, que sería posible si dejamos la contraseña por defecto por ser estas conocidas o que pueden encontrarse fácilmente en internet.

- **No compartir las contraseñas con nadie:** Si compartimos nuestras contraseñas estas dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de los siguiente:
  - no debemos compartirlas con nadie;
  - no debemos apuntarlas en papeles o post-it;
  - no debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.
- **Las contraseñas deben ser robustas:** Para que nuestras contraseñas sean fuertes, difíciles de adivinar o calcular, debemos cumplir las siguientes directrices:
  - deben contener al menos ocho caracteres;
  - deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
    - palabras sencillas en cualquier idioma (palabras de diccionarios);
    - nombres propios, fechas, lugares o datos de carácter personal;
    - palabras que estén formadas por caracteres próximos en el teclado;
    - palabras excesivamente cortas.
  - tampoco utilizaremos claves que estén formadas solamente por elementos o palabras que puedan ser públicas o fácilmente adivinables (ej. Nombre + fecha de nacimiento);
  - se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas;
  - se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo *passphrase* (contraseña larga formada por una secuencia de palabras).
- **No utilizar la misma contraseña para servicios diferentes:** Nunca debemos utilizar la misma contraseña para diferentes servicios. Tampoco utilizaremos las mismas contraseñas para uso profesional y doméstico. De esta forma evitaremos tener que cambiar todas nuestras contraseñas en el caso de que solo una haya sido comprometida.
- **Cambiar las contraseñas periódicamente:** Para garantizar la confidencialidad de nuestras contraseñas deber ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.

- **No hacer uso del recordatorio de contraseñas:** No es recomendable el utilizar las funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personal no autorizado. Esto es especialmente frecuente en el uso de navegadores web.
- **Utilizar gestores de contraseñas:** Debemos considerar el uso de gestores de contraseñas en aquellos casos en los que tengamos que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implantar doble factor de autentificación para acceder al mismo. Como recomendación de uso, se puede usar "LassPass" que se trata de un buen gestor de contraseñas, con un gran número de funcionalidades que nos pueden ayudar a administrar las nuestras y además es gratuito.

#### 2.1.5.4.7 Responsable

Cada persona de la empresa será la propia responsable de implementar dicho control en sus contraseñas, es decir, cada uno tendrá que realizar todas las acciones necesarias para que su contraseña cumpla con las especificaciones.

#### 2.1.5.4.8 Dispositivos

No es necesario ningún dispositivo, ya que cada usuario se encargará de crear sus propias contraseñas, no necesitamos de ningún programa de gestión de contraseñas.

#### 2.1.5.4.9 Costes

- **Implantación:** 0 €, ya que realizar estas medidas en las contraseñas sólo cuesta tiempo, pero no tiene ningún coste monetario.
- **Ejecución y mantenimiento:** 0 €, no supone ningún gasto por el mismo motivo que el anterior.
- **Búsqueda de irregularidades:** Cada empleado deberá preocuparse del mantenimiento de sus contraseñas, como debe actualizarlas cada mes, entonces cada vez tendrá que repasar que todo está en correcto estado.

#### 2.1.5.4.10 Rentabilidad

La suplantación de identidad o los accesos no autorizados pueden afectar a una gran parte de nuestro SI, por lo tanto, ya hemos estudiado anteriormente que esto puede ser un problema muy grave, por lo que realizar este control es muy importante.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar este control en nuestro SI, vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 80 %, ya que puede fallar por:

- Un olvido de la persona responsable
- Una mala configuración de la contraseña
- No cumplir con los requisitos de la contraseña
- Olvido de revisión del responsable

Activo: Información de pacientes (S1)

Amenazas: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 54575,6 | 0 | 0 | 54575,6 | 109151,2 | 163726,8 | 218302,4 | 272878 |
| 1091,51 | 0 | 0 | 1091,51 | 2183,02 | 3274,53 | 4366,04 | 5457,55 |

*Tabla 175. Rentabilidad amenaza AUX1 - [A.11] activo S1*

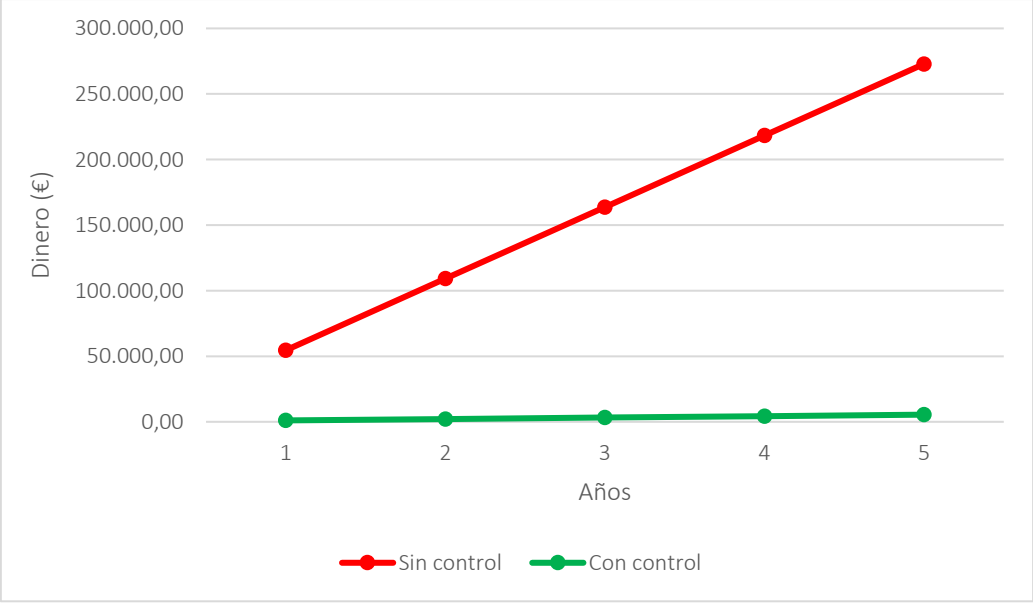



*Ilustración 169. Rentabilidad amenaza AUX1 - [A.11] activo S1*

### Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 909593,31 | 0 | 0 | 909593,31 | 1819186,6 | 2728779,93 | 3638373,24 | 4547966,55 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 176. Rentabilidad amenaza D1 - [A.11] activo S1*

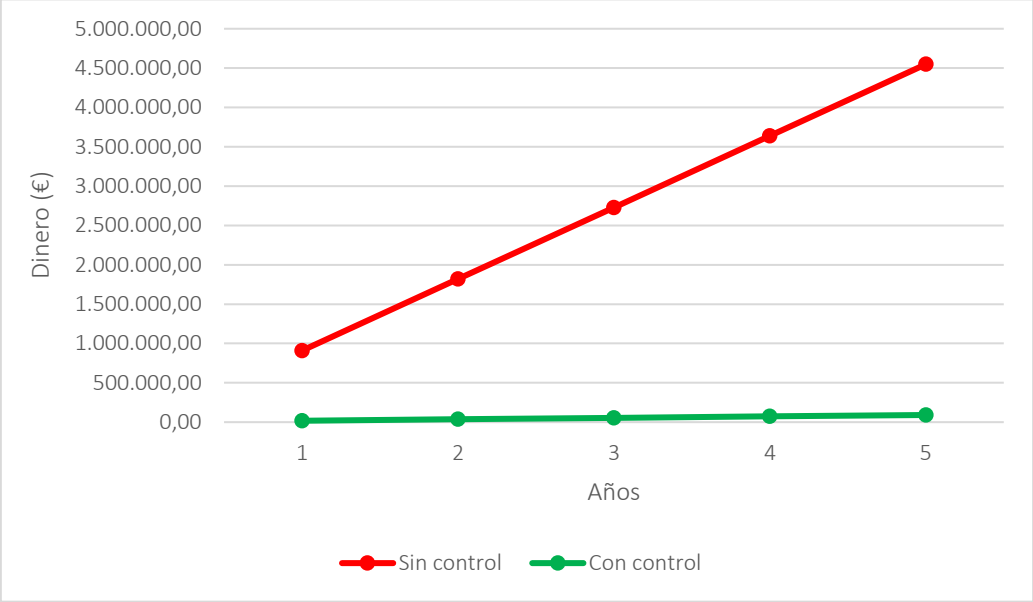



*Ilustración 170.Rentabilidad amenaza D1 - [A.11] activo S1*

### Amenaza: SW1 – [A.5] Suplantación de la identidad de usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 3638,37 | 0 | 0 | 3638,37 | 7276,74 | 10915,11 | 14553,48 | 18191,85 |

*Tabla 177. Rentabilidad amenaza SW1 - [A.5] activo S1*

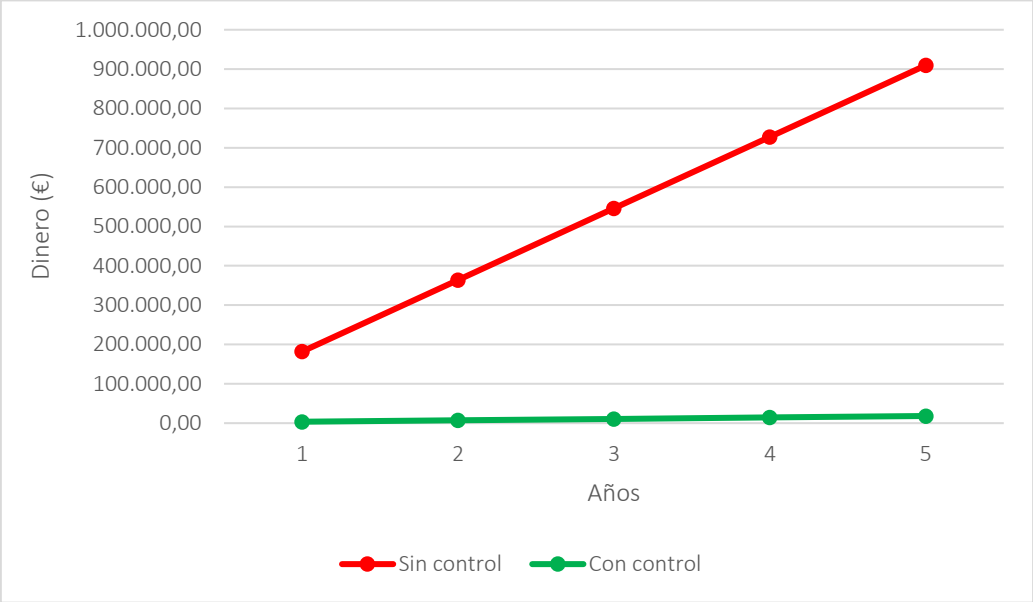



*Ilustración 171. Rentabilidad amenaza SW1 - [A.5] activo S1*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 3638,37 | 0 | 0 | 3638,37 | 7276,74 | 10915,11 | 14553,48 | 18191,85 |

*Tabla 178. Rentabilidad amenaza SRVD1 - [A.11] activo S1*

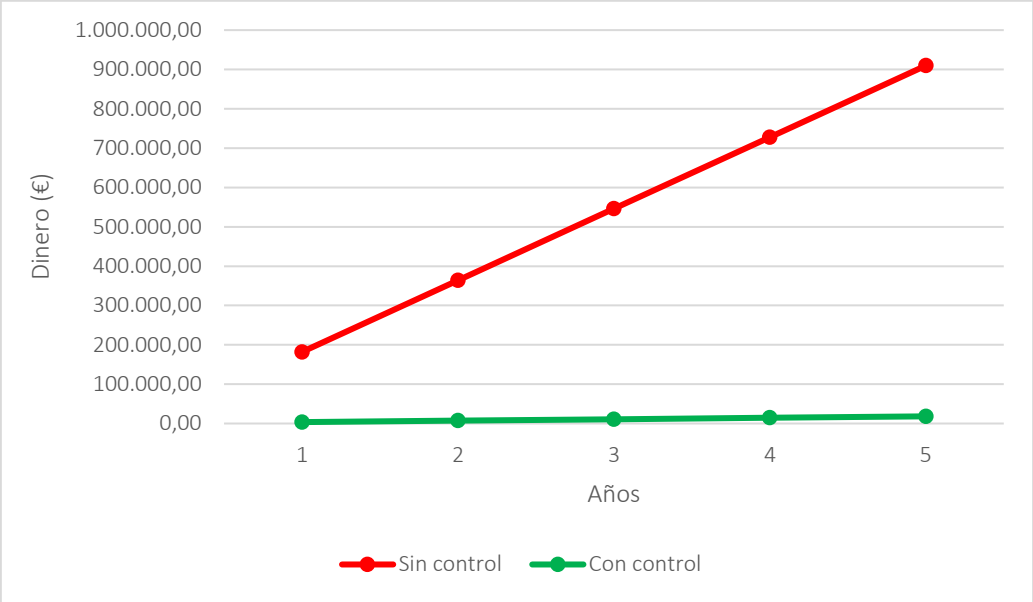



*Ilustración 172. Rentabilidad amenaza SRVD1 - [A.11] activo S1*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 6063,96 | 0 | 0 | 6063,96 | 12127,92 | 18191,88 | 24255,84 | 30319,8 |
| 121,28 | 0 | 0 | 121,28 | 242,56 | 363,84 | 485,12 | 606,4 |

*Tabla 179. Rentabilidad amenaza T1 - [A.11] activo S1*

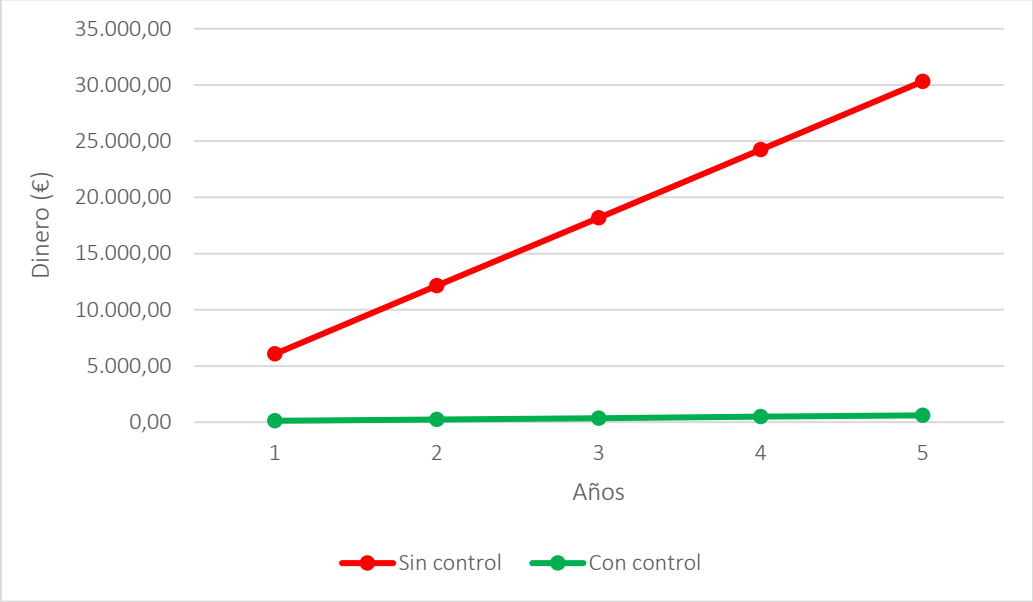



*Ilustración 173. Rentabilidad amenaza T1 - [A.11] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenazas: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 731,27 | 0 | 0 | 731,27 | 1462,54 | 2193,81 | 2925,08 | 3656,35 |

*Tabla 180. Rentabilidad amenaza AUX1 - [A.11] activo S3*

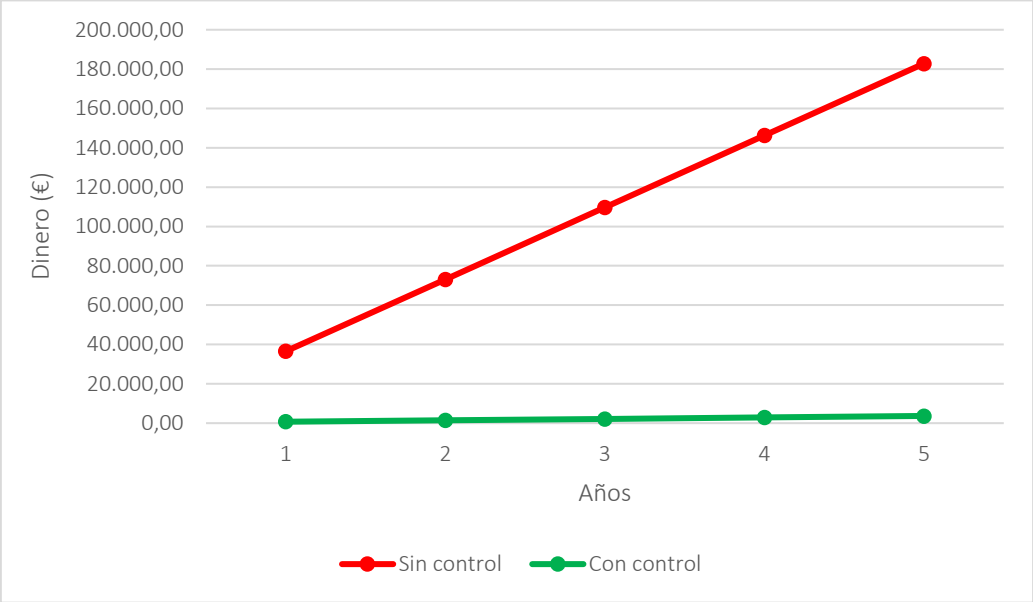



*Ilustración 174. Rentabilidad amenaza AUX1 - [A.11] activo S3*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 181. Rentabilidad amenaza D1 - [A.11] activo S3*

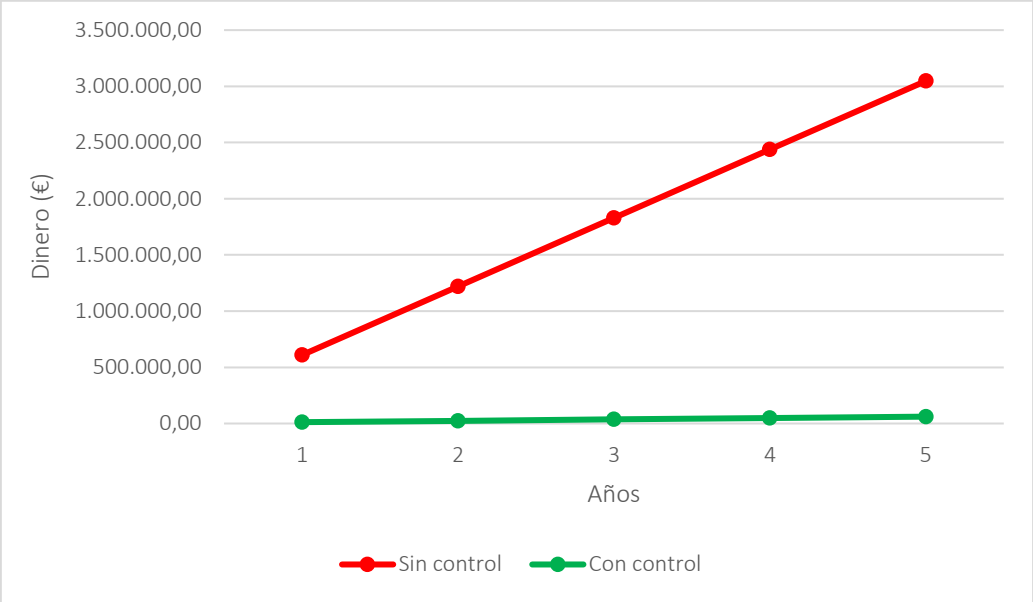



*Ilustración 175. Rentabilidad amenaza D1 - [A.11] activo S3*

## Amenaza: SW1 – [A.5] Suplantación de la identidad de usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 182. Rentabilidad amenaza SW1 - [A.5] activo S3*

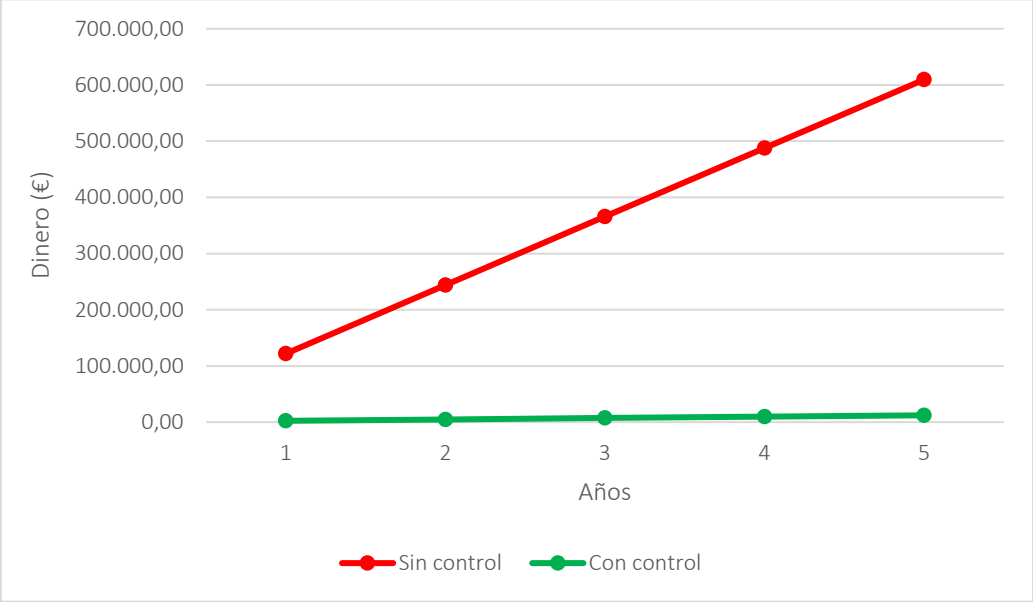



*Ilustración 176. Rentabilidad amenaza SW1 - [A.5] activo S3*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 183. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

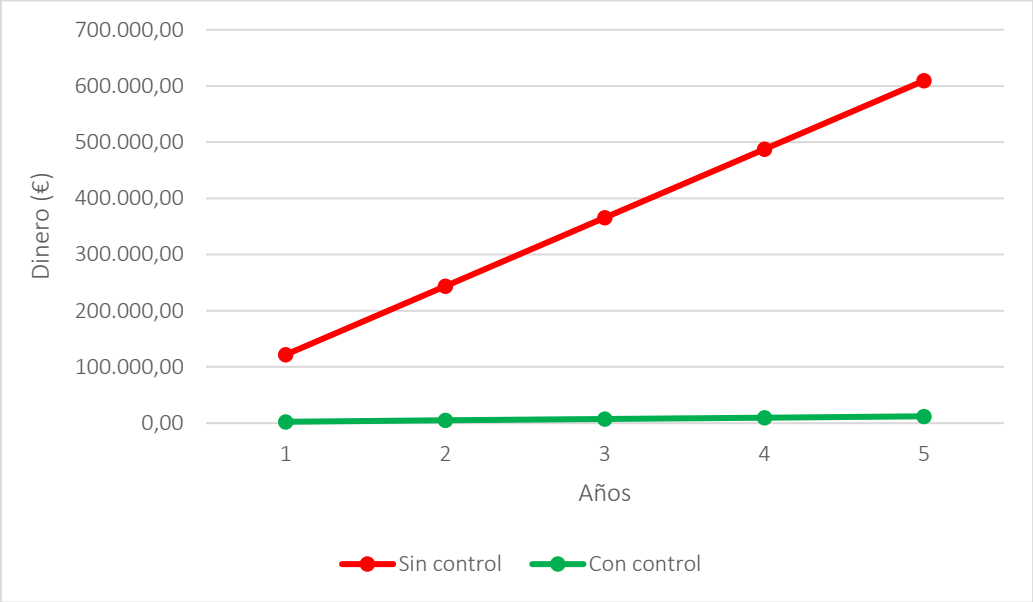



*Ilustración 177. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 81,25 | 0 | 0 | 81,25 | 162,5 | 243,75 | 325 | 406,25 |

*Tabla 184. Rentabilidad amenaza T1 - [A.11] activo S3*

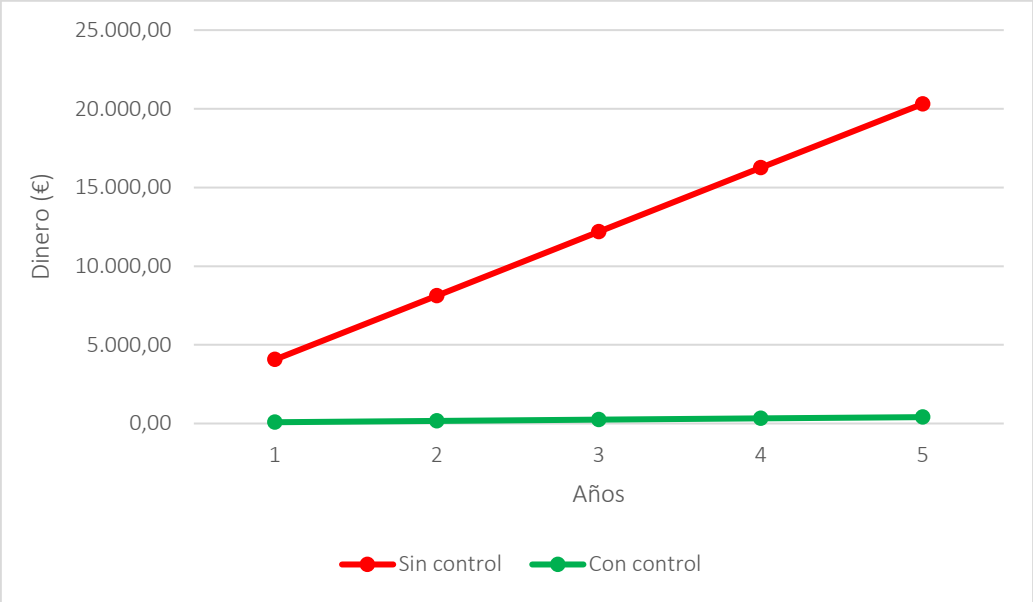



*Ilustración 178. Rentabilidad amenaza T1 - [A.11] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenazas: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36562,54 | 0 | 0 | 36562,54 | 73125,08 | 109687,62 | 146250,16 | 182812,7 |
| 731,25 | 0 | 0 | 731,25 | 1462,5 | 2193,75 | 2925 | 3656,25 |

*Tabla 185. Rentabilidad amenaza AUX1 - [A.11] activo S4*

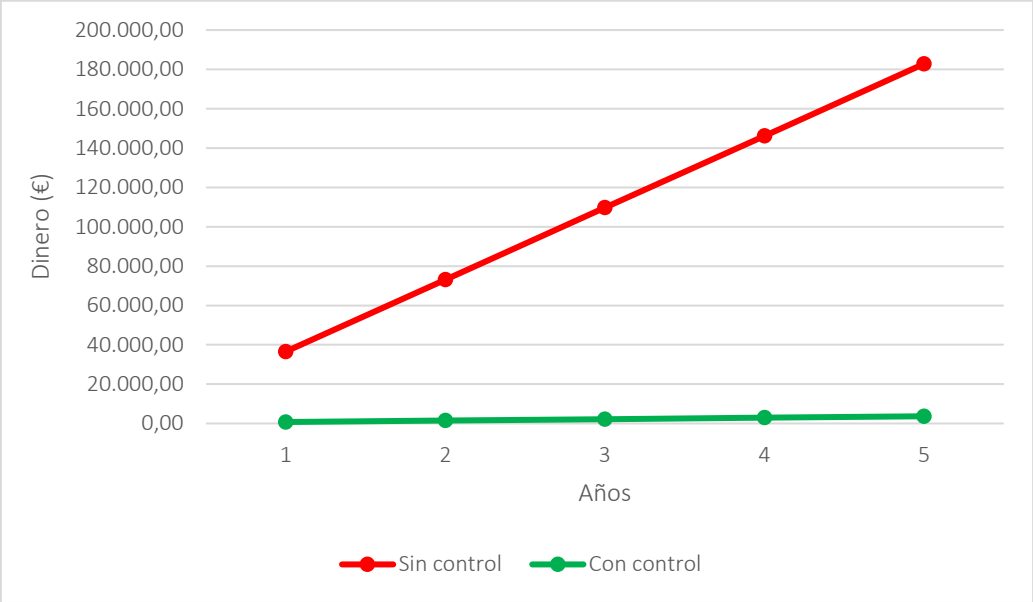



*Ilustración 179. Rentabilidad amenaza AUX1 - [A.11] activo S4*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609375,71 | 0 | 0 | 609375,71 | 1218751,4 | 1828127,13 | 2437502,84 | 3046878,55 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 186.Rentabilidad amenaza D1 - [A.11] activo S4*

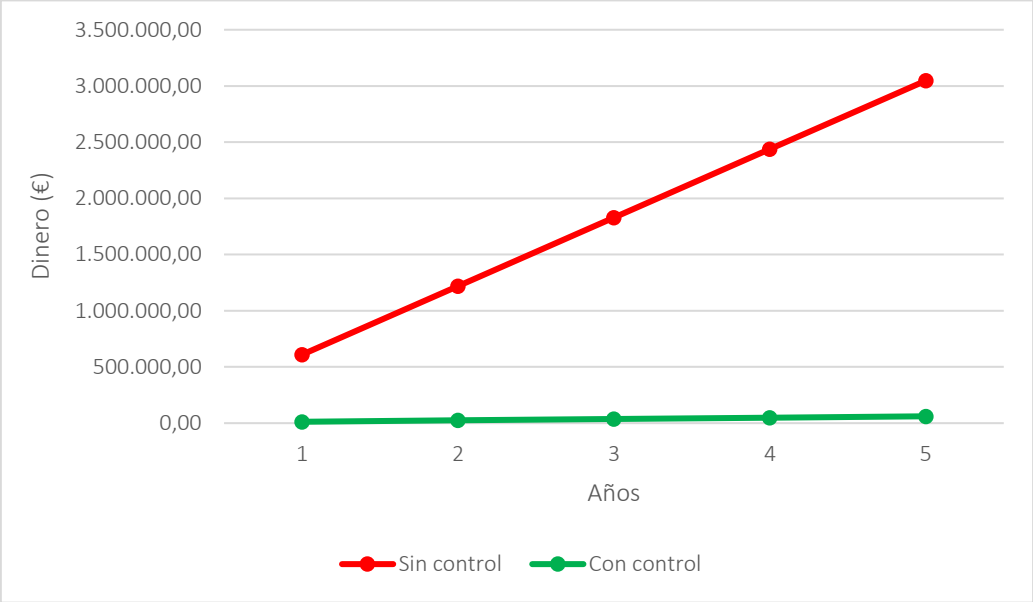



*Ilustración 180. Rentabilidad amenaza D1 - [A.11] activo S4*

Amenaza: SW1 – [A.5] Suplantación de la identidad de usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 2437,5 | 0 | 0 | 2437,5 | 4875 | 7312,5 | 9750 | 12187,5 |

*Tabla 187. Rentabilidad amenaza SW1 - [A.5] activo S4*

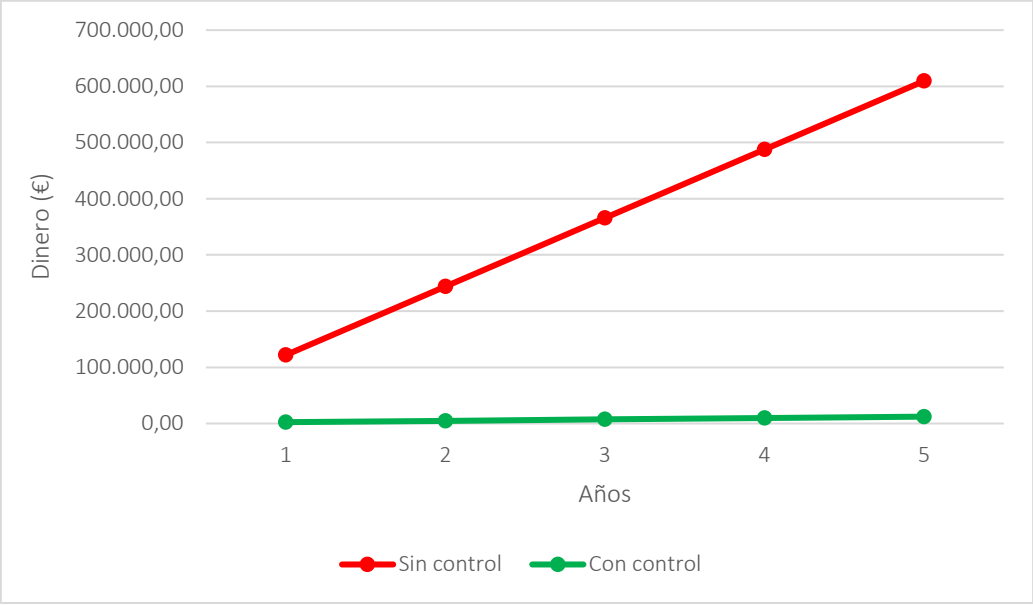



*Ilustración 181. Rentabilidad amenaza SW1 - [A.5] activo S4*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 2437,5 | 0 | 0 | 2437,5 | 4875 | 7312,5 | 9750 | 12187,5 |

*Tabla 188. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

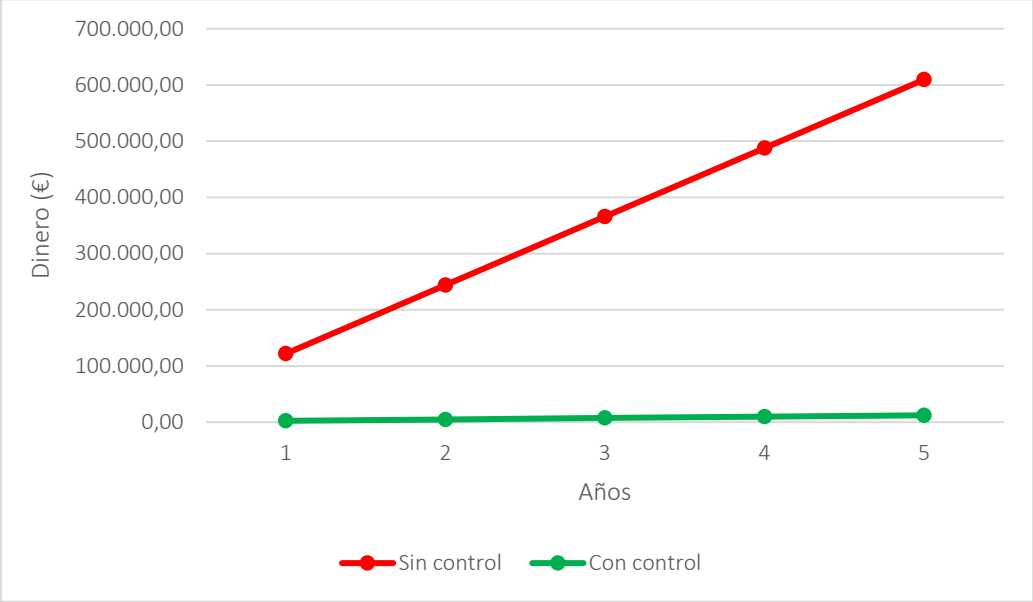



*Ilustración 182. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

## Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,5 | 0 | 0 | 4062,5 | 8125 | 12187,5 | 16250 | 20312,5 |
| 81,25 | 0 | 0 | 81,25 | 162,5 | 243,75 | 325 | 406,25 |

*Tabla 189. Rentabilidad amenaza T1 - [A.11] activo S4*

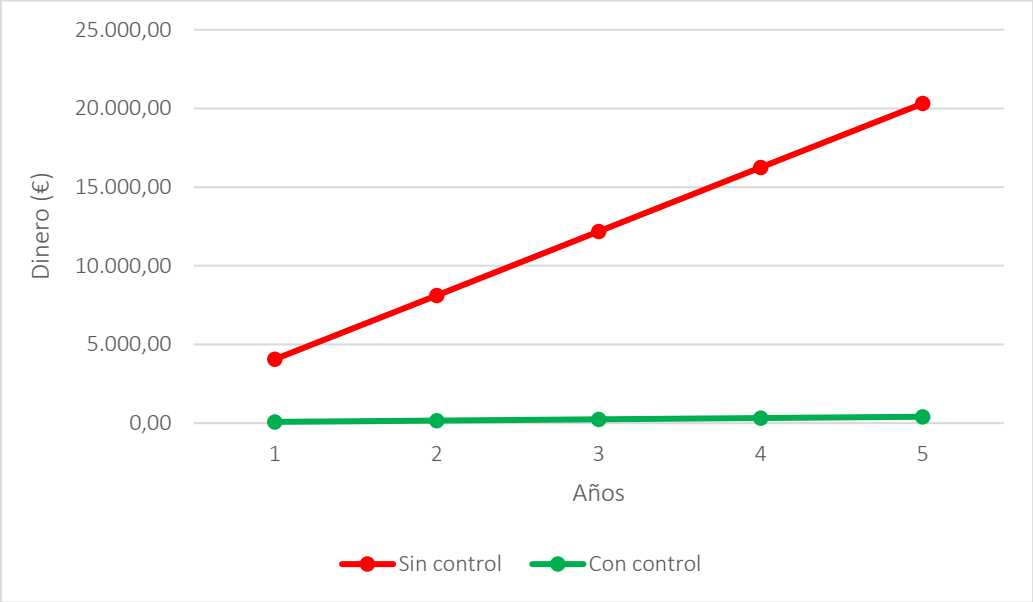



*Ilustración 183. Rentabilidad amenaza T1 - [A.11] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenazas: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 731,27 | 0 | 0 | 731,27 | 1462,54 | 2193,81 | 2925,08 | 3656,35 |

*Tabla 190. Rentabilidad amenaza AUX1 - [A.11] activo S5*

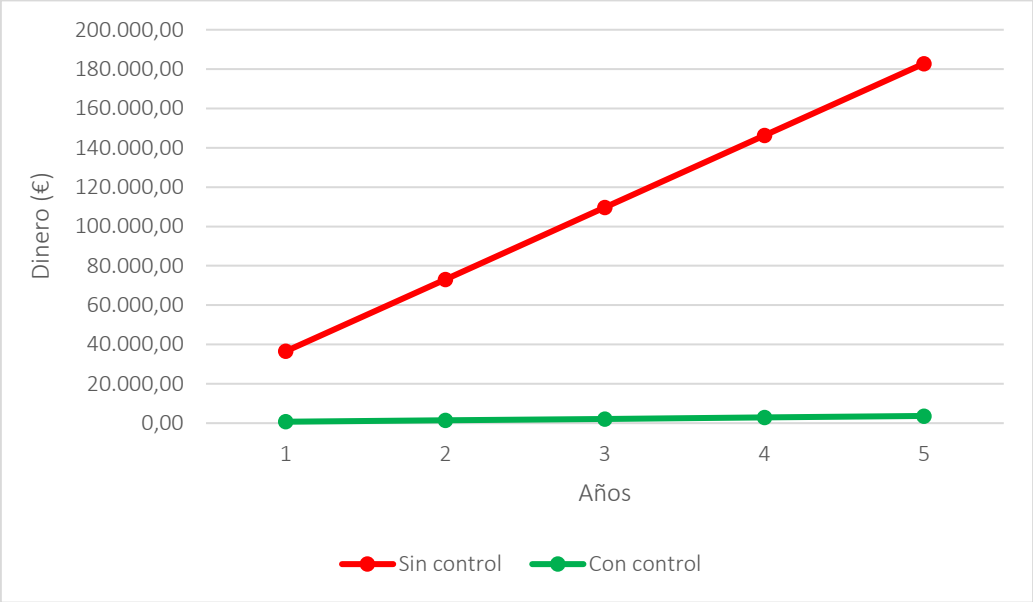



*Ilustración 184. Rentabilidad amenaza AUX1 - [A.11] activo S5*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 191. Rentabilidad amenaza D1 - [A.11] activo S5*

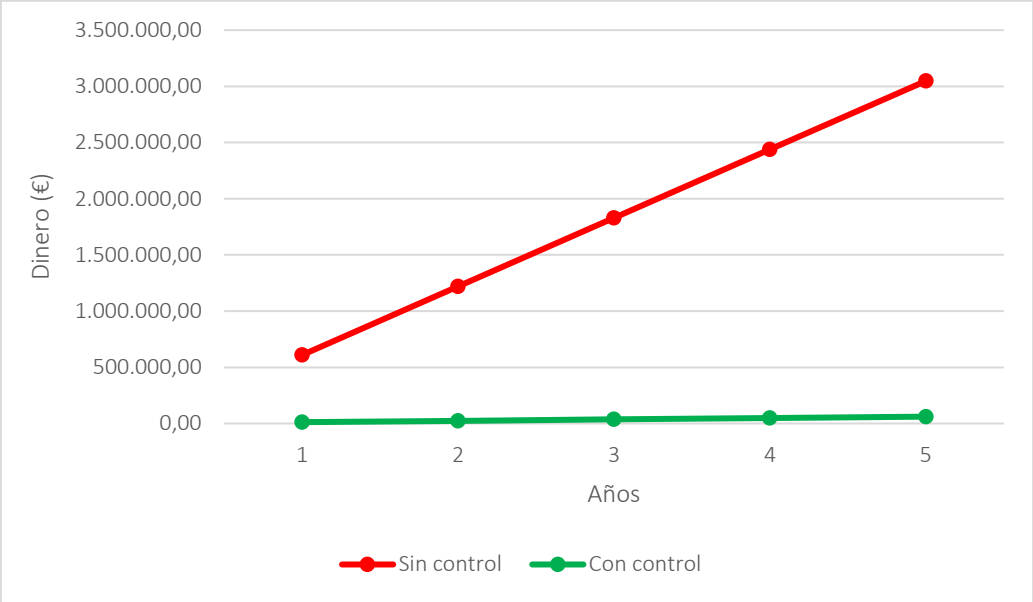



*Ilustración 185. Rentabilidad amenaza D1 - [A.11] activo S5*

## Amenaza: SW1 – [A.5] Suplantación de la identidad de usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 192. Rentabilidad amenaza SW1 - [A.5] activo S5*

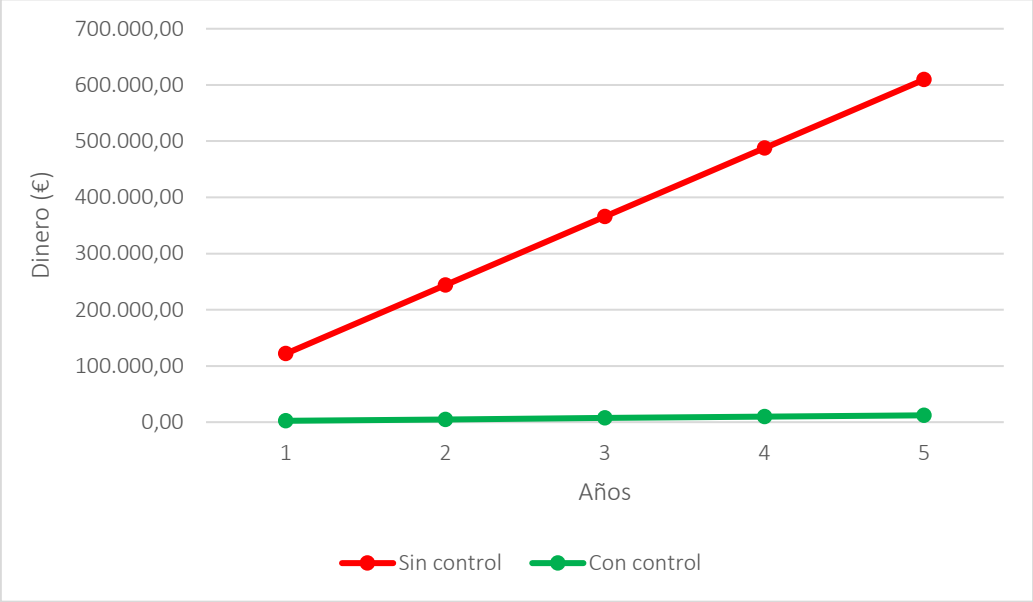



*Ilustración 186. Rentabilidad amenaza SW1 - [A.5] activo S5*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 193. Rentabilidad amenaza SRVD1 - [A.11] activo S5*

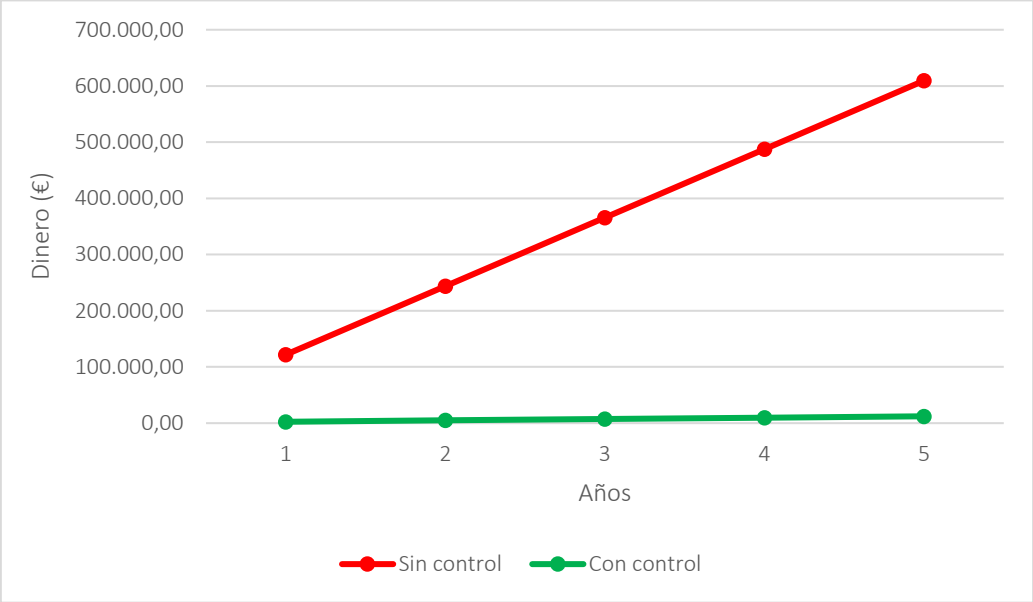



*Ilustración 187. Rentabilidad amenaza SRVD1 - [A.11] activo S5*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 81,25 | 0 | 0 | 81,25 | 162,5 | 243,75 | 325 | 406,25 |

*Tabla 194. Rentabilidad amenaza T1 - [A.11] activo S5*

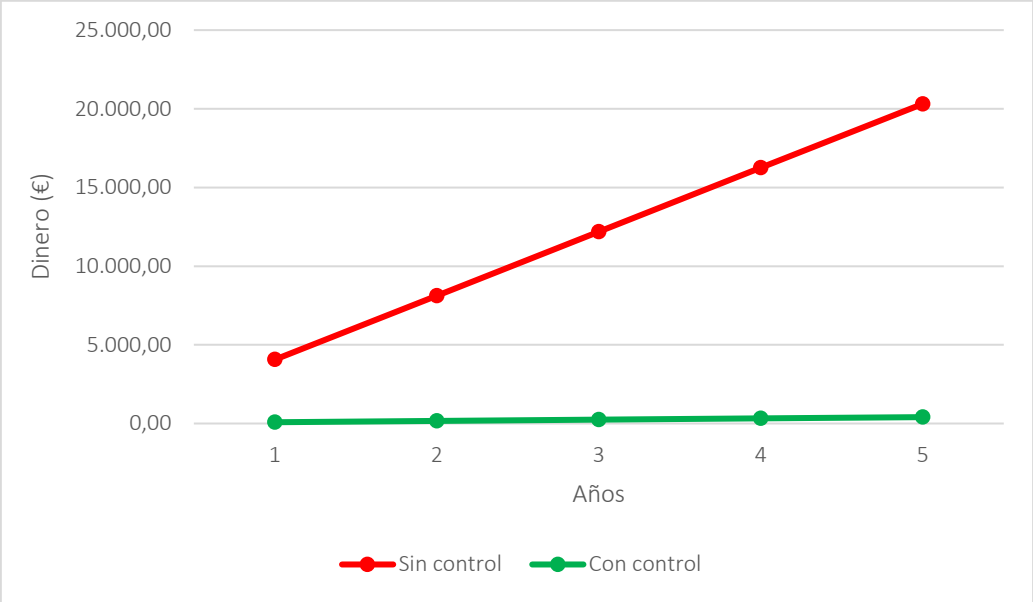



*Ilustración 188. Rentabilidad amenaza T1 - [A.11] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenazas: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 731,27 | 0 | 0 | 731,27 | 1462,54 | 2193,81 | 2925,08 | 3656,35 |

*Tabla 195. Rentabilidad amenaza AUX1 - [A.11] activo S6*

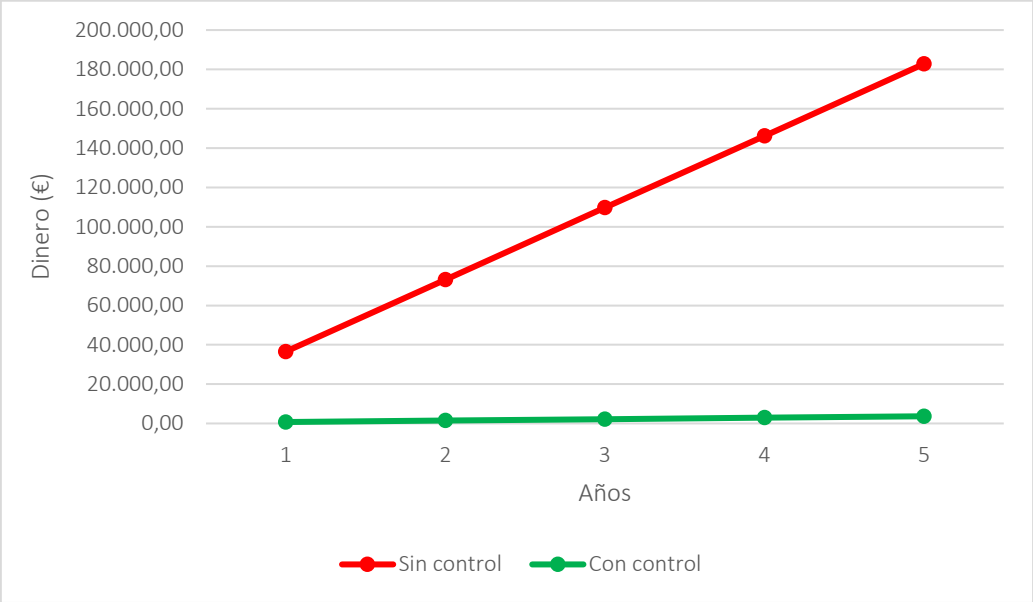



*Ilustración 189. Rentabilidad amenaza AUX1 - [A.11] activo S6*

Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 196. Rentabilidad amenaza D1 - [A.11] activo S6*

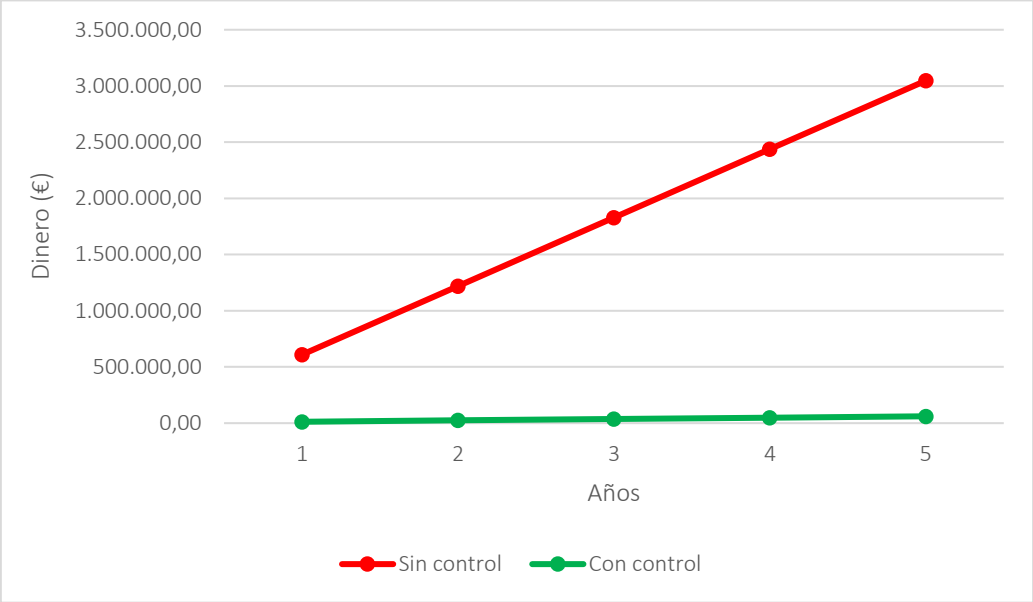



*Ilustración 190. Rentabilidad amenaza D1 - [A.11] activo S6*

## Amenaza: SW1 – [A.5] Suplantación de la identidad de usuario

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 197. Rentabilidad amenaza SW1 - [A.5] activo S6*

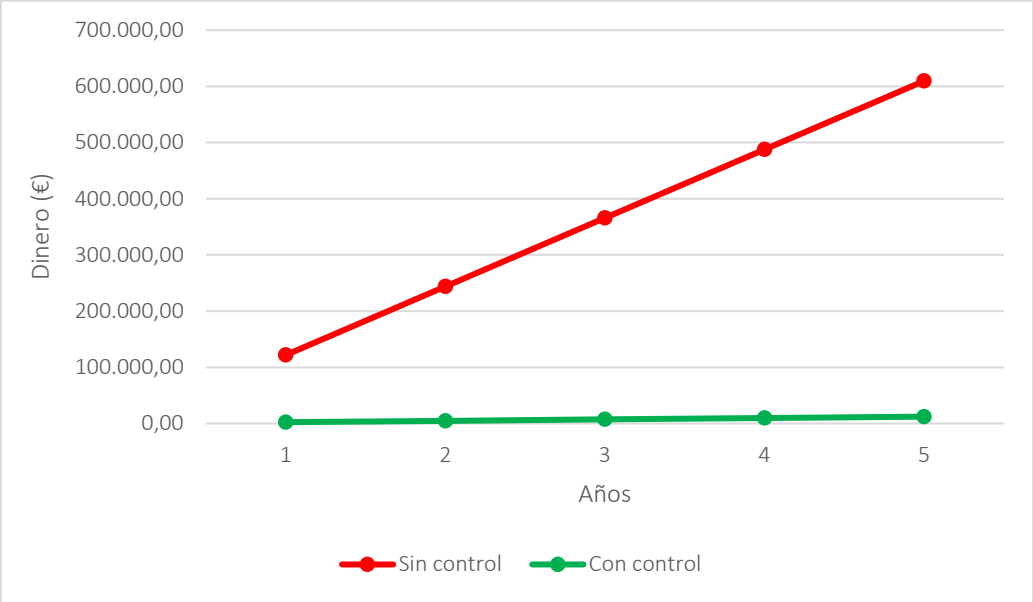



*Ilustración 191. Rentabilidad amenaza SW1 - [A.5] activo S6*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 2437,57 | 0 | 0 | 2437,57 | 4875,14 | 7312,71 | 9750,28 | 12187,85 |

*Tabla 198. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

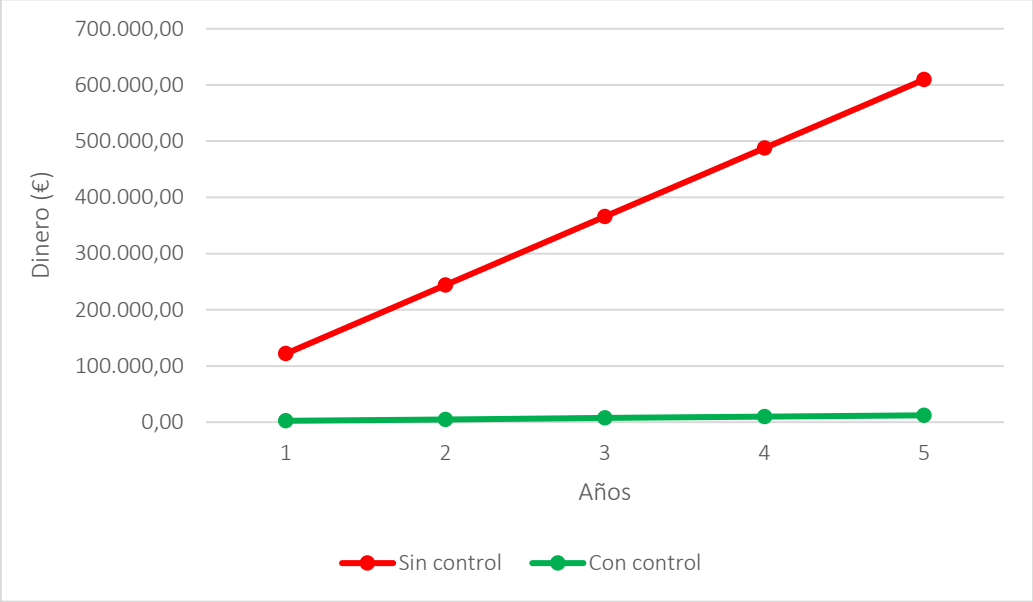



*Ilustración 192. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

## Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 81,25 | 0 | 0 | 81,25 | 162,5 | 243,75 | 325 | 406,25 |

*Tabla 199. Rentabilidad amenaza T1 - [A.11] activo S6*

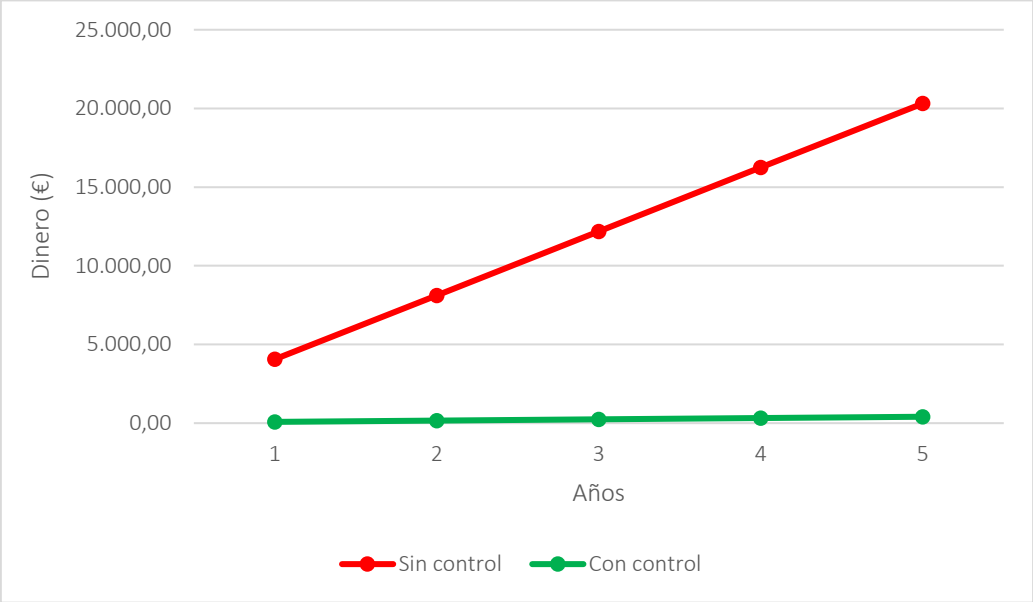



*Ilustración 193. Rentabilidad amenaza T1 - [A.11] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.5 Quinto control

##### 2.1.5.5.1 Título

Control de acceso de usuarios

##### 2.1.5.5.2 Finalidad

Una amenaza a la que podemos enfrentarnos en un Sistema de información son los abusos de privilegios de acceso, accesos no autorizados y uso no previsto de nuestros terminales, así que debemos seguir una serie de medidas para protegernos.

##### 2.1.5.5.3 Empresa

“Sanitaria AMS S.L.”

##### 2.1.5.5.4 Leyes aplicables

No hay referencias de leyes para este control.

#### 2.1.5.5.5 Normas aplicables

UNE-EN 12251:2004. Informática sanitaria. Identificación segura de usuario para sanidad. Gestión y seguridad de la autenticación por contraseñas.
UNE-EN ISO 22600-2:2014. Informática sanitaria. Gestión de privilegios y control de acceso. Parte 2: Modelos formales.
UNE-EN ISO 22600-3:2014. Informática sanitaria. Gestión de privilegios y control de acceso. Parte 3: Implementaciones

#### 2.1.5.5.6 Descripción del control

Controlar quien accede a la información de nuestra empresa es un primer paso para protegerla. Es esencial que podemos distinguir quién tiene permisos para acceder a nuestra información, como, cuando y con qué finalidad.

Por otra parte, el registro de los accesos en logs de los sistemas va a ser determinante para analizar los incidentes de seguridad.

Aunque se trate de una empresa pequeña no por eso debemos descuidar nuestro control de accesos. En caso de que alguien realice alguna acción que perjudique nuestro SI, debemos tener un registro de quien y cuando lo ha hecho.

A continuación, se incluyen una serie de controles que deberemos cumplir para la política en lo relativo al control de acceso. Para ello, nos vamos a basar en una guía que ha elaborado el Instituto Nacional de Ciberseguridad. (INCIBE, n.d.-d)

Vamos a incluir una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al control de acceso. Por lo tanto, vamos a definir una “Checklist”, la cual debemos utilizar para comprobar que nuestro control de accesos cumple los requisitos necesarios.

| CONTROL | |
|---|---|
| **Política de usuarios y grupos**<br>*Defines los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.* | ☐ |
| **Asignación de permisos**<br>*Asignas los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso* | ☐ |
| **Creación/modificación/borrado de cuentas de usuario con permisos** | ☐ |

| | |
|---|---|
| *Defines y aplicas un procedimiento para dar de alta/baja o modificar las cuentas de usuario* | |
| **Cuentas de administración**<br>*Gestionas las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad* | ☐ |
| **Registro de eventos**<br>*Estableces mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de tu empresa* | ☐ |
| **Revisión de permisos**<br>*Revisas cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados* | ☐ |
| **Revocación de permisos y eliminación de cuentas**<br>*Desactivas los permisos de acceso y eliminas las cuentas de usuario una vez finalizada la relación contractual* | ☐ |

***Tabla 200. Checklist control de usuarios***

- **Política de usuarios y grupos:** Definiremos una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos:
  - en función del área o departamento al que pertenezca el empleado;
  - en función del tipo de información a la qué accederá;
  - en función de las operaciones permitidas sobre la información a la que se tiene acceso.

  En función de los criterios anteriores podemos establecer diversos perfiles de usuarios.

  Por lo tanto, tendríamos dos grupos, un grupo de administradores en el que sólo entran las cuentas que se van a usar para la administración y tendrán acceso a todo el SI, en este grupo sólo estarán las cuentas de los dos dueños de la empresa. Y, por otro lado, el grupo de los empleados, con el que sólo se podrán acceder a las partes que no tengan que ver con la administración del sistema de información, en este grupo estarán los demás empleados de la empresa.

- **Asignación de permisos:** Una vez establecidos los tipos de información, los perfiles de usuario y los grupos existentes, podremos concretar los tipos

de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.

- **Creación/modificación/borrado de cuentas de usuario:** Para permitir el acceso real a los sistemas de información de la empresa debemos tener un procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios indicando quien debe autorizarlo. Se detallarán los datos identificativos de las mismas, las acciones que se permiten y las dotaremos de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.

  En cuanto al procedimiento se hará de la siguiente manera, cuando creemos la cuenta debemos definir todos los datos identificativos de esta, a continuación, las acciones que se le van a permitir realizar a dicha cuenta y se deberán de crear las credenciales de acceso y se le entregarán de manera confidencial al dueño de la cuenta.

- **Cuentas de administración:** Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuentas los siguientes aspectos:

  - utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración;
  - registrar convenientemente todas sus acciones (registro de logs);
  - el acceso como administrador debería ser notificado convenientemente;
  - evitar que los privilegios de las cuentas de administrador puedan ser heredaros;
  - las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia;

- **Registro de eventos:** Estableceremos los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la

empresa. Se deberá registrar convenientemente quién accede a nuestra información, cuándo y cómo. Como el propio programa que se usa para la gestión del sistema de información de la empresa tiene su propio mecanismo de registro de eventos, tendremos que activar estas opciones para que se registre quien accede, hora y fecha de acceso y desde que terminal de la empresa lo ha hecho.

- **Revisión de permisos:** Se revisará una vez al mes que los permisos concedidos a los usuarios son los adecuados.
- **Revocación de permisos y eliminación de cuentas:** Al finalizar la relación contractual con el empleado es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Eliminaremos sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones.

#### 2.1.5.5.7 Responsable

Administrador del SI, será el responsable de realizar todas las acciones relativas a las cuentas para el control de acceso, las creará, le asignará los permisos pertinentes y se las entregará a la persona correspondiente.

#### 2.1.5.5.8 Dispositivos

No es necesario ningún dispositivo, ya que las cuentas y permisos que se creen/modifiquen/eliminen se harán con el propio software utilizado por la empresa.

#### 2.1.5.5.9 Costes

- **Implantación:** 0 €, ya que realizar estas medidas de las cuentas se harán con el software que ya usa la empresa para su gestión.
- **Ejecución y mantenimiento:** 0 €, no supone ningún gasto por el mismo motivo que anteriormente.
- **Búsquedas de irregularidades:** En caso de que el propietario de cada cuenta note cualquier anomalía en ésta, ya sea de problema de *login* o problemas de permisos, deberá comunicárselo en la menor brevedad posible al administrador del sistema para solucione los problemas.

#### 2.1.5.5.10 Rentabilidad

El abuso de privilegios de acceso y el uso no previsto dentro de la empresa pueden afectar a una gran parte de nuestro SI, por lo tanto, ya hemos estudiado anteriormente que esto puede ser un problema muy grave, por lo que realizar este control es muy importante. Además, con este control podemos controlar también de donde viene el problema en caso de que haya fugas de información.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar este control en nuestro SI, vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 90 %, ya que puede fallar por:

- Un olvido de la persona responsable.
- Una mala configuración del responsable.
- Olvido de revisión del responsable.

Activo: Información de pacientes (S1)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

*Tabla 201. Rentabilidad amenaza D1 - [E.19] activo S1*

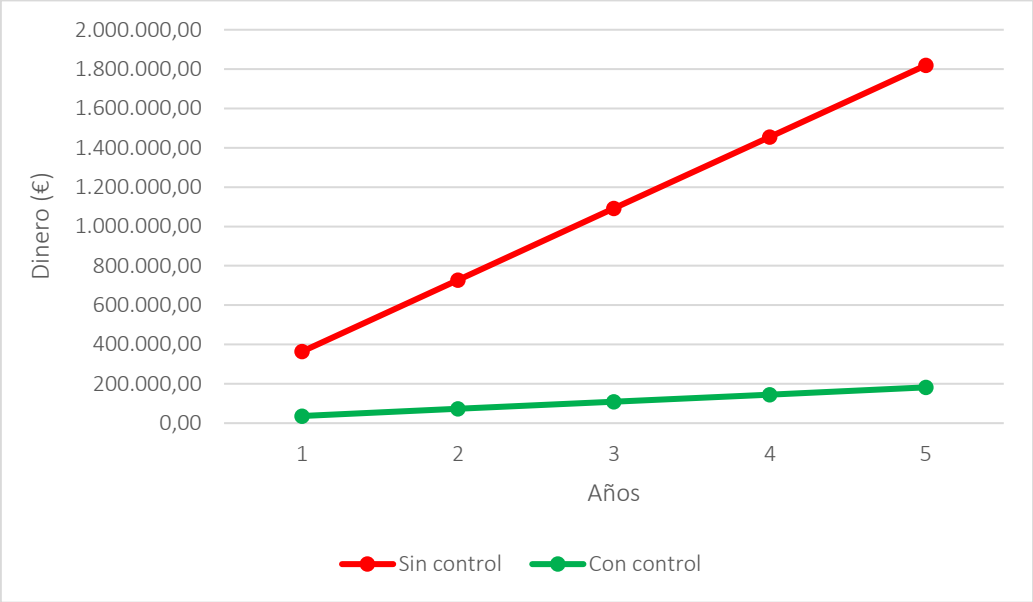



*Ilustración 194. Rentabilidad amenaza D1 - [E.19] activo S1*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 909593,31 | 0 | 0 | 909593,31 | 1819186,6 | 2728779,93 | 3638373,24 | 4547966,55 |
| 90959,33 | 0 | 0 | 90959,33 | 181918,66 | 272877,99 | 363837,32 | 454796,65 |

*Tabla 202. Rentabilidad amenaza D1 - [A.6] activo S1*

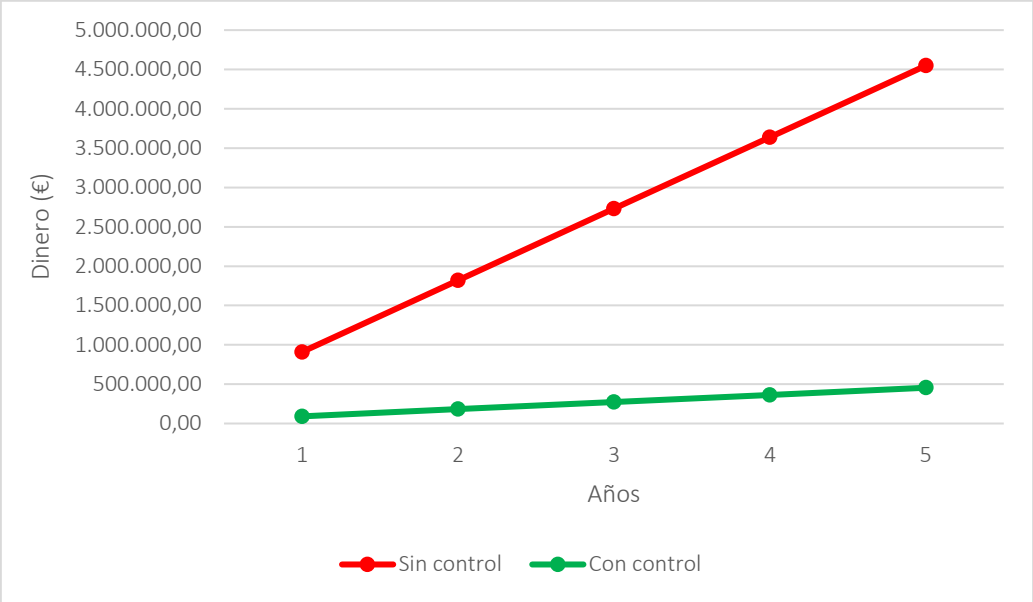



*Ilustración 195. Rentabilidad amenaza D1 - [A.6] activo S1*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

***Tabla 203. Rentabilidad amenaza HW1 - [A.6] activo S1***

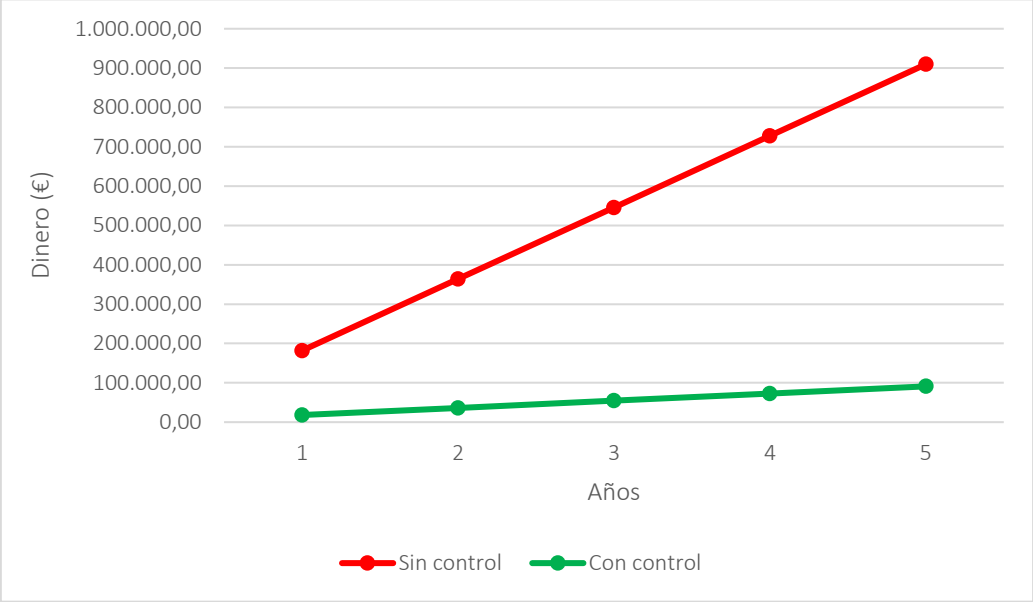



***Ilustración 196. Rentabilidad amenaza HW1 - [A.6] activo S1***

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

***Tabla 204. Rentabilidad amenaza HW1 - [A.7] activo S1***

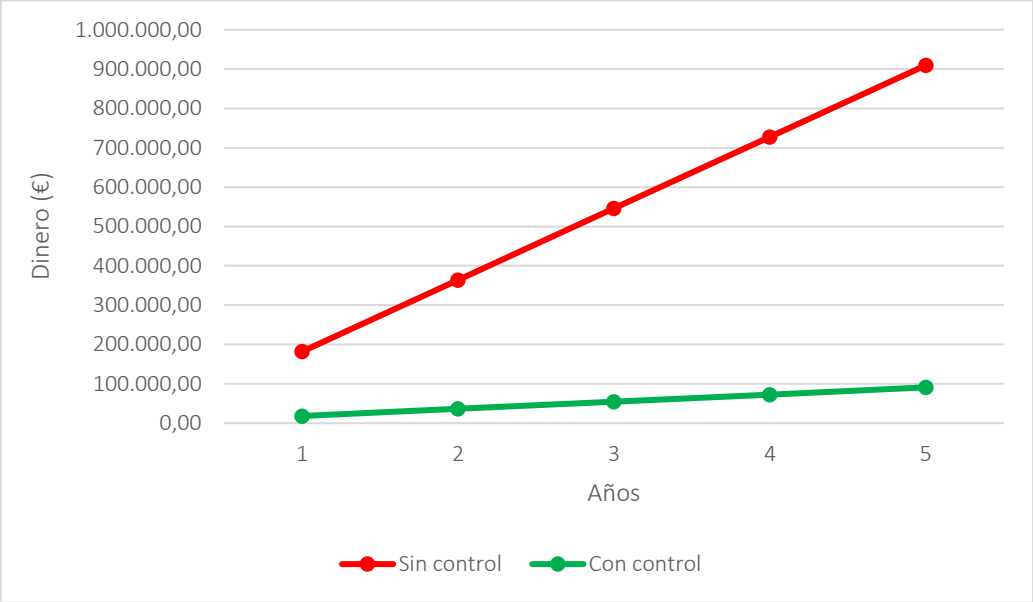



*Ilustración 197. Rentabilidad amenaza HW1 - [A.7] activo S1*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 205. Rentabilidad amenaza SW1 - [E.14] activo S1*

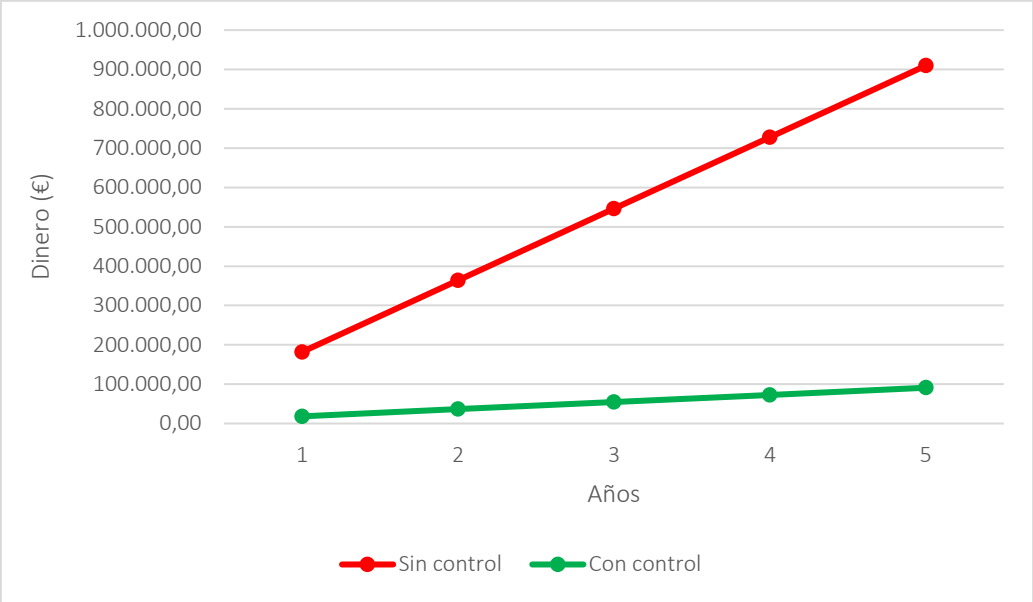



*Ilustración 198. Rentabilidad amenaza SW1 - [E.14] activo S1*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

***Tabla 206. Rentabilidad amenaza SW1 - [E.19] activo S1***

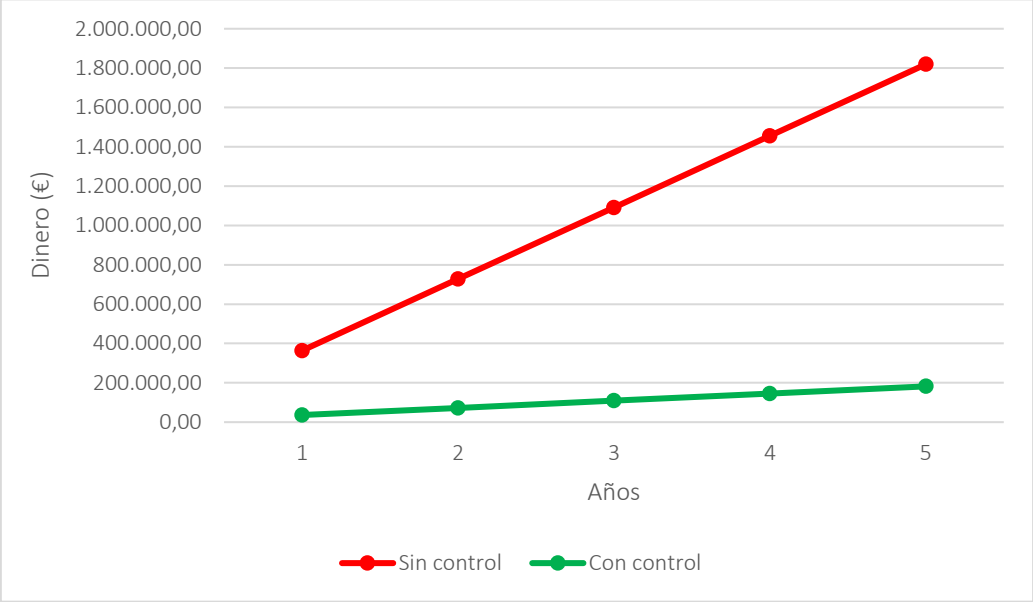



***Ilustración 199. Rentabilidad amenaza SW1 - [E.19] activo S1***

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

***Tabla 207. Rentabilidad amenaza SRVD1 - [A.6] activo S1***

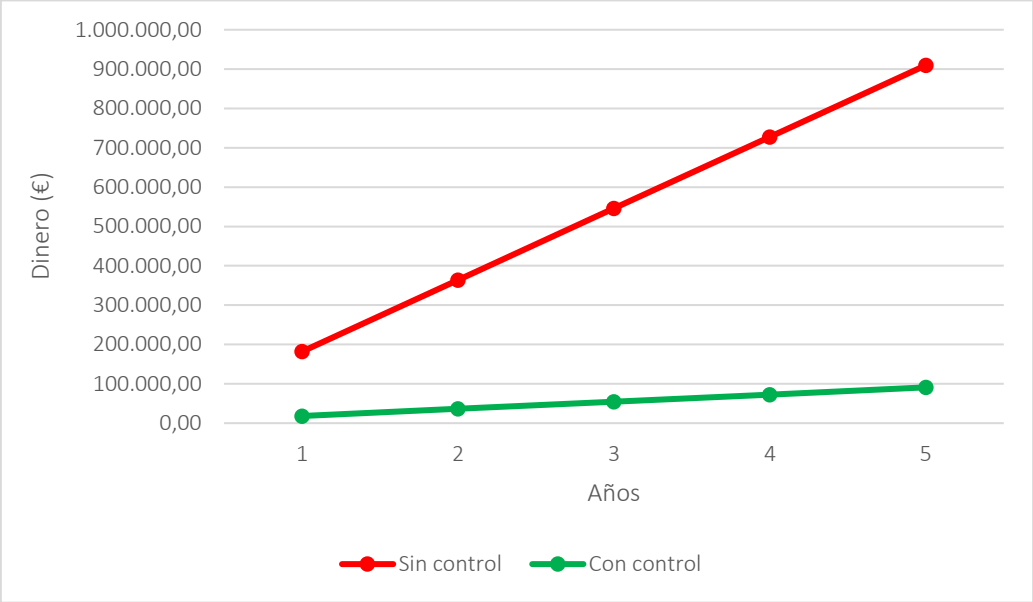



*Ilustración 200. Rentabilidad amenaza SRVD1 - [A.6] activo S1*

## Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 208. Rentabilidad amenaza SRVD1 - [A.7] activo S1*

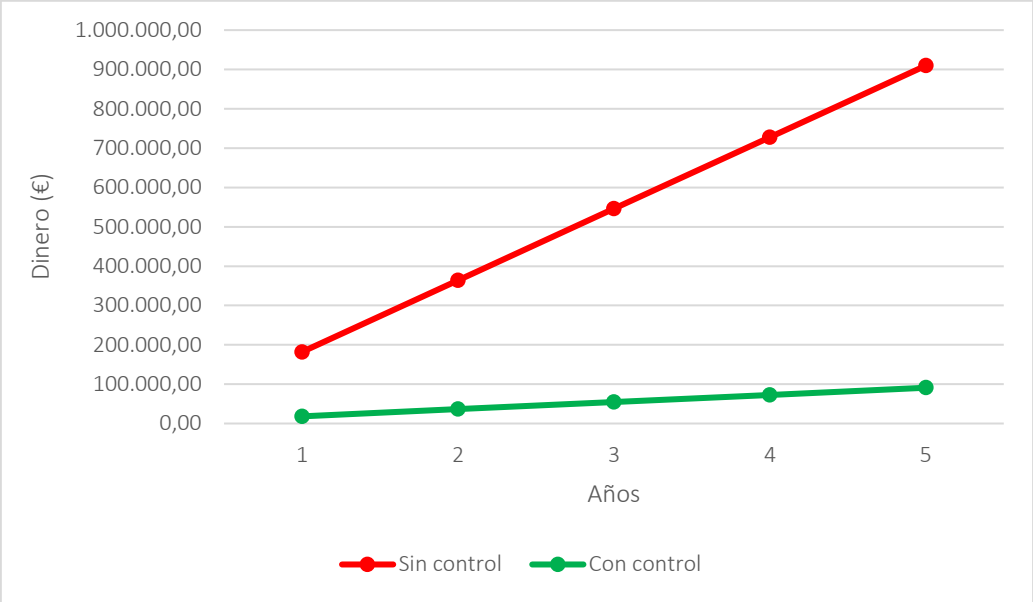



*Ilustración 201. Rentabilidad amenaza SRVD1 - [A.7] activo S1*

Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 6063,96 | 0 | 0 | 6063,96 | 12127,92 | 18191,88 | 24255,84 | 30319,8 |
| 606,4 | 0 | 0 | 606,4 | 1212,8 | 1819,2 | 2425,6 | 3032 |

*Tabla 209. Rentabilidad amenaza T1 - [A.6] activo S1*

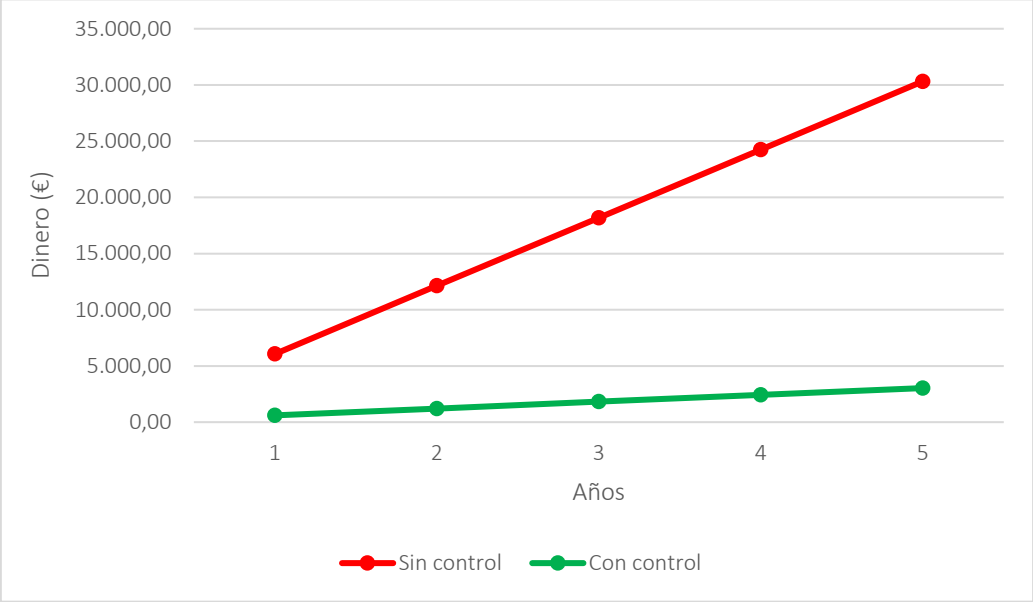



*Ilustración 202. Rentabilidad amenaza T1 - [A.6] activo S1*

Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 6063,96 | 0 | 0 | 6063,96 | 12127,92 | 18191,88 | 24255,84 | 30319,8 |
| 606,4 | 0 | 0 | 606,4 | 1212,8 | 1819,2 | 2425,6 | 3032 |

*Tabla 210. Rentabilidad amenaza T1 - [A.7] activo S1*

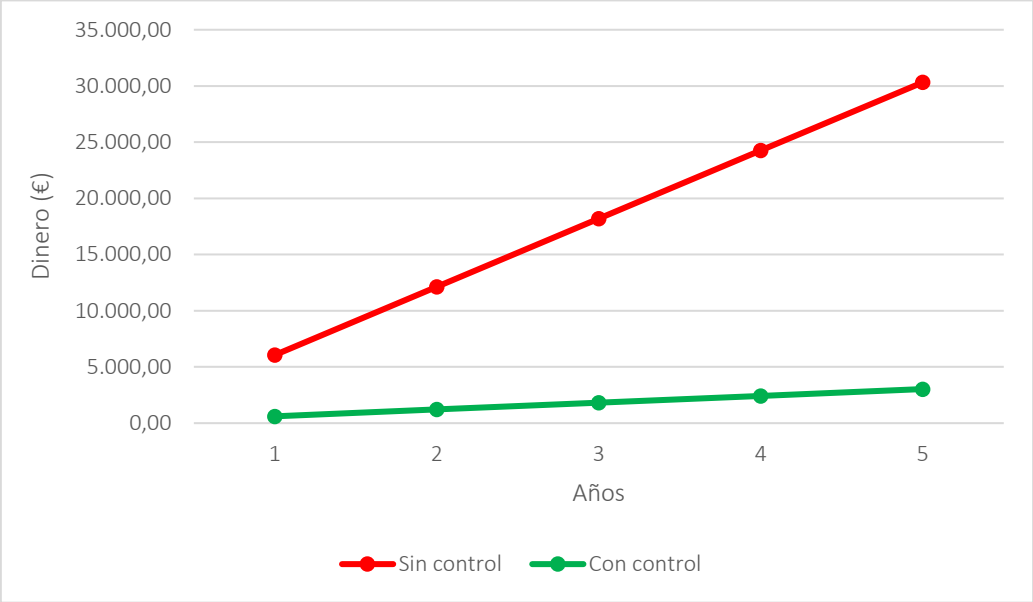



*Ilustración 203. Rentabilidad amenaza T1 - [A.7] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 211. Rentabilidad amenaza D1 - [E.19] activo S2*

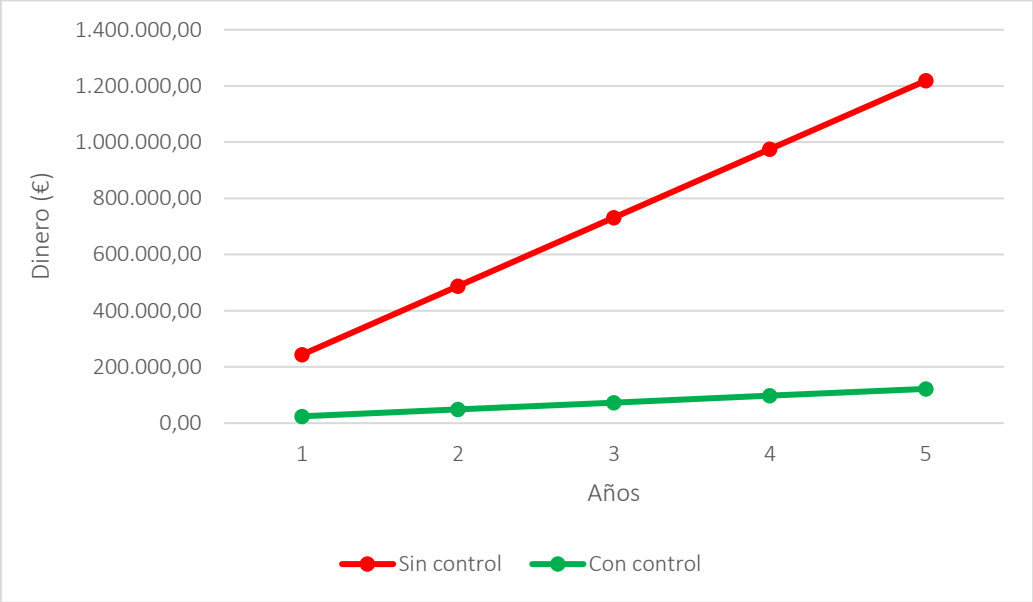



*Ilustración 204. Rentabilidad amenaza D1 - [E.19] activo S2*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 212. Rentabilidad amenaza D1 - [A.6] activo S2*

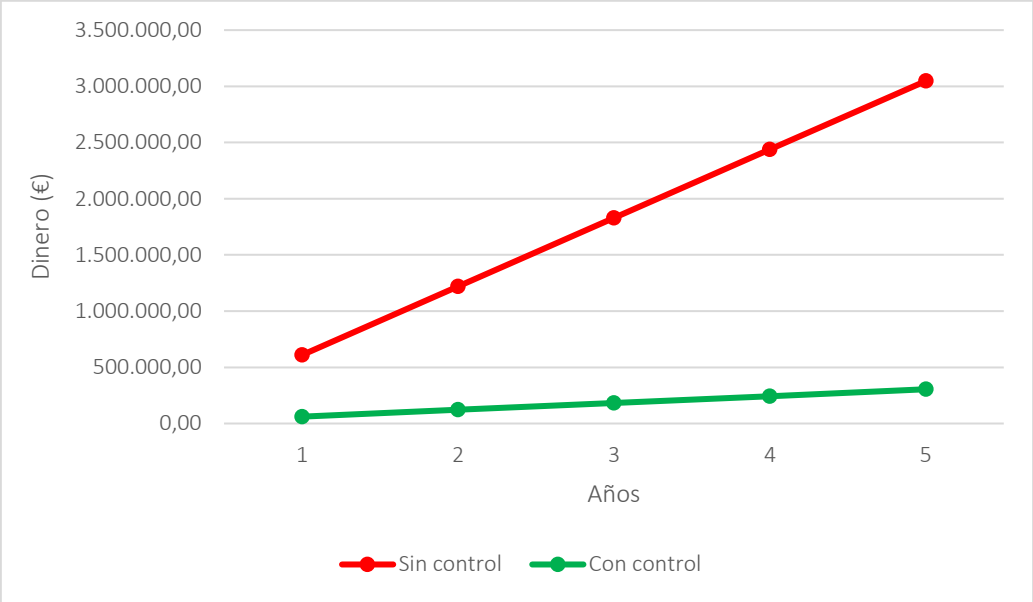



*Ilustración 205. Rentabilidad amenaza D1 - [A.6] activo S2*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 213. Rentabilidad amenaza HW1 - [A.6] activo S2***

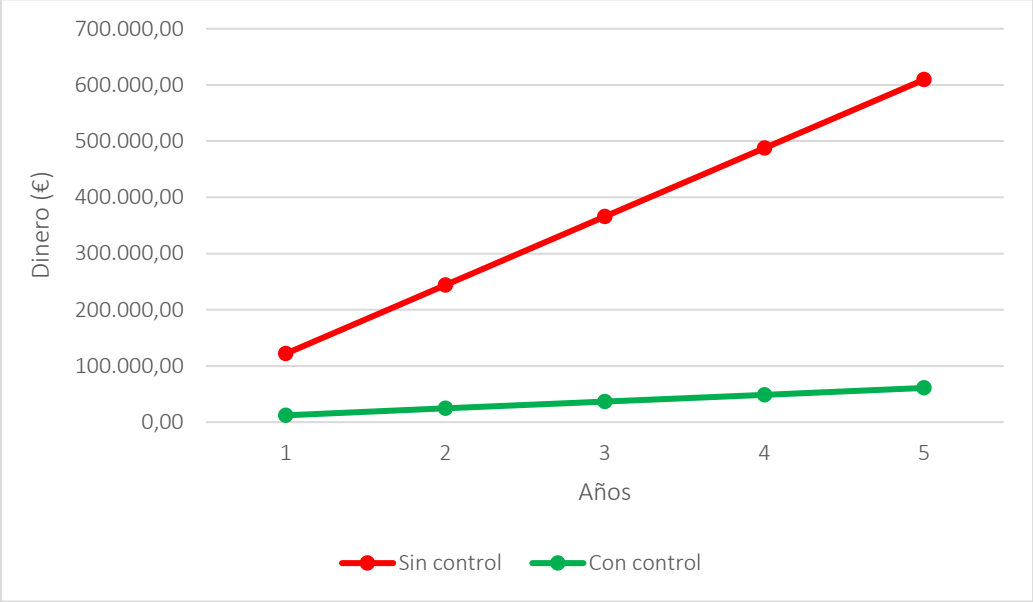



***Ilustración 206. Rentabilidad amenaza HW1 - [A.6] activo S2***

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 214. Rentabilidad amenaza HW1 - [A.7] activo S2***

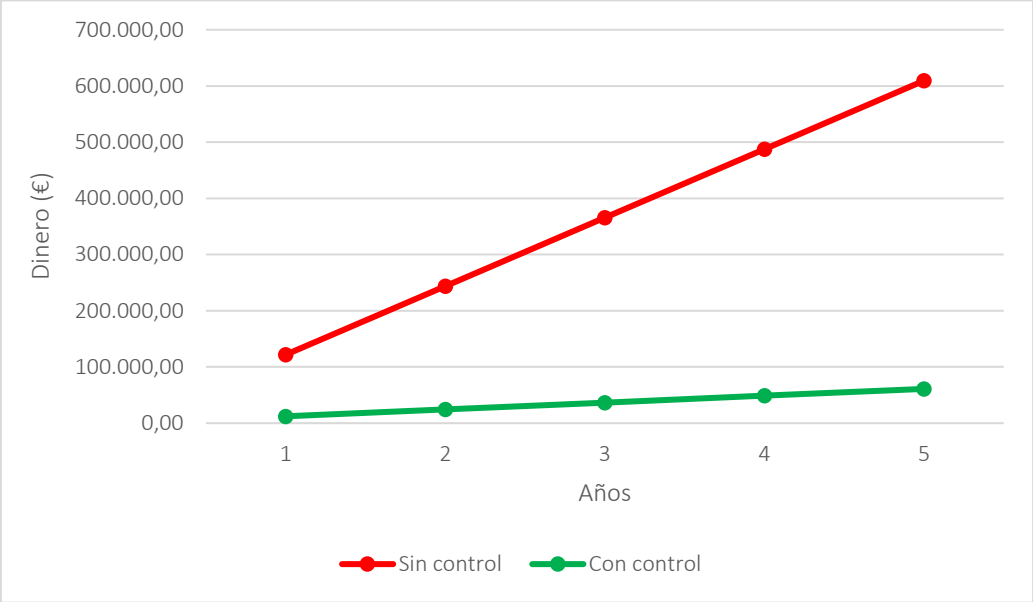



*Ilustración 207. Rentabilidad amenaza HW1 - [A.7] activo S2*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 215. Rentabilidad amenaza SW1 - [E.14] activo S2*

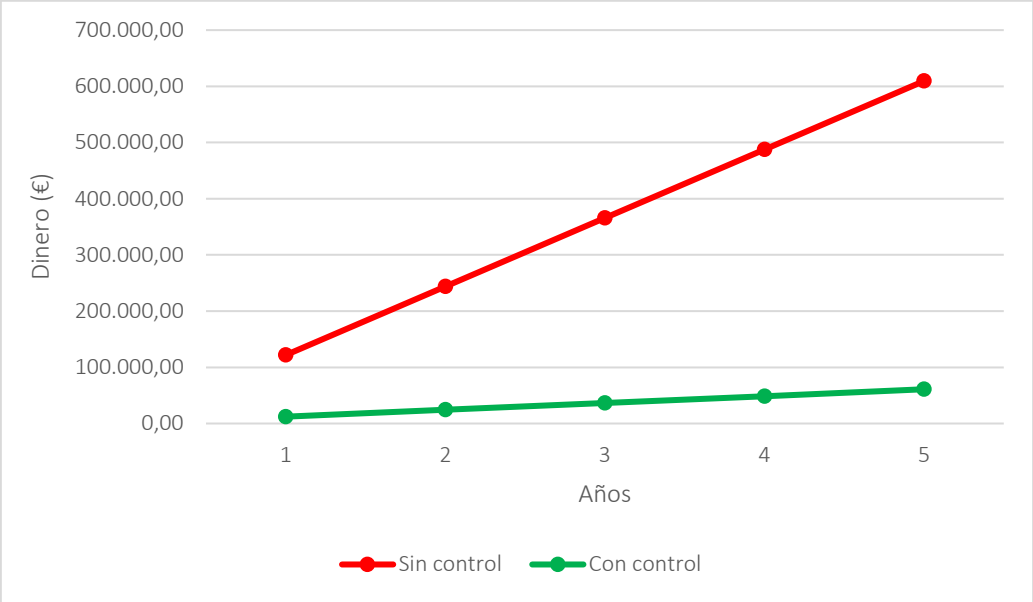



*Ilustración 208. Rentabilidad amenaza SW1 - [E.14] activo S2*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 216. Rentabilidad amenaza SW1 - [E.19] activo S2***

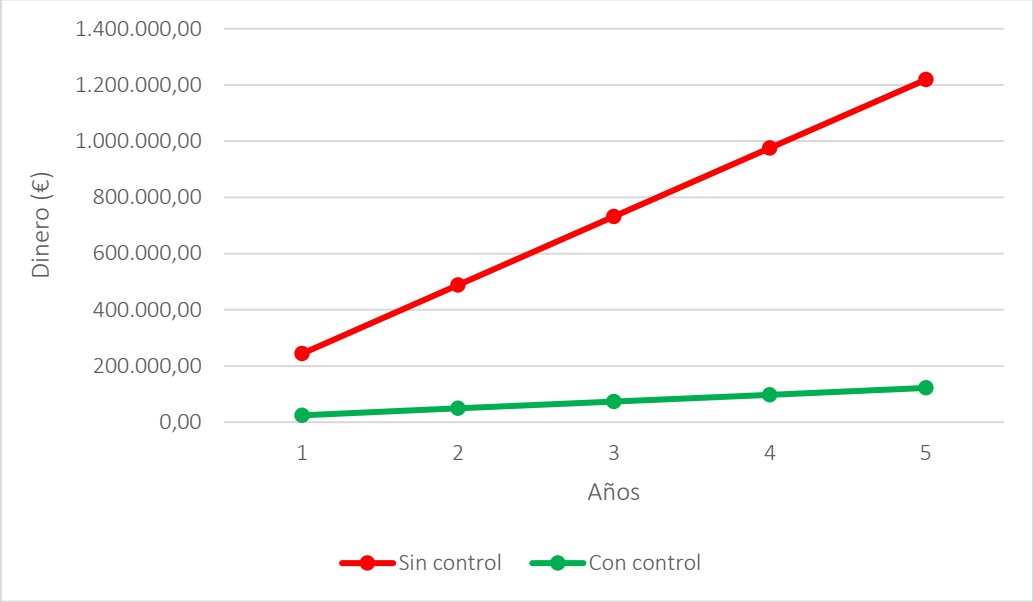



***Ilustración 209. Rentabilidad amenaza SW1 - [E.19] activo S2***

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 217. Rentabilidad amenaza SRVD1 - [A.6] activo S2***

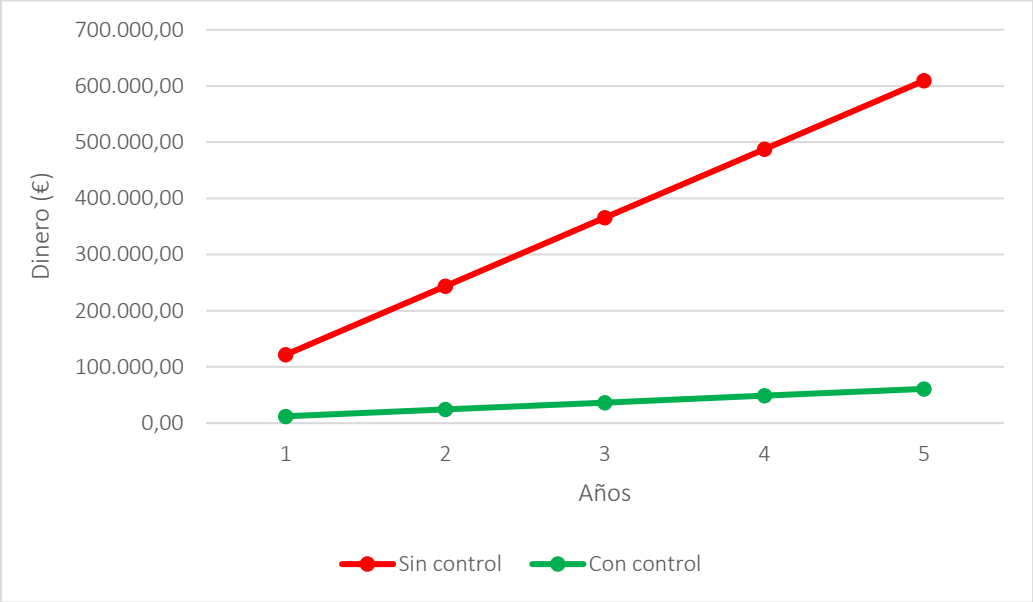



*Ilustración 210. Rentabilidad amenaza SRVD1 - [A.6] activo S2*

## Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 218. Rentabilidad amenaza SRVD1 - [A.7] activo S2*

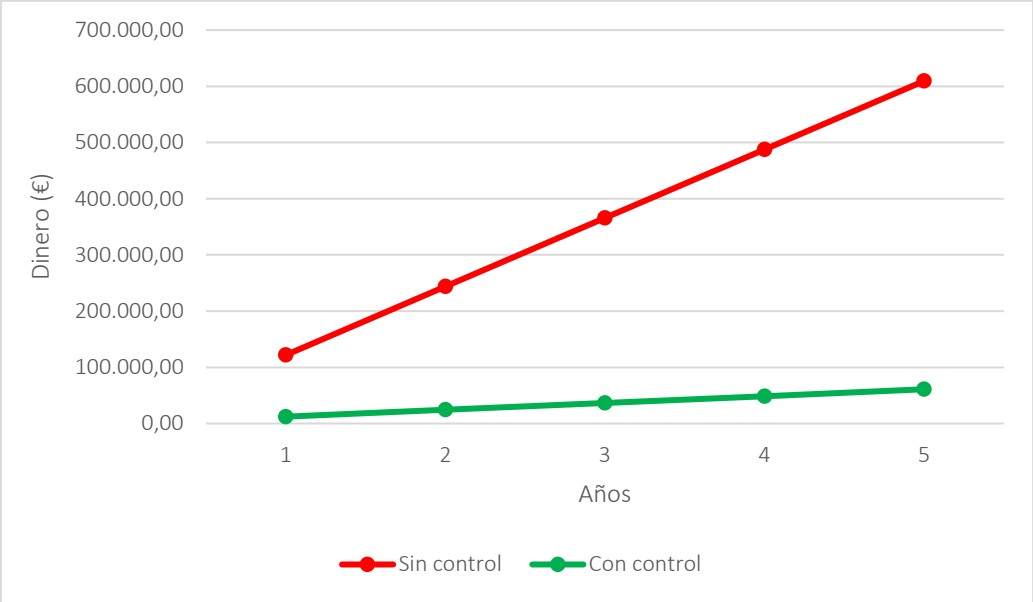



*Ilustración 211. Rentabilidad amenaza SRVD1 - [A.7] activo S2*

Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 219. Rentabilidad amenaza T1 - [A.6] activo S2*

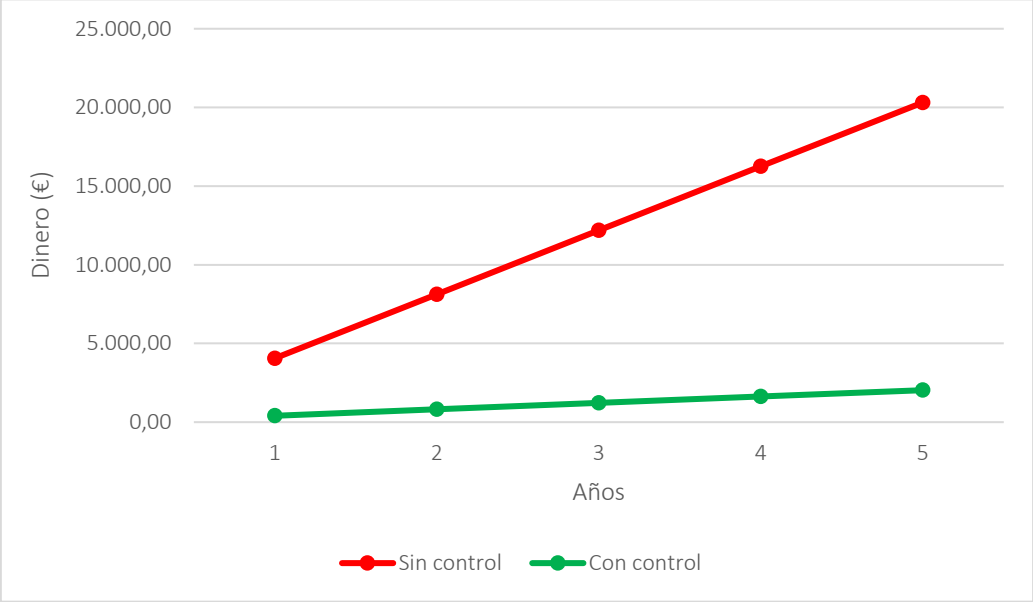



*Ilustración 212. Rentabilidad amenaza T1 - [A.6] activo S2*

Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 220. Rentabilidad amenaza T1 - [A.7] activo S2*

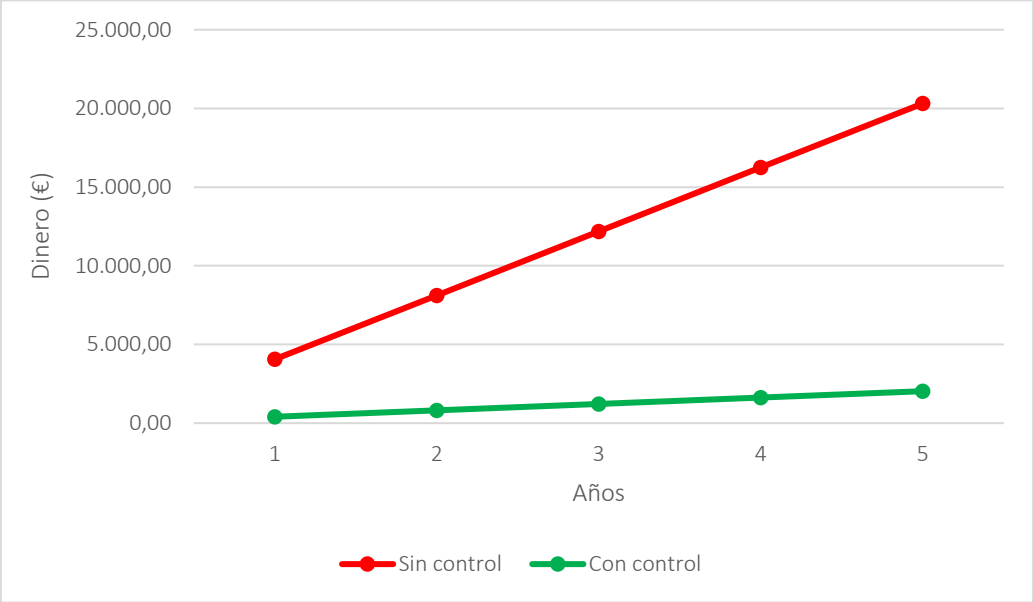



*Ilustración 213. Rentabilidad amenaza T1 - [A.7] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 221. Rentabilidad amenaza D1 - [E.19] activo S3*

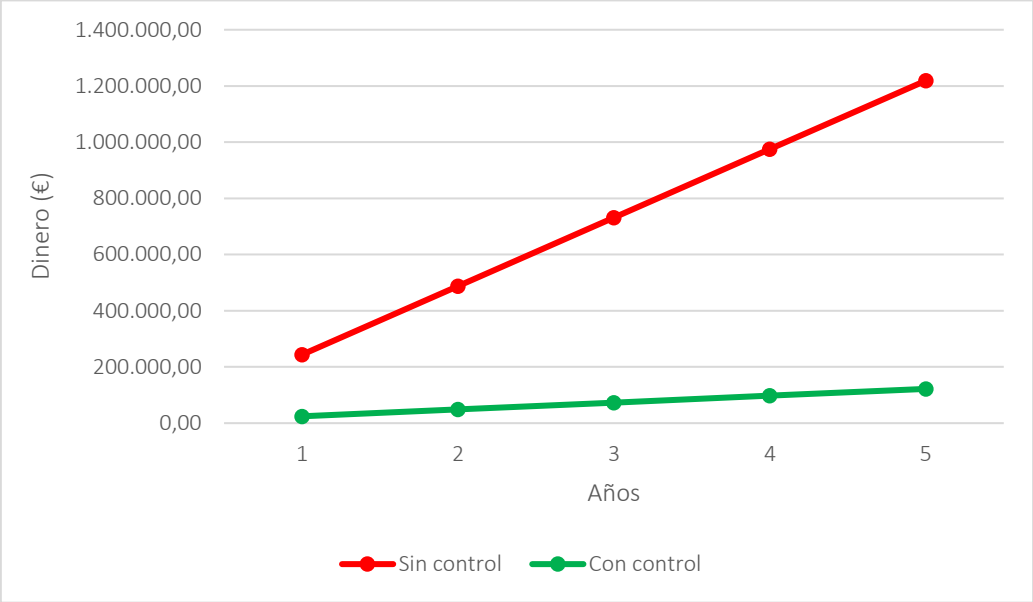



*Ilustración 214. Rentabilidad amenaza D1 - [E.19] activo S3*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 222. Rentabilidad amenaza D1 - [A.6] activo S3*

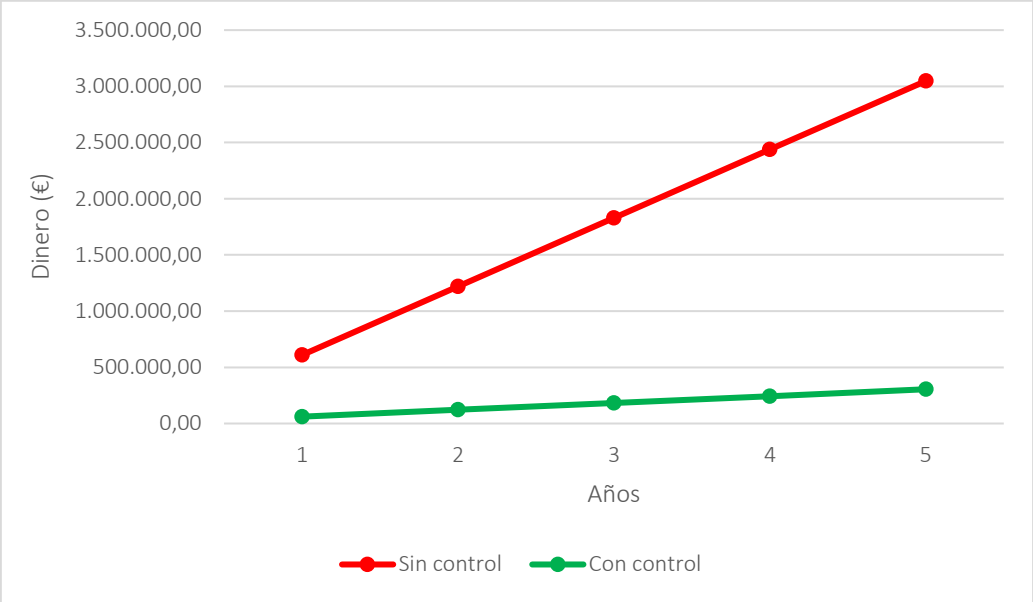



*Ilustración 215. Rentabilidad amenaza D1 - [A.6] activo S3*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 223. Rentabilidad amenaza HW1 - [A.6] activo S3***

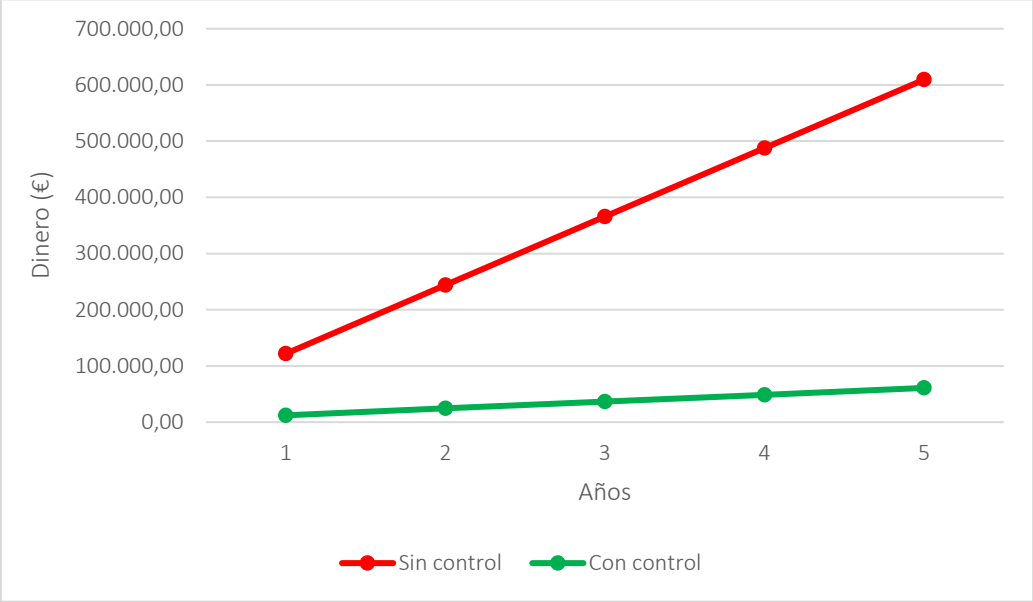



***Ilustración 216. Rentabilidad amenaza HW1 - [A.6] activo S3***

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 224. Rentabilidad amenaza HW1 - [A.7] activo S3***

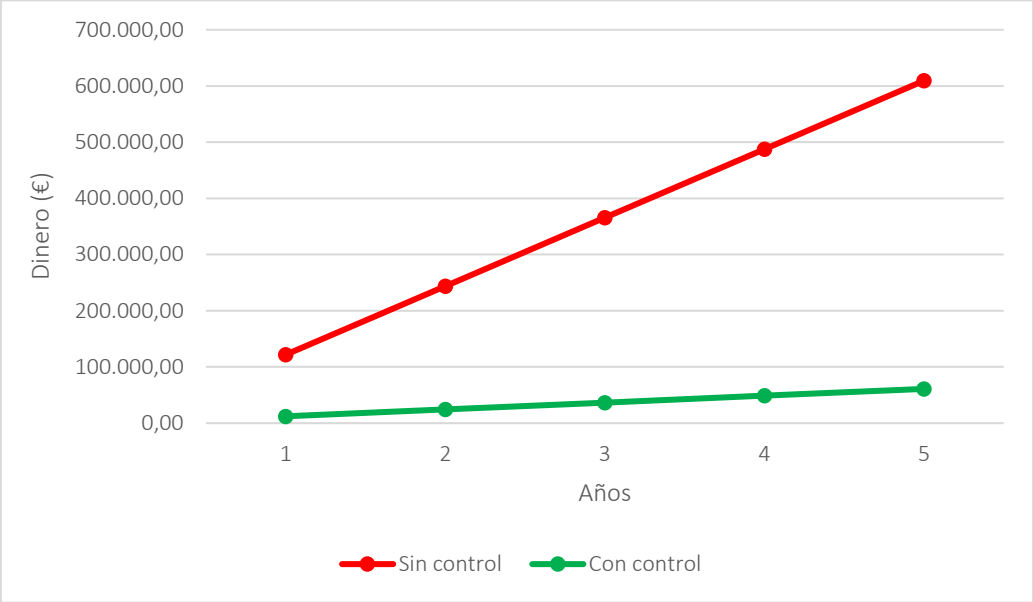



*Ilustración 217. Rentabilidad amenaza HW1 - [A.7] activo S3*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 225. Rentabilidad amenaza SW1 - [E.14] activo S3*

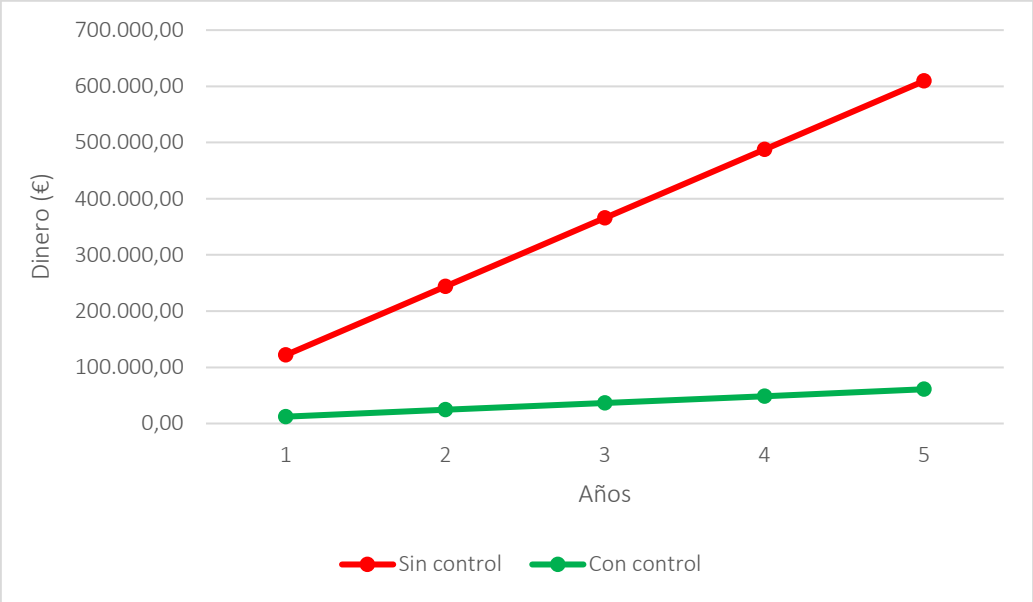



*Ilustración 218. Rentabilidad amenaza SW1 - [E.14] activo S3*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 226. Rentabilidad amenaza SW1 - [E.19] activo S3***

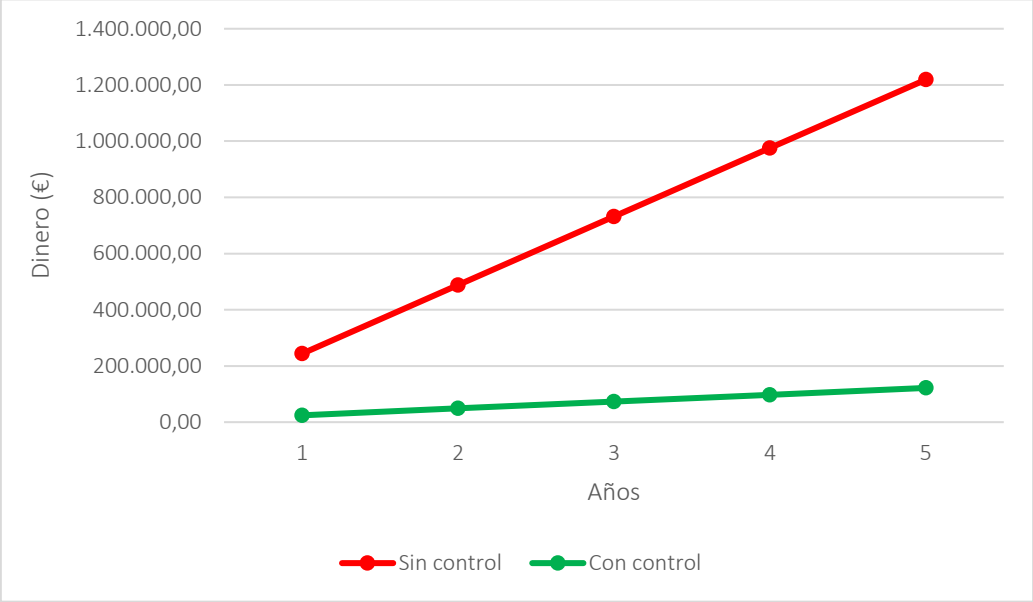



***Ilustración 219. Rentabilidad amenaza SW1 - [E.19] activo S3***

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 227. Rentabilidad amenaza SRVD1 - [A.6] activo S3***

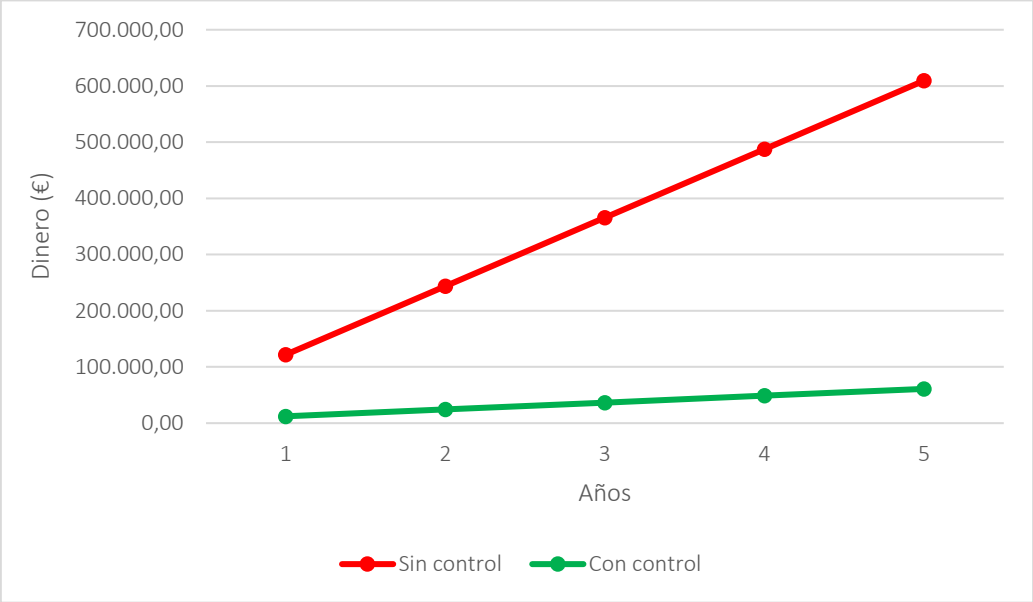



*Ilustración 220. Rentabilidad amenaza SRVD1 - [A.6] activo S3*

## Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 228. Rentabilidad amenaza SRVD1 - [A.7] activo S3*

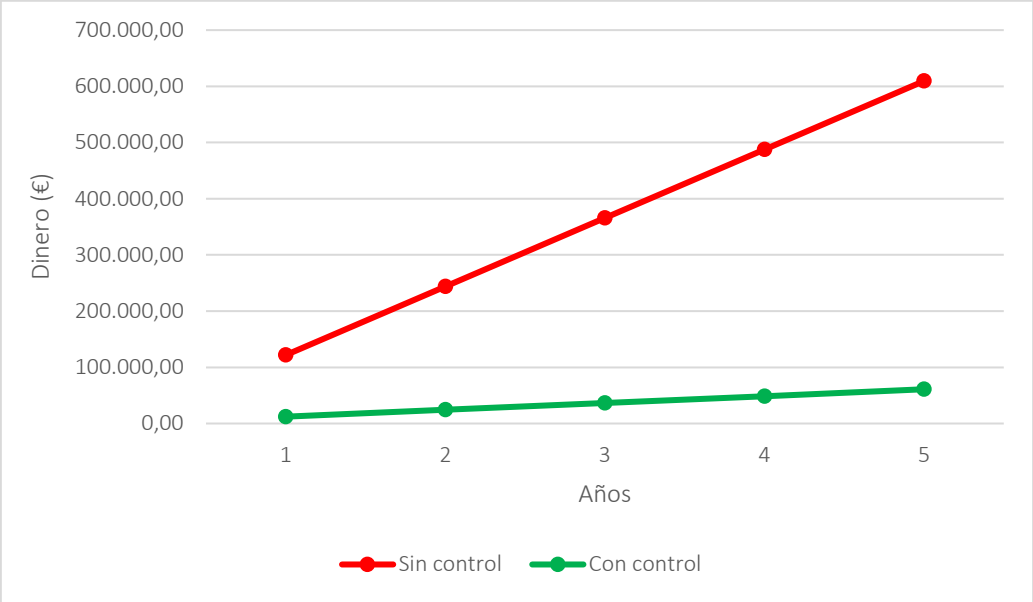



*Ilustración 221. Rentabilidad amenaza SRVD1 - [A.7] activo S3*

Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 229. Rentabilidad amenaza T1 - [A.6] activo S3*

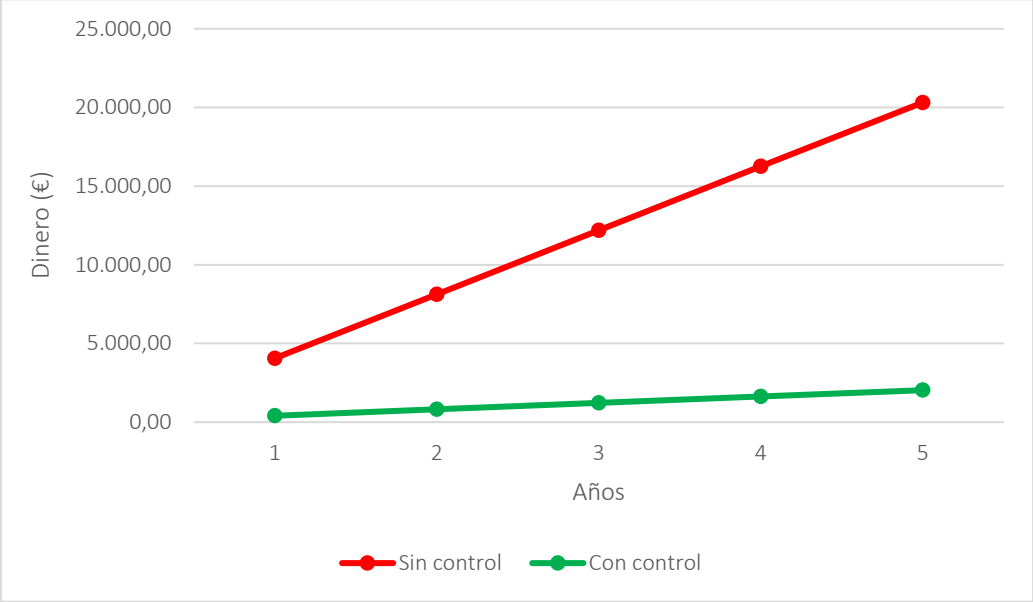



*Ilustración 222. Rentabilidad amenaza T1 - [A.6] activo S3*

Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 230. Rentabilidad amenaza T1 - [A.7] activo S3*

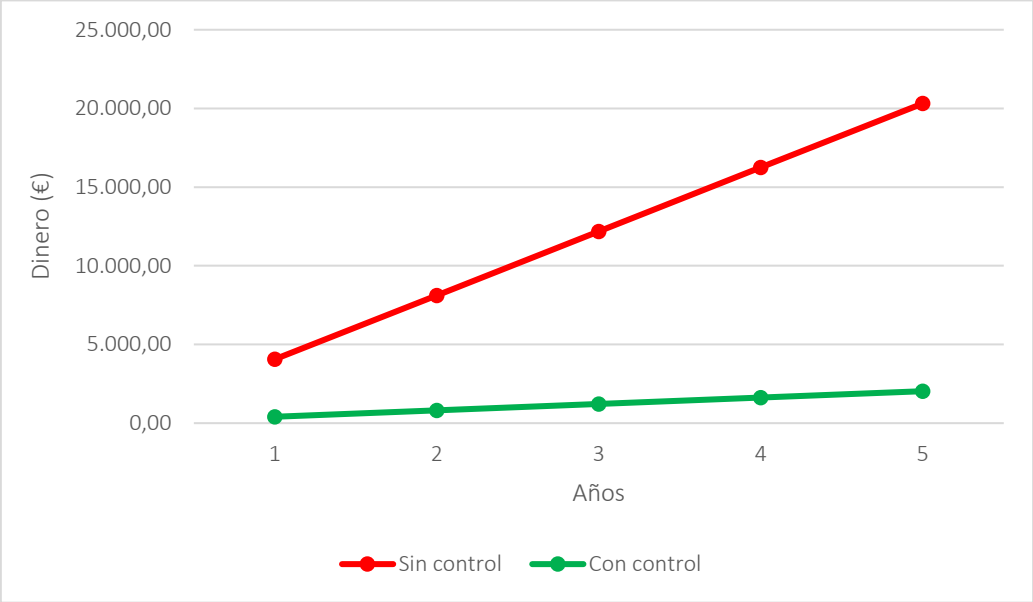



*Ilustración 223. Rentabilidad amenaza T1 - [A.7] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

*Tabla 231. Rentabilidad amenaza D1 - [E.19] activo S4*

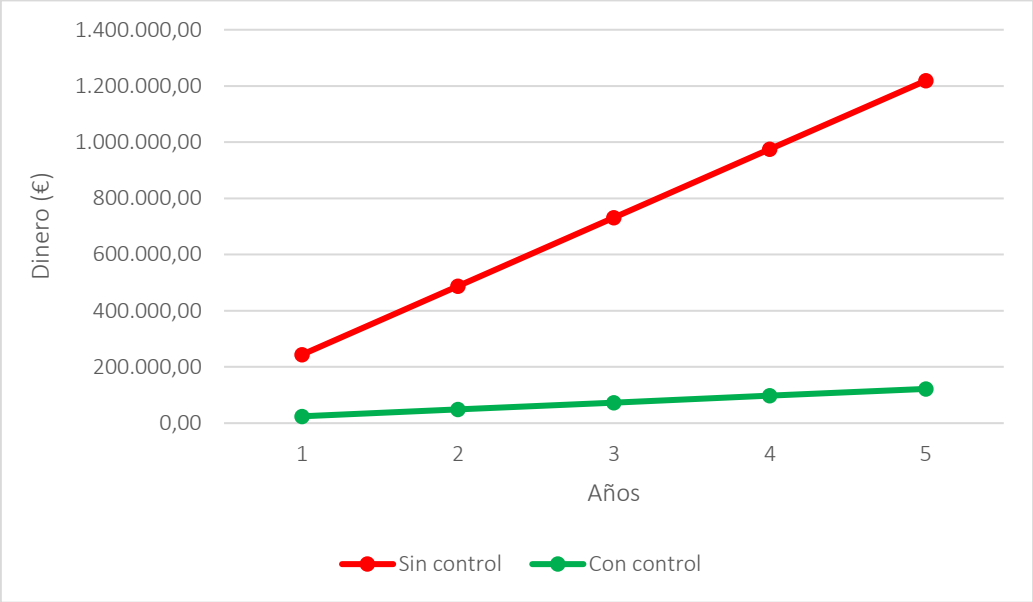



*Ilustración 224. Rentabilidad amenaza D1 - [E.19] activo S4*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609375,71 | 0 | 0 | 609375,71 | 1218751,4 | 1828127,13 | 2437502,84 | 3046878,55 |
| 60937,57 | 0 | 0 | 60937,57 | 121875,14 | 182812,71 | 243750,28 | 304687,85 |

*Tabla 232. Rentabilidad amenaza D1 - [A.6] activo S4*

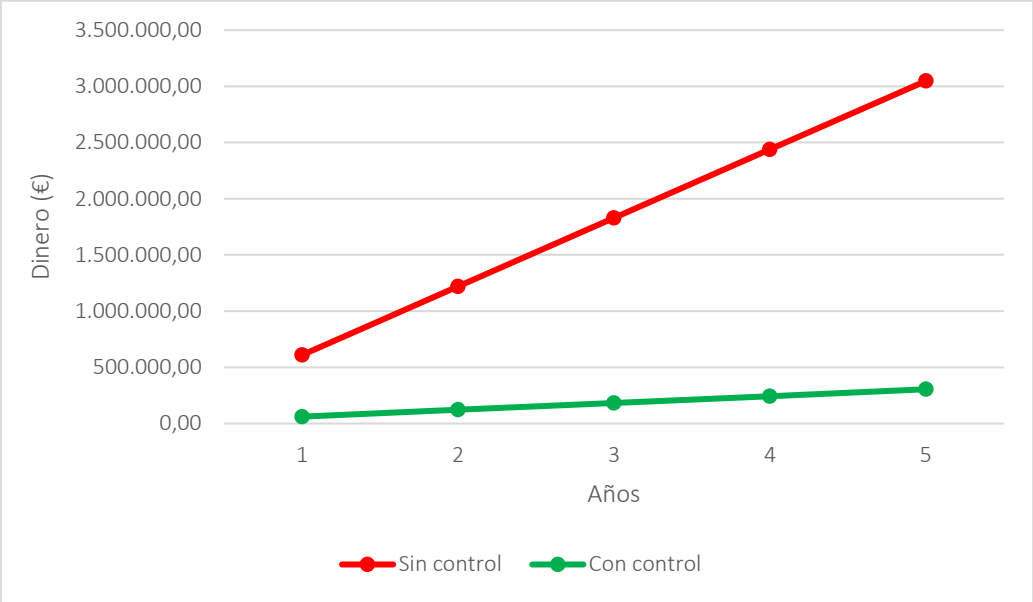



*Ilustración 225. Rentabilidad amenaza D1 - [A.6] activo S4*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

***Tabla 233. Rentabilidad amenaza HW1 - [A.6] activo S4***

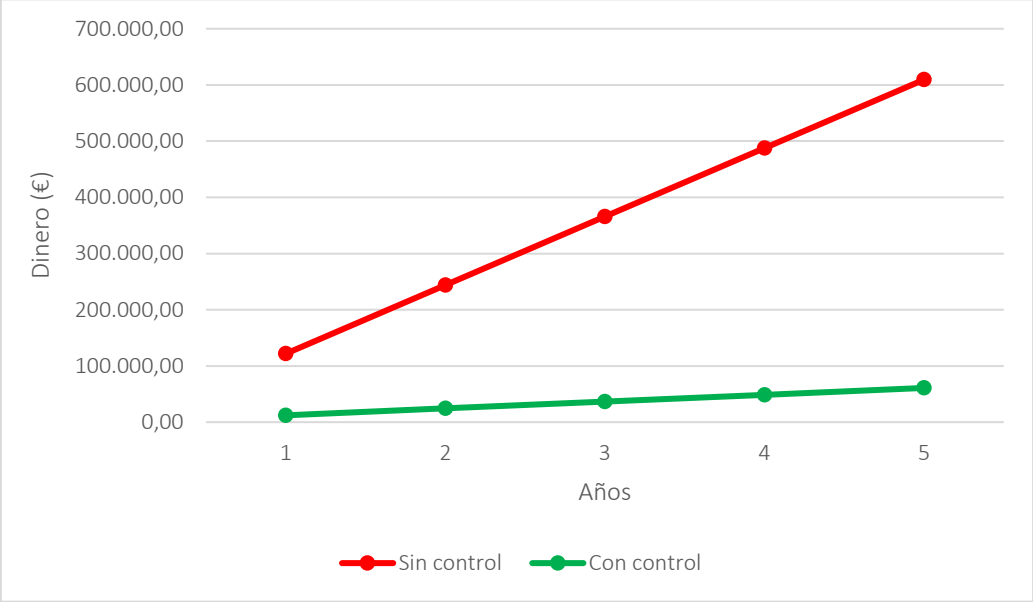



***Ilustración 226. Rentabilidad amenaza HW1 - [A.6] activo S4***

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

***Tabla 234. Rentabilidad amenaza HW1 - [A.7] activo S4***

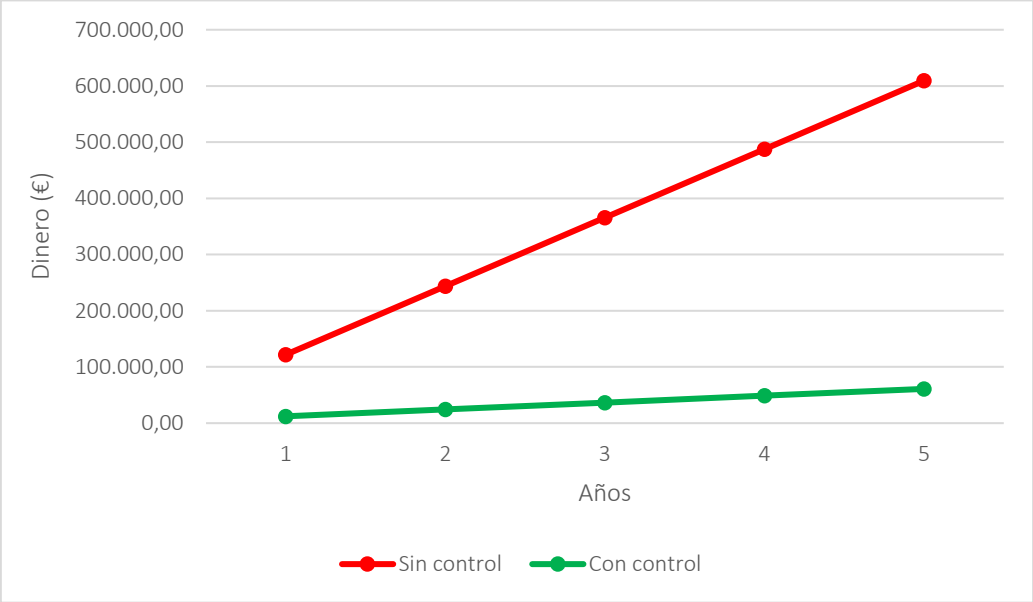



*Ilustración 227. Rentabilidad amenaza HW1 - [A.7] activo S4*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 235. Rentabilidad amenaza SW1 - [E.14] activo S4*

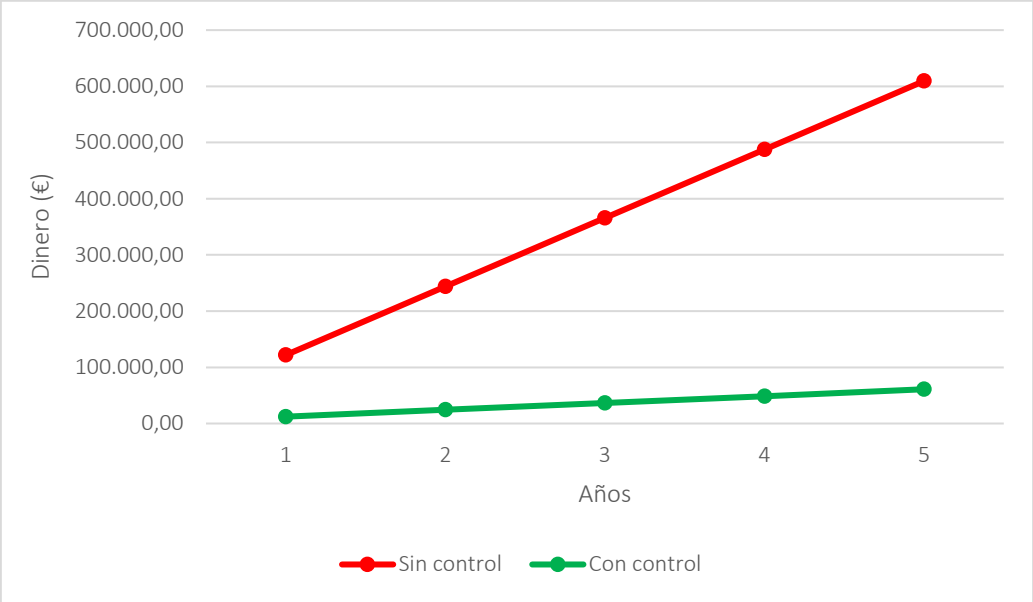



*Ilustración 228. Rentabilidad amenaza SW1 - [E.19] activo S4*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

***Tabla 236. Rentabilidad amenaza SW1 - [E.19] activo S4***

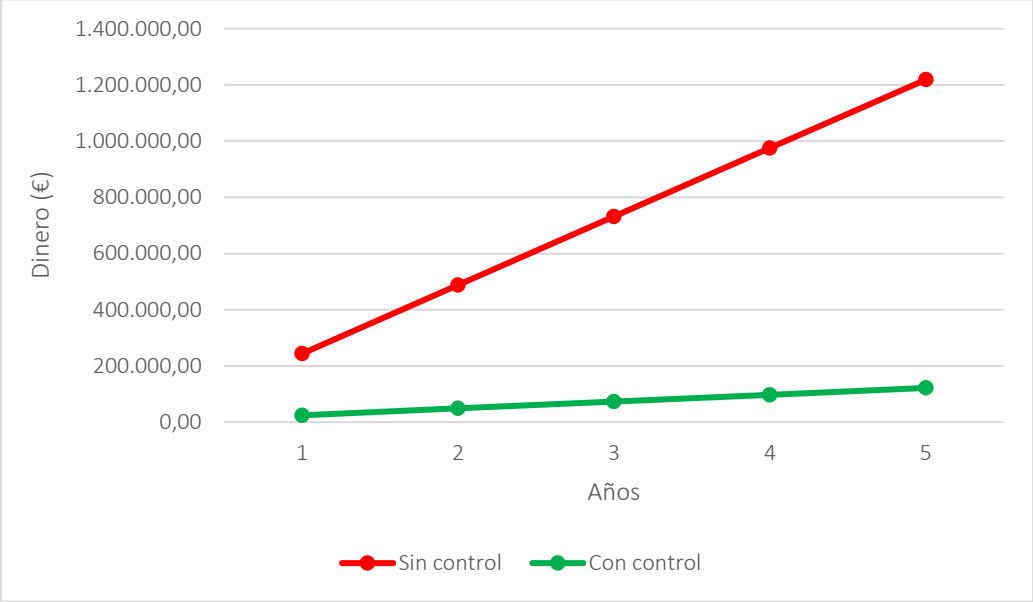



***Ilustración 229. Rentabilidad amenaza SW1 - [E.19] activo S4***

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

***Tabla 237. Rentabilidad amenaza SRVD1 - [A.6] activo S4***

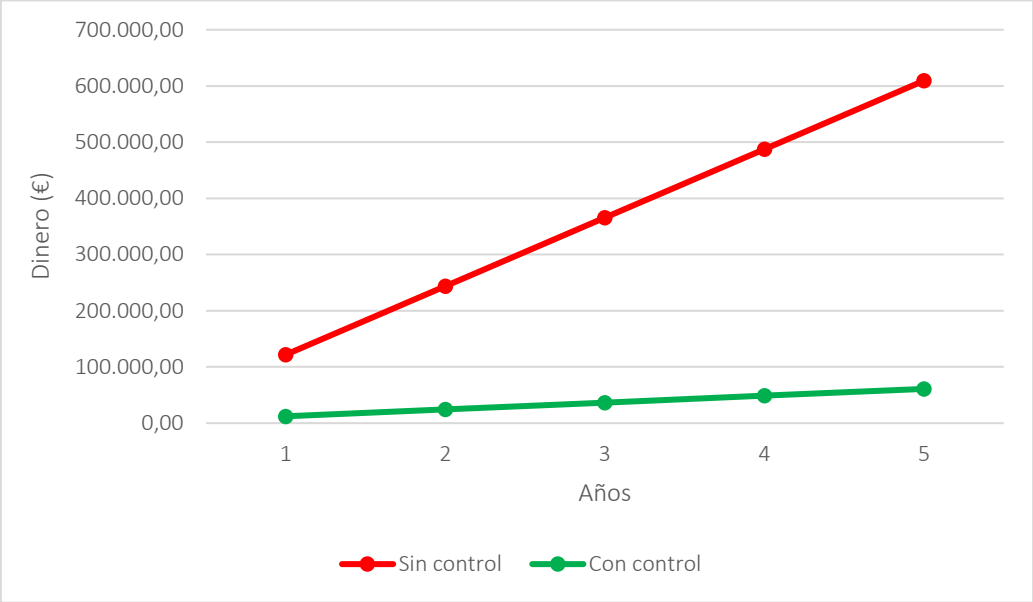



*Ilustración 230. Rentabilidad amenaza SRVD1 - [A.6] activo S4*

Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 238. Rentabilidad amenaza SRVD1 - [A.7] activo S4*

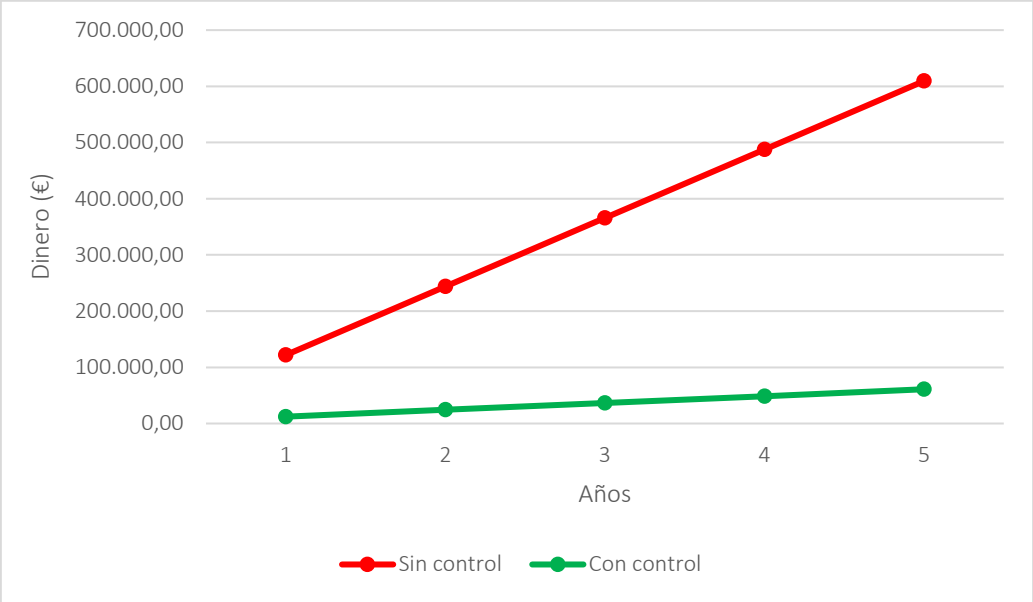



*Ilustración 231. Rentabilidad amenaza SRVD1 - [A.7] activo S4*

Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,5 | 0 | 0 | 4062,5 | 8125 | 12187,5 | 16250 | 20312,5 |
| 406,25 | 0 | 0 | 406,25 | 812,5 | 1218,75 | 1625 | 2031,25 |

*Tabla 239. Rentabilidad amenaza T1 - [A.6] activo S4*

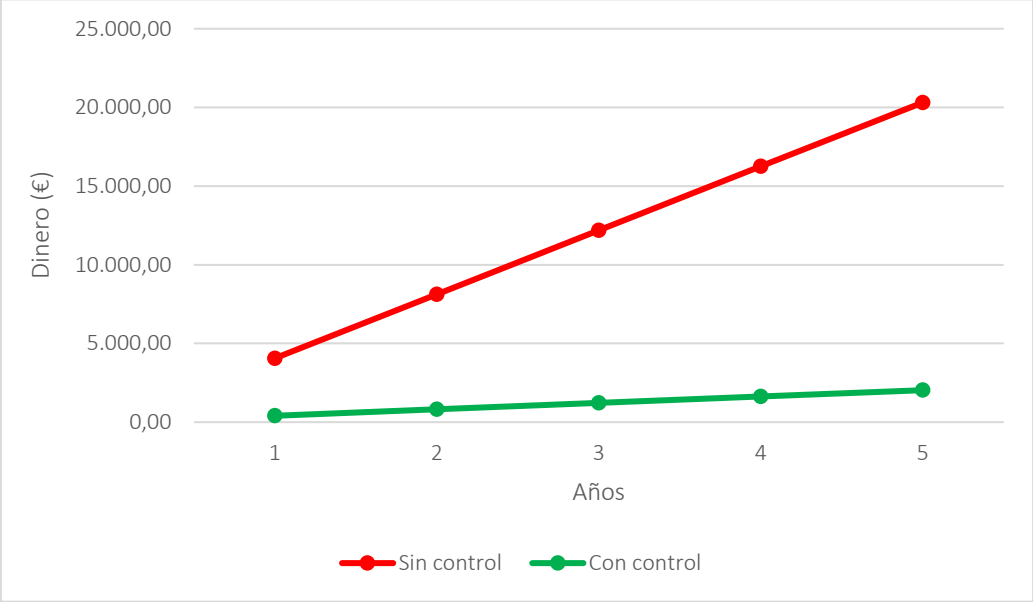



*Ilustración 232. Rentabilidad amenaza T1 - [A.6] activo S4*

Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,5 | 0 | 0 | 4062,5 | 8125 | 12187,5 | 16250 | 20312,5 |
| 406,25 | 0 | 0 | 406,25 | 812,5 | 1218,75 | 1625 | 2031,25 |

*Tabla 240. Rentabilidad amenaza T1 - [A.7] activo S4*

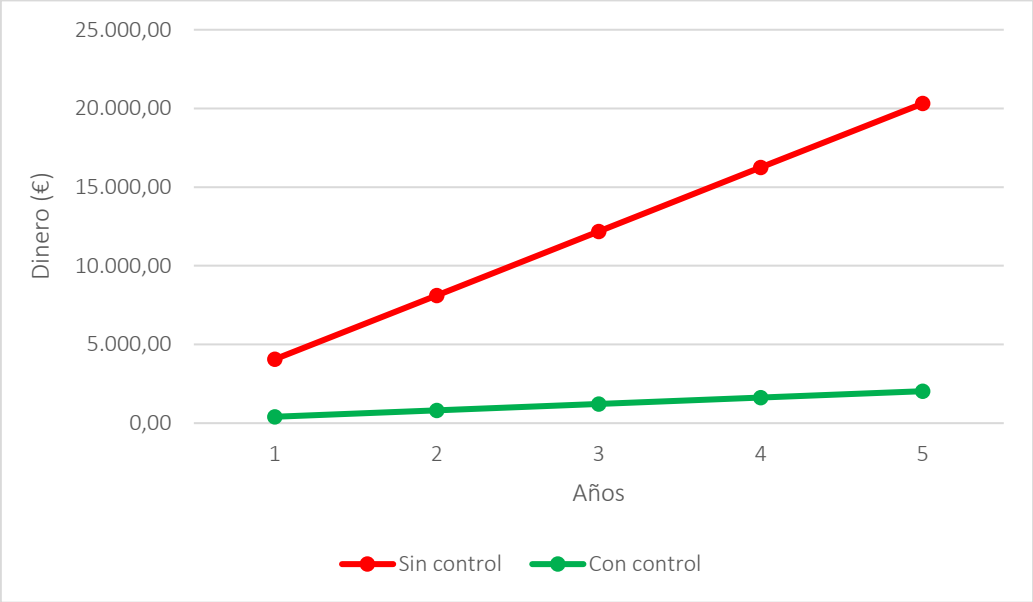



*Ilustración 233. Rentabilidad amenaza T1 - [A.7] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 241. Rentabilidad amenaza D1 - [E.19] activo S5*

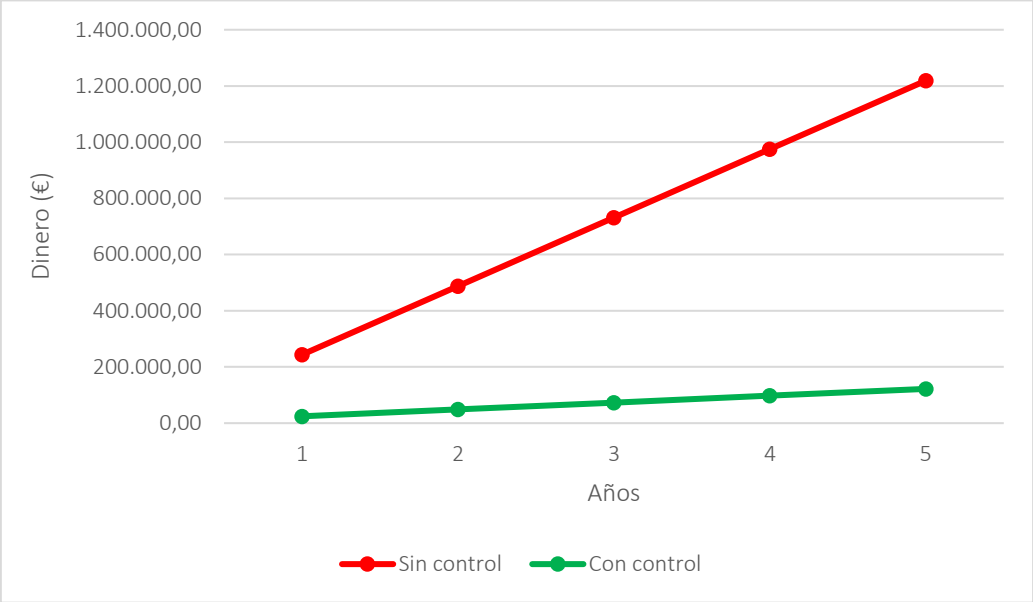



*Ilustración 234. Rentabilidad amenaza D1 - [E.19] activo S5*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 242. Rentabilidad amenaza D1 - [A.6] activo S5*

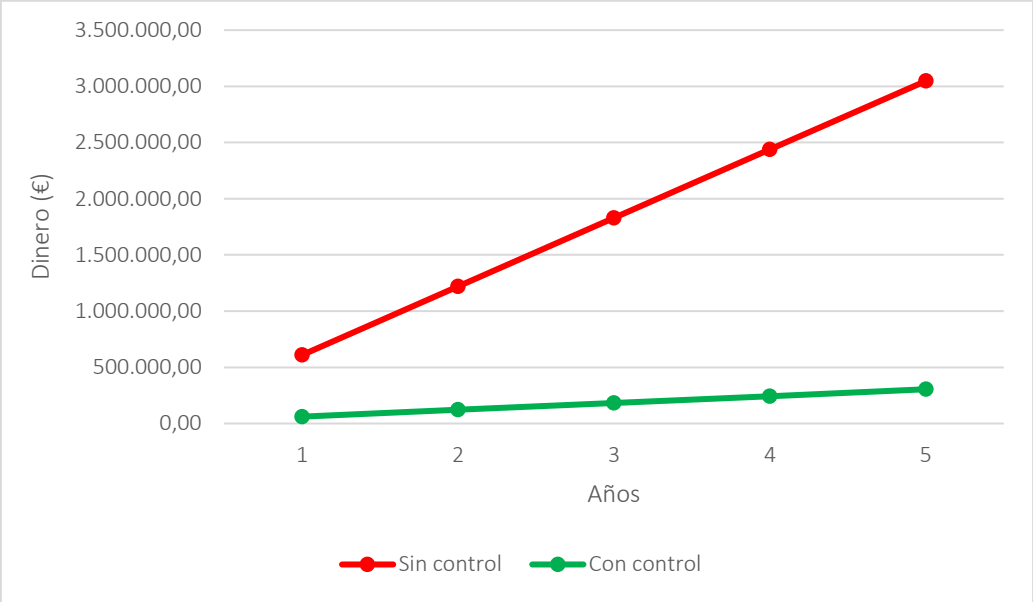



*Ilustración 235. Rentabilidad amenaza D1 - [A.6] activo S5*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 243. Rentabilidad amenaza HW1 - [A.6] activo S5*

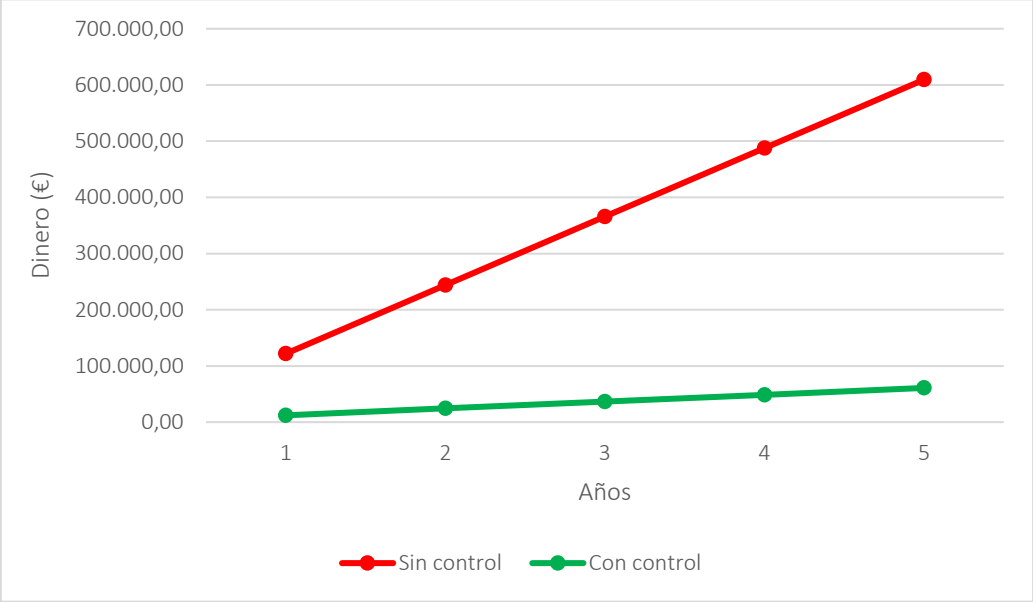



*Ilustración 236. Rentabilidad amenaza HW1 - [A.6] activo S5*

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 244. Rentabilidad amenaza HW1 - [A.7] activo S5*

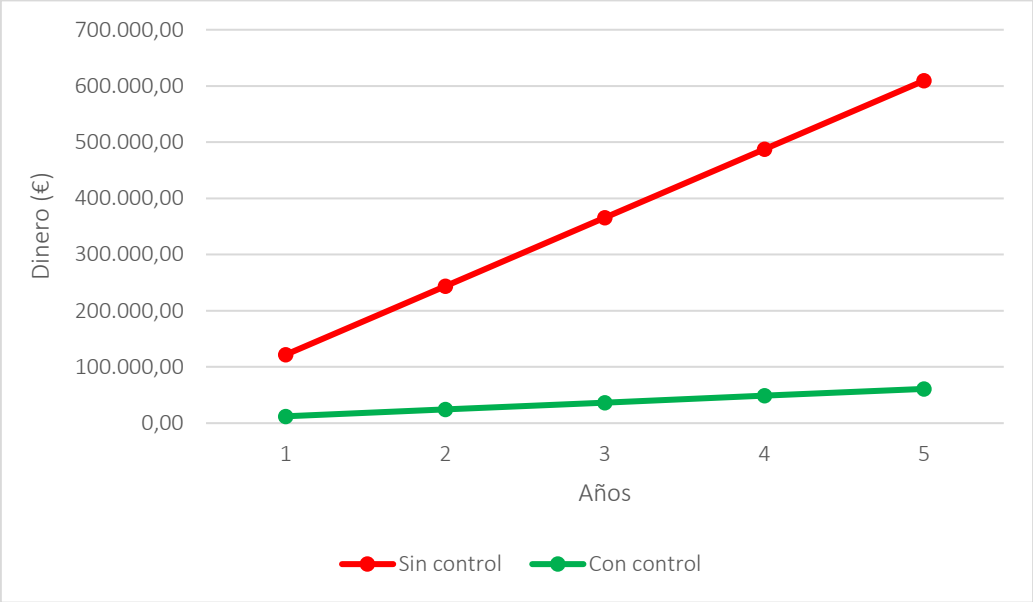



*Ilustración 237. Rentabilidad amenaza HW1 - [A.7] activo S5*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 245. Rentabilidad amenaza SW1 - [E.14] activo S5*

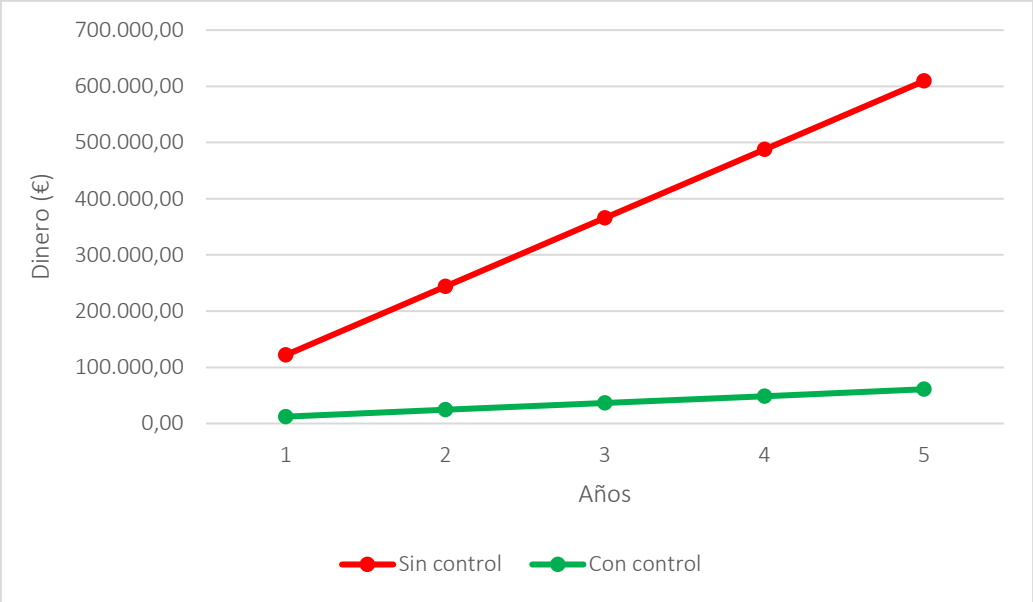



*Ilustración 238. Rentabilidad amenaza SW1 - [E.14] activo S5*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 246. Rentabilidad amenaza SW1 - [E.19] activo S5***

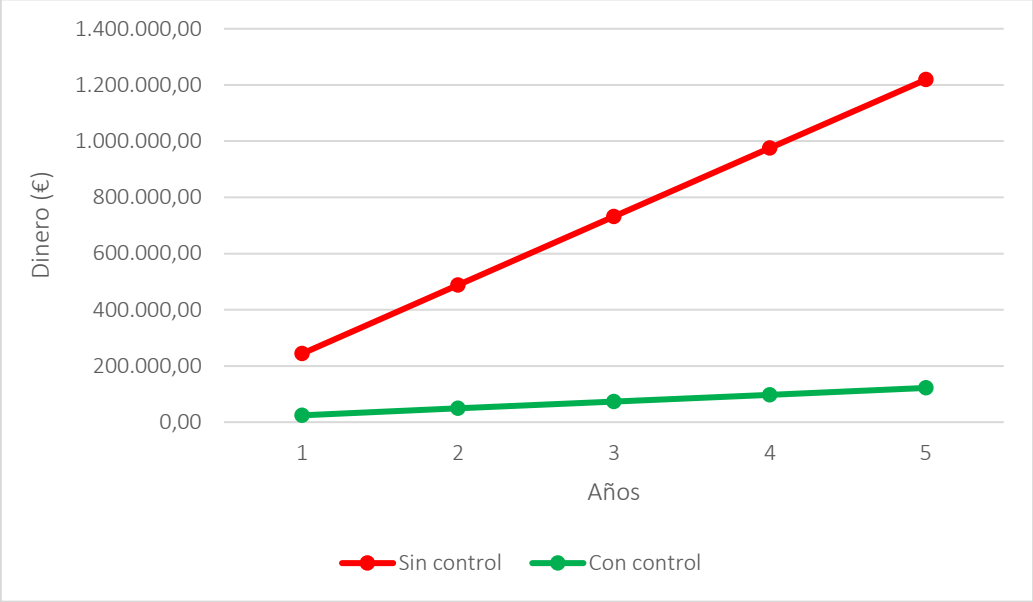



***Ilustración 239. Rentabilidad amenaza SW1 - [E.19] activo S5***

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 247. Rentabilidad amenaza SRVD1 - [A.6] activo S5***

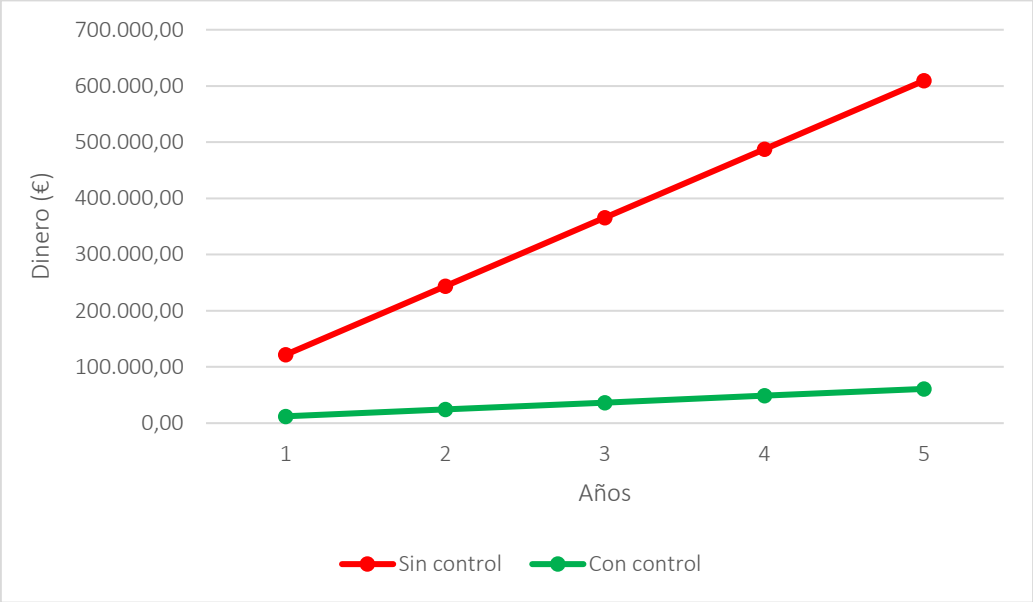



*Ilustración 240. Rentabilidad amenaza SRVD1 - [A.6] activo S5*

## Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 248. Rentabilidad amenaza SRVD1 - [A.7] activo S5*

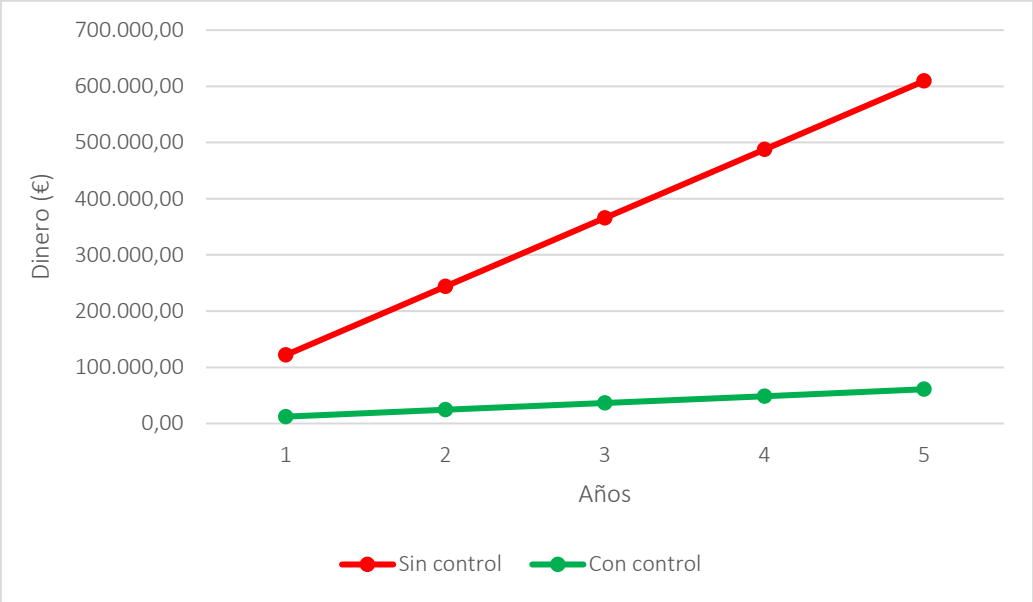



*Ilustración 241. Rentabilidad amenaza SRVD1 - [A.7] activo S5*

## Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 249. Rentabilidad amenaza T1 - [A.6] activo S5*

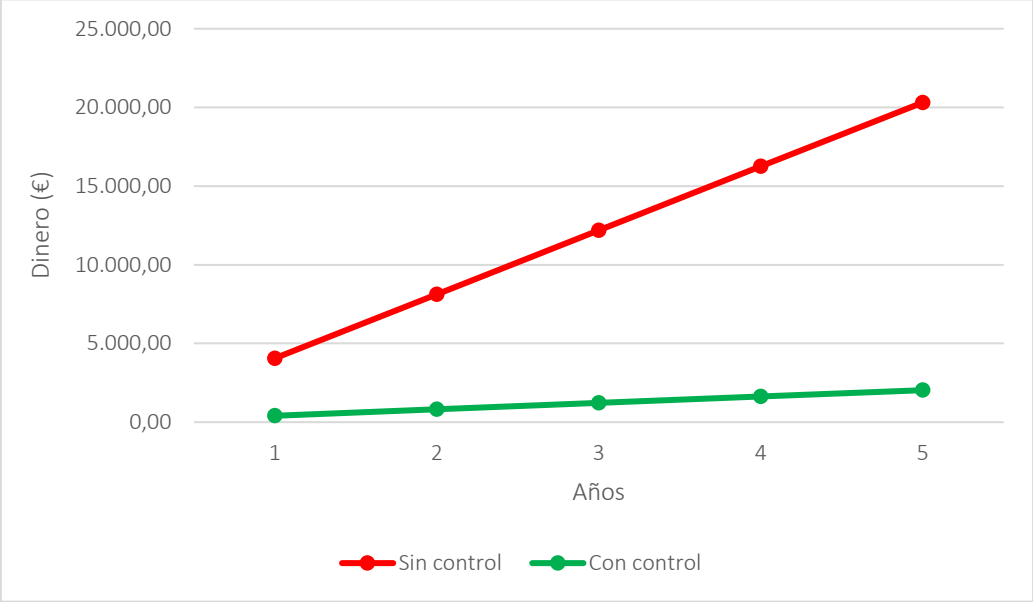



*Ilustración 242. Rentabilidad amenaza T1 - [A.6] activo S5*

## Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 250. Rentabilidad amenaza T1 - [A.7] activo S5*

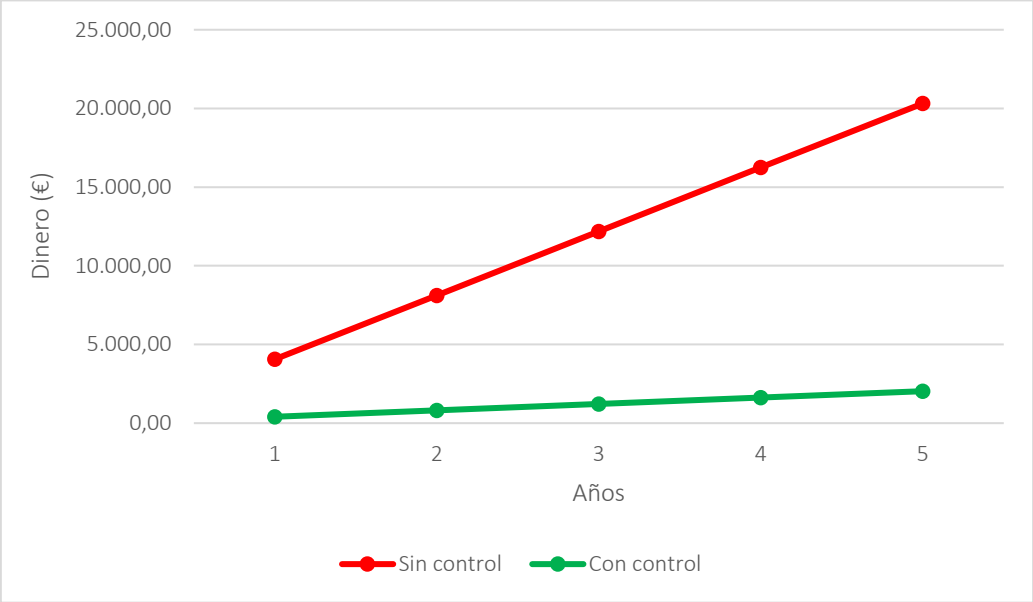



*Ilustración 243. Rentabilidad amenaza T1 - [A.7] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 251. Rentabilidad amenaza D1 - [E.19] activo S6*

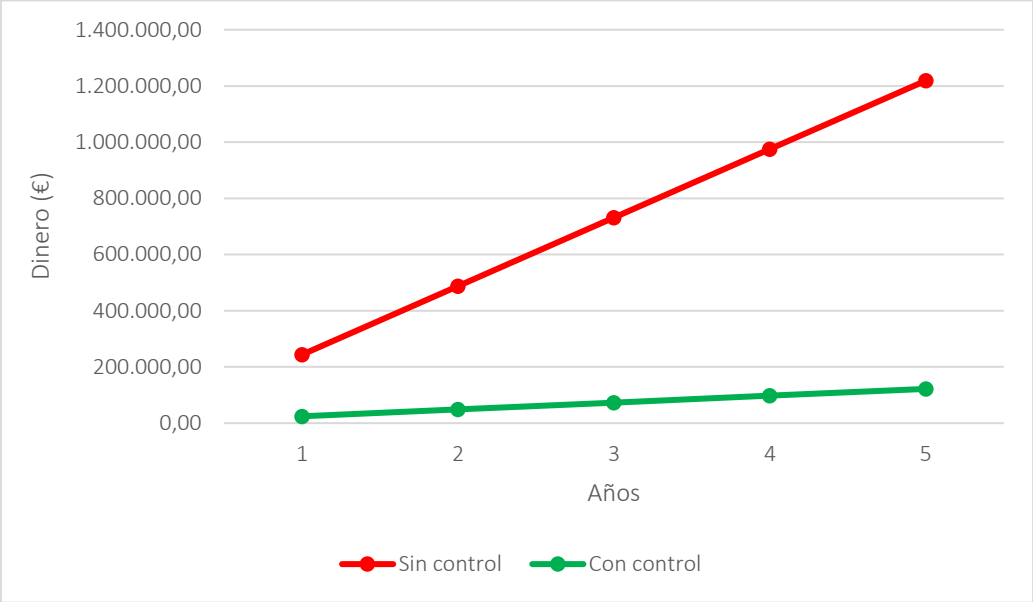



*Ilustración 244. Rentabilidad amenaza D1 - [E.19] activo S6*

Amenaza: D1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 252. Rentabilidad amenaza D1 - [A.6] activo S6*

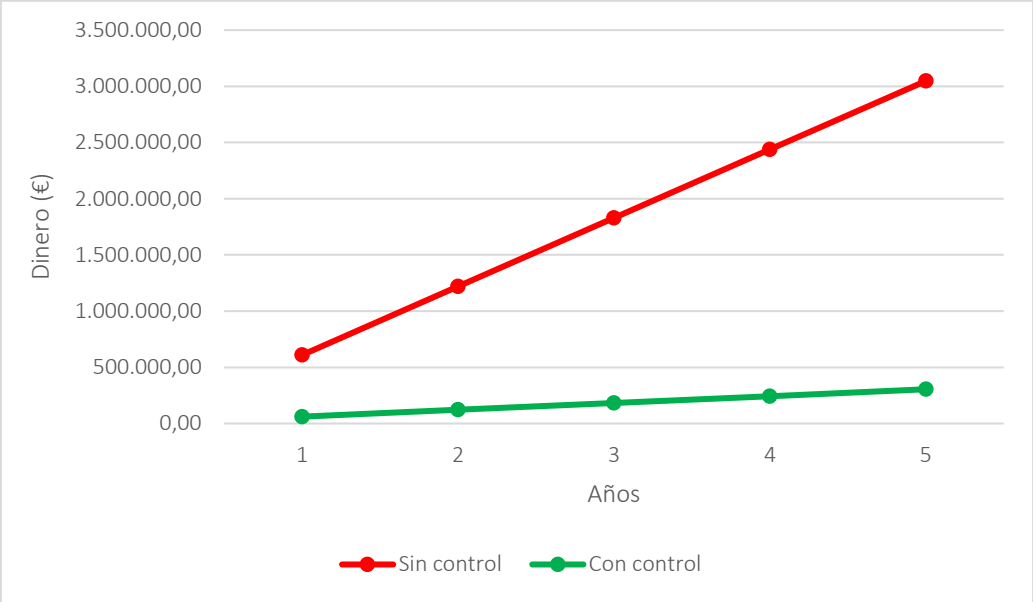



*Ilustración 245. Rentabilidad amenaza D1 - [A.6] activo S6*

## Amenaza: HW1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 253. Rentabilidad amenaza HW1 - [A.6] activo S6***

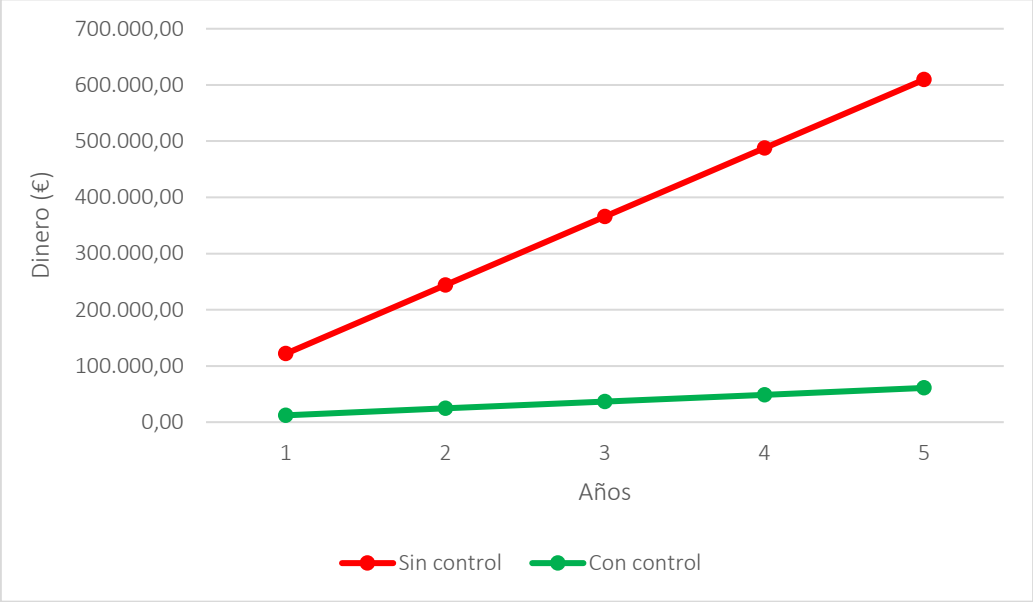



***Ilustración 246. Rentabilidad amenaza HW1 - [A.6] activo S6***

## Amenaza: HW1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

***Tabla 254. Rentabilidad amenaza HW1 - [A.7] activo S6***

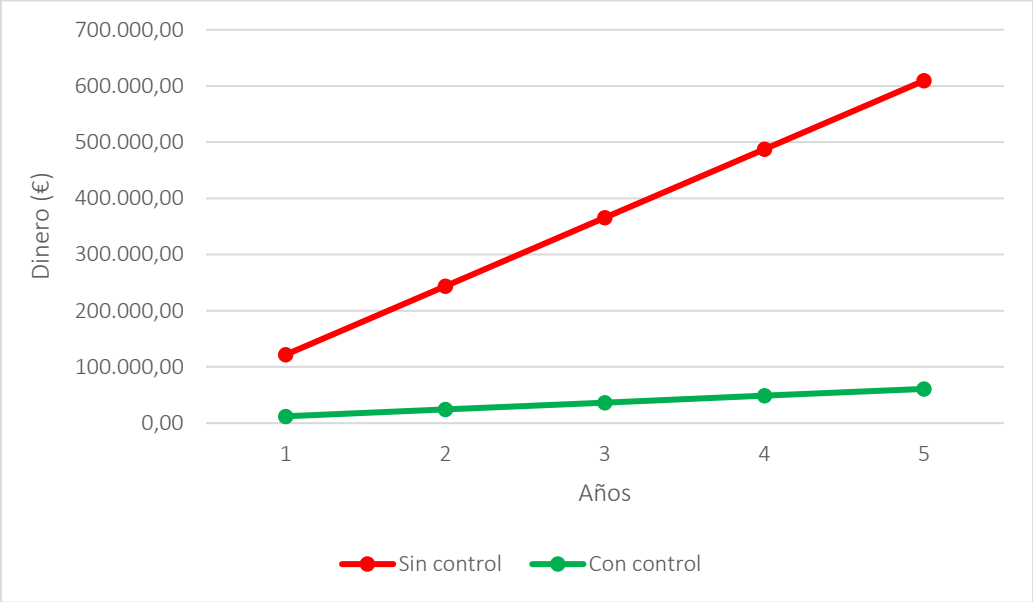



*Ilustración 247. Rentabilidad amenaza HW1 - [A.7] activo S6*

## Amenaza: SW1 – [E.14] Escapes de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 255. Rentabilidad amenaza SW1 - [E.14] activo S6*

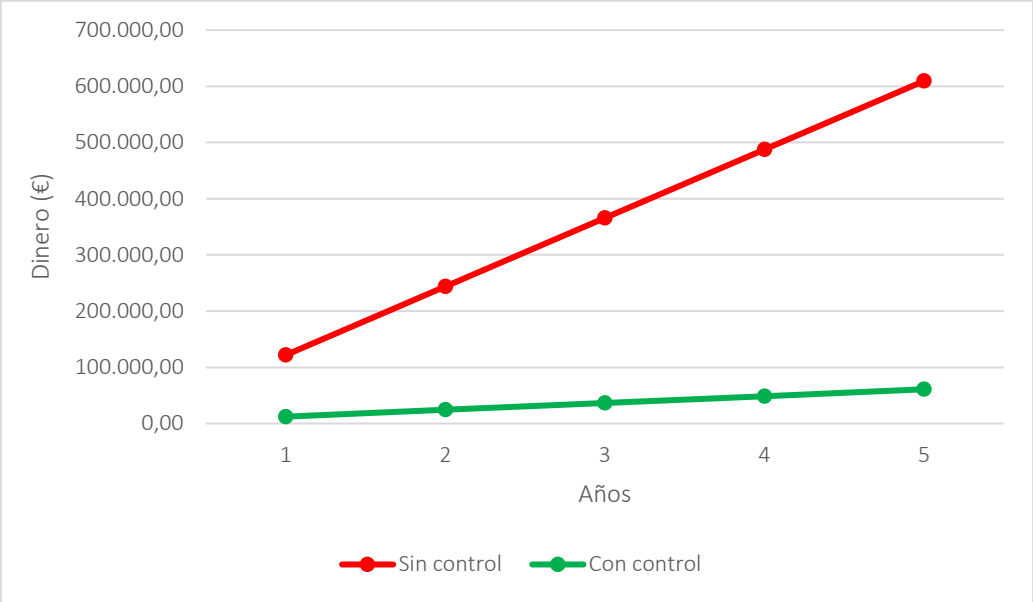



*Ilustración 248. Rentabilidad amenaza SW1 - [E.14] activo S6*

## Amenaza: SW1 – [E.19] – Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 256. Rentabilidad amenaza SW1 - [E.19] activo S6*

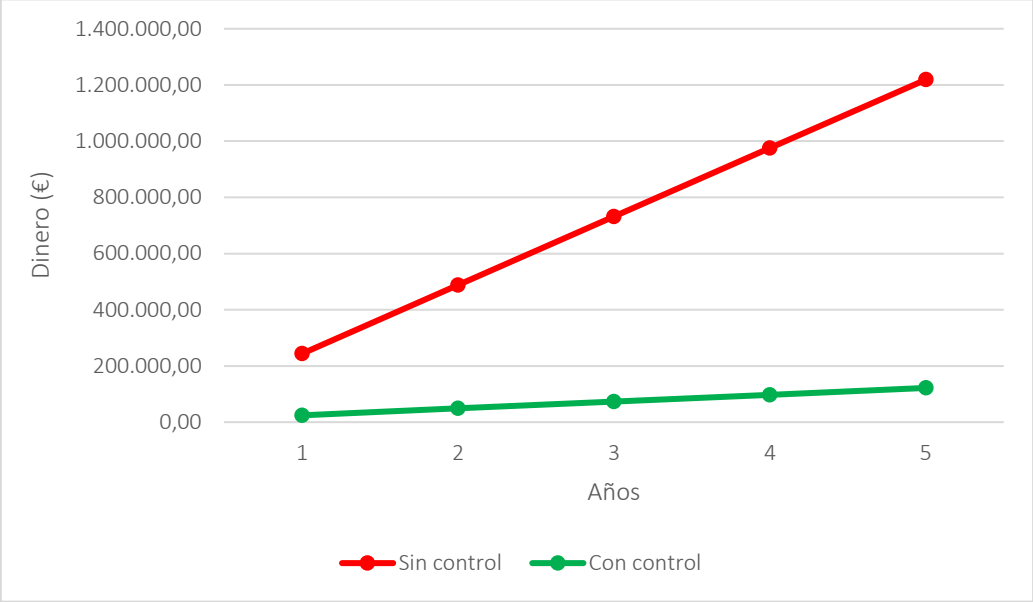



*Ilustración 249. Rentabilidad amenaza SW1 - [E.19] activo S6*

## Amenaza: SRVD1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 257. Rentabilidad amenaza SRVD1 - [A.6] activo S6*

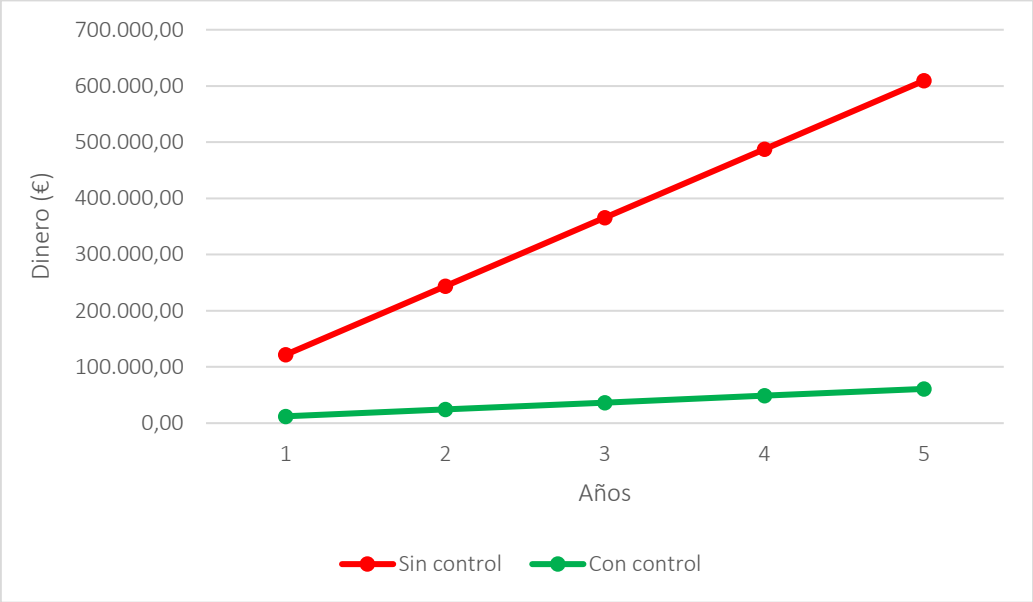



*Ilustración 250. Rentabilidad amenaza SRVD1 - [A.6] activo S6*

## Amenaza: SRVD1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 258. Rentabilidad amenaza SRVD1 - [A.7] activo S6*

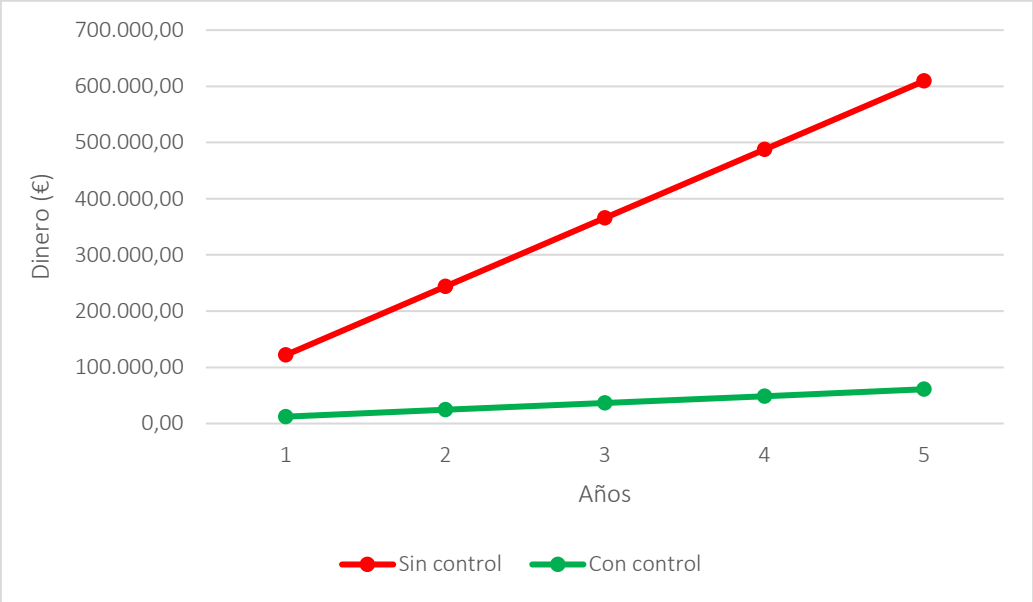



*Ilustración 251. Rentabilidad amenaza SRVD1 - [A.7] activo S6*

## Amenaza: T1 – [A.6] Abuso de privilegios de acceso

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 259. Rentabilidad amenaza T1 - [A.6] activo S6*

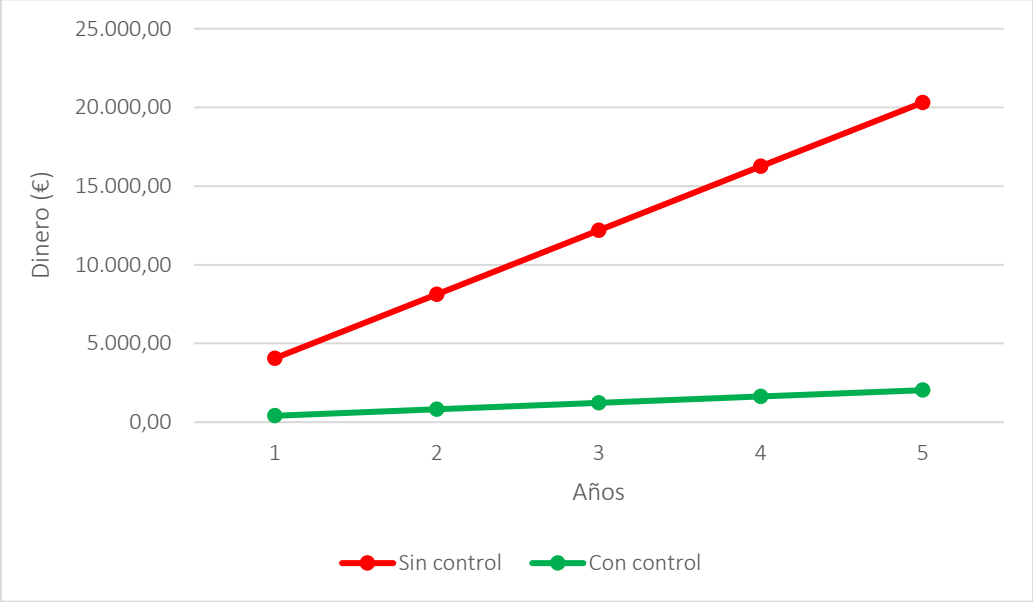



*Ilustración 252. Rentabilidad amenaza T1 - [A.6] activo S6*

## Amenaza: T1 – [A.7] Uso no previsto

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 260. Rentabilidad amenaza T1 - [A.7] activo S6*

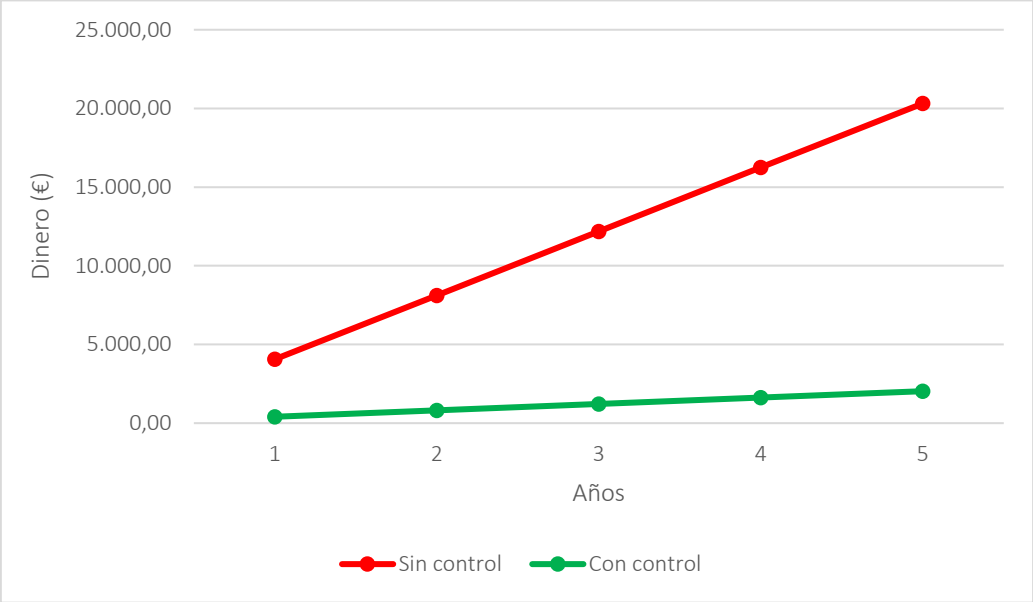



*Ilustración 253. Rentabilidad amenaza T1 - [A.7] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.6 Sexto control

##### 2.1.5.6.1 Título

Control de copias de seguridad

##### 2.1.5.6.2 Finalidad

En un Sistema de información la parte más importante son sus datos, por lo tanto, debemos protegernos de las amenazas que pueden afectar a estos. Además, la información que maneje el Sistema de información puede ser importante y confidencial y dependemos de ella para que nuestro negocio siga adelante.

Debemos tener en cuenta que los soportes donde esos datos están recogidos suelen tener una vida útil limitada. Por todos estos motivos tenemos que implementar las medidas para proteger el mayor activo que almacenamos, la información.

Por otro lado, y no menos importante, la implantación de este control también nos ayudará con el cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

#### 2.1.5.6.3 Empresa

"Sanitaria AMS S.L."

#### 2.1.5.6.4 Leyes aplicables

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

#### 2.1.5.6.5 Normas aplicables

No hay referencias de normas para este control.

#### 2.1.5.6.6 Descripción del control

Para el desarrollo de este control se ha tomado como referencia una guía proporcionada por el Instituto Nacional de Ciberseguridad, "Copias de seguridad". (INCIBE, 2018a)

##### 2.1.5.2.6.1 ¿Qué información vamos a copiar?

Vamos a destacar en primer lugar, que las copias de seguridad se realizaran de todos los activos de la empresa; Información de pacientes, pedidos, citas, facturación, control compra y venta y productos del almacén.

Los criterios que se han seguido para seleccionar que contendrán nuestras copias de seguridad son tres:

- Nivel de accesibilidad o confidencialidad: se tratan de datos altamente confidenciales al ser de tipo sanitario y por lo tanto tener el máximo nivel en cuanto a la Protección de Datos.

- Utilidad o funcionalidad: todos los activos seleccionados son imprescindibles para la empresa, sin alguno de estos, el Sistema de información no podría desarrollar su actividad de manera correcta.

- Impacto en caso de robo, borrado o pérdida: como hemos especificado anteriormente, se tratan de datos con el máximo nivel de seguridad dentro del Régimen General de Protección de Datos, por lo tanto, en caso de que se dé algún impacto de los nombrados anteriores, podría dañarse la imagen de la empresa, tener consecuencias legales y económicas graves y paralización de la actividad empresarial.

#### 2.1.5.2.6.2 Periodicidad

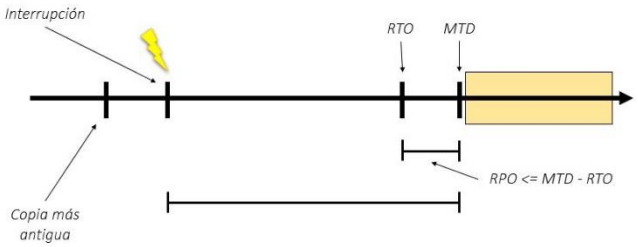
Ventana de interrupción

A continuación, vamos a calcular la ventana de interrupción para determinar cada cuanto tiempo es necesario hacer las copias de seguridad.

- **MTD (Maximum Tolerable Downtime):** Es el tiempo que puedo mantener el sistema fuera de servicio.
- **RTO (Recovery Time Objective):** Es el tiempo que un negocio necesita para recuperar sus sistemas después de inactividad producida por un incidente.
- **RPO (Recovery Point Objective):** Se refiere al volumen de datos en riesgo que la organización considera tolerable.

Datos necesarios para el cálculo de la ventana de interrupción:

- Facturación diaria: 1023.55 €
- Reservas para eventualidades[5]: 1.500 €




Cálculo de la ventana de interrupción:

- Pérdidas por hora = Facturación diaria/8 = 1023.55/8 = 127.95 €
- MTD = Reservas para eventualidades / Pérdidas x hora = 1500/127.95 = 11.73 horas
- RTO debe ser menor o igual a 11.73 horas, para disminuir el tiempo de riesgo, vamos a decretar que se debe hacer una copia de seguridad cada 7 horas; RTO = 7 horas
- RPO <= MTD – RTO = 11.73 – 7 = 4.73 horas
- **RPO = 4.73 horas ≈ 4 horas y media**

[5] La cantidad es referente al Seguro de Responsabilidad Civil que tenga la empresa contratado

Por lo tanto, después de calcular la ventana de interrupción, vamos a decretar que se debe **hacer una copia de seguridad** de los datos del Sistema de información **cada 4 horas y media**, esto es para que en caso de interrupción no sea catastrófico o imposible recuperar la información perdida.

#### 2.1.5.2.6.3 Tipos de copias

Antes de nada, debemos destacar que estamos trabajando antes una PYME, por lo tanto, el volumen y tamaño de las copias de seguridad son fácilmente manejables y de un tamaño pequeño. Así que, en primer lugar, vamos a realizar una copia completa de todos los datos de nuestro sistema, para de esta manera asegurarnos que tenemos una copia de segura.

A continuación, la forma en que haremos la copia de seguridad será una **copia de seguridad** de tipo **diferencial**, la primera vez que se lleve a cabo esta copia, se copiarán todos los datos que hayan cambiado desde el respaldo anterior. Sin embargo, cada vez que se vuelva a lanzar, no solo se copiarán los datos que se hayan modificado desde la última copia, si no todos los que se hayan modificado desde la última copia completa realizada. Esto significa que, con el tiempo, estos archivos se van haciendo más grandes, hasta que se vuelve a realizar la copia completa.

Las principales ventajas que tenemos en este tipo de copia son:

- No requieren tanto espacio de almacenamiento como una copia completa.
- A la hora de recuperar un fichero, sólo habrá que comprobar su existencia en dos copias de respaldo: la última copia diferencial realizada y la última copia completa realizada.

#### 2.1.5.2.6.4 Estrategia 3-2-1

Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable. Sus claves de actuación son las siguientes:

**3.** Mantener 3 copias de cualquier fichero importante: el archivo original y 2 *backups.*
**2.** Almacenar las copias de seguridad en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos.
**1.** Almacenar 1 copia de seguridad fuera de nuestra empresa, lo que se también se conoce como *backup offsite*.


*Ilustración 254. Estrategia 3-2-1*

Por lo tanto, siguiendo esta estrategia en nuestra empresa, debemos realizar las tres copias, una será el propio archivo original guardado en nuestro equipo, dos copias que una será un disco duro extraíble SSD[6] y la otra se hará en un servicio de almacenamiento en la nube. Con la copia en la nube cumplimos los requisitos de tener las copias en dos formatos de almacenamiento distintos y además almacenar una de ellas fuera del lugar de trabajo, además, para este servicio de copias de seguridad en la nube, los dos dueños de la empresa deberán buscar y contratar una empresa adecuada que se ajuste a las necesidades de su empresa y le dé un servicio correcto.

En este control se ha buscado una empresa dedicada a ello, pero no por ello tiene que ser la misma empresa, debe ser similar y que cumpla con las necesidades adecuadas, esta empresa se llama “Datos 101” y el almacenamiento de copias de seguridad en la nube tiene un precio de 29.95 €/mes[7].

En cuanto a la copia de seguridad en nuestro disco duro, estas se pueden realizar de manera correcta cumpliendo con todos los requisitos desde el propio programa de gestión que usa la empresa, ya que tiene implementada esta función correctamente. Dentro de la cuota que paga la empresa por este servicio tenemos incluido la atención al cliente y el servicio técnico. Por lo tanto, para esta acción de realizar las copias de seguridad, el administrador del SI se deberá poner en contacto con dicho servicio técnico para informarse y documentarse correctamente de todos los pasos que se deberán seguir para realizar una copia de manera correcta.

#### 2.1.5.2.6.5 Control de soportes

Los dispositivos de almacenamiento se deterioran con el tiempo, son susceptibles a los fallos mecánicos, pueden sufrir las consecuencias de cualquier

[6] https://www.pccomponentes.com/samsung-t5-ssd-externo-250gb-usb-31-azul
[7] https://www.datos101.com/copias-de-seguridad/

desastre, ser objeto de errores humanos en su manipulación o simplemente la obsolescencia[8]. Por lo tanto, para garantizar la conservación e integridad de nuestros datos seguir las siguientes pautas:

- Comprobar la vida útil de nuestro disco duro extraíble SSD que usamos para realizar las copias de seguridad, una vez al mes.
- Debemos actualizar nuestro software de copias de seguridad cada vez que salga una nueva actualización para prevenir cualquier intrusión o infección.

#### 2.1.5.2.6.6 ¿Cuánto tiempo deben conservarse las copias?

En primer lugar, los documentos mercantiles; libros de contabilidad, correspondencia, documentación sobre la empresa y otros justificantes que hagan referencia al ámbito mercantil. En este caso, el Código del Comercio obliga a las empresas a guardar esta documentación durante 6 años. Pero por si en un futuro es necesario hacer algún tipo de consulta, es recomendable guardar los registros contables de forma indefinida.

En segundo lugar, documentos fiscales, la normativa fiscal marca que los documentos referentes a impuestos y declaraciones tienen un plazo de prescripción de 4 años, que empiezan a contar desde el momento que se presentan a la administración. Sin embargo, en el caso de que se presenten pérdidas o deducciones, el plazo de prescripción aumenta hasta los 10 años.

En tercer lugar, facturas; la Ley General Tributaria establece que todas las empresas y profesionales tienen la obligación de conservar facturas o documentos equivalentes durante un plazo de 4 años. Sin embargo, la normativa de prevención de blanqueo de capitales marca que el plazo de conservación será de diez años.

En último lugar, desde la llegada del Reglamento General de Protección de Datos (RGPD) se obliga a las empresas a establecer una fecha a partir de la cual estos documentos deben ser destruidos de forma segura. Además, la empresa debe ser capaz de destruir de forma segura los datos personales que acumula, a petición del individuo en cuestión.

[8] La obsolescencia es la caída en desuso de las máquinas, equipos y tecnologías motivada no por un mal funcionamiento de estos, sino por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado.

#### 2.1.5.2.6.7 Comprobar la validez de las copias.

Las copias de seguridad son uno de los elementos esenciales que garantizan la continuidad de nuestro negocio y uno de los pilares principales del Plan de Contingencia por lo que, si no probamos que las copias de seguridad pueden restaurarse correctamente no garantizaremos que la información se pueda recuperar. No debemos asumir que por haber realizado el proceso de copia está todo hecho, por lo que debemos programar periódicamente pruebas de restauración de las copias para asegurar que el día que no sea una simulación se conocen todos los procesos y funcionan correctamente.

Por lo tanto, anteriormente ya hemos detallado los pasos de cómo se debe hacer una copia de seguridad correctamente. Además, deberemos comprobar una vez cada dos semanas que la copia de seguridad se está realizando correctamente.

#### 2.1.5.2.6.8 Cifrado de la información

Para garantizar la confidencialidad e integridad de la información sensible cuando está almacenada, utilizaremos herramientas de cifrado que protejan nuestros datos, haciéndolos ilegibles por aquellos que no dispongan de la clave de cifrado.

Cifrando la información confidencial y la almacenada en copias de seguridad protegemos los datos en caso de robo de información o accesos no autorizados, reduce el riesgo de sanciones y podría evitar que tengamos que informar a los usuarios en caso de brecha de seguridad. Además, se cumplirá con el deber de salvaguarda que exige el Reglamento General de Protección de datos.

Por lo tanto, toda la información deberá estar cifrada con una clave criptográfica asimétrica, esto lo deberá hacer el propio programa que utilicemos para realizar las copias de seguridad, como ya hemos explicado anteriormente.

#### 2.1.5.2.6.9 Documentación del proceso

Debemos etiquetas e identificar los soportes dónde se realizan las copias de seguridad, de manera que se pueda llevar un registro de los soportes que se ha realizado algún respaldo. Así, en caso de necesitar recuperar alguna información concreta, será más sencillo consultar en que soporte está almacenada.

La aplicación que usamos para realizar las copias de seguridad nos proporcionará la información necesaria que necesitamos para registrar las copias de seguridad realizadas. Nuestra hoja de registro deberá incluir los siguientes campos:

- **Identificador de soporte** código que identifica el soporte en el que se ha realizado la copia.
- **Tipos de copia**: se indicará si es un copia total, incremental, etc.
- **Fecha y hora**: cuándo se llevó a cabo la copia de seguridad.
- **Lugar de almacenamiento**: ubicación física donde se encuentra la copia de seguridad.
- **Personal a cargo de la copia**: responsables de la realización y conservación de la copia durante el tiempo que se haya establecido.

#### 2.1.5.2.6.10 Borrado

Cuando llega la hora de desechar los soportes que han sido utilizados para realizar copias de seguridad, debemos asegurarnos de destruirlos de forma segura. Es muy importante asegurarse de que esa información nunca volverá a ser accesible para evitar posibles accesos malintencionados ya que estos datos pueden ser de carácter sensible y confidenciales.

Por estos motivos, para la destrucción de nuestra información y soportes, debemos elegir la destrucción certificada, ya que se trata de datos personales o confidenciales. Para ello debemos buscar una empresa dedicada a la destrucción de datos de manera segura y que nos dé un presupuesto adecuado y ajustado a nuestras características.

### 2.1.5.6.7 Responsables

Administrador del SI, será el encargado de realizar todo el proceso necesario para el correcto funcionamiento de las copias de seguridad. En dicho proceso van incluidos todos los aspectos descritos anteriormente, en modo de resumen y como aclaratorio, el administrador del SI deberá:

- Configurar todo el sistema para que realice las copias de manera correcta, con ayuda del servicio técnico.
- Configurar el servicio de almacenamiento en la nube, también con ayuda del servicio técnico que proporcione la compañía contratada si lo necesitase.

- Configurar las copias para que la información copiada quede cifrada correctamente.
- Configurar las copias para que haya un registro de cómo, cuándo y quién ha hecho las copias de seguridad.

Además, el administrador del SI deberá comprobar una vez cada dos semanas:

- Control de soportes de almacenamiento.
- Comprobar la validez de las copias.

#### 2.1.5.6.8 Dispositivos

En cuanto al sistema de copias de seguridad, va incluido en el propio programa, además la configuración la hará el administrador del SI que es uno de los trabajadores de la empresa. Por lo tanto, para esta parte no hace falta la contratación de ningún trabajador extra. Se necesitará el disco duro extraíble SSD especificado anteriormente, o uno de características similares, que será el soporte donde se realicen las copias, este tiene un precio de 75 €.

Por otro lado, para el servicio de almacenamiento en la nube es necesario la contratación de una cuota mensual con un coste de 29,95 €/mes.

#### 2.1.5.6.9 Costes

- **Implantación:** 75 €, del disco duro extraíble, el cual se utilizará como soporte para realizar las copias.
- **Ejecución y mantenimiento:** Cada mes hay que pagar la cuota de 29.95 €/mes para mantener el servicio de almacenamiento en la nube. Por lo tanto, tendrá un precio de 359.4 € al año.
- **Búsqueda de irregularidades:** Si en algún momento se detecta algún fallo en alguna parte del sistema de copias de seguridad, ya sea en algún soporte o en la configuración de las mismas, el administrador del SI deberá sustituir en caso del soporte por otro igual y en caso de la configuración, deberá volver a configurarlo todo para que funcione correctamente de la misma manera.

#### 2.1.5.6.10 Rentabilidad

Como ya hemos estado describiendo en la mayoría de puntos anteriores, los datos son el activo más importante de las empresas, esto conlleva también que estén expuestos a un gran número de amenazas, las cuales en caso de producirse pueden derivar en problemas catastróficos para nuestra empresa. Por lo tanto, debemos protegernos de manera adecuada para poder afrontarlos con los mínimos problemas posibles.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar dicho control en nuestro SI. Vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenaza se ejecuta.

Determinamos que el control tiene una eficacia del 95 % ya que:

- Puede fallar por una mala configuración.
- Puede fallar por un olvido del responsable.
- Puede fallar por un fallo de los soportes de almacenamiento.

Activo: Información pacientes (S1)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 3438,26 | 0 | 0 | 3438,26 | 6876,52 | 10314,78 | 13753,04 | 17191,3 |
| 171,91 | 75 | 359,4 | 606,31 | 1137,62 | 1668,93 | 2200,24 | 2731,55 |

*Tabla 261. Rentabilidad amenaza AUX1 - [I.5] activo S1*

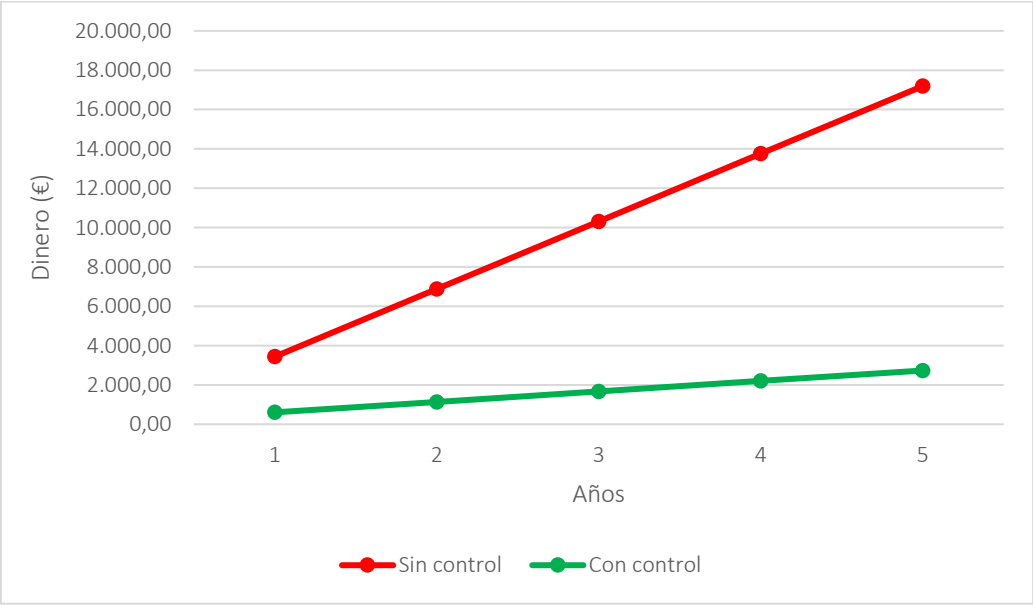



*Ilustración 255. Rentabilidad amenaza AUX1 - [I.5] activo S1*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 78225,02 | 0 | 0 | 78225,02 | 156450,04 | 234675,06 | 312900,08 | 391125,1 |
| 3911,25 | 75 | 359,4 | 4345,65 | 8616,3 | 12886,95 | 17157,6 | 21428,25 |

*Tabla 262. Rentabilidad amenaza AUX1 - [I.10] activo S1*

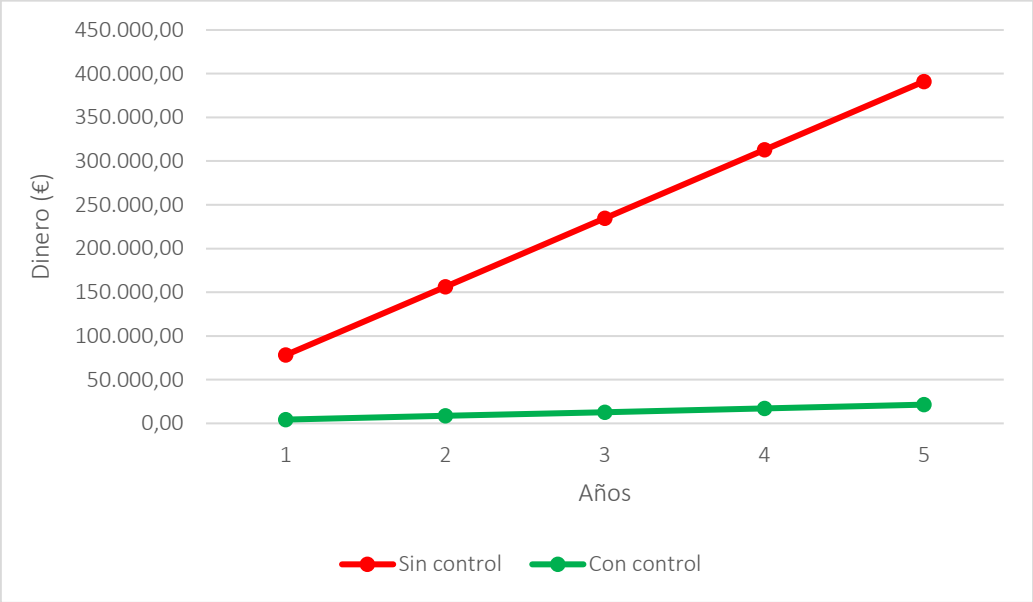



*Ilustración 256. Rentabilidad amenaza AUX1 - [I.10] activo S1*

Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 545755,99 | 0 | 0 | 545755,99 | 1091512 | 1637267,97 | 2183023,96 | 2728779,95 |
| 27287,8 | 75 | 359,4 | 27722,2 | 55369,4 | 83016,6 | 110663,8 | 138311 |

*Tabla 263. Rentabilidad amenaza AUX1 - [E.4] activo S1*

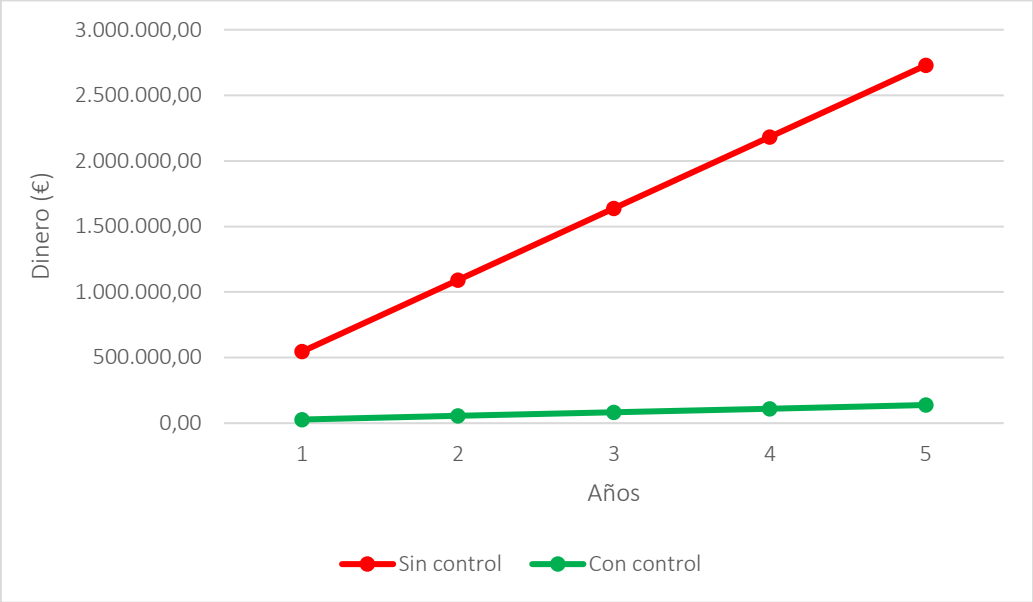



*Ilustración 257. Rentabilidad amenaza AUX1 - [E.4] activo S1*

Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1819186,62 | 0 | 0 | 1819186,62 | 3638373,2 | 5457559,86 | 7276746,48 | 9095933,1 |
| 90959,33 | 75 | 359,4 | 91393,73 | 182712,46 | 274031,19 | 365349,92 | 456668,65 |

*Tabla 264. Rentabilidad amenaza D1 - [E.15] activo S1*

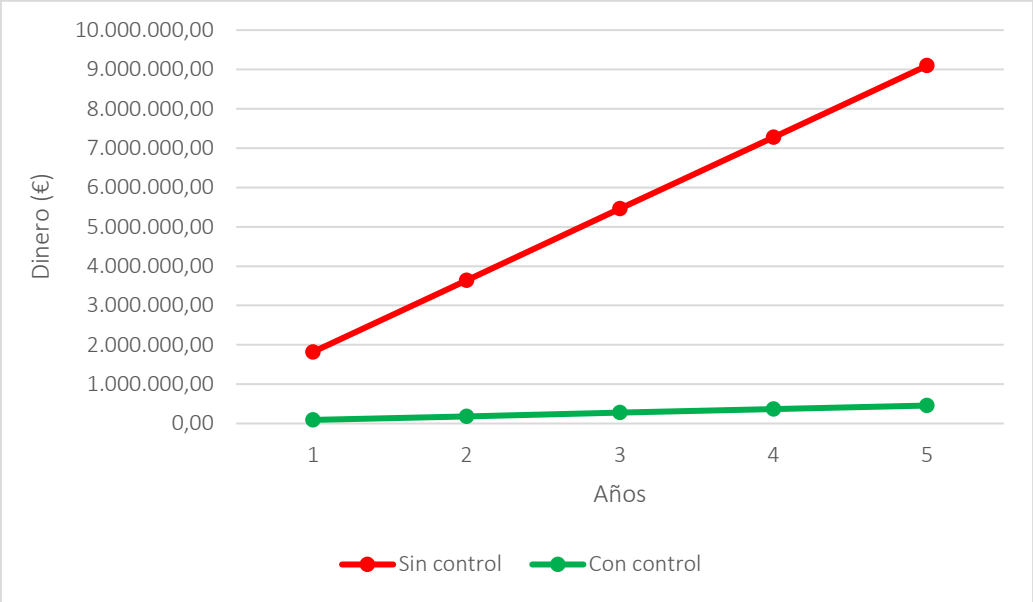



*Ilustración 258. Rentabilidad amenaza D1 - [E.15] activo S1*

## Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 18191,87 | 75 | 359,4 | 18626,27 | 37177,54 | 55728,81 | 74280,08 | 92831,35 |

***Tabla 265. Rentabilidad amenaza D1 - [E.18] activo S1***

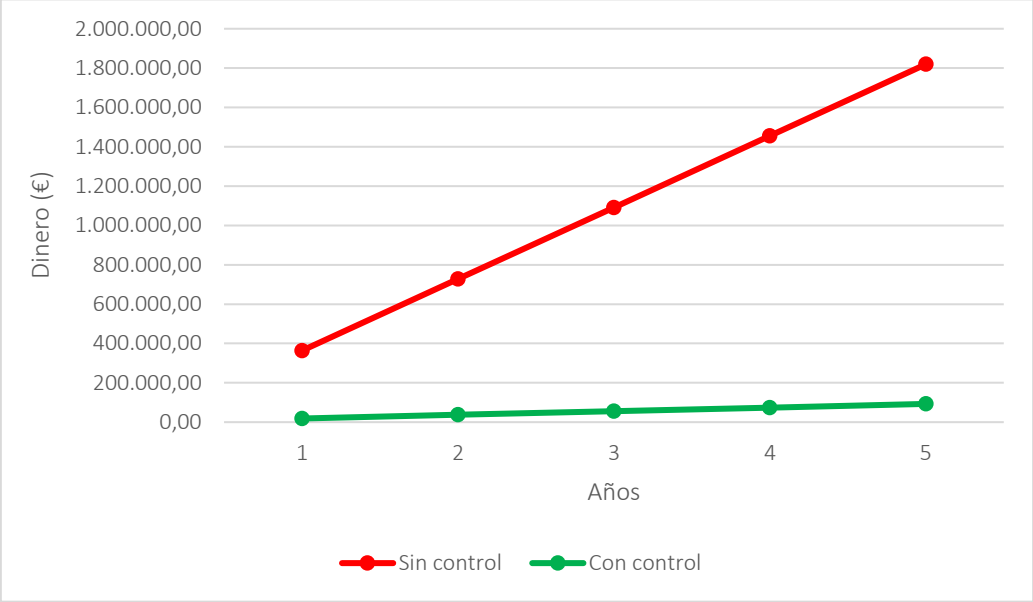



***Ilustración 259. Rentabilidad amenaza D1 - [E.18] activo S1***

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 18191,87 | 75 | 359,4 | 18626,27 | 37177,54 | 55728,81 | 74280,08 | 92831,35 |

***Tabla 266. Rentabilidad amenaza D1 - [A.18] activo S1***

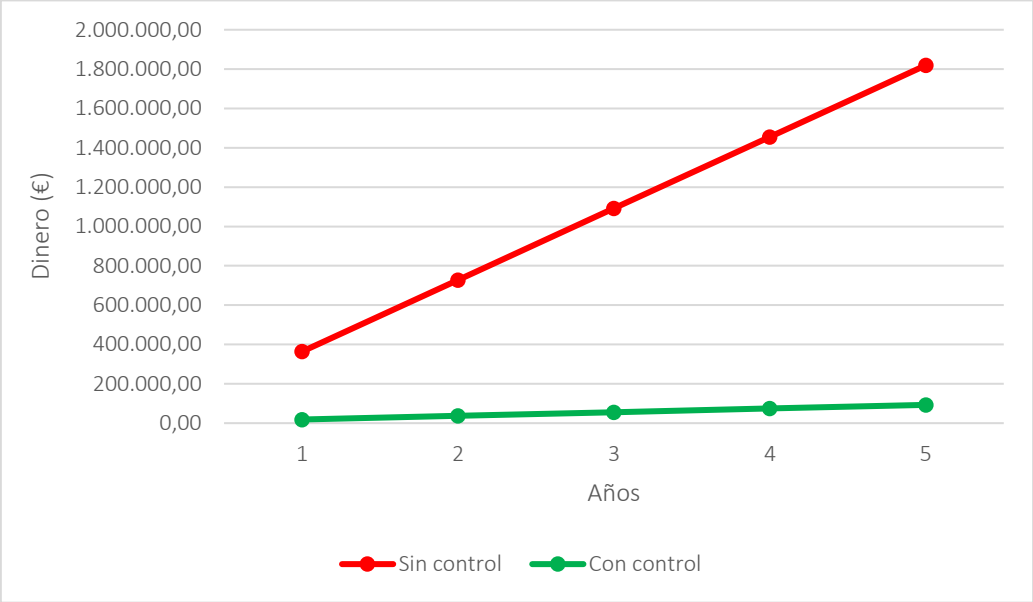



*Ilustración 260. Rentabilidad amenaza D1 - [A.18] activo S1*

## Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 127343,06 | 0 | 0 | 127343,06 | 254686,12 | 382029,18 | 509372,24 | 636715,3 |
| 6367,15 | 75 | 359,4 | 6801,55 | 13528,1 | 20254,65 | 26981,2 | 33707,75 |

*Tabla 267. Rentabilidad amenaza SW1 - [A.18] activo S1*

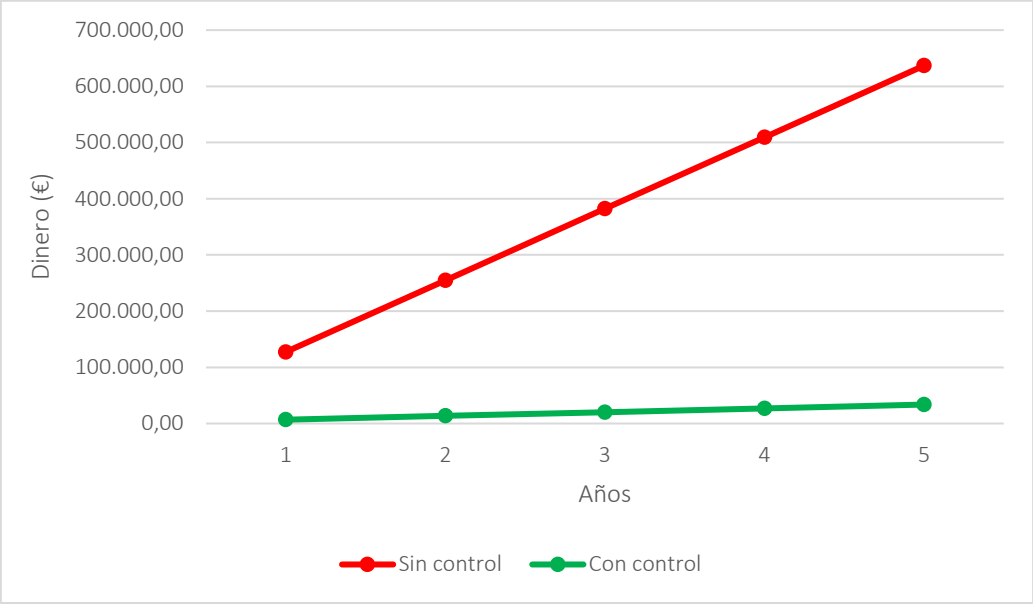



*Ilustración 261. Rentabilidad amenaza SW1 - [A.18] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2303,5 | 0 | 0 | 2303,5 | 4607 | 6910,5 | 9214 | 11517,5 |
| 115,17 | 75 | 359,4 | 549,57 | 1024,14 | 1498,71 | 1973,28 | 2447,85 |

*Tabla 268. Rentabilidad amenaza AUX1 - [I.5] activo S2*

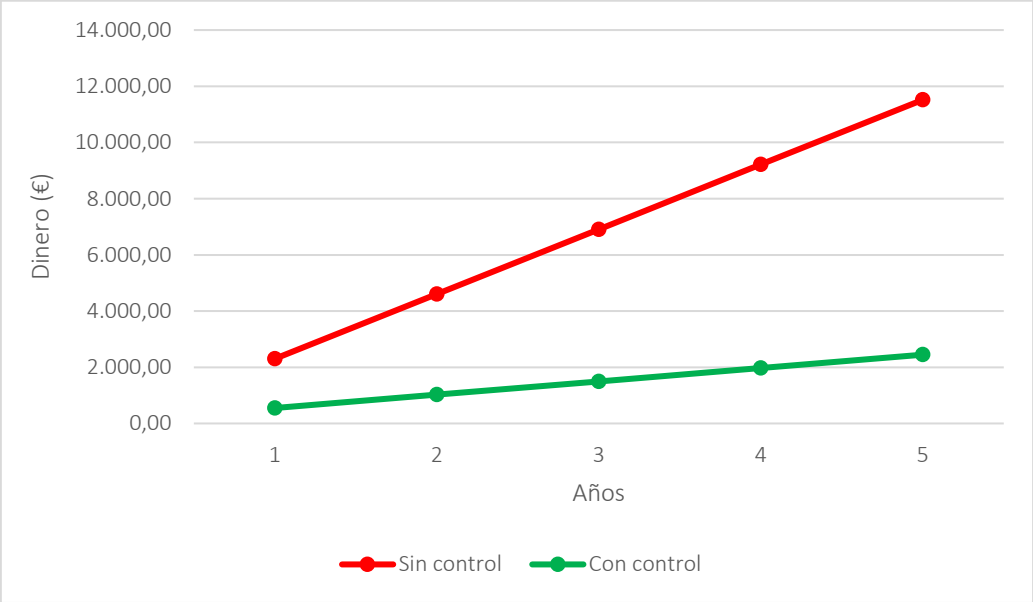



*Ilustración 262. Rentabilidad amenaza AUX1 - [I.5] activo S2*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 52407,67 | 0 | 0 | 52407,67 | 104815,34 | 157223,01 | 209630,68 | 262038,35 |
| 2620,38 | 75 | 359,4 | 3054,78 | 6034,56 | 9014,34 | 11994,12 | 14973,9 |

*Tabla 269. Rentabilidad amenaza AUX1 - [I.10] activo S2*

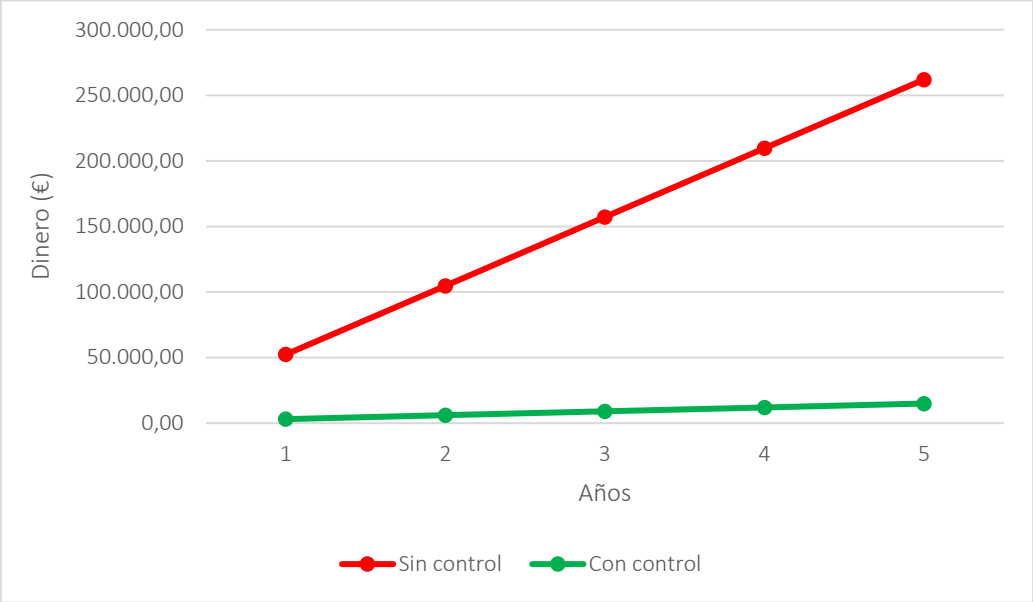



*Ilustración 263. Rentabilidad amenaza AUX1 - [I.10] activo S2*

Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 365634,89 | 0 | 0 | 365634,89 | 731269,78 | 1096904,67 | 1462539,56 | 1828174,45 |
| 18281,74 | 75 | 359,4 | 18716,14 | 37357,28 | 55998,42 | 74639,56 | 93280,7 |

*Tabla 270. Rentabilidad amenaza AUX1 - [E.4] activo S2*

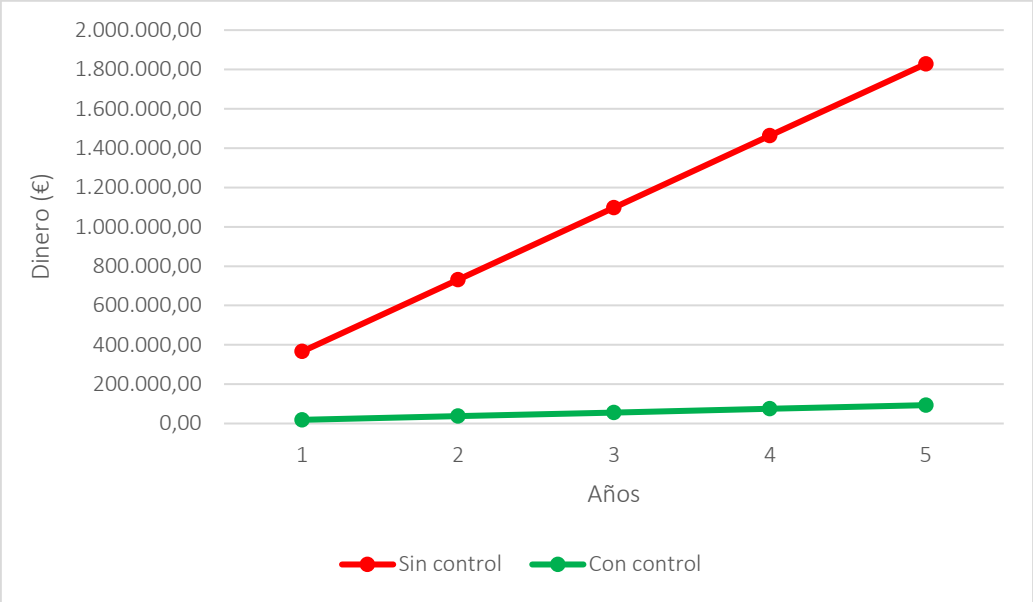



*Ilustración 264. Rentabilidad amenaza AUX1 - [E.4] activo S2*

## Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 60939,15 | 75 | 359,4 | 61373,55 | 122672,1 | 183970,65 | 245269,2 | 306567,75 |

*Tabla 271. Rentabilidad amenaza D1 - [E.15] activo S2*

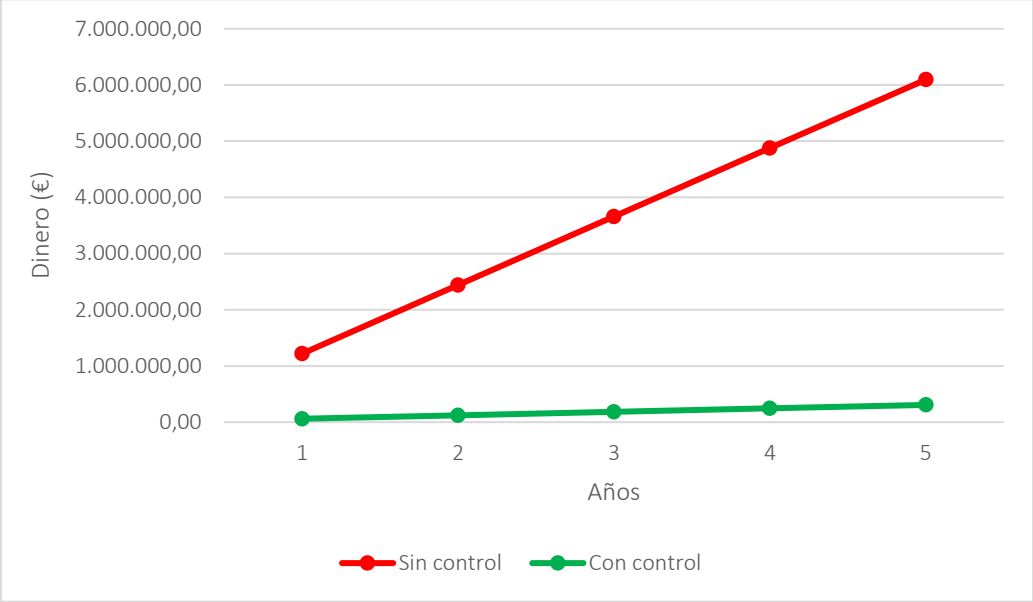



*Ilustración 265. Rentabilidad amenaza D1 - [E.15] activo S2*

## Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 272. Rentabilidad amenaza D1 - [E.18] activo S2*

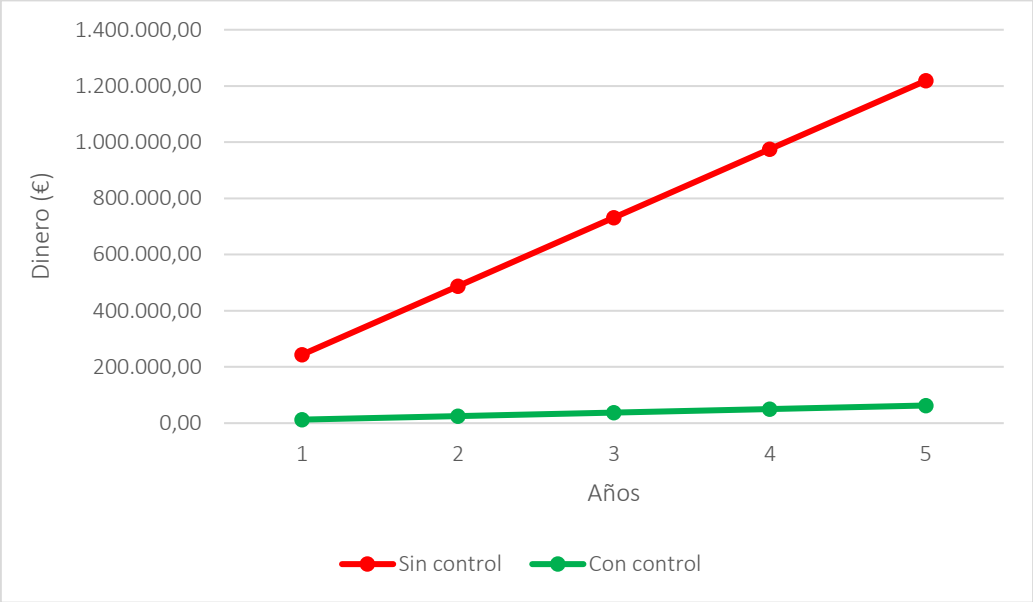



*Ilustración 266. Rentabilidad amenaza D11 - [E.18] activo S2*

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 273. Rentabilidad amenaza D1 - [A.18] activo S2*

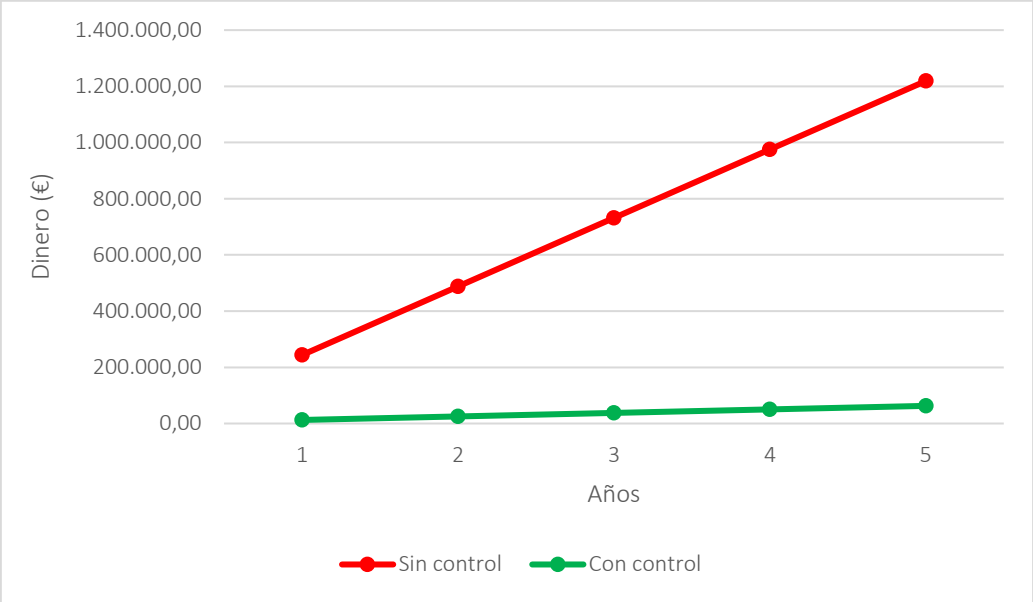



*Ilustración 267. Rentabilidad amenaza D1 - [A.18] activo S2*

Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 4265,74 | 75 | 359,4 | 4700,14 | 9325,28 | 13950,42 | 18575,56 | 23200,7 |

*Tabla 274. Rentabilidad amenaza SW1 - [A.18] activo S2*

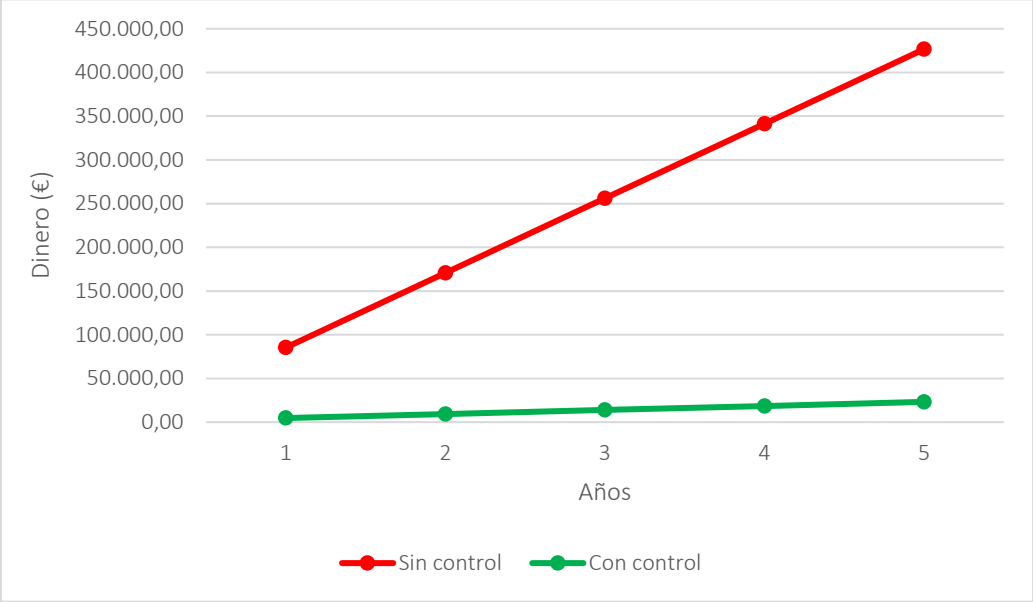



*Ilustración 268. Rentabilidad amenaza SW1 - [A.18] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2303,5 | 0 | 0 | 2303,5 | 4607 | 6910,5 | 9214 | 11517,5 |
| 115,17 | 75 | 359,4 | 549,57 | 1024,14 | 1498,71 | 1973,28 | 2447,85 |

*Tabla 275. Rentabilidad amenaza AUX1 - [I.5] activo S3*

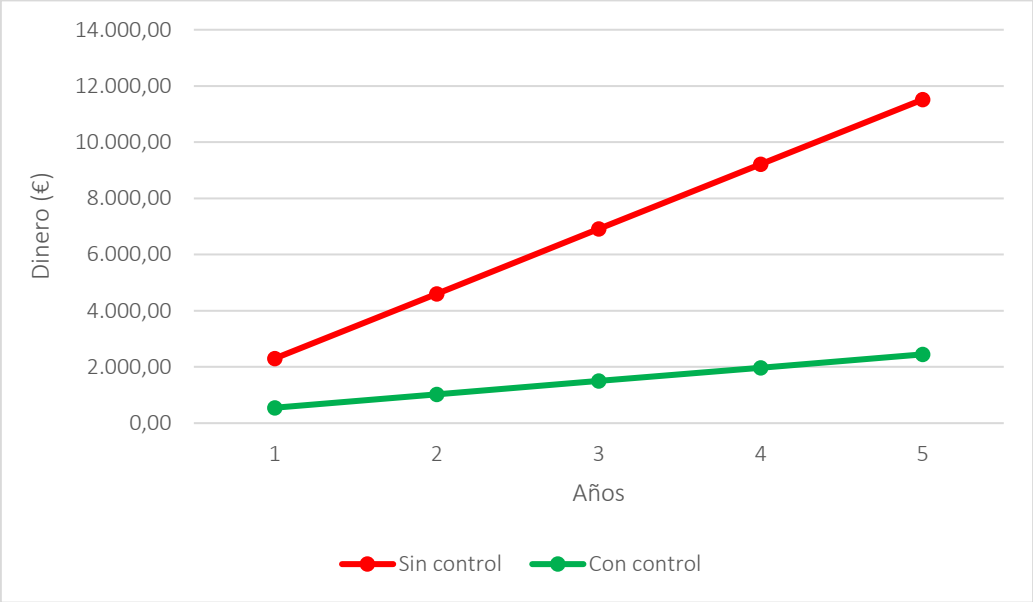



*Ilustración 269. Rentabilidad amenaza AUX1 - [I.5] activo S3*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 52407,67 | 0 | 0 | 52407,67 | 104815,34 | 157223,01 | 209630,68 | 262038,35 |
| 2620,38 | 75 | 359,4 | 3054,78 | 6034,56 | 9014,34 | 11994,12 | 14973,9 |

*Tabla 276. Rentabilidad amenaza AUX1 - [I.10] activo S3*

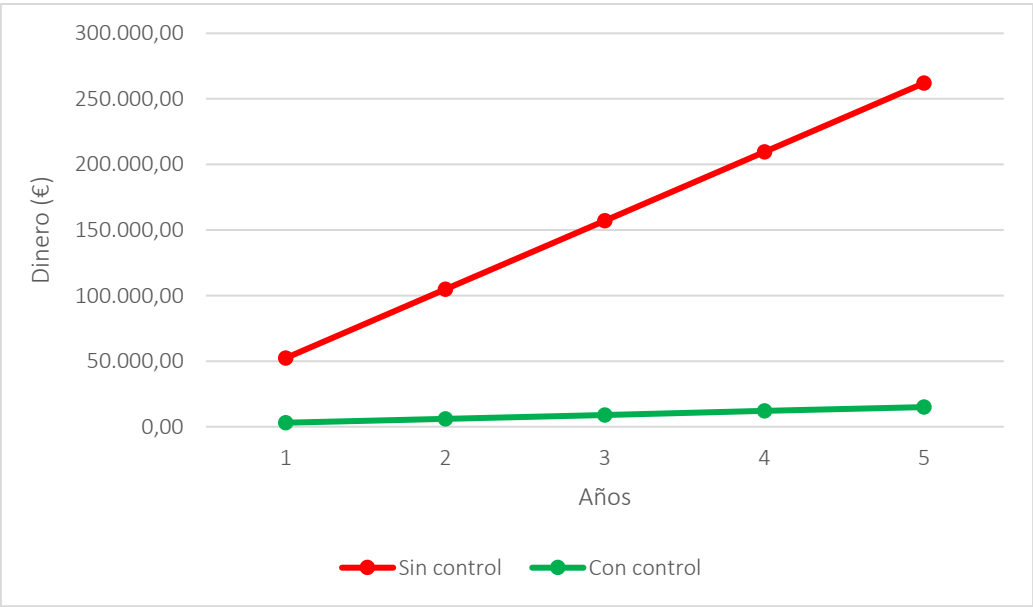



*Ilustración 270. Rentabilidad amenaza AUX1 - [I.10] activo S3*

## Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 365634,89 | 0 | 0 | 365634,89 | 731269,78 | 1096904,67 | 1462539,56 | 1828174,45 |
| 18281,74 | 75 | 359,4 | 18716,14 | 37357,28 | 55998,42 | 74639,56 | 93280,7 |

***Tabla 277. Rentabilidad amenaza AUX1 - [E.4] activo S3***

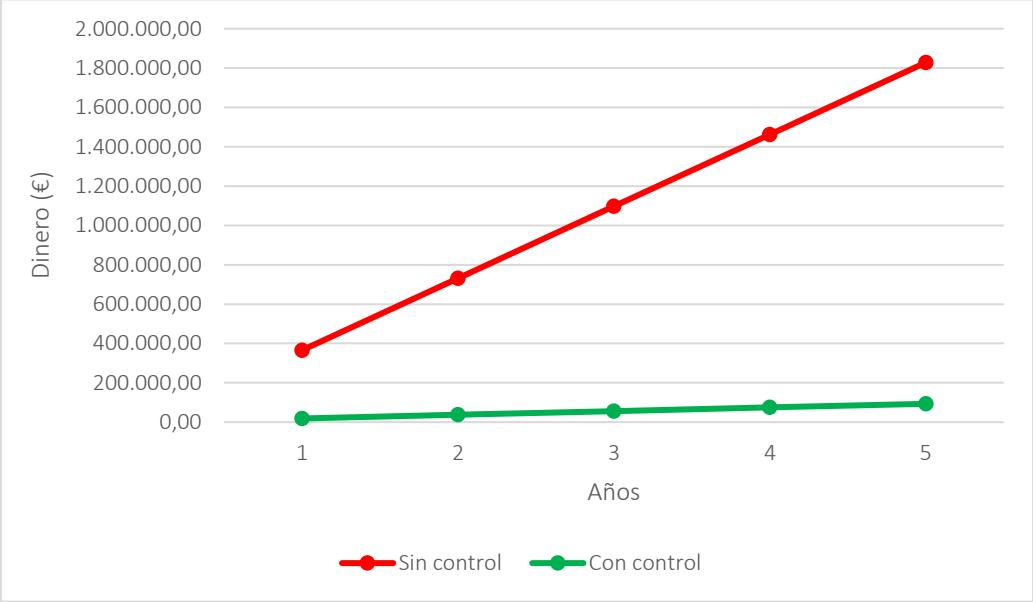



***Ilustración 271. Rentabilidad amenaza AUX1 - [E.4] activo S3***

## Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 60939,15 | 75 | 359,4 | 61373,55 | 122672,1 | 183970,65 | 245269,2 | 306567,75 |

***Tabla 278. Rentabilidad amenaza D1 - [E.15] activo S3***

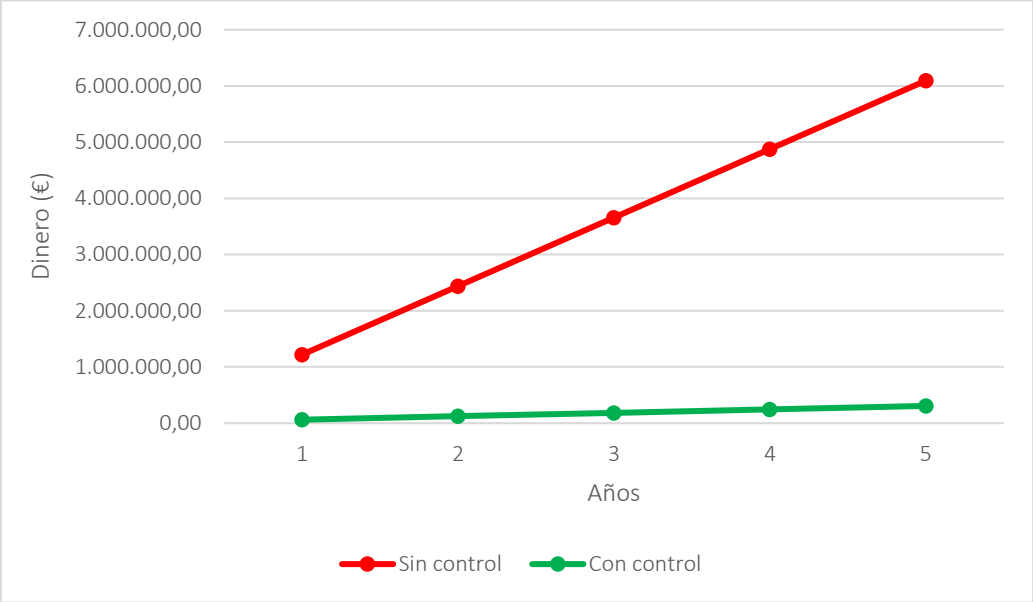



*Ilustración 272. Rentabilidad amenaza D1 - [E.5] activo S3*

Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 279. Rentabilidad amenaza D1 - [E.18] activo S3*

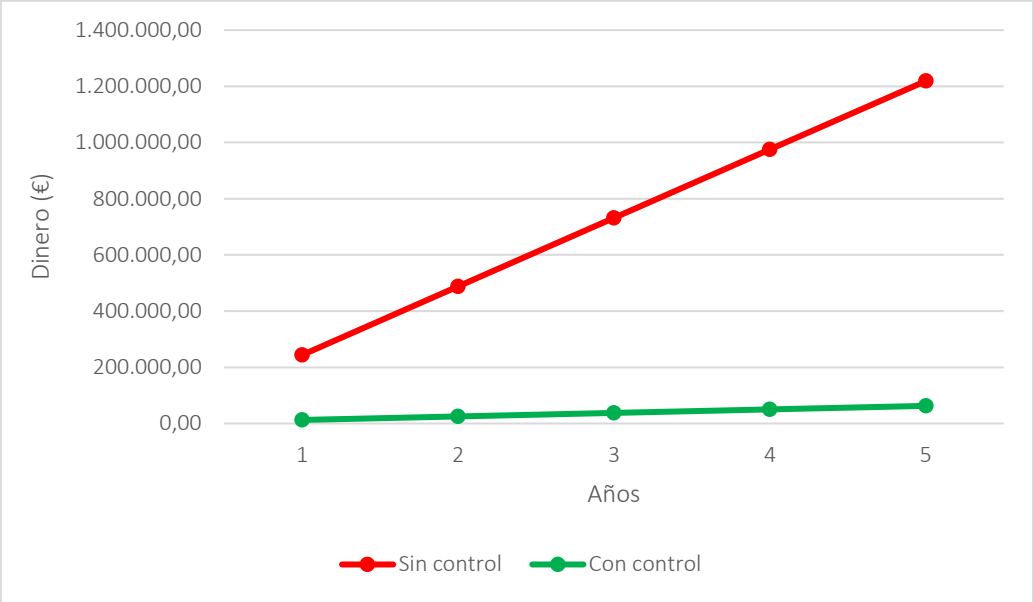



*Ilustración 273. Rentabilidad amenaza D1 - [E.18] activo S3*

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

***Tabla 280. Rentabilidad amenaza D1 - [A.18] activo S3***

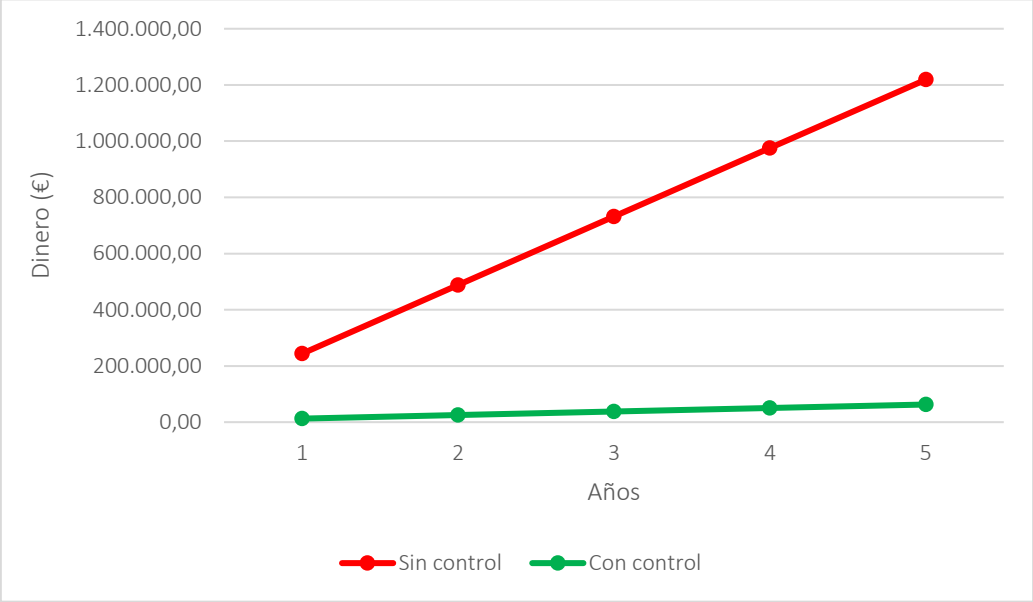



***Ilustración 274. Rentabilidad amenaza D1 - [A.18] activo S3***

## Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 4265,74 | 75 | 359,4 | 4700,14 | 9325,28 | 13950,42 | 18575,56 | 23200,7 |

***Tabla 281. Rentabilidad amenaza SW1 - [A.18] activo S3***

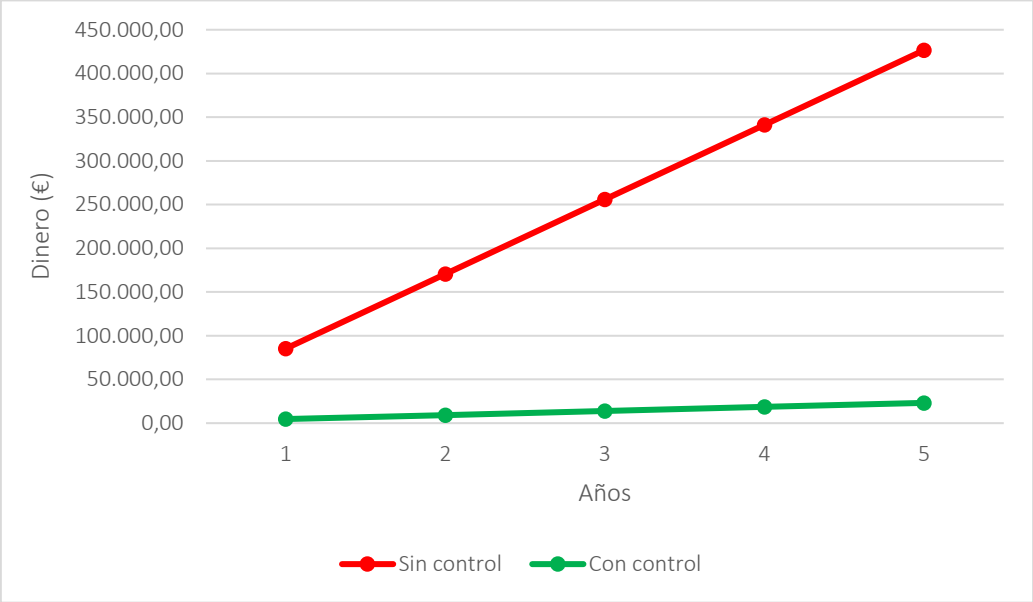



*Ilustración 275. Rentabilidad amenaza SW1 - [A.18] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2303,44 | 0 | 0 | 2303,44 | 4606,88 | 6910,32 | 9213,76 | 11517,2 |
| 115,17 | 75 | 359,4 | 549,57 | 1024,14 | 1498,71 | 1973,28 | 2447,85 |

*Tabla 282. Rentabilidad amenaza AUX1 - [I.5] activo S4*

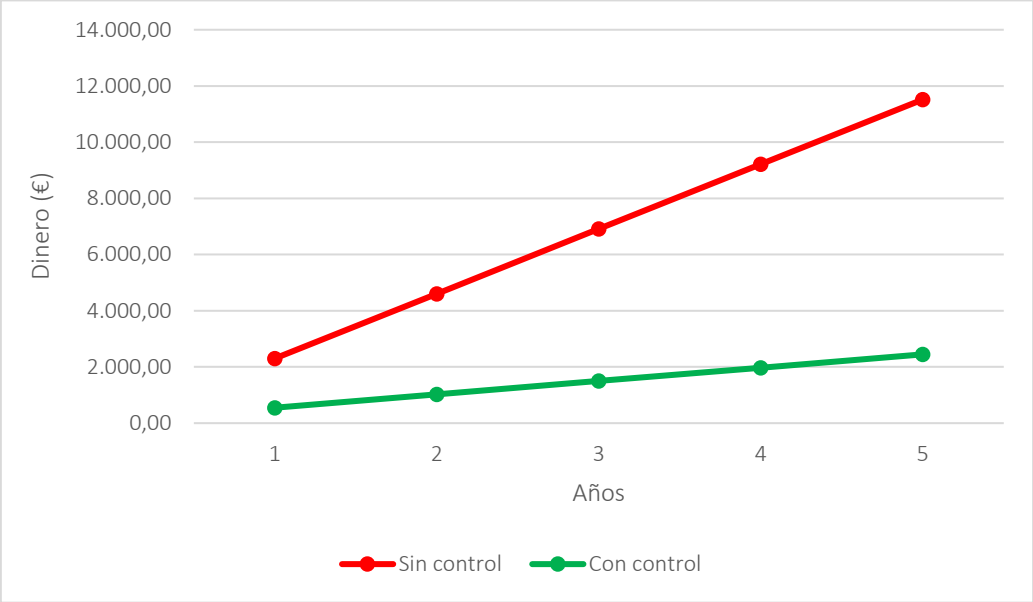



*Ilustración 276. Rentabilidad amenaza AUX1 - [I.5] activo S4*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 52406,31 | 0 | 0 | 52406,31 | 104812,62 | 157218,93 | 209625,24 | 262031,55 |
| 2620,32 | 75 | 359,4 | 3054,72 | 6034,44 | 9014,16 | 11993,88 | 14973,6 |

*Tabla 283. Rentabilidad amenaza AUX1 - [I.10] activo S4*

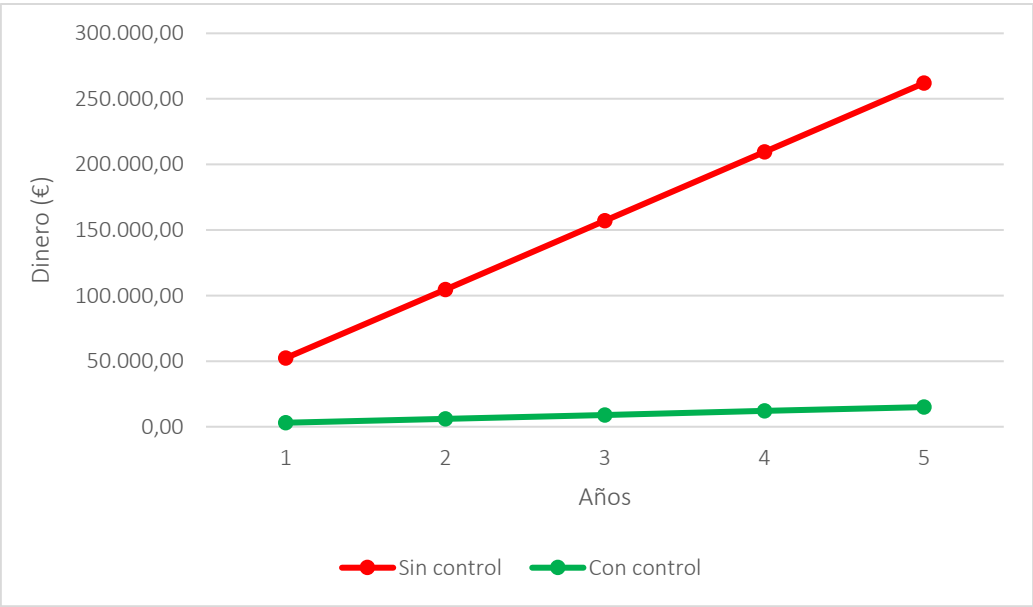



*Ilustración 277. Rentabilidad amenaza AUX1 - [I.10] activo S4*

## Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 365625,42 | 0 | 0 | 365625,42 | 731250,84 | 1096876,26 | 1462501,68 | 1828127,1 |
| 18281,27 | 75 | 359,4 | 18715,67 | 37356,34 | 55997,01 | 74637,68 | 93278,35 |

***Tabla 284. Rentabilidad amenaza AUX1 - [E.4] activo S4***

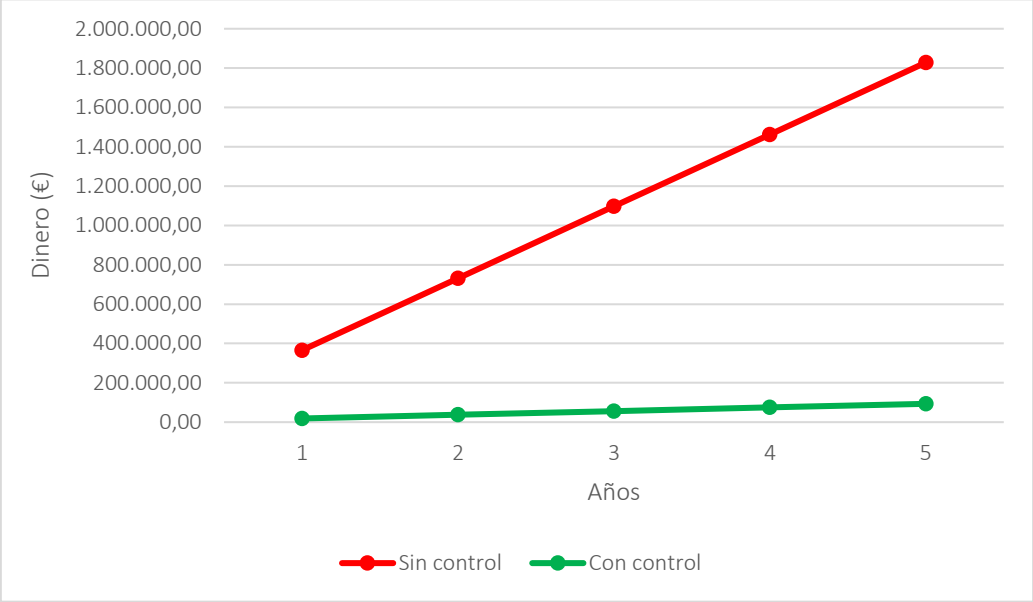



***Ilustración 278. Rentabilidad amenaza AUX1 - [E.4] activo S4***

## Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218751,41 | 0 | 0 | 1218751,41 | 2437502,8 | 3656254,23 | 4875005,64 | 6093757,05 |
| 60937,57 | 75 | 359,4 | 61371,97 | 122668,94 | 183965,91 | 245262,88 | 306559,85 |

***Tabla 285. Rentabilidad amenaza D1 - [E.15] activo S4***

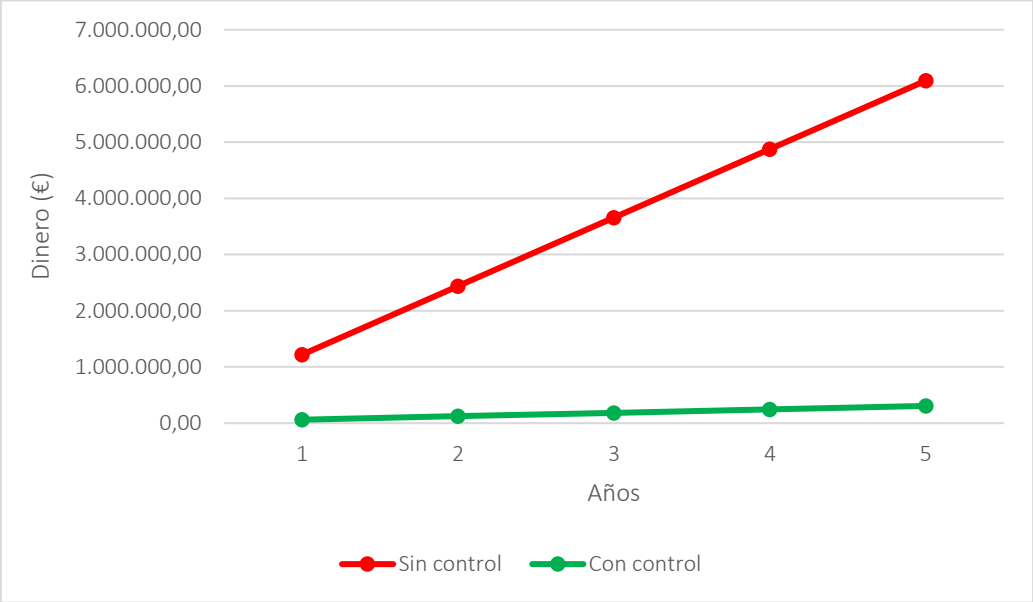



*Ilustración 279. Rentabilidad amenaza D1 - [E.15] activo S4*

## Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 12187,51 | 75 | 359,4 | 12621,91 | 25168,82 | 37715,73 | 50262,64 | 62809,55 |

*Tabla 286. Rentabilidad amenaza D1 - [E.18] activo S4*

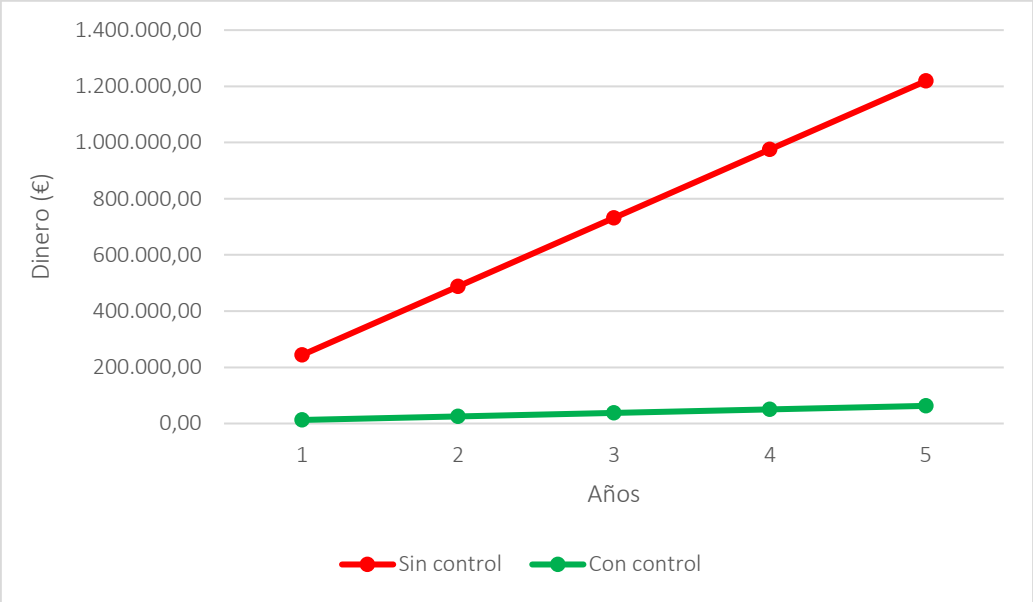



*Ilustración 280. Rentabilidad amenaza D1 - [E.18] activo S4*

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 12187,51 | 75 | 359,4 | 12621,91 | 25168,82 | 37715,73 | 50262,64 | 62809,55 |

*Tabla 287. Rentabilidad amenaza D1 - [A.18] activo S4*

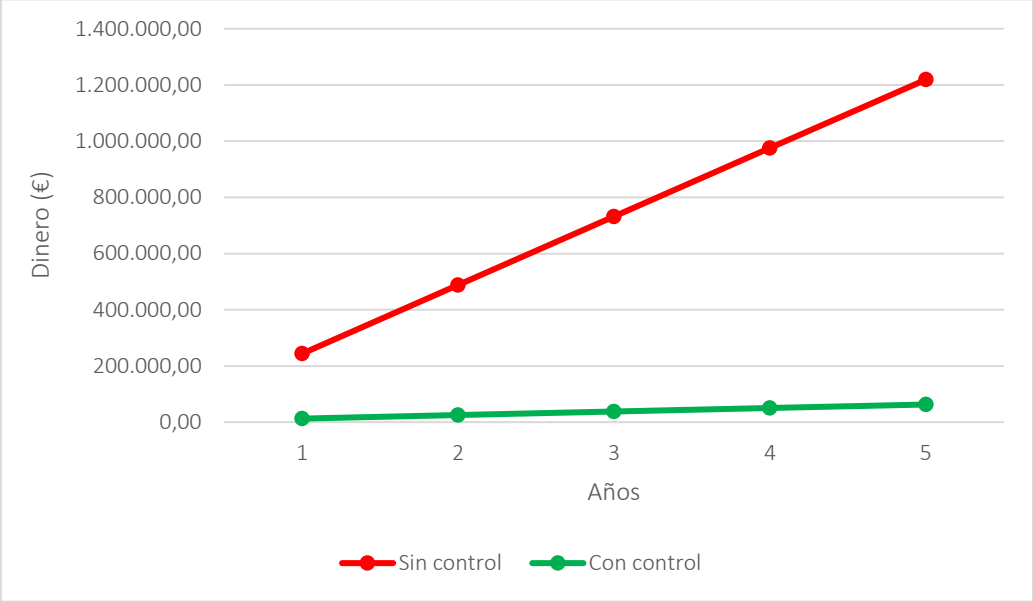



*Ilustración 281. Rentabilidad amenaza D1 - [A.18] activo S4*

## Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85312,6 | 0 | 0 | 85312,6 | 170625,2 | 255937,8 | 341250,4 | 426563 |
| 8531,26 | 75 | 359,4 | 8965,66 | 17856,32 | 26746,98 | 35637,64 | 44528,3 |

*Tabla 288. Rentabilidad amenaza SW1 - [A.18] activo S4*

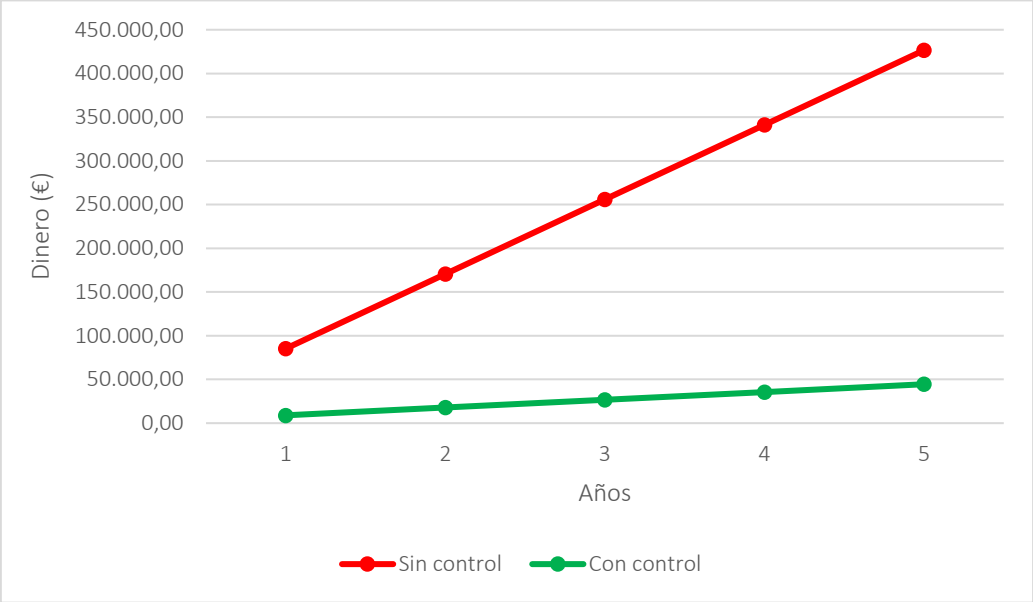



*Ilustración 282. Rentabilidad amenaza SW1 - [A.18] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2303,5 | 0 | 0 | 2303,5 | 4607 | 6910,5 | 9214 | 11517,5 |
| 115,17 | 75 | 359,4 | 549,57 | 1024,14 | 1498,71 | 1973,28 | 2447,85 |

*Tabla 289. Rentabilidad amenaza AUX1 - [I.5] activo S5*

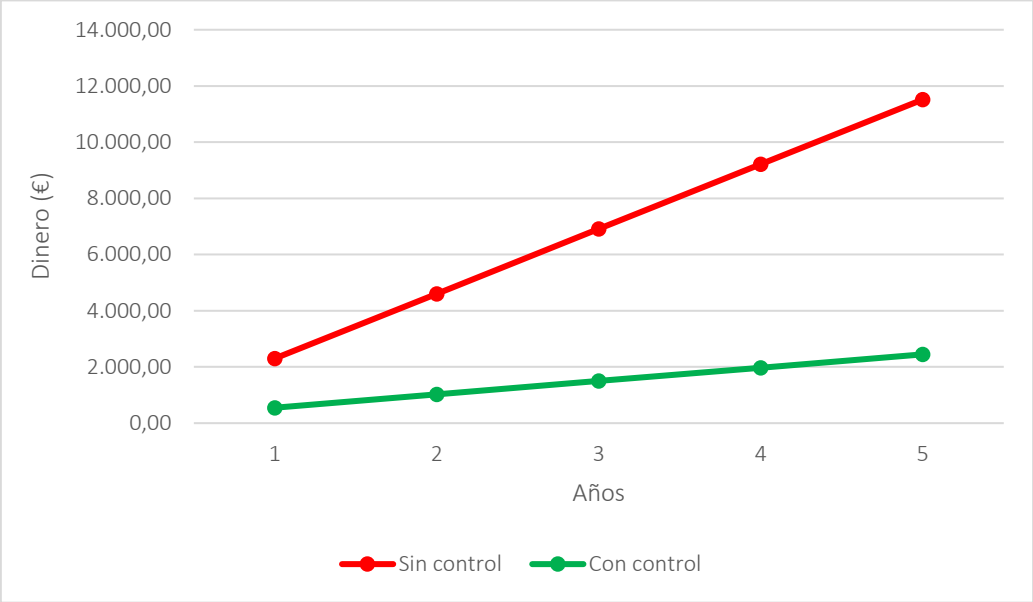



*Ilustración 283. Rentabilidad amenaza AUX1 - [I.5] activo S5*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 52407,67 | 0 | 0 | 52407,67 | 104815,34 | 157223,01 | 209630,68 | 262038,35 |
| 2620,38 | 75 | 359,4 | 3054,78 | 6034,56 | 9014,34 | 11994,12 | 14973,9 |

*Tabla 290. Rentabilidad amenaza AUX1 - [I.10] activo S5*

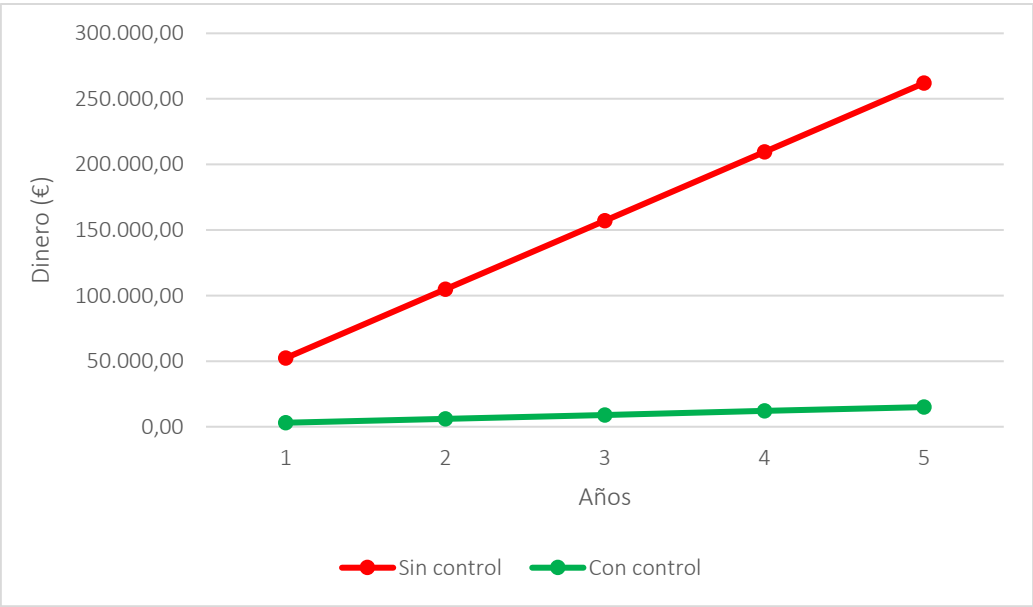



*Ilustración 284. Rentabilidad amenaza AUX1 - [I.10] activo S5*

## Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 365634,89 | 0 | 0 | 365634,89 | 731269,78 | 1096904,67 | 1462539,56 | 1828174,45 |
| 18281,74 | 75 | 359,4 | 18716,14 | 37357,28 | 55998,42 | 74639,56 | 93280,7 |

***Tabla 291. Rentabilidad amenaza AUX1 - [E.4] activo S5***

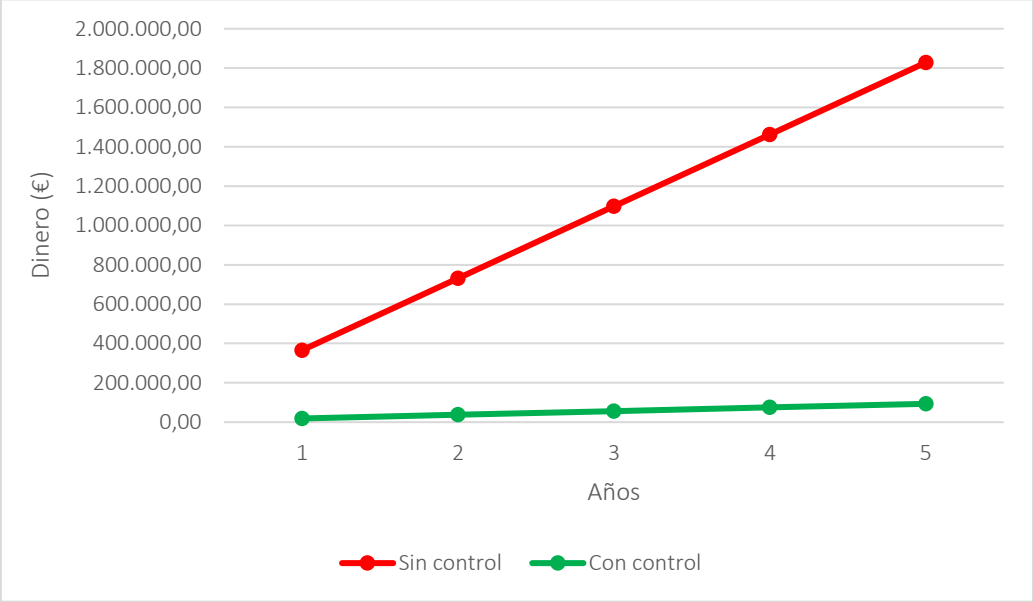



***Ilustración 285. Rentabilidad amenaza AUX1 - [E.4] activo S5***

## Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 60939,15 | 75 | 359,4 | 61373,55 | 122672,1 | 183970,65 | 245269,2 | 306567,75 |

***Tabla 292. Rentabilidad amenaza D1 - [E.15] activo S5***

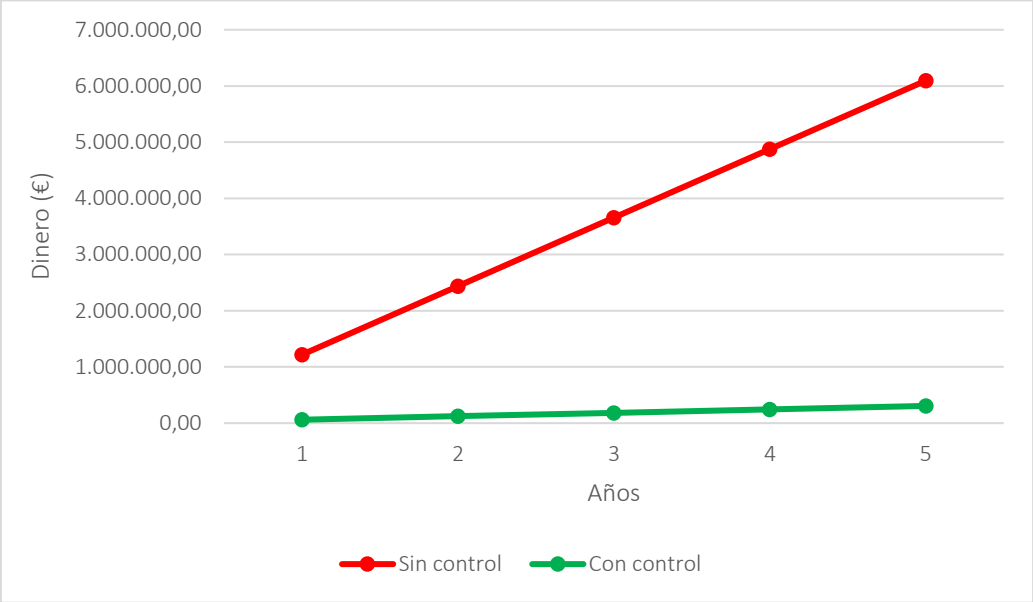



*Ilustración 286. Rentabilidad amenaza D1 - [E.15] activo S5*

Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 293. Rentabilidad amenaza D1 - [E.18] activo S5*

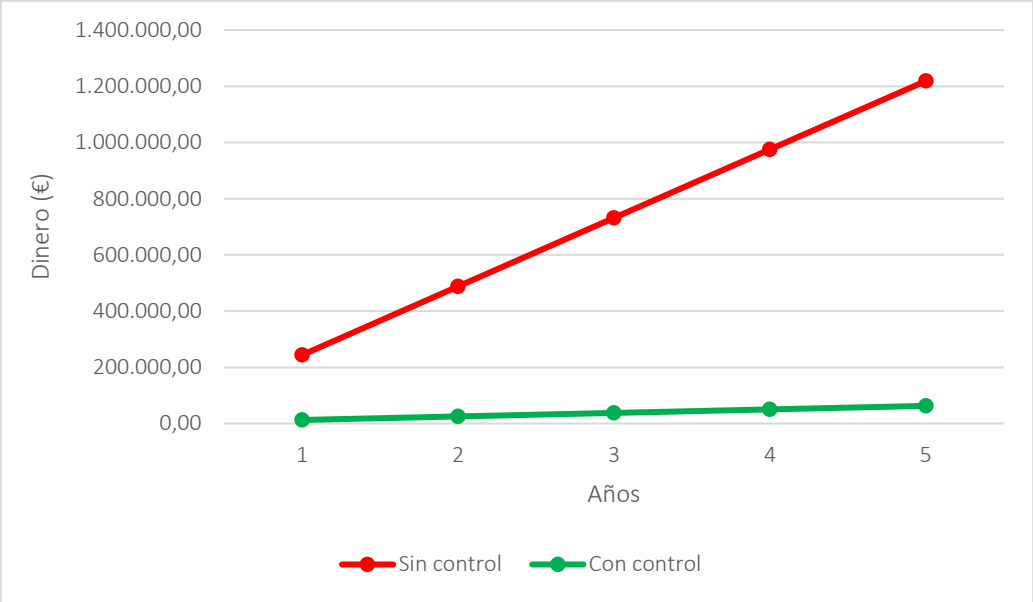



*Ilustración 287. Rentabilidad amenaza D1 - [E.18] activo S5*

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

***Tabla 294. Rentabilidad amenaza D1 - [A.18] activo S5***

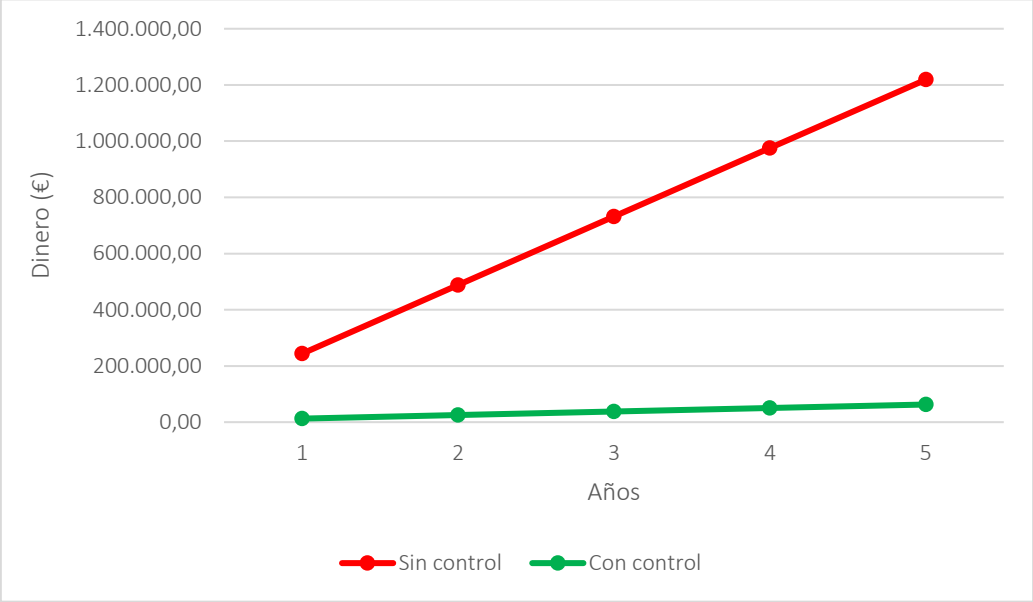



***Ilustración 288. Rentabilidad amenaza D1 - [A.18] activo S5***

## Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 4265,74 | 75 | 359,4 | 4700,14 | 9325,28 | 13950,42 | 18575,56 | 23200,7 |

***Tabla 295. Rentabilidad amenaza SW1 - [A.18] activo S5***

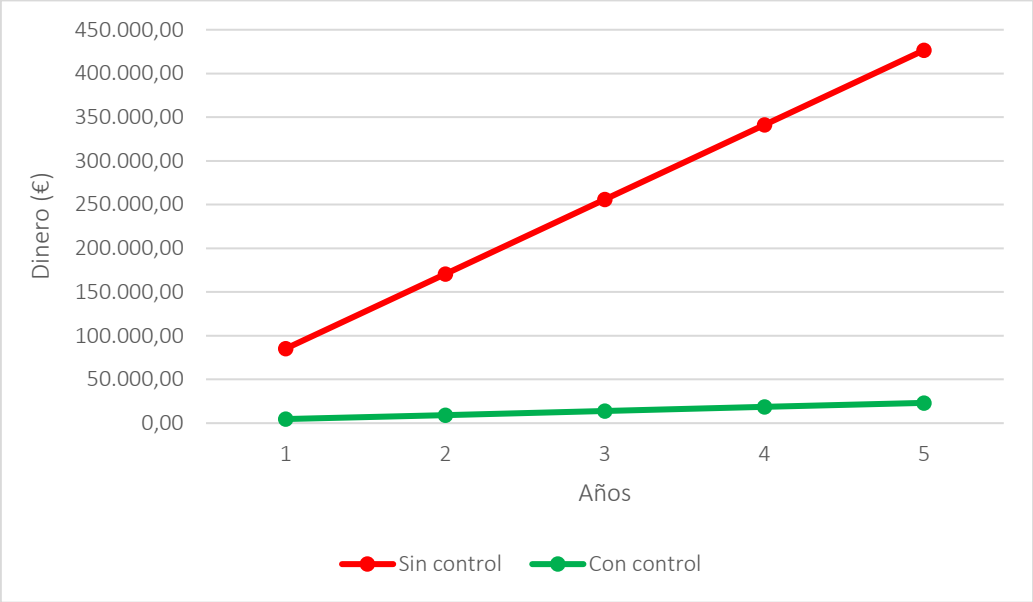



*Ilustración 289. Rentabilidad amenaza SW1 - [A.18] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: AUX1 – [I.5] Avería de origen físico o lógico

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 2303,5 | 0 | 0 | 2303,5 | 4607 | 6910,5 | 9214 | 11517,5 |
| 115,17 | 75 | 359,4 | 549,57 | 1024,14 | 1498,71 | 1973,28 | 2447,85 |

*Tabla 296. Rentabilidad amenaza AUX1 - [I.5] activo S6*

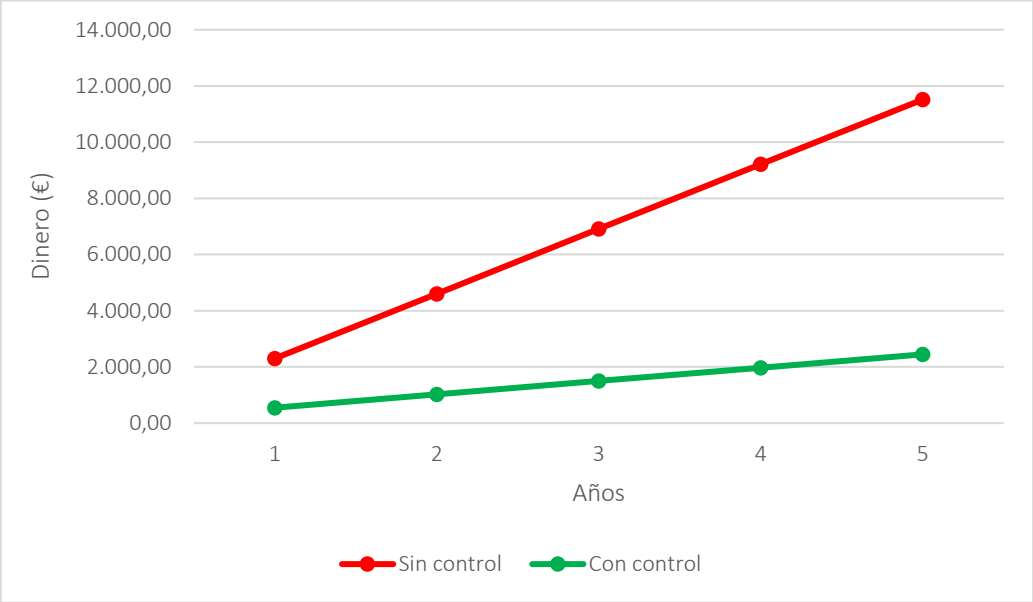



*Ilustración 290. Rentabilidad amenaza AUX1 - [I.5] activo S6*

Amenaza: AUX1 – [I.10] Degradación de los soportes de almacenamiento de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 52407,67 | 0 | 0 | 52407,67 | 104815,34 | 157223,01 | 209630,68 | 262038,35 |
| 2620,38 | 75 | 359,4 | 3054,78 | 6034,56 | 9014,34 | 11994,12 | 14973,9 |

*Tabla 297. Rentabilidad amenaza AUX1 - [I.10] activo S6*

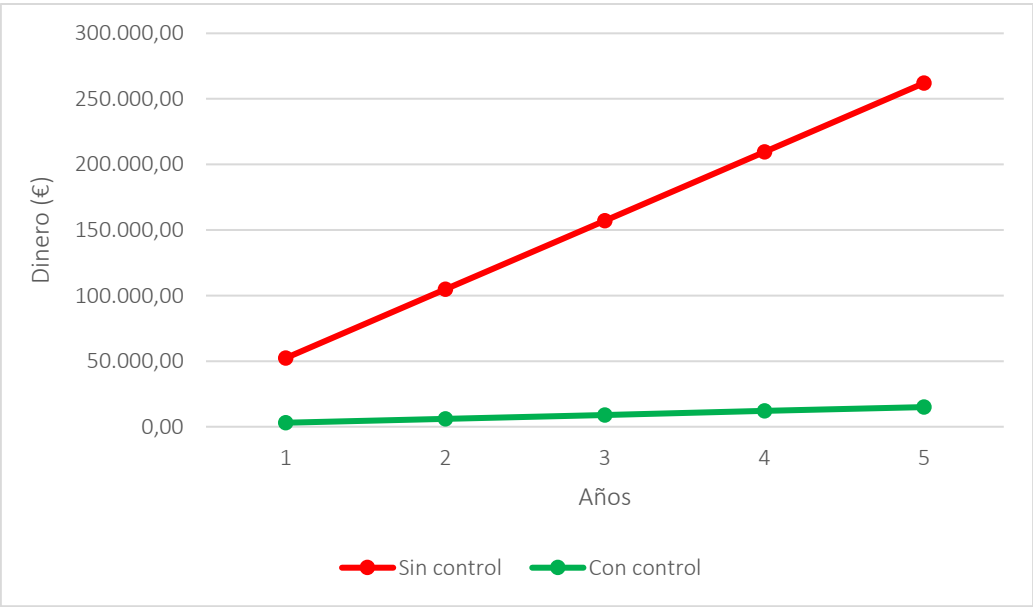



*Ilustración 291. Rentabilidad amenaza AUX1 - [I.10] activo S6*

## Amenaza: AUX1 – [E.4] Errores de configuración

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 365634,89 | 0 | 0 | 365634,89 | 731269,78 | 1096904,67 | 1462539,56 | 1828174,45 |
| 18281,74 | 75 | 359,4 | 18716,14 | 37357,28 | 55998,42 | 74639,56 | 93280,7 |

*Tabla 298. Rentabilidad amenaza AUX1 - [E.4] activo S6*

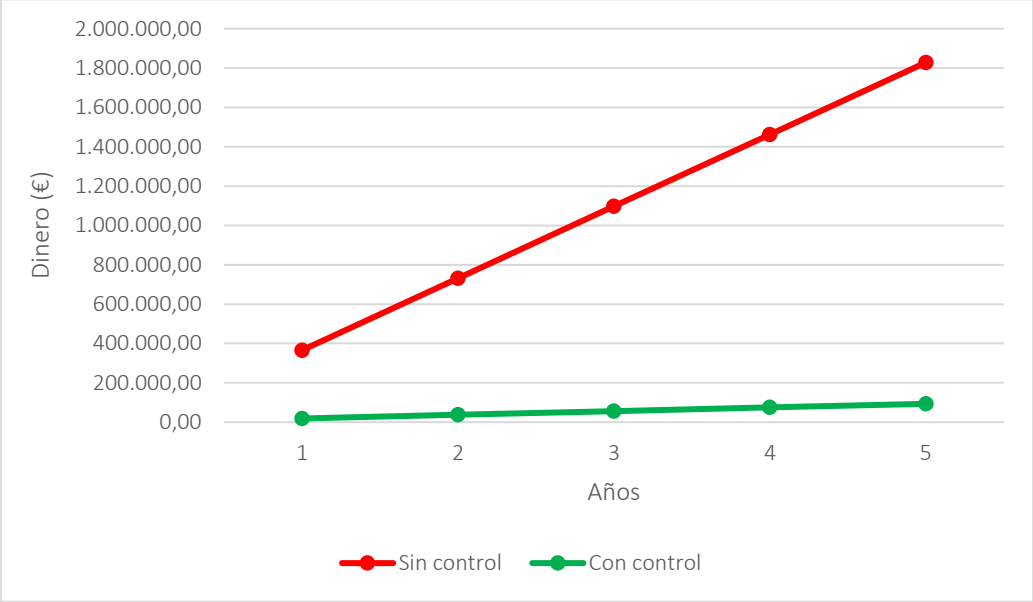



*Ilustración 292. Rentabilidad amenaza AUX1 - [E.4] activo S6*

## Amenaza: D1 – [E.15] Alteración accidental de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 1218782,98 | 0 | 0 | 1218782,98 | 2437566 | 3656348,94 | 4875131,92 | 6093914,9 |
| 60939,15 | 75 | 359,4 | 61373,55 | 122672,1 | 183970,65 | 245269,2 | 306567,75 |

*Tabla 299. Rentabilidad amenaza D1 - [E.15] activo S6*

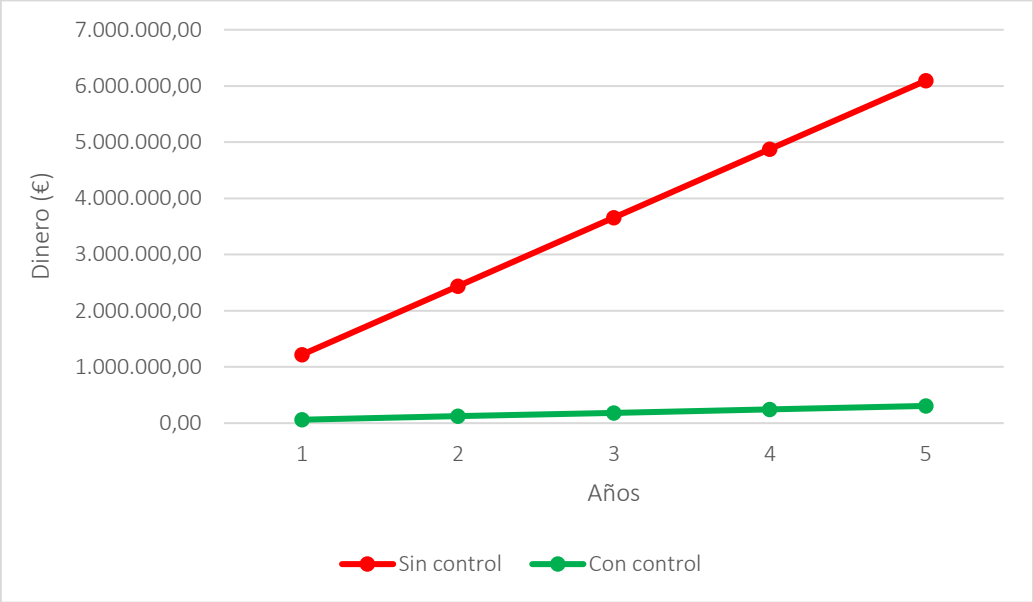



*Ilustración 293. Rentabilidad amenaza D1 - [E.15] activo S6*

## Amenaza: D1 – [E.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 300. Rentabilidad amenaza D1 - [E.18] activo S6*

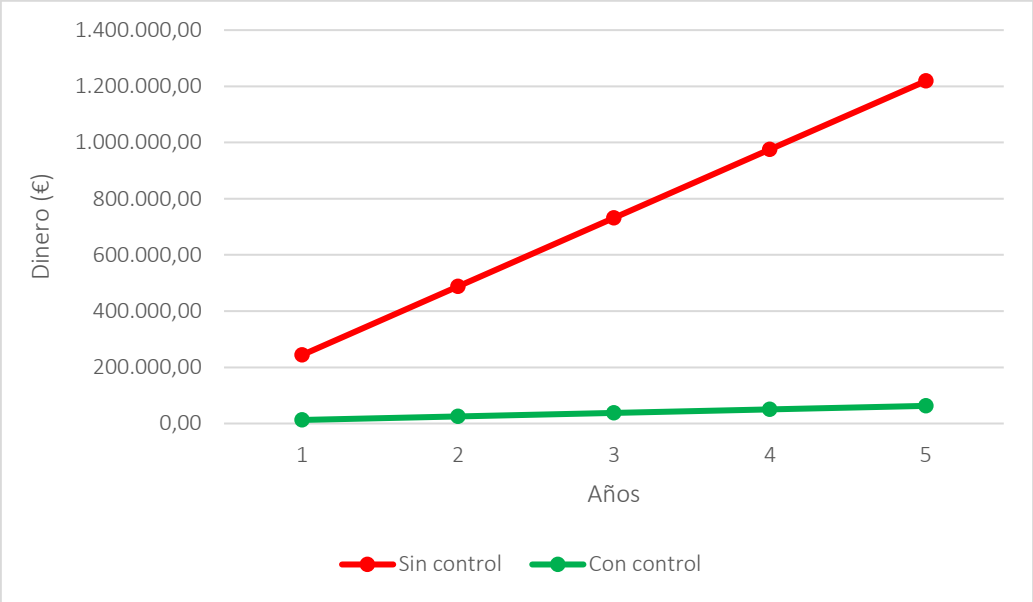



*Ilustración 294. Rentabilidad amenaza D1 - [E.18] activo S6*

## Amenaza: D1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 12187,83 | 75 | 359,4 | 12622,23 | 25169,46 | 37716,69 | 50263,92 | 62811,15 |

*Tabla 301. Rentabilidad amenaza D1 - [A.18] activo S6*

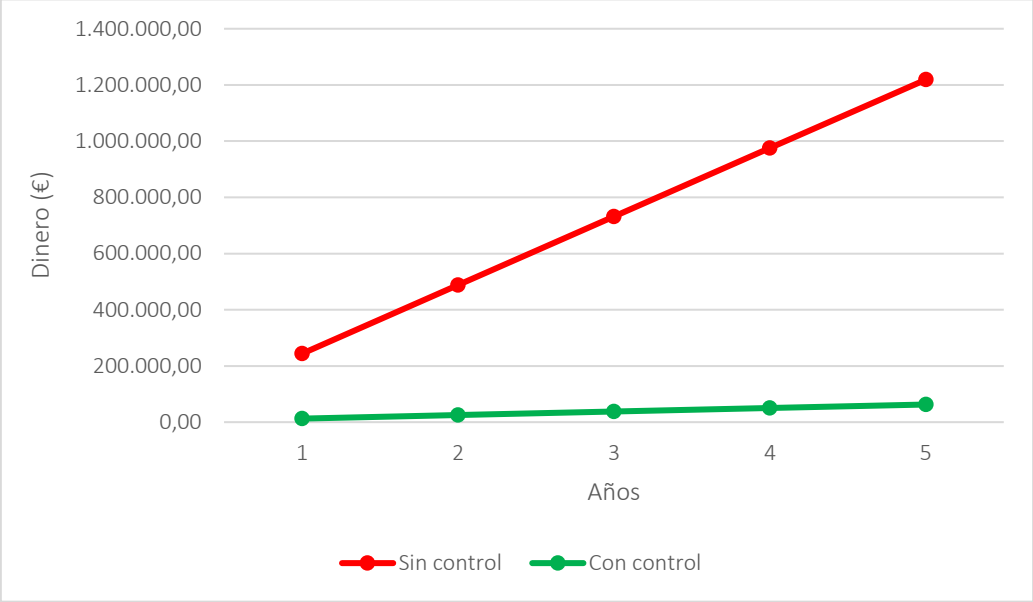



*Ilustración 295. Rentabilidad amenaza D1 - [A.18] activo S6*

## Amenaza: SW1 – [A.18] Destrucción de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 4265,74 | 75 | 359,4 | 4700,14 | 9325,28 | 13950,42 | 18575,56 | 23200,7 |

*Tabla 302. Rentabilidad amenaza SW1 - [A.18] activo S6*

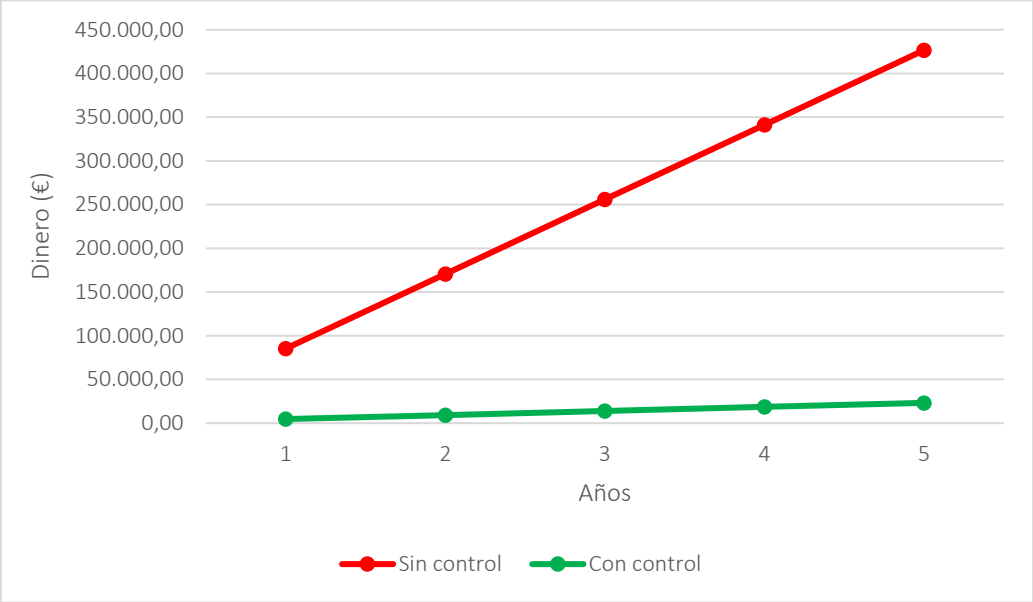



*Ilustración 296. Rentabilidad amenaza SW1 - [A.18] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

#### 2.1.5.7 Séptimo control

##### 2.1.5.7.1 Título

Control de cumplimiento de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

##### 2.1.5.7.2 Finalidad

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido en el artículo 18.4 de la Constitución española. El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismo o lesivo para la dignidad y los derechos de los afectados.

Por lo tanto, como hemos estudiado anteriormente, hemos podido comprobar que hay un gran número de amenazas que puedan darse en nuestra empresa y poner en riesgo el cumplimiento de dicha ley, y, por tanto, suponer un impacto muy grave o incluso irreparable para la misma.

Así que en este control vamos a detallar las medidas que debemos cumplir para que no hay ningún tipo de problema con respecto al cumplimiento de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

#### 2.1.5.7.3 Empresa

“Sanitaria AMS S.L.”

#### 2.1.5.7.4 Leyes aplicables

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

#### 2.1.5.7.5 Normas aplicables

No hay referencias de normas para este control.

#### 2.1.5.7.6 Descripción del control

Vamos a describir cuales son los pasos que se deben seguir para realizar el cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE, 2018)

¿Cómo se cumple con la LOPD?

El primer paso para cumplir con la LOPD es remitir, a través de los formularios correspondientes, los ficheros con los datos de carácter personal a la Agencial Española de Protección de Datos (AEPD).

Se trata de notificar el tipo de datos que tratamos en nuestro negocio (no se facilitan los datos personales en sí, si no los campos que se manejan). Sin embargo, no basta con darlos de alta, sino que hay que mantenerlos actualizados.

Además, a la hora de dar de alta los ficheros, debemos tener en cuenta que existen varios grados de seguridad, que varían según la naturaleza de los datos tratados.

¿Qué debo tener además de los ficheros inscritos?

Como hemos mencionado anteriormente, además de notificar a la AEPD sobre los ficheros, debemos contar con una copia de seguridad actualiza y aplicar las medidas y procedimiento que estable el reglamento.

No disponer de un documento de seguridad significaría que no estamos adoptando las medidas necesarias para evitar la alteración, robo o pérdida de datos, lo cual se considera una infracción grave.

En este apartado vamos a detallar las principales normativas que una empresa debe seguir para cumplir con Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Toda aquella empresa, autónomo, comercio, que recoja datos de personas físicas se encuentra obligada a cumplir con las normativas correspondientes a la LOPD. En este sentido, entre las obligaciones que las entidades deben realizar en su negocio para adaptar su actividad se encuentran:

#### 2.1.5.7.7 Responsables

Dueños de la empresa, estos serán los encargados de se cumple la ley dentro de la empresa y además la cumplan todos los trabajadores de la misma, debe comprobar continuamente que se están siguiendo las pautas y medidas correctas.

#### 2.1.5.7.8 Dispositivos

No es necesario ningún dispositivo, ya que se trata de un control que se lleva a cabo siguiendo una serie de medidas descritas anteriormente y además en el Boletín Oficial del Estado.

#### 2.1.5.7.9 Costes

- **Implantación:** 0 €, ya que realizar estas medidas en la empresa simplemente cuestan el esfuerzo de los trabajadores de ella.
- **Ejecución y mantenimiento:** 0 €, no supone ningún gasto por el mismo motivo que anteriormente.
- **Búsquedas de irregularidades:** En caso de que cualquier trabajador note que cualquier anomalía, deberá comunicárselo a los dueños de la empresa y estos deberán informar al trabajador/a de las pautas que tiene que seguir para la correcta realización de dicho control.

#### 2.1.5.7.10 Rentabilidad

Todo lo que tenga que ver con los datos de la empresa, ya sea uso, creación, modificación, actualización o borrado, se deben seguir una serie de pautas para cumplir con la LOPD y no tener consecuencias graves en la empresa, por lo tanto, hemos estudiado cuales pueden ser algunas de las consecuencias que podemos tener. Así que, con este control, nos protegerá de todas estas consecuencias que se puedan dar en nuestro SI y nuestra empresa.

A continuación, vamos a realizar un estudio de rentabilidad para ver si es rentable utilizar este control en nuestro SI, vamos a estudiar cómo afecta a cada uno de nuestros activos y sobre que amenazas se ejecuta.

Determinamos que el control tiene una eficacia del 90 %, ya que puede fallar por:

- Un fallo de cualquier trabajador de la empresa.
- Olvido de cualquier responsable
- No cumplimiento de cualquiera de los aspectos de la LOPD.

Activo: Información de pacientes (S1)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 54575,6 | 0 | 0 | 54575,6 | 109151,2 | 163726,8 | 218302,4 | 272878 |
| 5457,56 | 0 | 0 | 5457,56 | 10915,12 | 16372,68 | 21830,24 | 27287,8 |

*Tabla 303. Rentabilidad amenaza AUX1 - [A.11] activo S1*

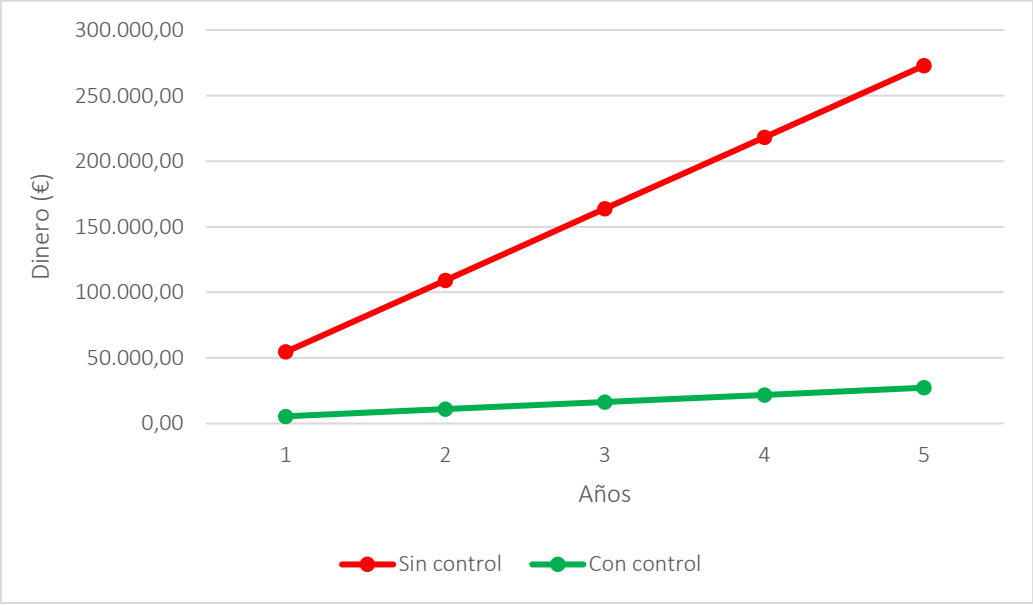



*Ilustración 297. Rentabilidad amenaza AUX1 - [A.11] activo S1*

## Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

***Tabla 304. Rentabilidad amenaza D1 - [E.19] activo S1***

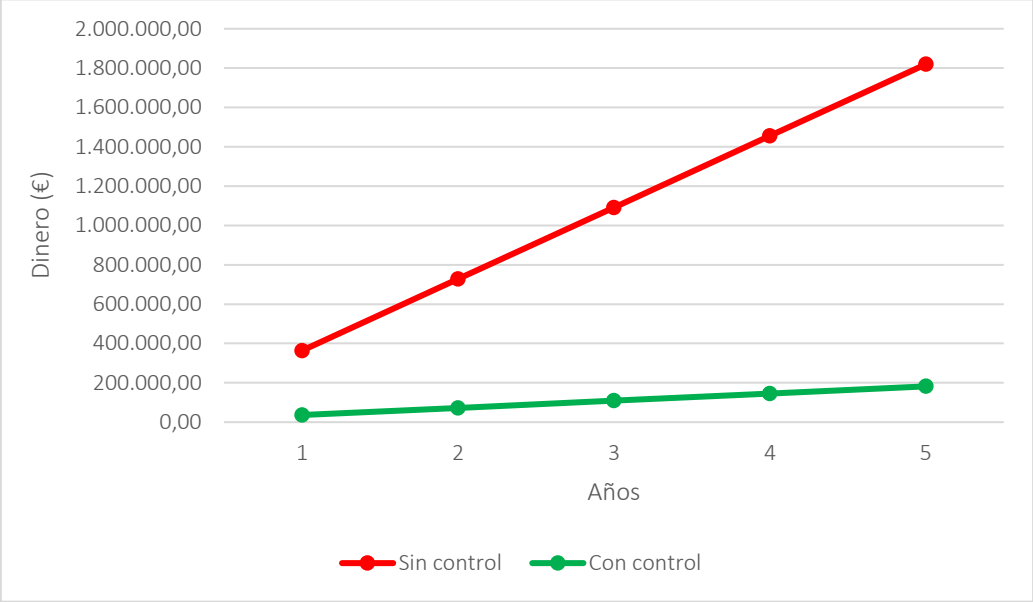



***Ilustración 298. Rentabilidad amenaza D1 - [E.19] activo S1***

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 909593,31 | 0 | 0 | 909593,31 | 1819186,6 | 2728779,93 | 3638373,24 | 4547966,55 |
| 90959,33 | 0 | 0 | 90959,33 | 181918,66 | 272877,99 | 363837,32 | 454796,65 |

***Tabla 305. Rentabilidad amenaza D1 - [A.11] activo S1***

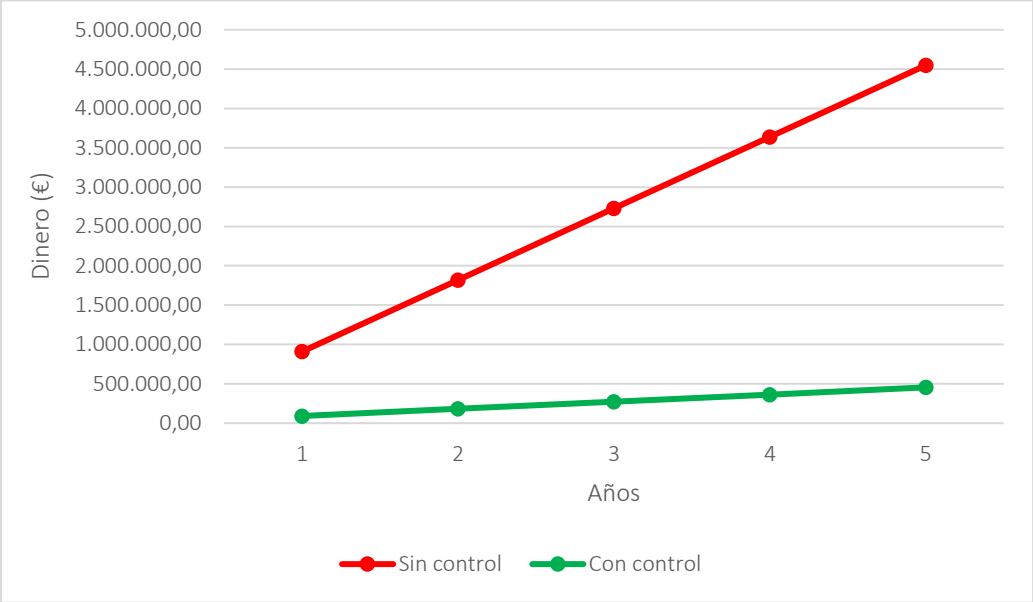



*Ilustración 299. Rentabilidad amenaza D1 - [A.11] activo S1*

Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

*Tabla 306. Rentabilidad amenaza D1 - [A.18] activo S1*

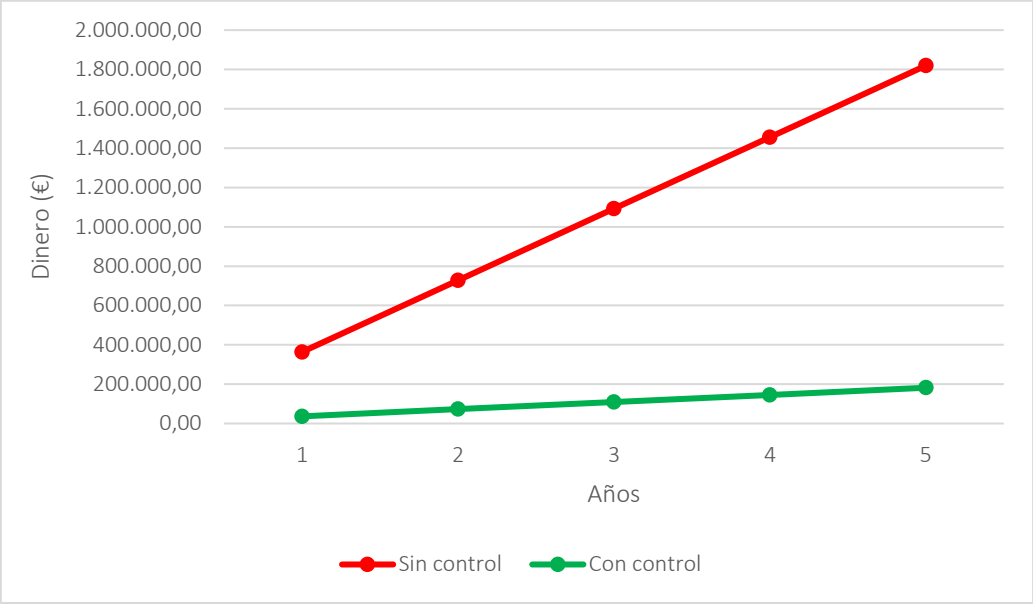



*Ilustración 300. Rentabilidad amenaza D1 - [A.18] activo S1*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 363837,32 | 0 | 0 | 363837,32 | 727674,64 | 1091511,96 | 1455349,28 | 1819186,6 |
| 36383,73 | 0 | 0 | 36383,73 | 72767,46 | 109151,19 | 145534,92 | 181918,65 |

***Tabla 307. Rentabilidad amenaza D1 - [A.19] activo S1***

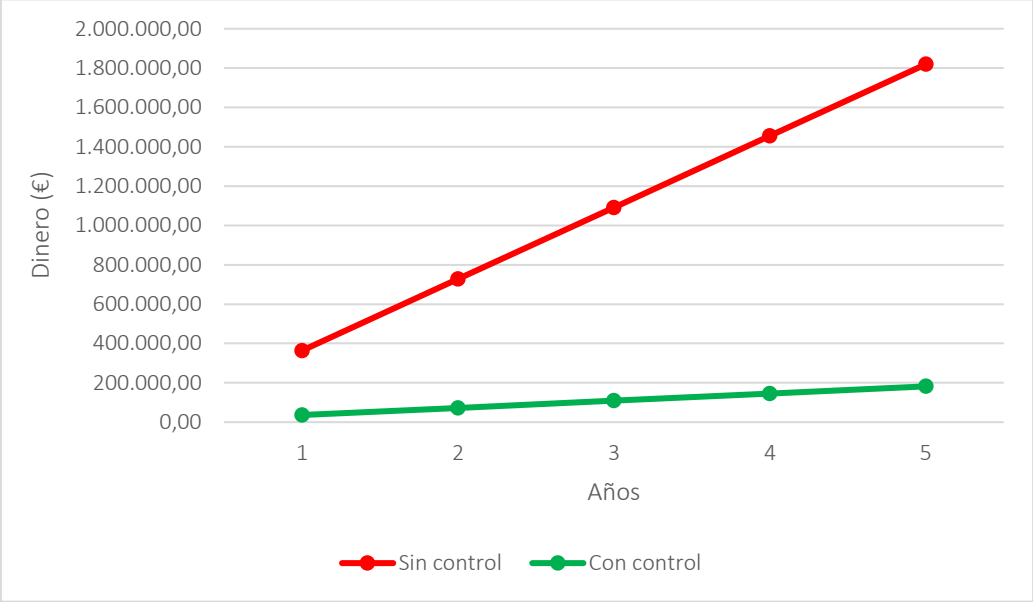



***Ilustración 301. Rentabilidad amenaza D1 - [A.19] activo S1***

## Amenaza: SW1 – [A.18] Destrucción de información

***Tabla 308. Rentabilidad amenaza SW1 - [A.18] activo S1***

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 127343,06 | 0 | 0 | 127343,06 | 254686,12 | 382029,18 | 509372,24 | 636715,3 |
| 12734,31 | 0 | 0 | 12734,31 | 25468,62 | 38202,93 | 50937,24 | 63671,55 |

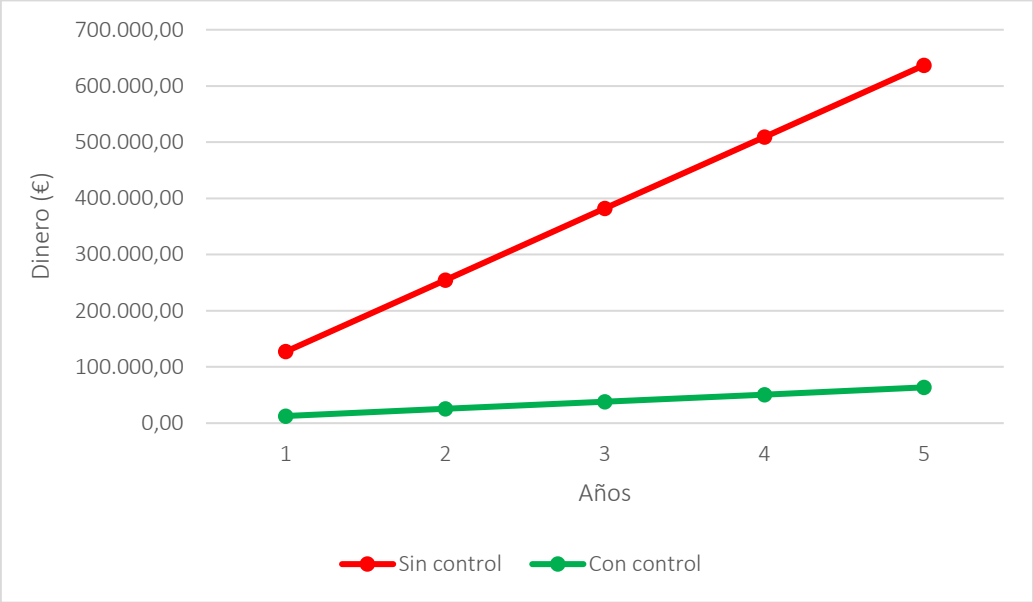



*Ilustración 302. Rentabilidad amenaza SW1 - [A.18] activo S1*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 127343,06 | 0 | 0 | 127343,06 | 254686,12 | 382029,18 | 509372,24 | 636715,3 |
| 12734,31 | 0 | 0 | 12734,31 | 25468,62 | 38202,93 | 50937,24 | 63671,55 |

*Tabla 309. Rentabilidad amenaza SW1 - [A.19] activo S1*

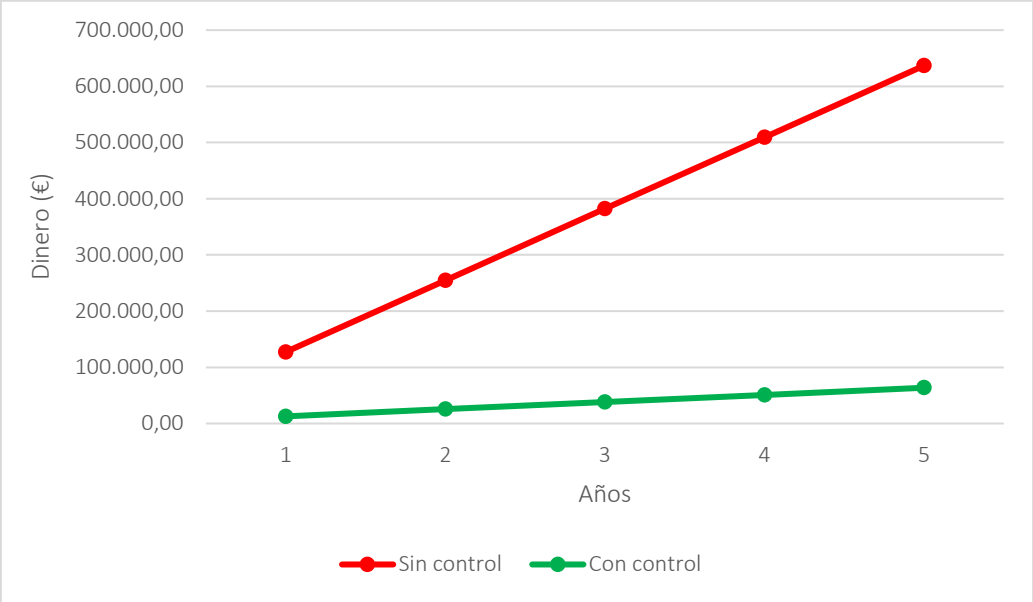



*Ilustración 303. Rentabilidad amenaza SW1 - [A.19] activo S1*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 181918,66 | 0 | 0 | 181918,66 | 363837,32 | 545755,98 | 727674,64 | 909593,3 |
| 18191,87 | 0 | 0 | 18191,87 | 36383,74 | 54575,61 | 72767,48 | 90959,35 |

*Tabla 310. Rentabilidad amenaza SRVD1 - [A.11] activo S1*

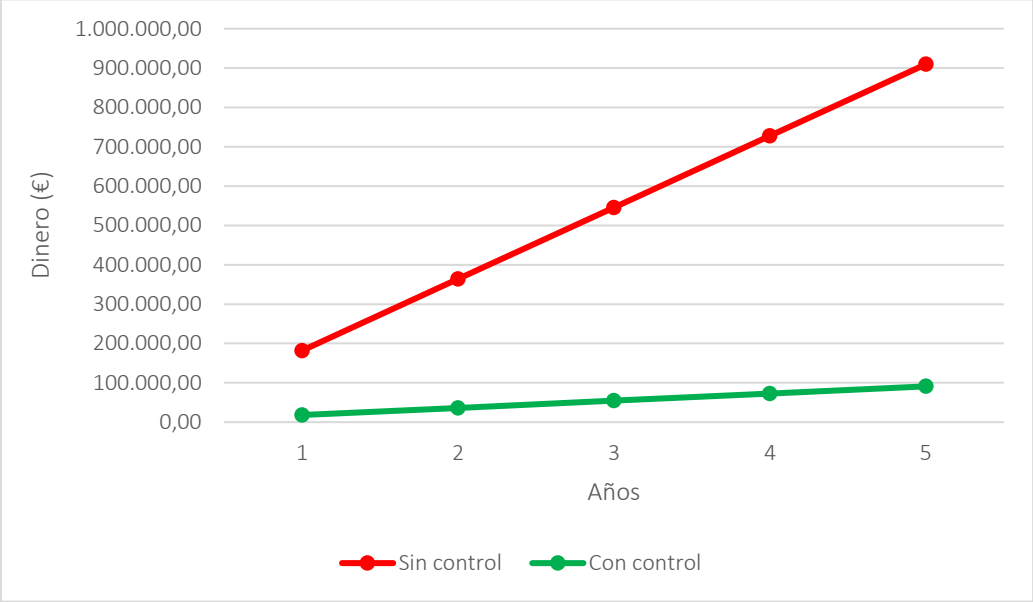



*Ilustración 304. Rentabilidad amenaza SRVD1 - [A.11] activo S1*

## Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 6063,96 | 0 | 0 | 6063,96 | 12127,92 | 18191,88 | 24255,84 | 30319,8 |
| 606,4 | 0 | 0 | 606,4 | 1212,8 | 1819,2 | 2425,6 | 3032 |

*Tabla 311. Rentabilidad amenaza T1 - [A.11] activo S1*

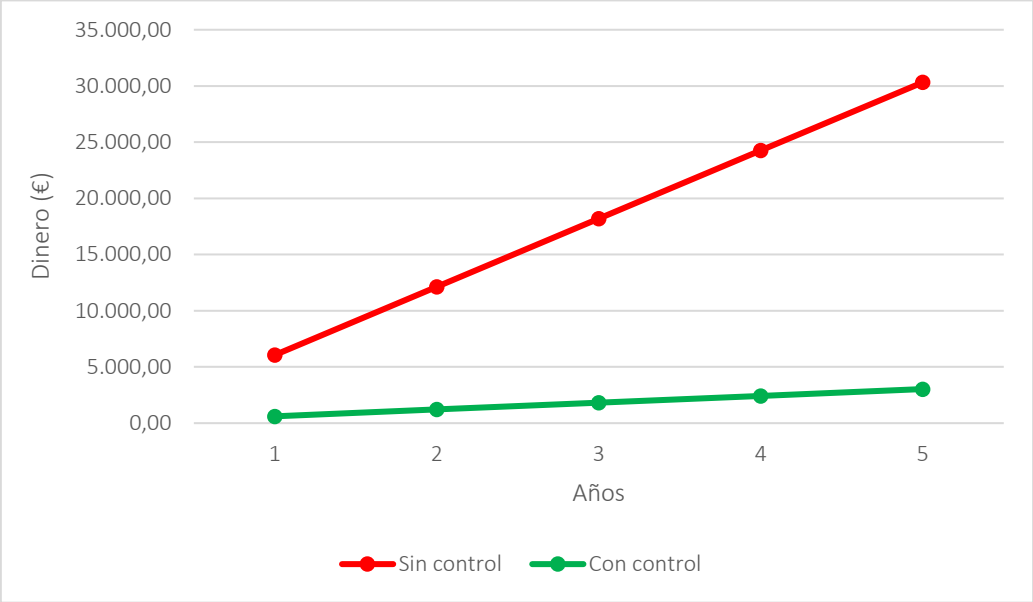



*Ilustración 305. Rentabilidad amenaza T1 - [A.11] activo S1*

Como podemos observar en todos los gráficos que hemos estudiado para el primer activo, “Información de pacientes”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Pedidos (S2)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 312. Rentabilidad amenaza AUX1 - [A.11] activo S2*

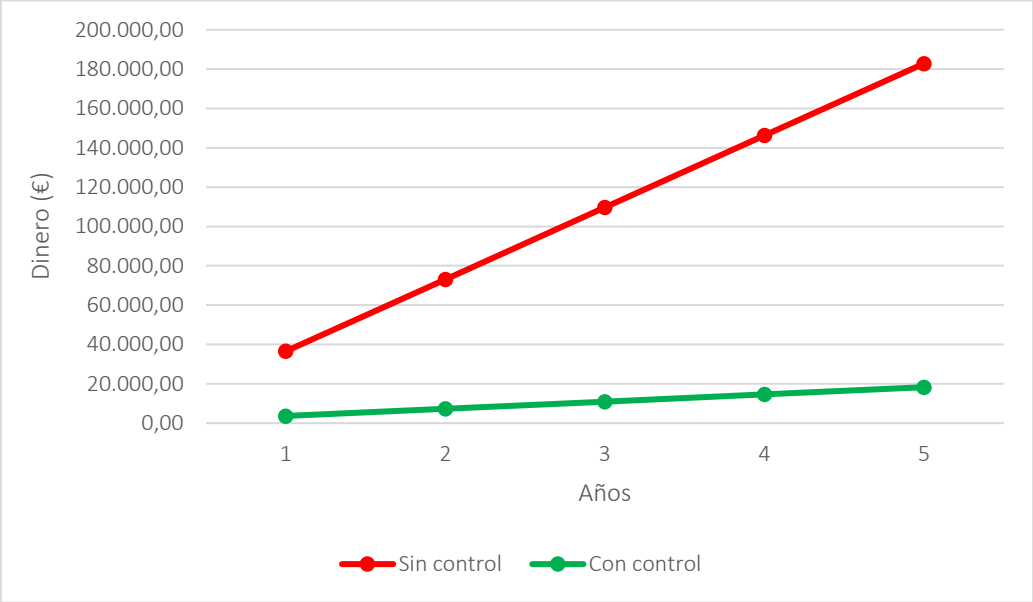



*Ilustración 306. Rentabilidad amenaza AUX1 - [A.11] activo S2*

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 313. Rentabilidad amenaza D1 - [E.19] activo S2*

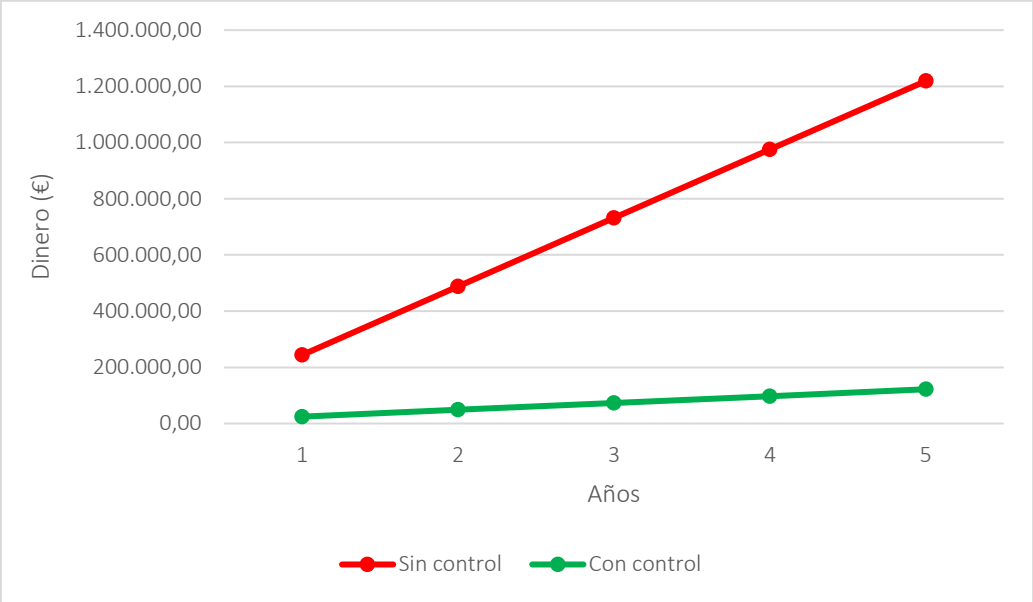



*Ilustración 307. Rentabilidad amenaza D1 - [E.19] activo S2*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

*Tabla 314. Rentabilidad amenaza D1 - [A.11] activo S2*

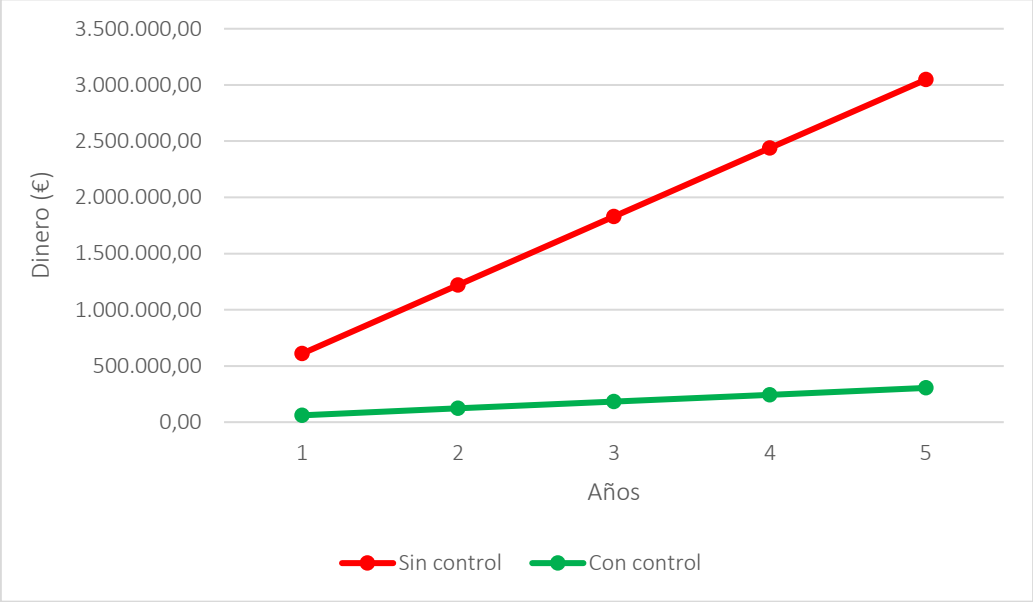



*Ilustración 308. Rentabilidad amenaza D1 - [A.11] activo S2*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 315. Rentabilidad amenaza D1 - [A.18] activo S2*

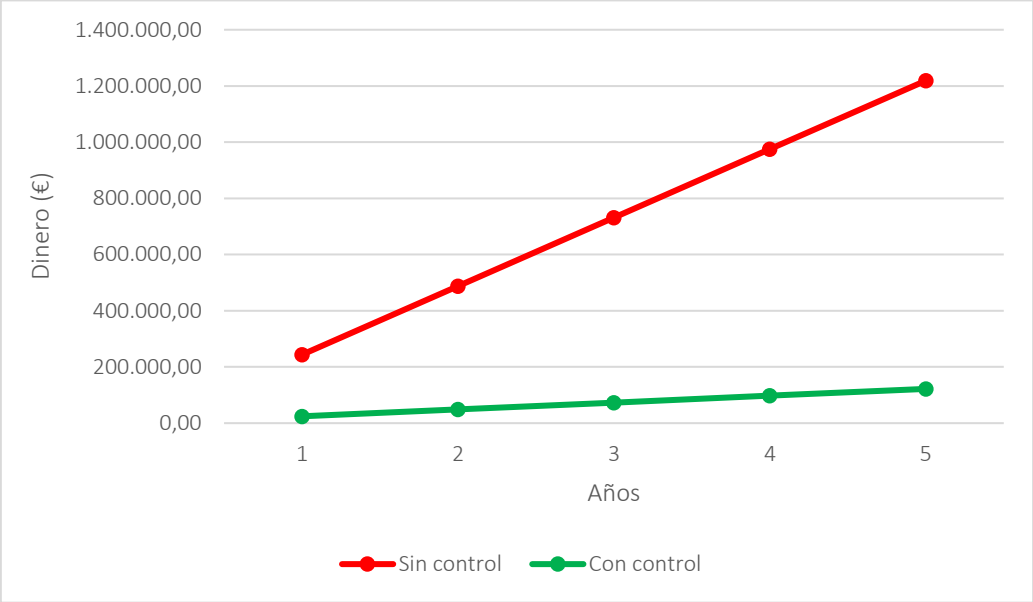



*Ilustración 309. Rentabilidad amenaza D1 - [A.18] activo S2*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 316. Rentabilidad amenaza D1 - [A.19] activo S2*

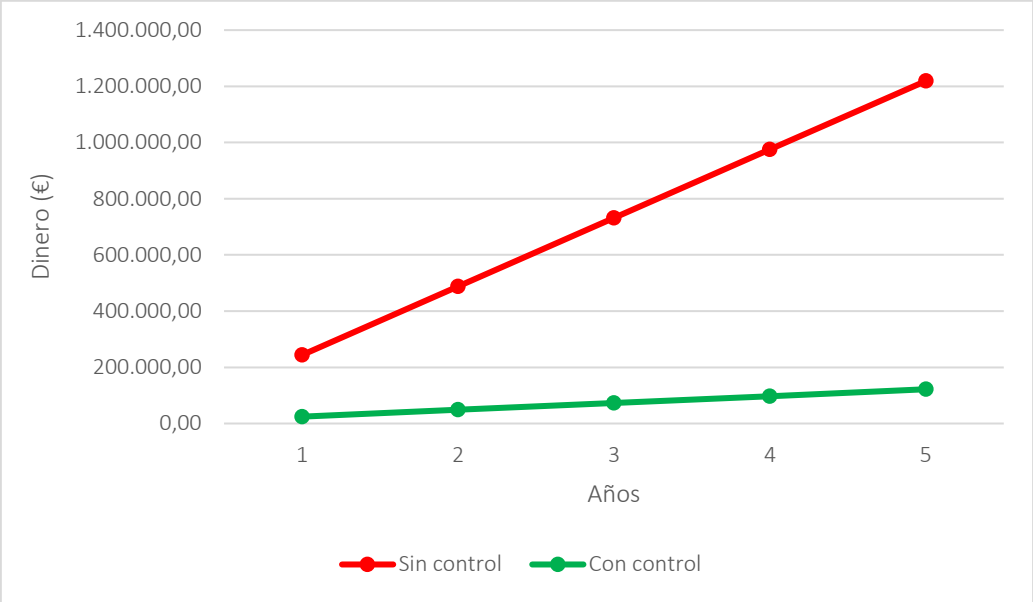



*Ilustración 310. Rentabilidad amenaza D1 - [A.19] activo S2*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 317. Rentabilidad amenaza SW1 - [A.18] activo S2*

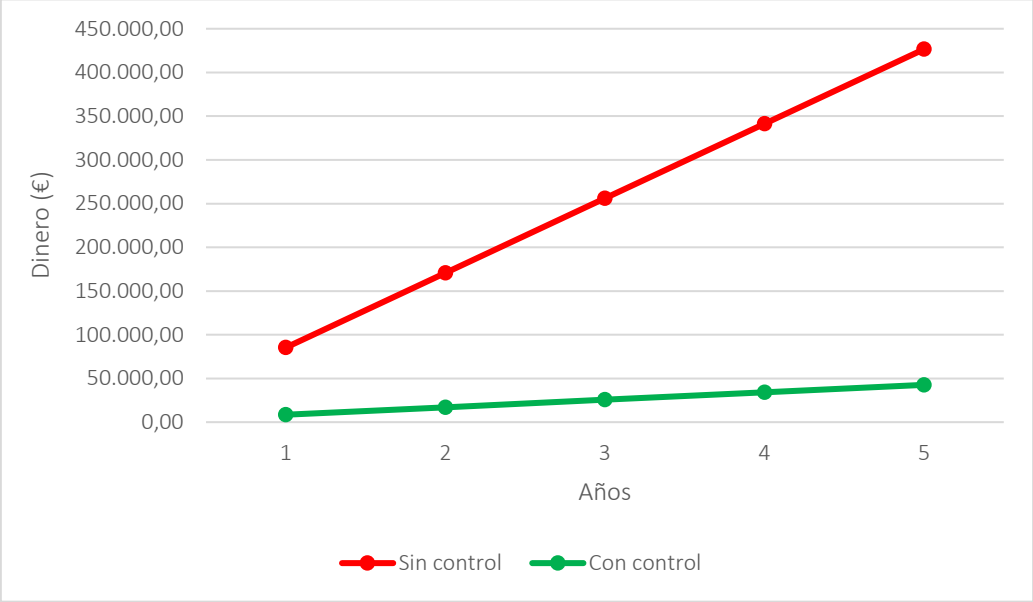



*Ilustración 311. Rentabilidad amenaza SW1 - [A.18] activo S2*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 318. Rentabilidad amenaza SW1 - [A.19] activo S2*

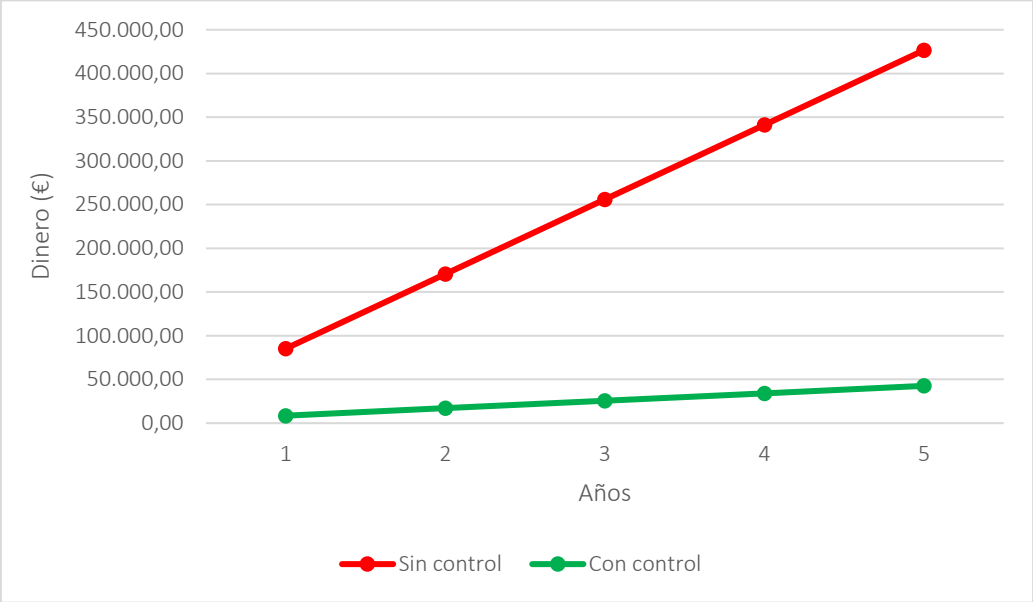



*Ilustración 312. Rentabilidad amenaza SW1 - [A.19] activo S2*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 319. Rentabilidad amenaza SRVD1 - [A.11] activo S2*

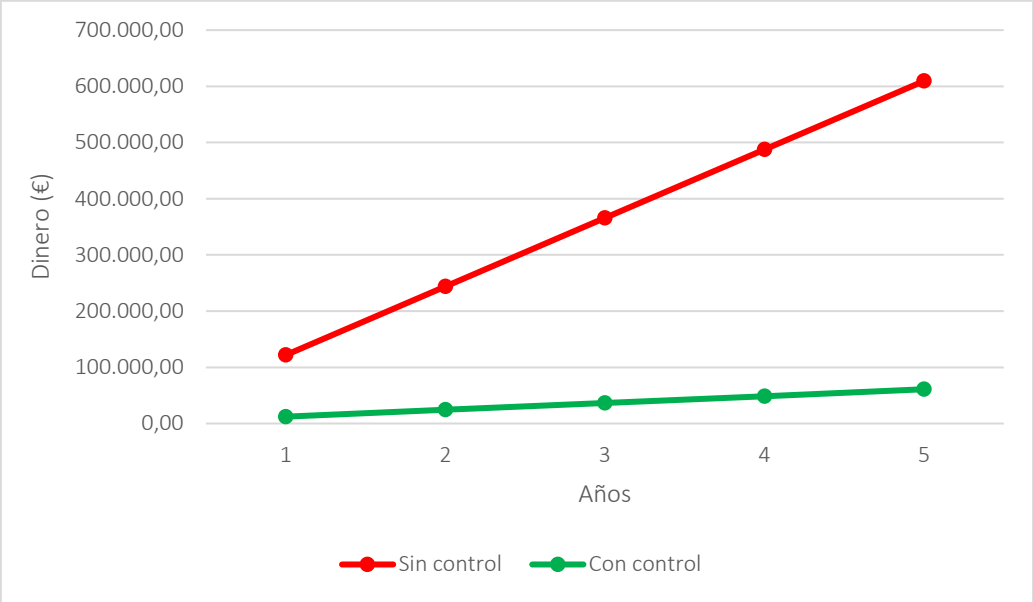



*Ilustración 313. Rentabilidad amenaza SRVD1 - [A.11] activo S2*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 320. Rentabilidad amenaza T1 - [A.11] activo S2*

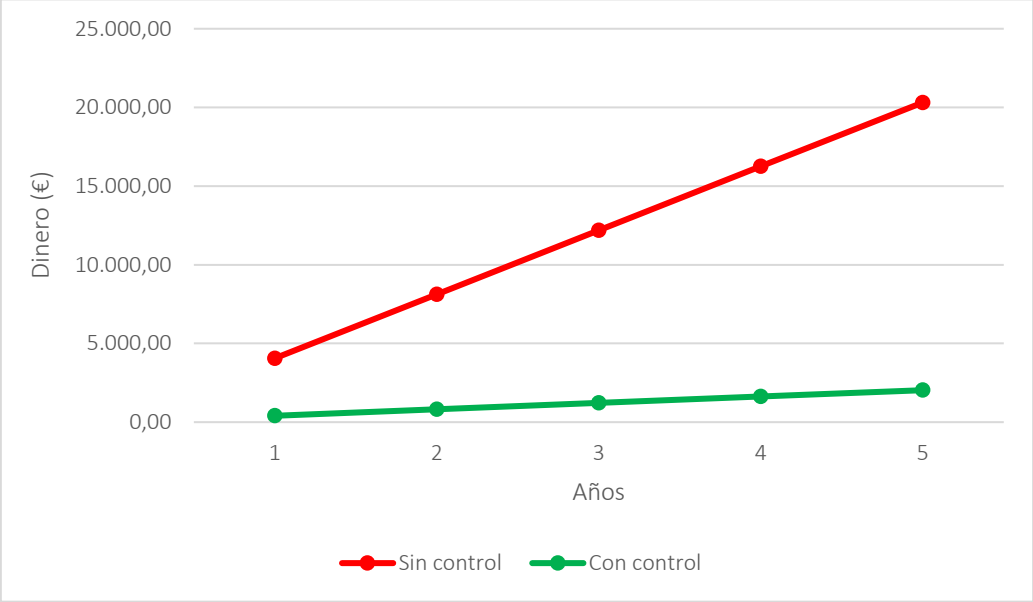



*Ilustración 314. Rentabilidad amenaza T1 - [A.11] activo S2*

Como podemos observar en todos los gráficos que hemos estudiado para el segundo activo, “Pedidos”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Citas (S3)

Amenaza: AUX1 – [A.11] Acceso no autorizado

*Tabla 321. Rentabilidad amenaza AUX1 - [A.11] activo S3*

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

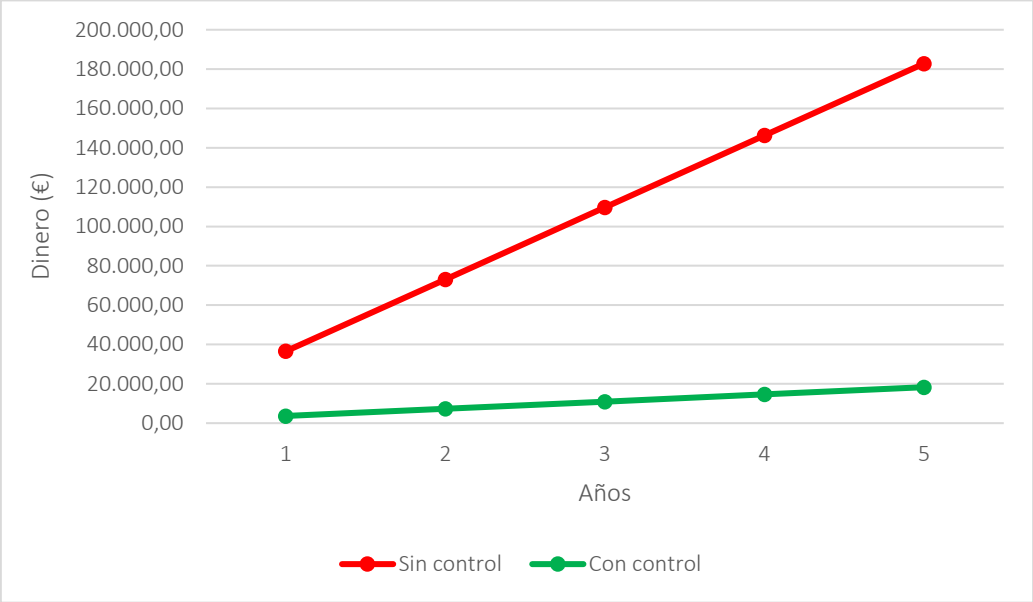



*Ilustración 315. Rentabilidad amenaza AUX1 - [A.11] activo S3*

## Amenaza: D1 – [E.19] Fugas de información

*Tabla 322. Rentabilidad amenaza D1 - [E.19] activo S3*

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

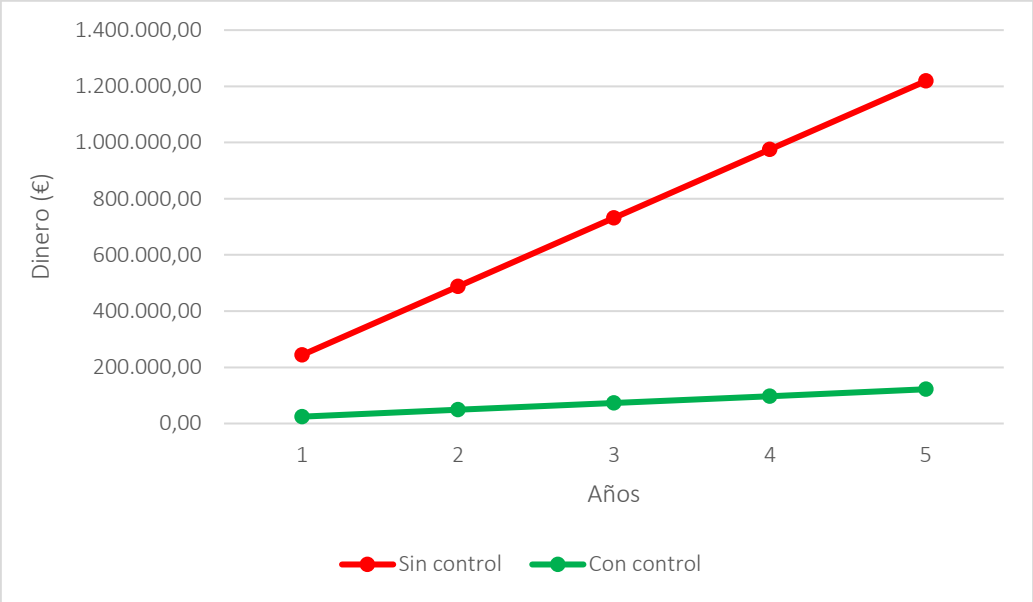



*Ilustración 316. Rentabilidad amenaza D1 - [E.19] activo S3*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

***Tabla 323. Rentabilidad amenaza D1 - [A.11] activo S3***

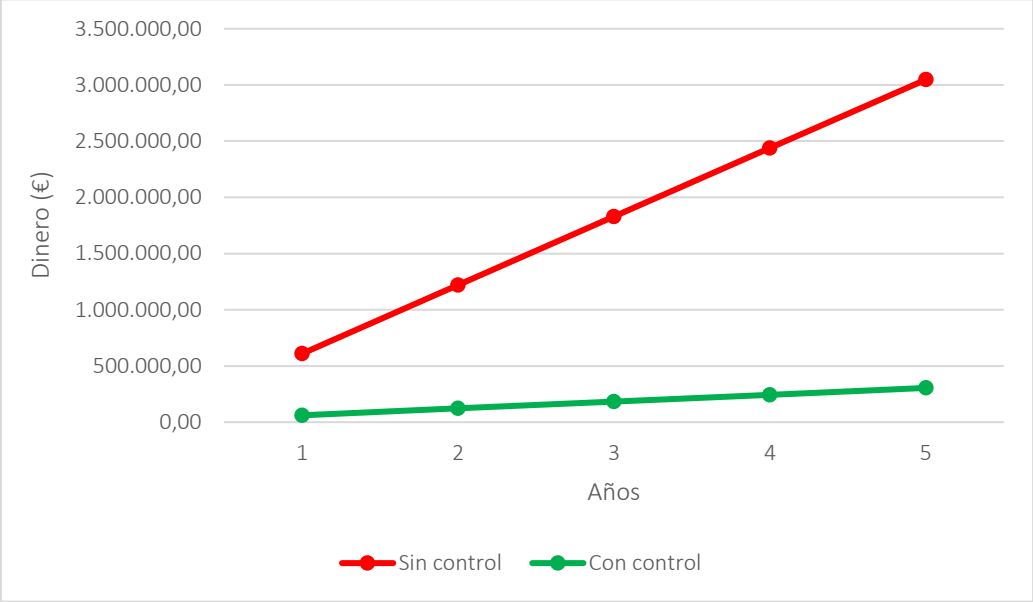



***Ilustración 317. Rentabilidad amenaza D1 - [A.11] activo S3***

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 324. Rentabilidad amenaza D1 - [A.18] activo S3***

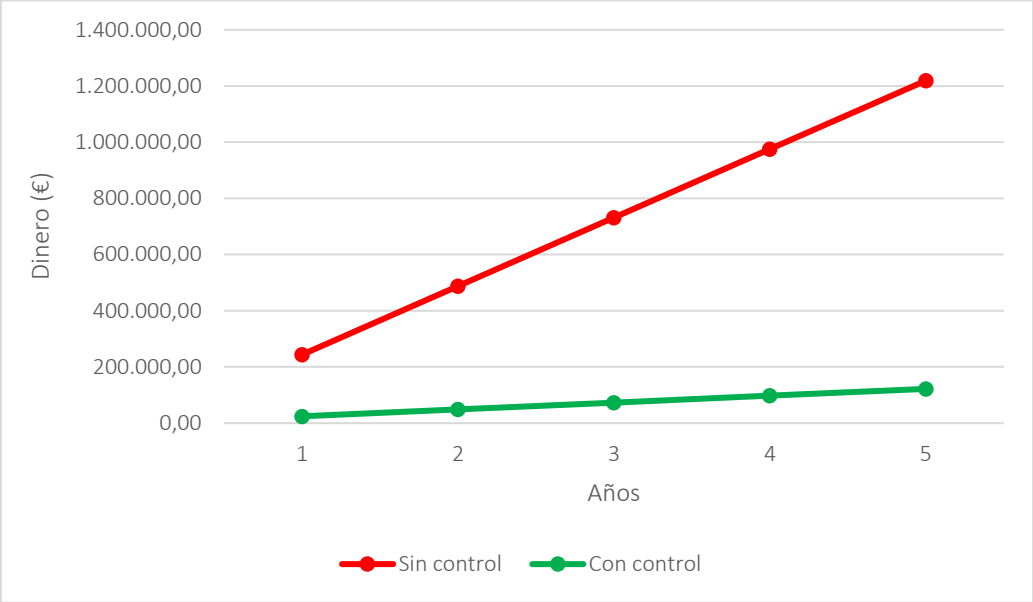



*Ilustración 318. Rentabilidad amenaza D1 - [A.18] activo S3*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 325. Rentabilidad amenaza D1 - [A.19] activo S3*

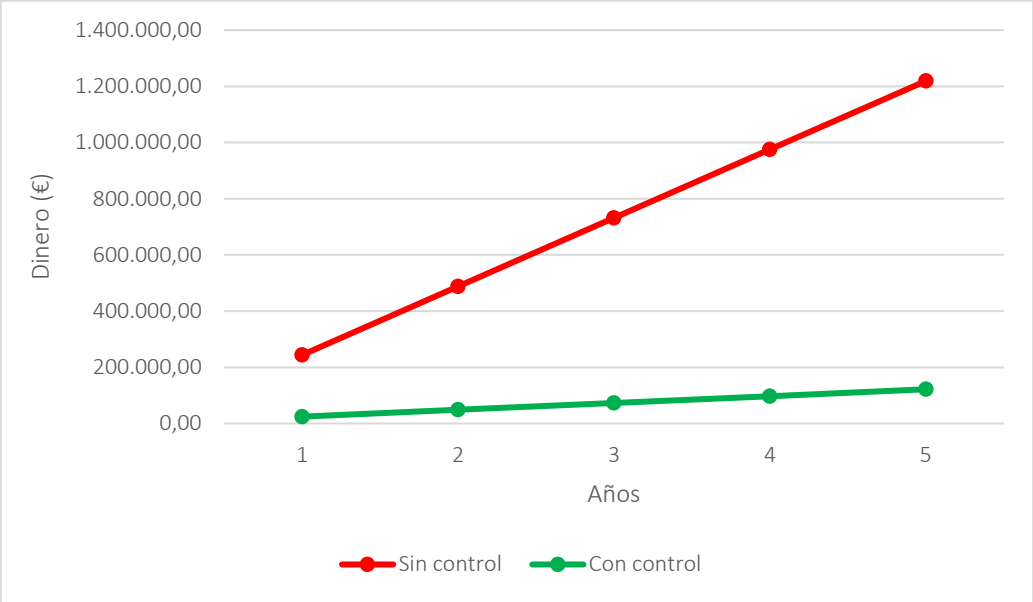



*Ilustración 319. Rentabilidad amenaza D1 - [A.19] activo S3*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 326. Rentabilidad amenaza SW1 - [A.18] activo S3*

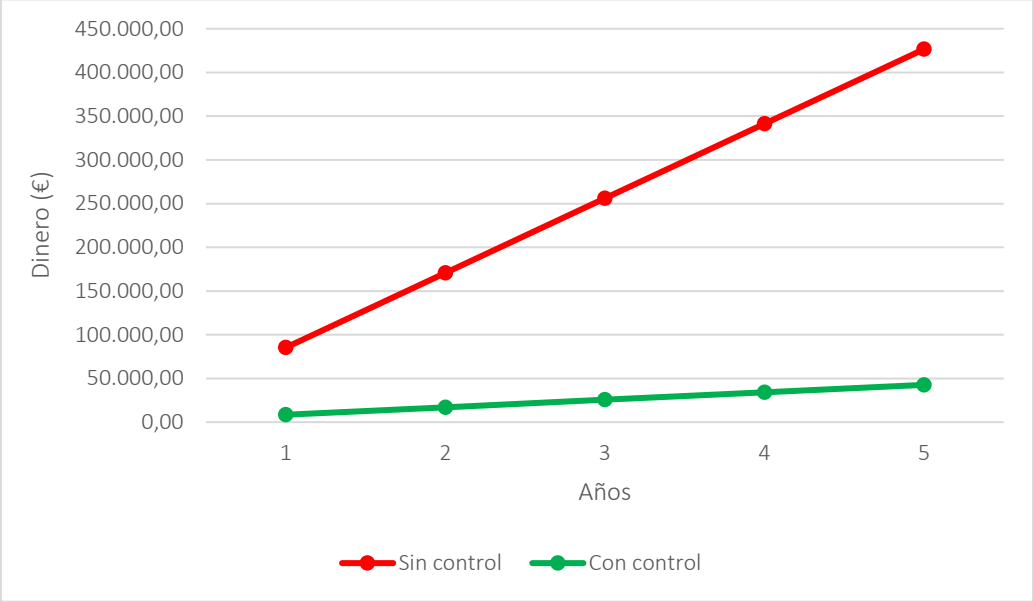



*Ilustración 320. Rentabilidad amenaza SW1 - [A.18] activo S3*

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

*Tabla 327. Rentabilidad amenaza SW1 - [A.19] activo S3*

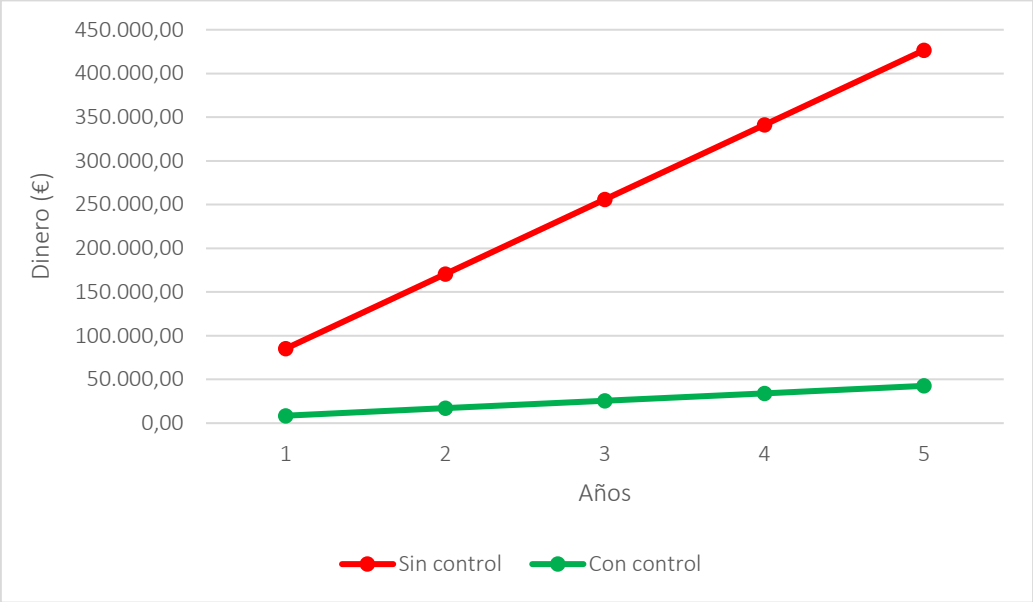



*Ilustración 321. Rentabilidad amenaza SW1 - [A.19] activo S3*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 328. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

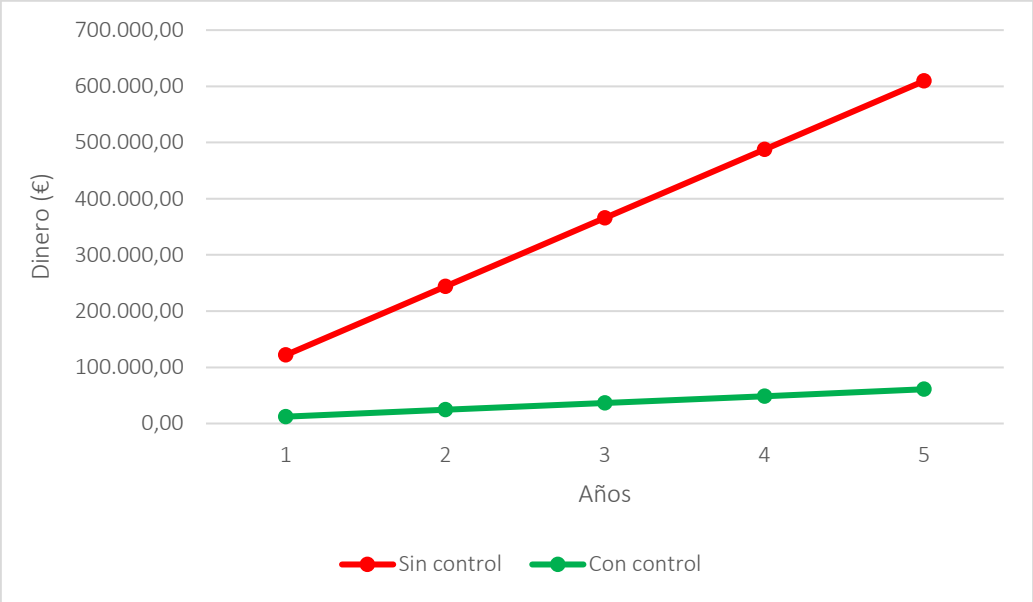



*Ilustración 322. Rentabilidad amenaza SRVD1 - [A.11] activo S3*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 329. Rentabilidad amenaza T1 - [A.11] activo S3*

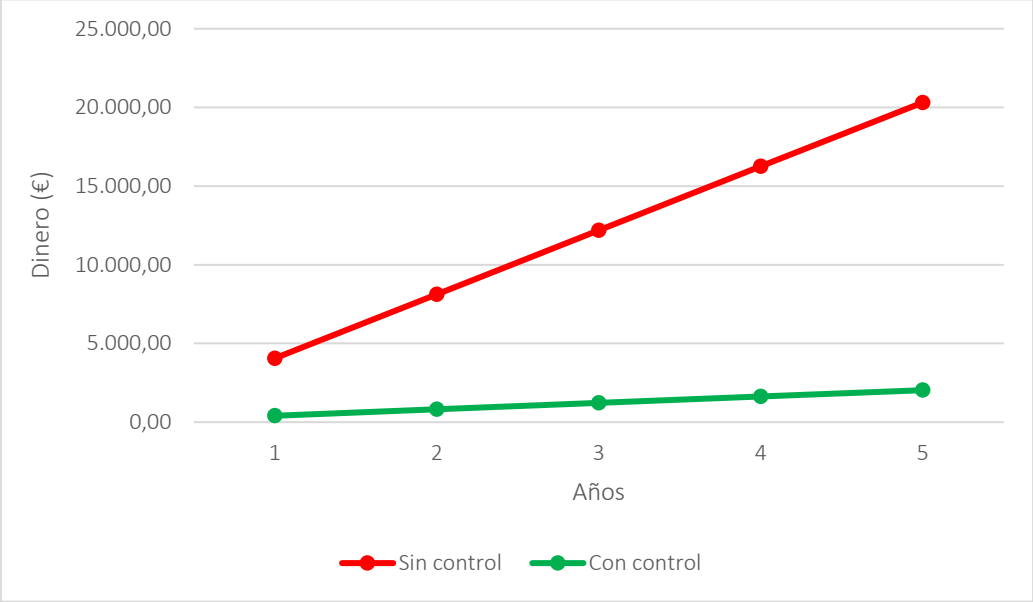



*Ilustración 323. Rentabilidad amenaza T1 - [A.11] activo S3*

Como podemos observar en todos los gráficos que hemos estudiado para el tercer activo, “Citas”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Facturación (S4)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36562,54 | 0 | 0 | 36562,54 | 73125,08 | 109687,62 | 146250,16 | 182812,7 |
| 3656,25 | 0 | 0 | 3656,25 | 7312,5 | 10968,75 | 14625 | 18281,25 |

*Tabla 330. Rentabilidad amenaza AUX1 - [A.11] activo S4*

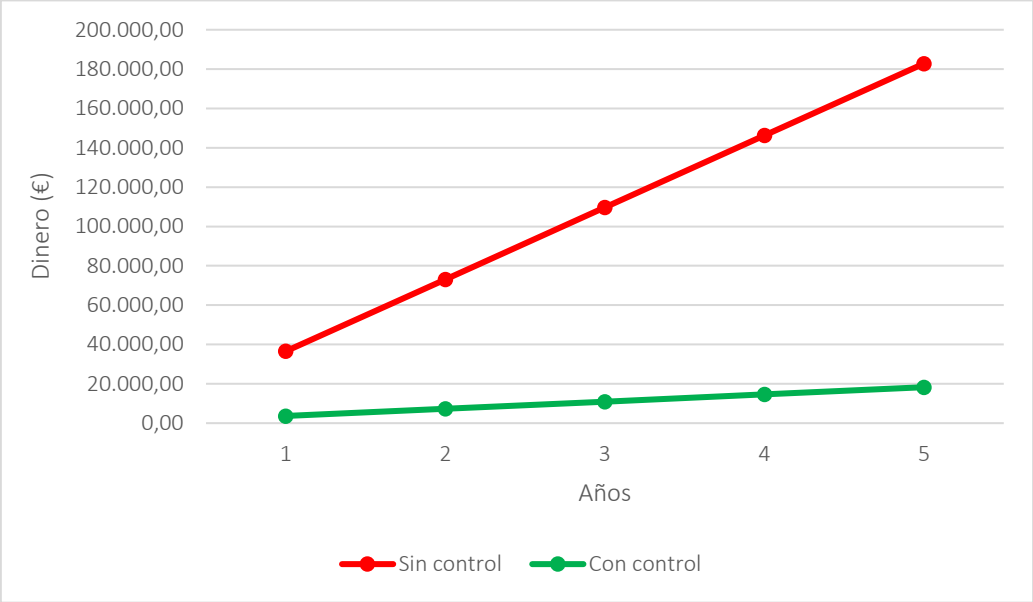



*Ilustración 324. Rentabilidad amenaza AUX1 - [A.11] activo S4*

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

*Tabla 331. Rentabilidad amenaza D1 - [E.19] activo S4*

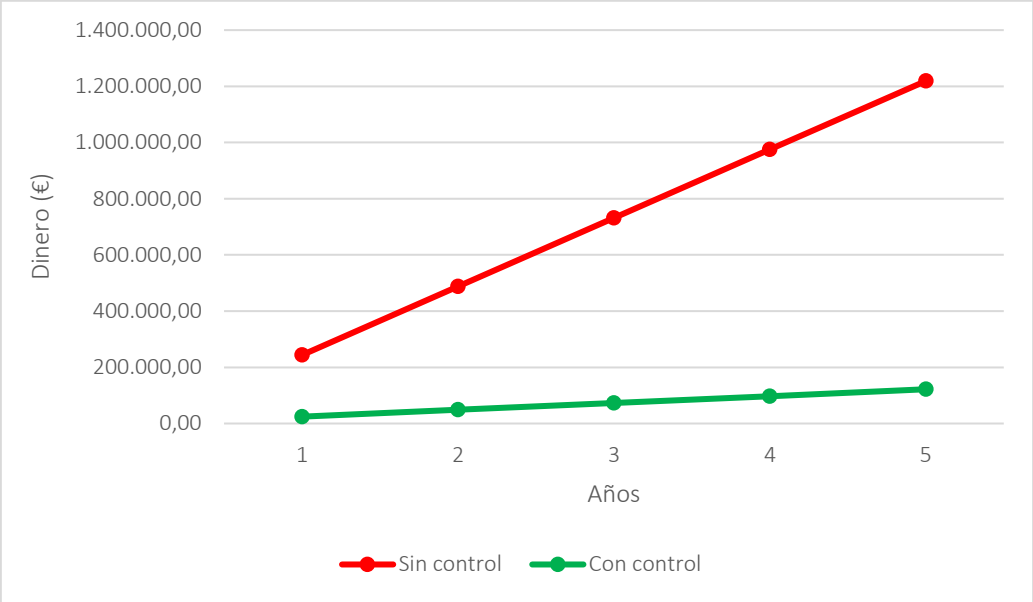



*Ilustración 325. Rentabilidad amenaza D1 - [E.19] activo S4*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609375,71 | 0 | 0 | 609375,71 | 1218751,4 | 1828127,13 | 2437502,84 | 3046878,55 |
| 60937,57 | 0 | 0 | 60937,57 | 121875,14 | 182812,71 | 243750,28 | 304687,85 |

*Tabla 332. Rentabilidad amenaza D1 - [A.11] activo S4*

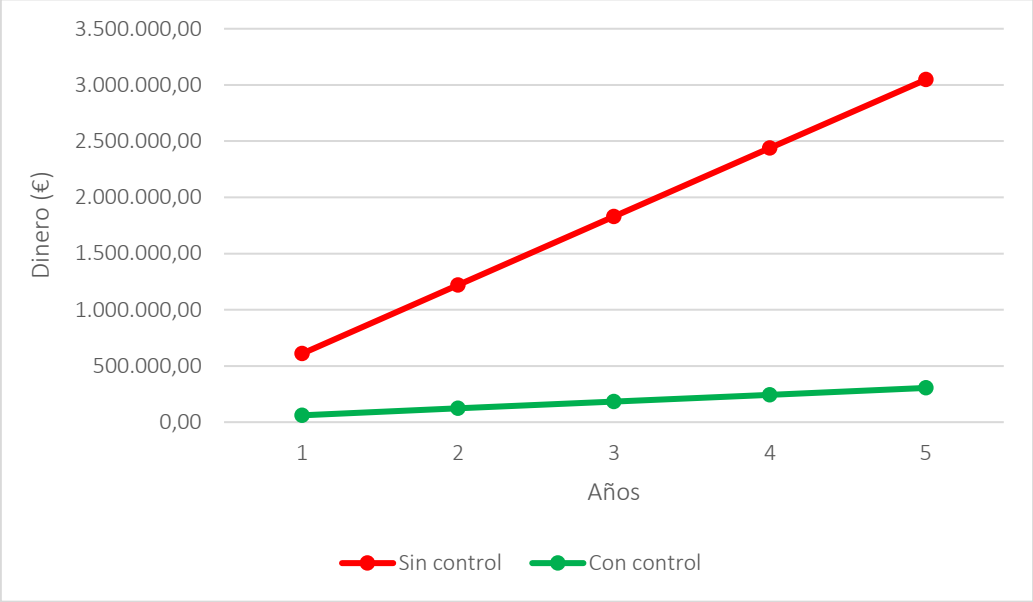



*Ilustración 326. Rentabilidad amenaza D1 - [A.11] activo S4*

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

*Tabla 333. Rentabilidad amenaza D1 - [A.18] activo S4*

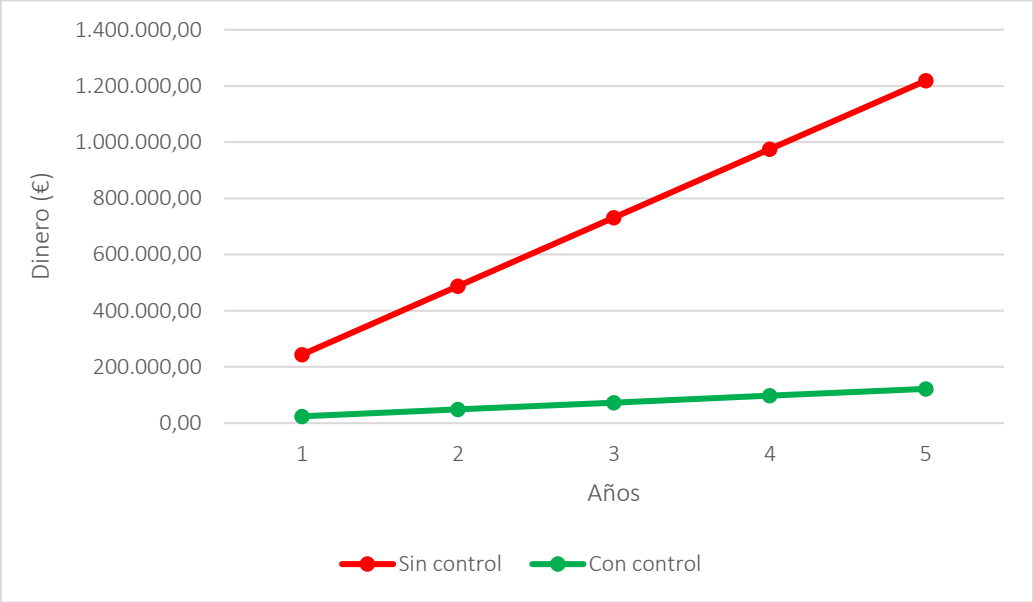



*Ilustración 327. Rentabilidad amenaza D1 - [A.18] activo S4*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243750,28 | 0 | 0 | 243750,28 | 487500,56 | 731250,84 | 975001,12 | 1218751,4 |
| 24375,03 | 0 | 0 | 24375,03 | 48750,06 | 73125,09 | 97500,12 | 121875,15 |

*Tabla 334. Rentabilidad amenaza D1 - [A.19] activo S4*

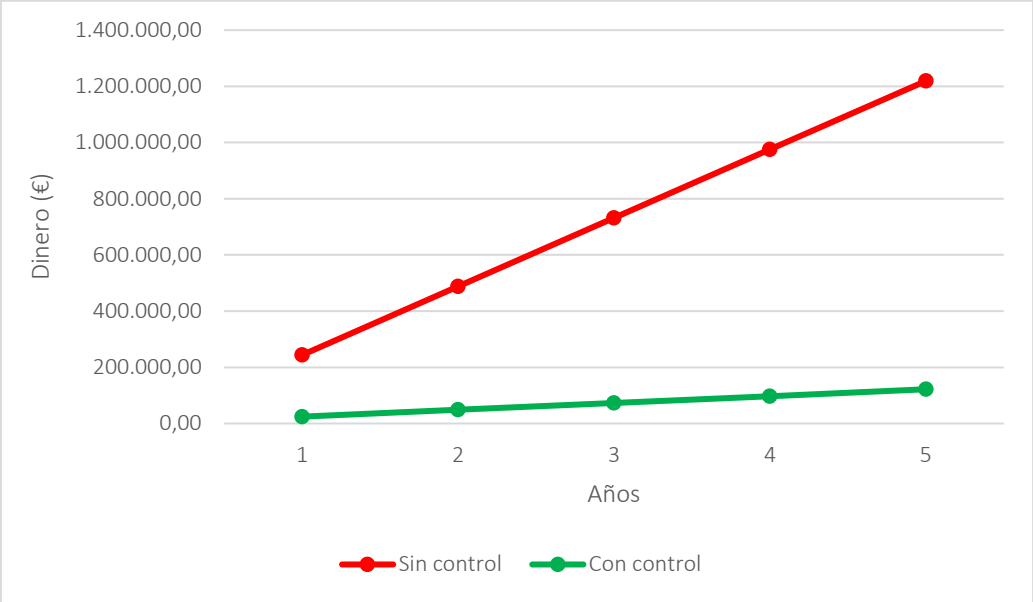



*Ilustración 328. Rentabilidad amenaza D1 - [A.19] activo S4*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85312,6 | 0 | 0 | 85312,6 | 170625,2 | 255937,8 | 341250,4 | 426563 |
| 8531,26 | 0 | 0 | 8531,26 | 17062,52 | 25593,78 | 34125,04 | 42656,3 |

***Tabla 335. Rentabilidad amenaza SW1 - [A.18] activo S4***

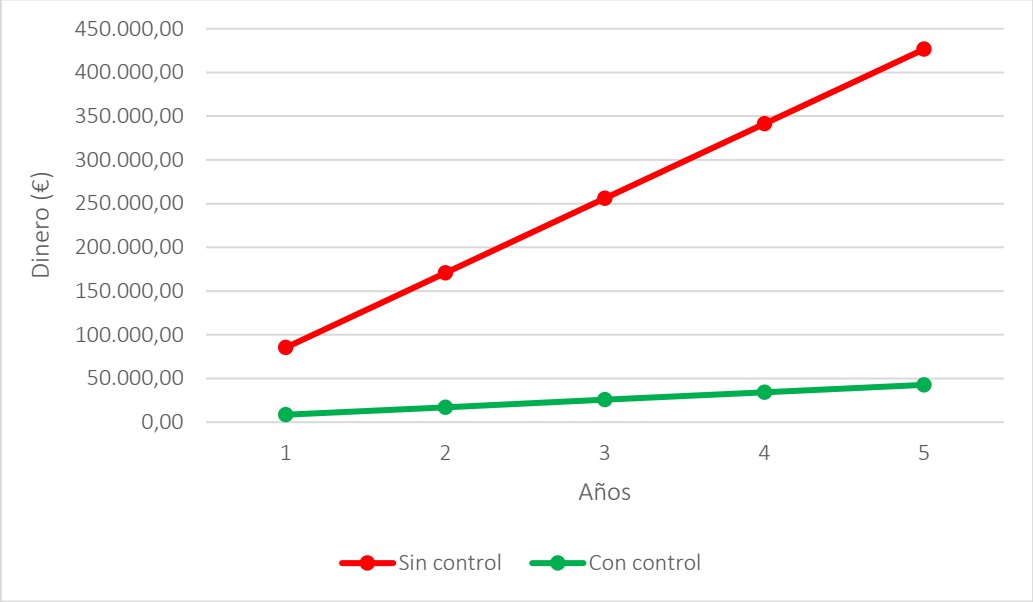



***Ilustración 329. Rentabilidad amenaza SW1 - [A.18] activo S4***

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85312,6 | 0 | 0 | 85312,6 | 170625,2 | 255937,8 | 341250,4 | 426563 |
| 8531,26 | 0 | 0 | 8531,26 | 17062,52 | 25593,78 | 34125,04 | 42656,3 |

***Tabla 336. Rentabilidad amenaza SW1 - [A.19] activo S4***

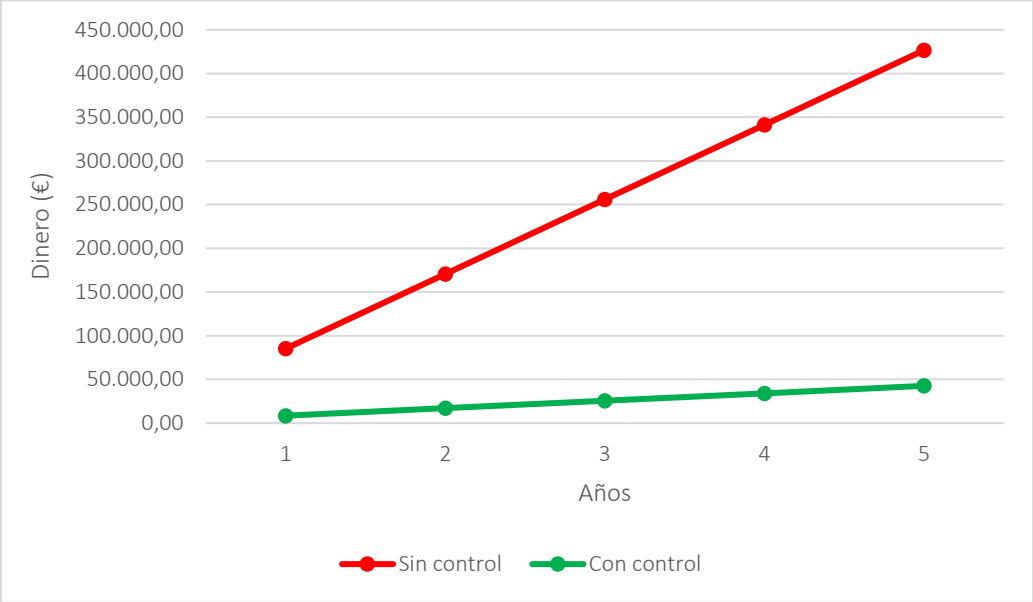



*Ilustración 330. Rentabilidad amenaza SW1 - [A.19] activo S4*

## Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121875,14 | 0 | 0 | 121875,14 | 243750,28 | 365625,42 | 487500,56 | 609375,7 |
| 12187,51 | 0 | 0 | 12187,51 | 24375,02 | 36562,53 | 48750,04 | 60937,55 |

*Tabla 337. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

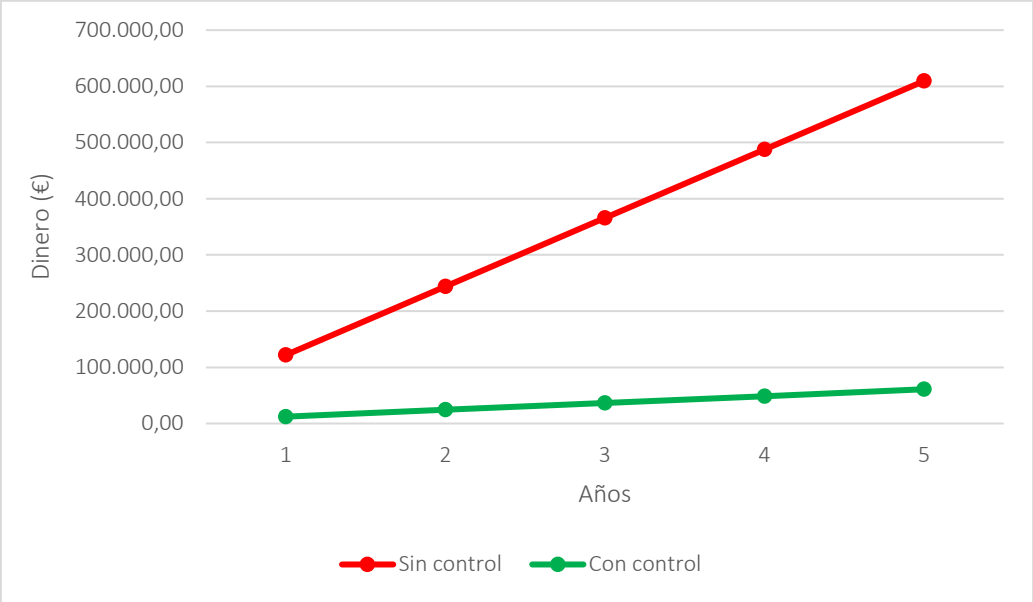



*Ilustración 331. Rentabilidad amenaza SRVD1 - [A.11] activo S4*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,5 | 0 | 0 | 4062,5 | 8125 | 12187,5 | 16250 | 20312,5 |
| 406,25 | 0 | 0 | 406,25 | 812,5 | 1218,75 | 1625 | 2031,25 |

*Tabla 338. Rentabilidad amenaza T1 - [A.11] activo S4*

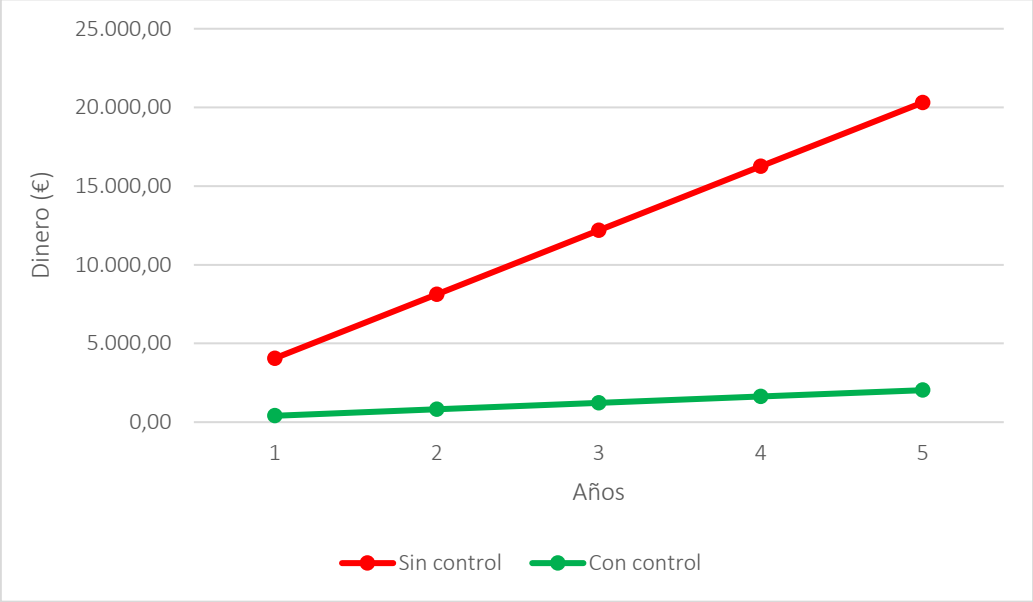



*Ilustración 332. Rentabilidad amenaza T1 - [A.11] activo S4*

Como podemos observar en todos los gráficos que hemos estudiado para el cuarto activo, “Facturación”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Control c-v (S5)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 339. Rentabilidad amenaza AUX1 - [A.11] activo S5*

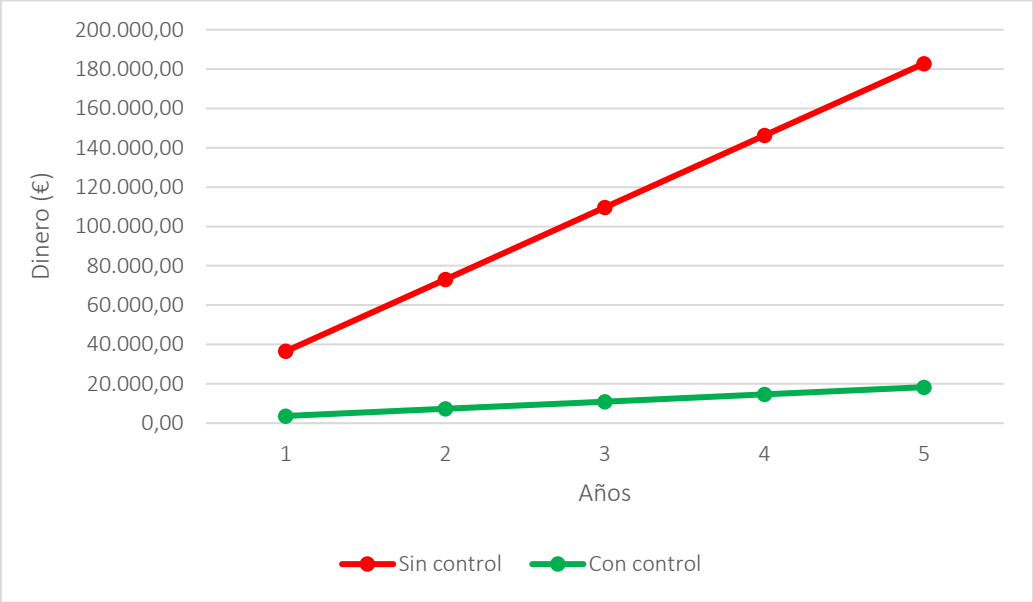



*Ilustración 333. Rentabilidad amenaza AUX1 - [A.11] activo S5*

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 340. Rentabilidad amenaza D1 - [E.19] activo S5*

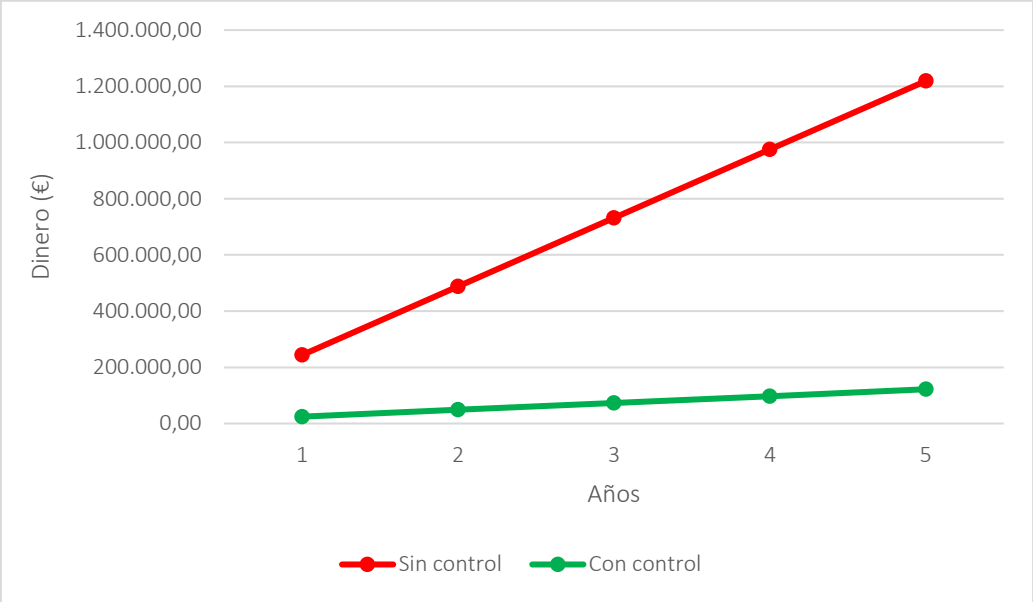



*Ilustración 334. Rentabilidad amenaza D1 - [E.19] activo S5*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

***Tabla 341. Rentabilidad amenaza D1 - [A.11] activo S5***

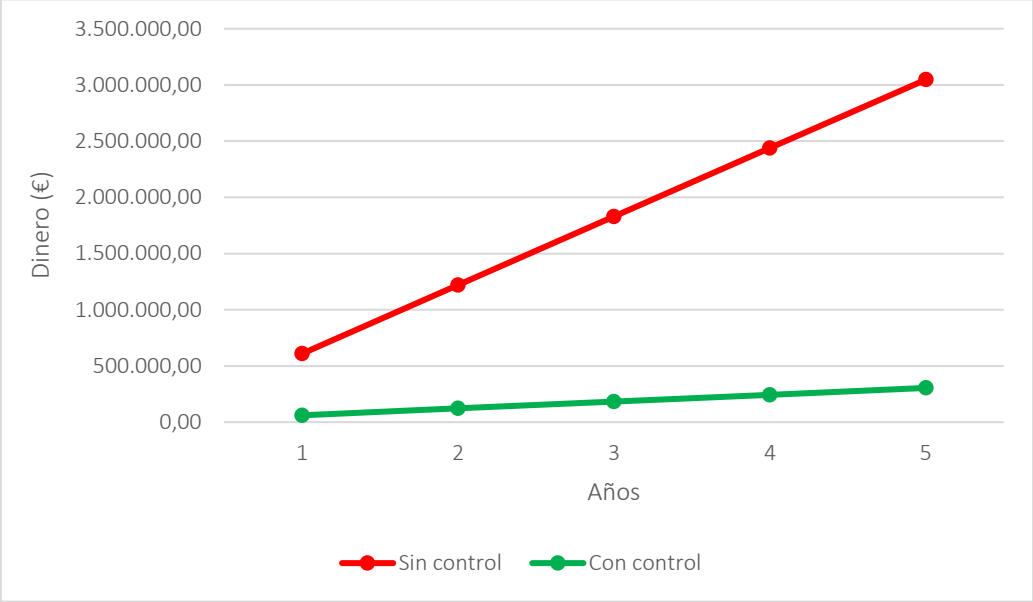



***Ilustración 335. Rentabilidad amenaza D1 - [A.11] activo S5***

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 342. Rentabilidad amenaza D1 - [A.18] activo S5***

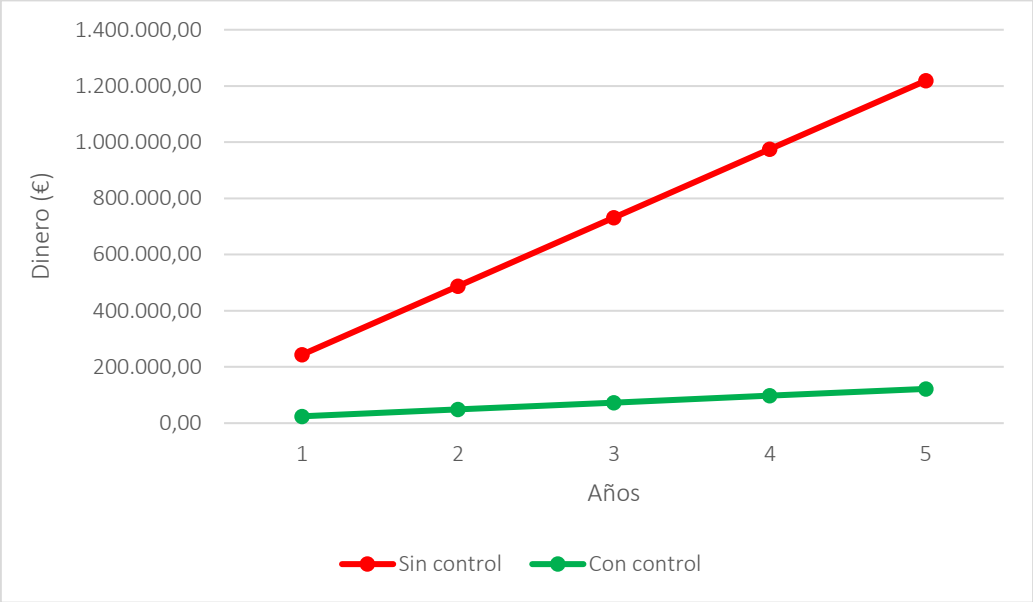



*Ilustración 336. Rentabilidad amenaza D1 - [A.18] activo S5*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 343. Rentabilidad amenaza D1 - [A.19] activo S5*

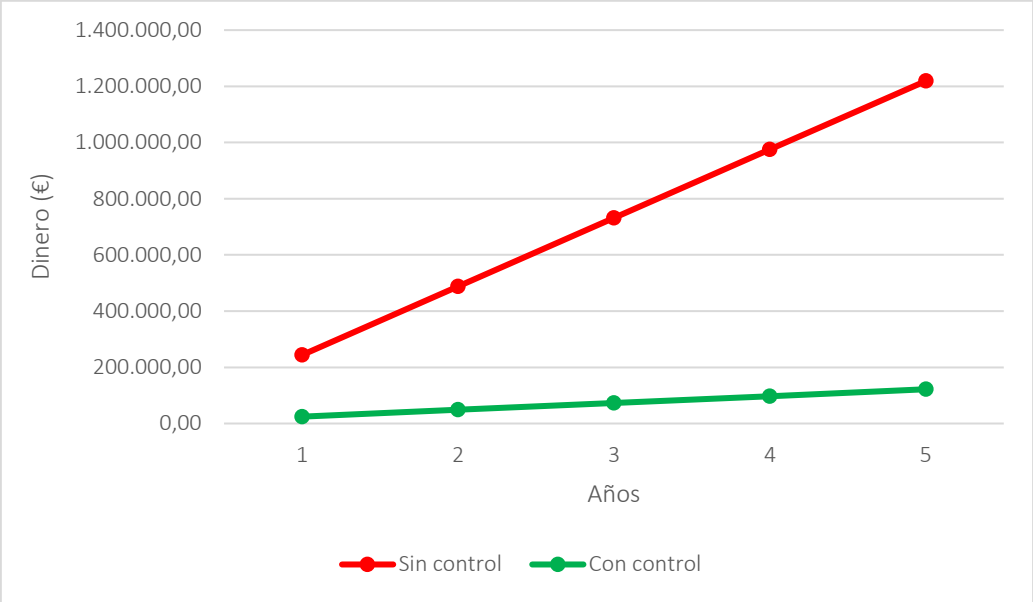



*Ilustración 337. Rentabilidad amenaza D1 - [A.19] activo S5*

## Amenaza: SW1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

***Tabla 344. Rentabilidad amenaza SW1 - [A.18] activo S5***

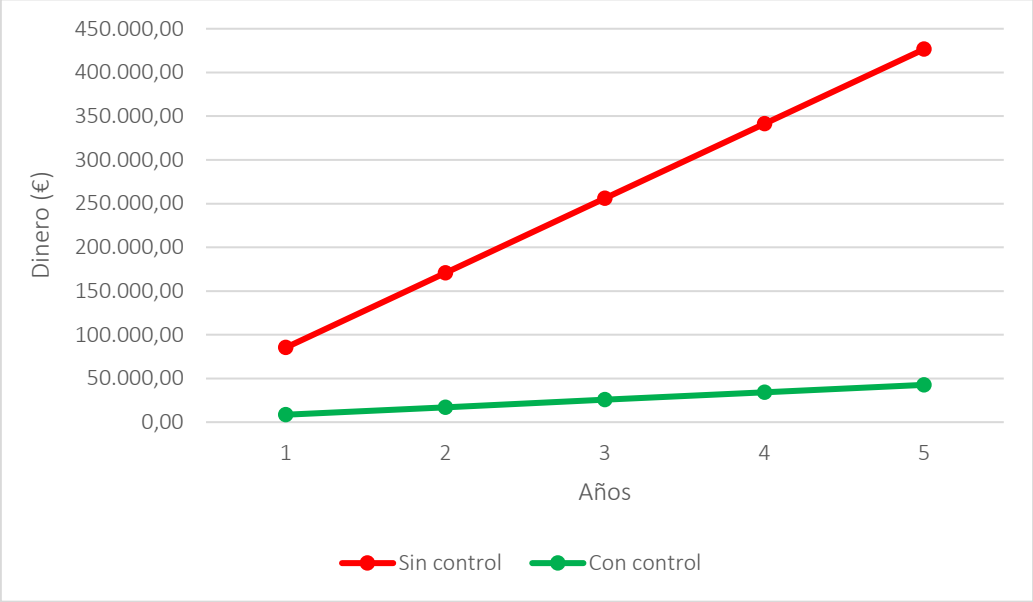



***Ilustración 338. Rentabilidad amenaza SW1 - [A.18] activo S5***

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

***Tabla 345. Rentabilidad amenaza SW1 - [A.19] activo S5***

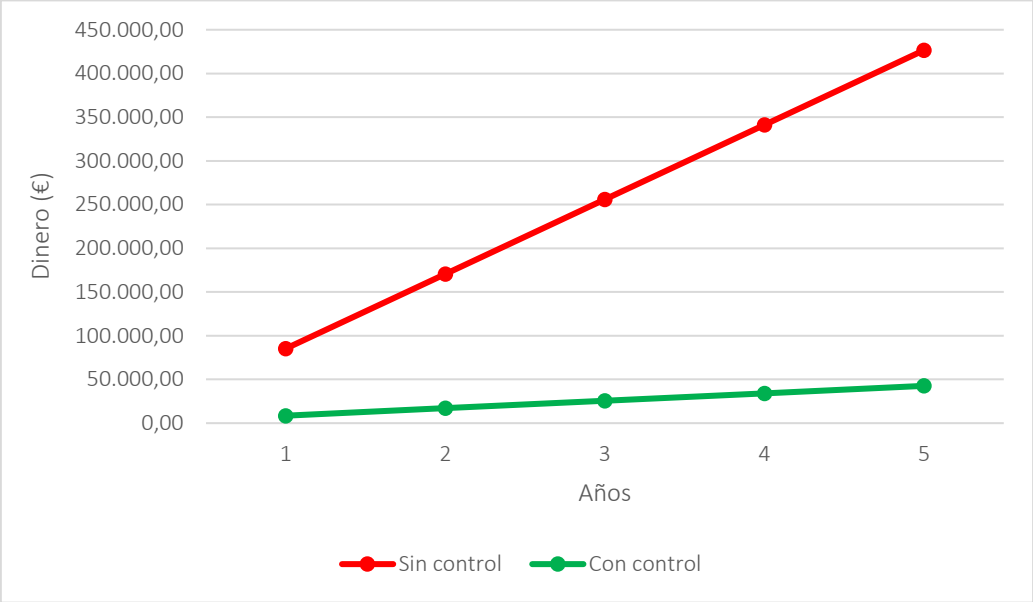



*Ilustración 339. Rentabilidad amenaza SW1 - [A.19] activo S5*

Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 346. Rentabilidad amenaza SRVD1 - [A.11] activo S5*

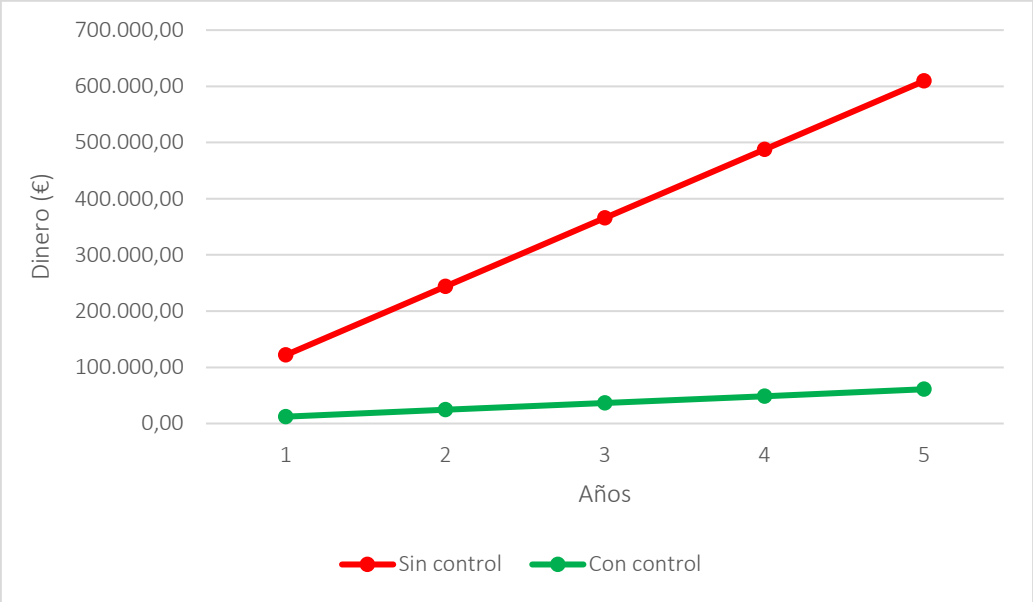



*Ilustración 340. Rentabilidad amenaza SRVD1 - [A.11] activo S5*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 347. Rentabilidad amenaza T1 - [A.11] activo S5*

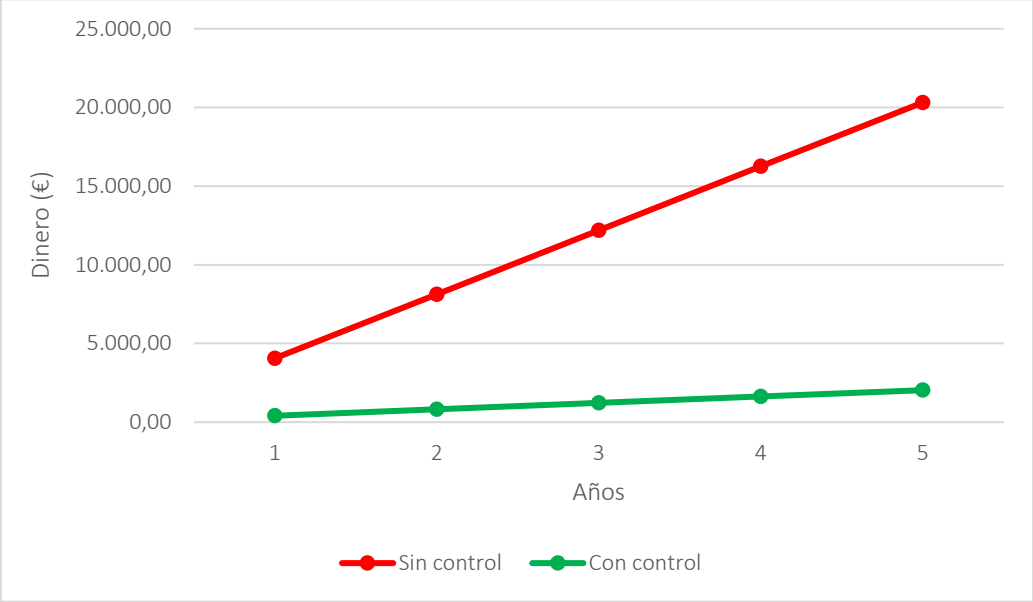



*Ilustración 341. Rentabilidad amenaza T1 - [A.11] activo S5*

Como podemos observar en todos los gráficos que hemos estudiado para el quinto activo, “Control c-v”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

Activo: Almacén (S6)

Amenaza: AUX1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 36563,49 | 0 | 0 | 36563,49 | 73126,98 | 109690,47 | 146253,96 | 182817,45 |
| 3656,35 | 0 | 0 | 3656,35 | 7312,7 | 10969,05 | 14625,4 | 18281,75 |

*Tabla 348. Rentabilidad amenaza AUX1 - [A.11] activo S6*

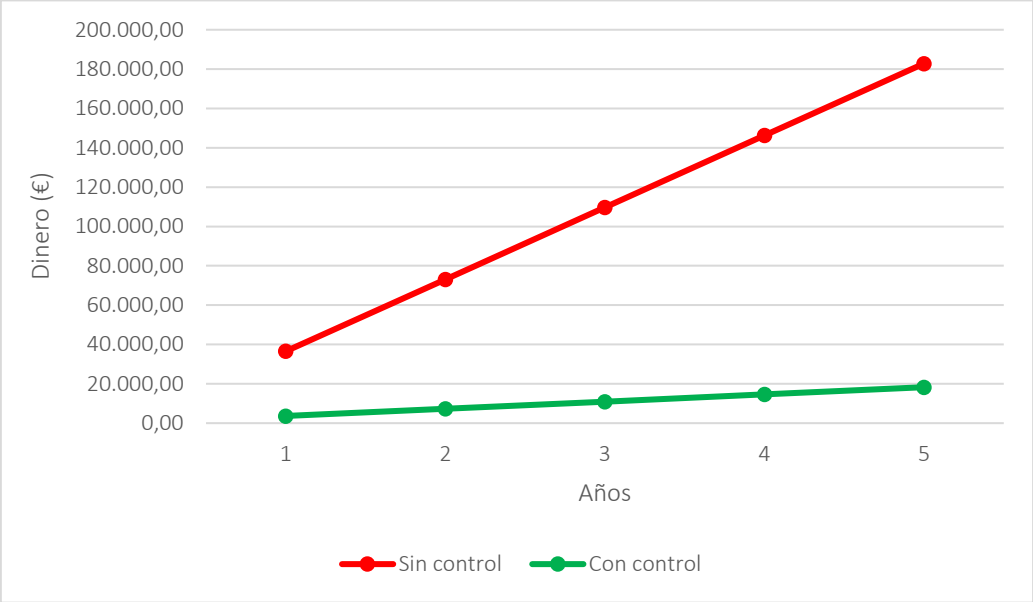



*Ilustración 342. Rentabilidad amenaza AUX1 - [A.11] activo S6*

Amenaza: D1 – [E.19] Fugas de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 349. Rentabilidad amenaza D1 - [E.19] activo S6*

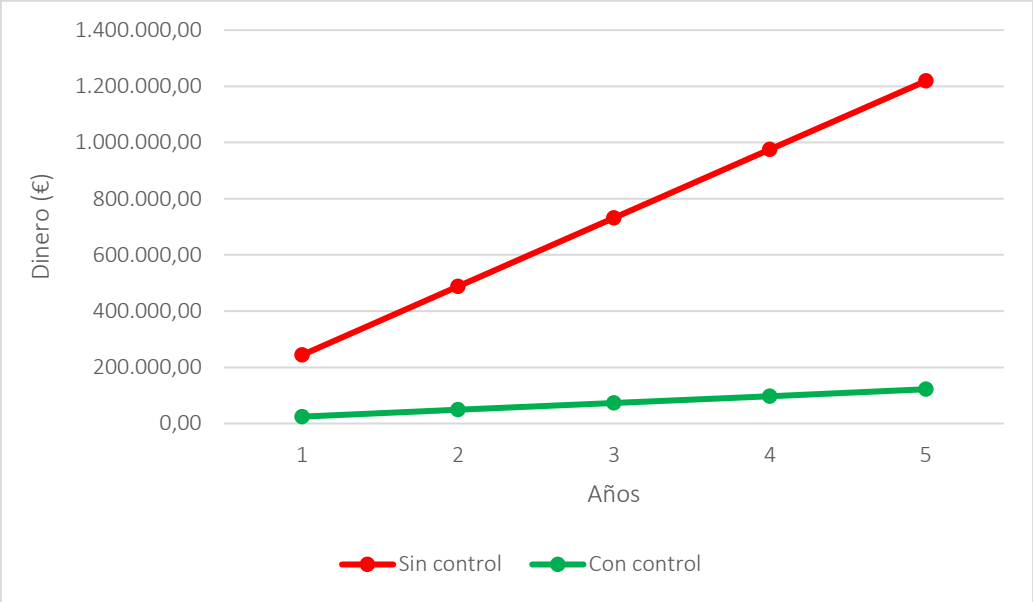



*Ilustración 343. Rentabilidad amenaza D1 - [E.19] activo S6*

## Amenaza: D1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 609391,49 | 0 | 0 | 609391,49 | 1218783 | 1828174,47 | 2437565,96 | 3046957,45 |
| 60939,15 | 0 | 0 | 60939,15 | 121878,3 | 182817,45 | 243756,6 | 304695,75 |

***Tabla 350. Rentabilidad amenaza D1 - [A.11] activo S6***

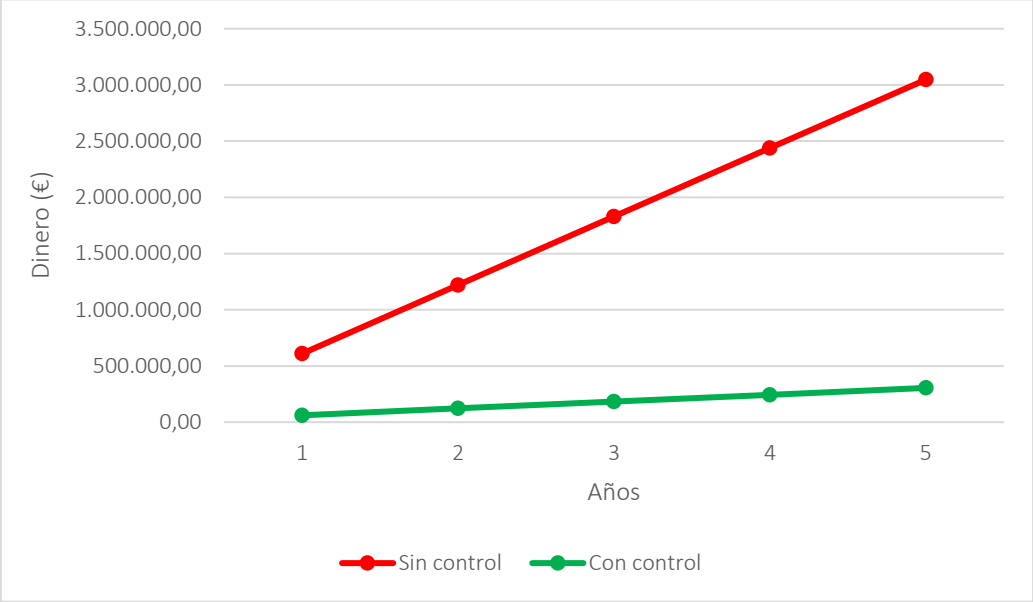



***Ilustración 344. Rentabilidad amenaza D1 - [A.11] activo S6***

## Amenaza: D1 – [A.18] Destrucción de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

***Tabla 351. Rentabilidad amenaza D1 - [A.18] activo S6***

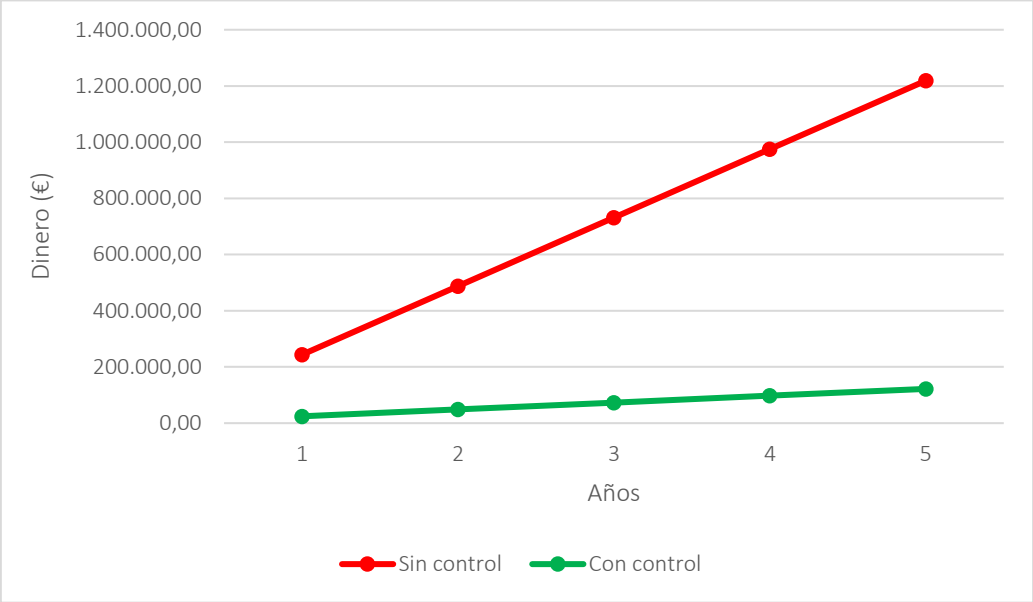



*Ilustración 345. Rentabilidad amenaza D1 - [A.18] activo S6*

## Amenaza: D1 – [A.19] Divulgación de la información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 243756,6 | 0 | 0 | 243756,6 | 487513,2 | 731269,8 | 975026,4 | 1218783 |
| 24375,66 | 0 | 0 | 24375,66 | 48751,32 | 73126,98 | 97502,64 | 121878,3 |

*Tabla 352. Rentabilidad amenaza D1 - [A.19] activo S6*

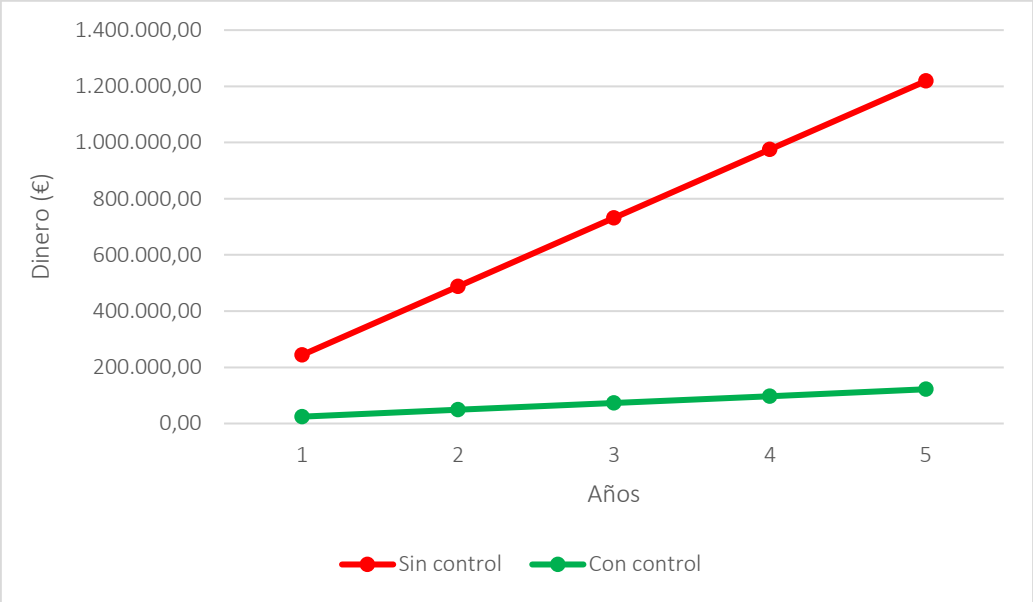



*Ilustración 346. Rentabilidad amenaza D1 - [A.19] activo S6*

## Amenaza: SW1 – [A.18] Destrucción de información

***Tabla 353. Rentabilidad amenaza SW1 - [A.18] activo S6***

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

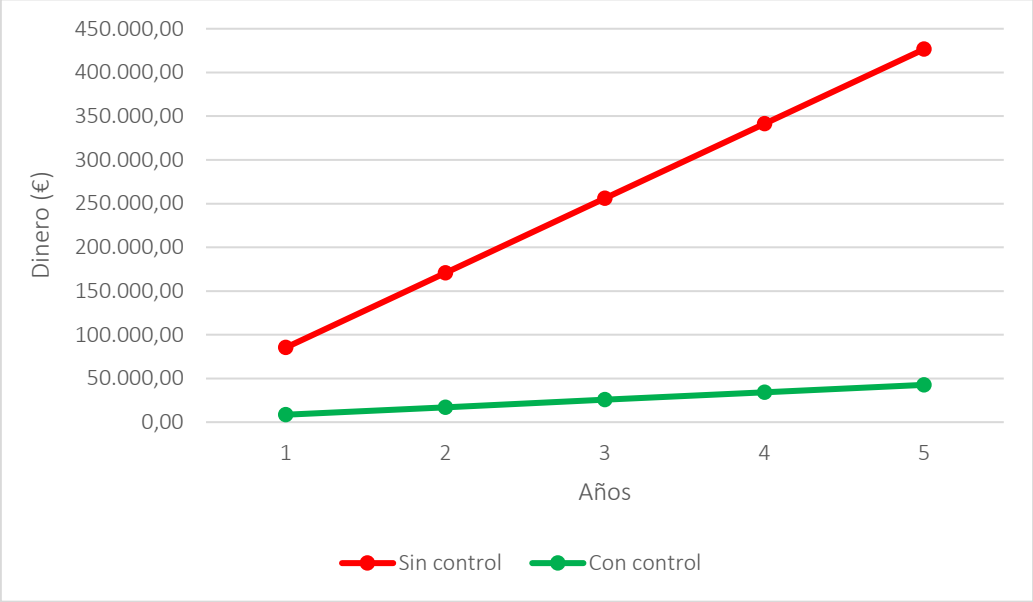



***Ilustración 347. Rentabilidad amenaza SW1 - [A.18] activo S6***

## Amenaza: SW1 – [A.19] Divulgación de información

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 85314,81 | 0 | 0 | 85314,81 | 170629,62 | 255944,43 | 341259,24 | 426574,05 |
| 8531,48 | 0 | 0 | 8531,48 | 17062,96 | 25594,44 | 34125,92 | 42657,4 |

***Tabla 354. Rentabilidad amenaza SW1 - [A.19] activo S6***

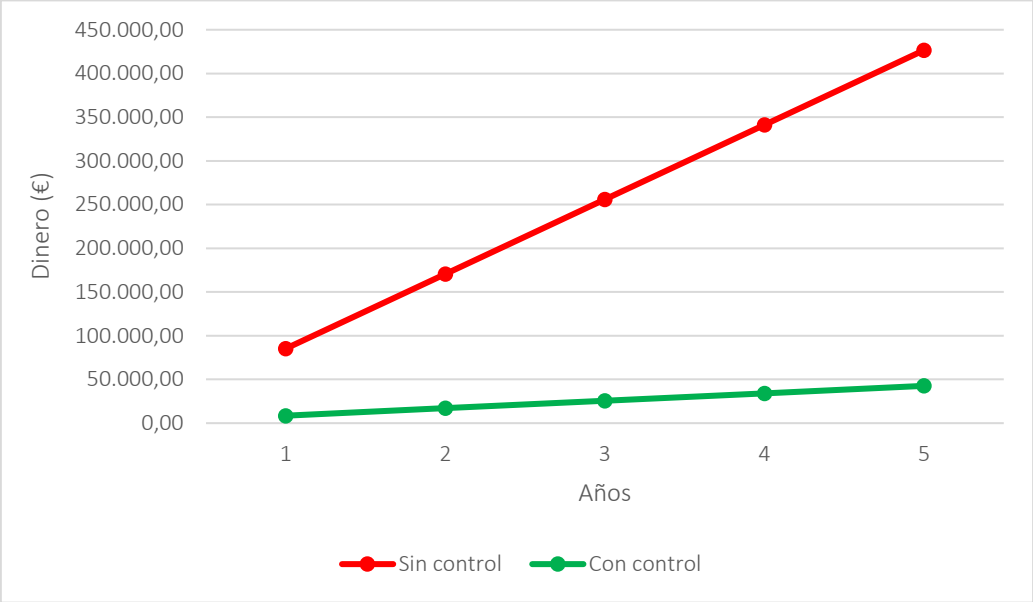



*Ilustración 348. Rentabilidad amenaza SW1 - [A.19] activo S6*

Amenaza: SRVD1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 121878,3 | 0 | 0 | 121878,3 | 243756,6 | 365634,9 | 487513,2 | 609391,5 |
| 12187,83 | 0 | 0 | 12187,83 | 24375,66 | 36563,49 | 48751,32 | 60939,15 |

*Tabla 355. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

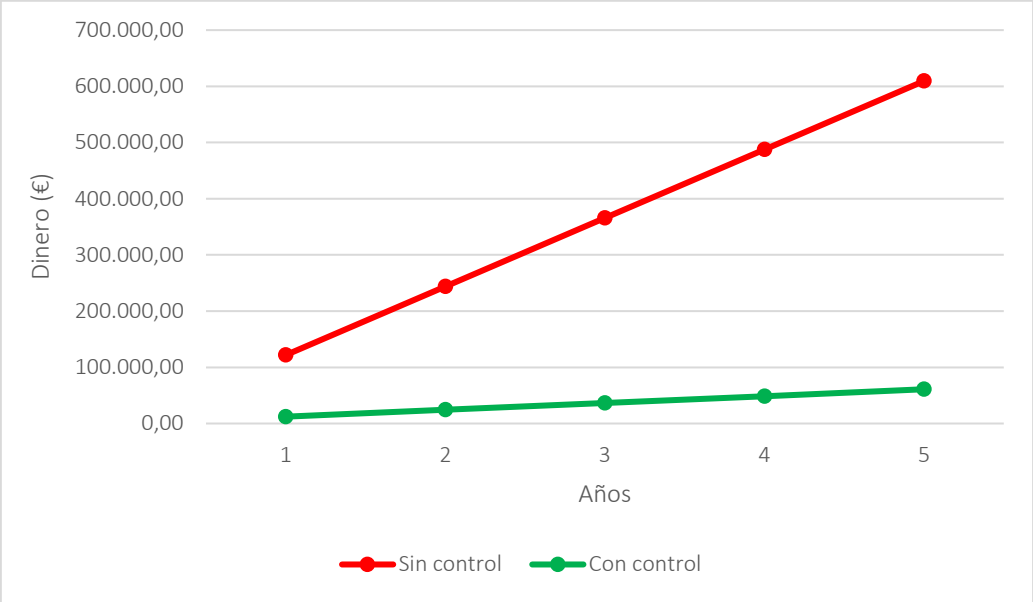



*Ilustración 349. Rentabilidad amenaza SRVD1 - [A.11] activo S6*

Amenaza: T1 – [A.11] Acceso no autorizado

| Riesgo residual | Coste implantación | Coste ejecución | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| 4062,61 | 0 | 0 | 4062,61 | 8125,22 | 12187,83 | 16250,44 | 20313,05 |
| 406,26 | 0 | 0 | 406,26 | 812,52 | 1218,78 | 1625,04 | 2031,3 |

*Tabla 356. Rentabilidad amenaza T1 - [A.11] activo S6*

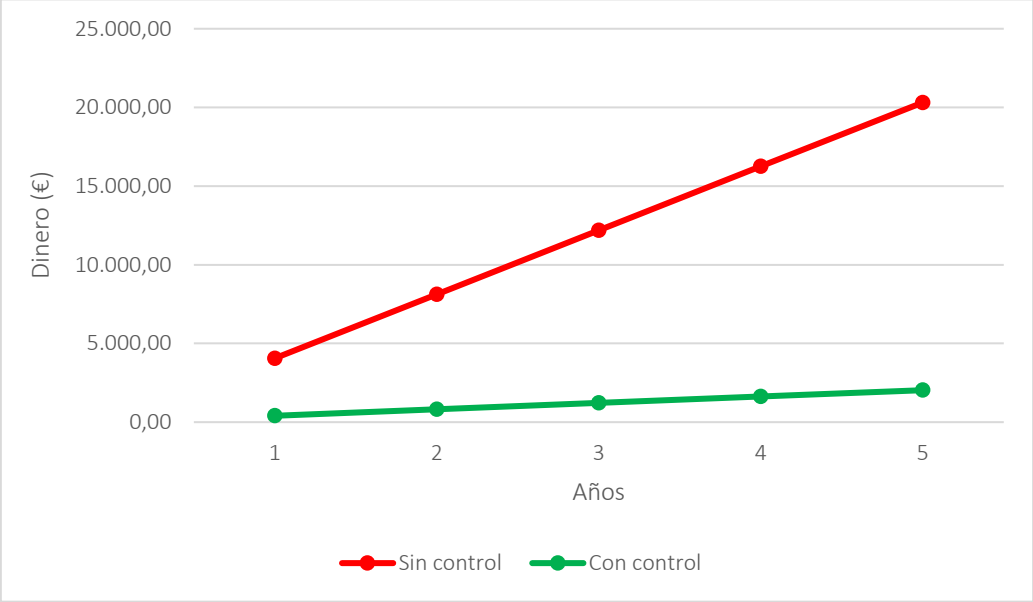



*Ilustración 350. Rentabilidad amenaza T1 - [A.11] activo S6*

Como podemos observar en todos los gráficos que hemos estudiado para el sexto activo, “Almacén”, podemos ver que el valor del riesgo residual es mucho mayor cuando no tenemos control. Por lo tanto, la rentabilidad del control es muy alta, ya que el coste de implantación es muy bajo con respecto al valor del riesgo residual sin control.

### 2.1.6 Riesgo residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. (Magerit, 2012b)

La vulnerabilidad es la debilidad de los controles que protegen a un activo determinado de una determinada amenaza. Teniendo en cuenta el valor de la vulnerabilidad, el riesgo residual lo calculamos con la siguiente formula:

$$Riesgo\ residual = Riesgo\ potencial\ x\ (1 - Vulnerabilidad) \quad (2.4)$$

El riesgo residual es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel del riesgo al que está sometido una compañía nunca puede erradicarse totalmente. Por lo tanto, el riesgo residual es aquel que permanece después de que la dirección desarrolle sus respuestas a los riesgos. (Magerit, 2012a)

Dentro de cada control, hay un apartado en el cual se calcula la rentabilidad de los controles teniendo en cuenta el riesgo residual provocado por cada uno de ellos. Por lo tanto, teniendo en cuenta la fórmula anterior, hemos calculado todos los riesgos residuales. En la siguiente tabla se recogen los valores de todos los riesgos residuales a modo de resumen.

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| S1 | 1819186,62 | AUX1 | [I.5] Avería de origen físico o lógico | 171,91 | | |
| | | | [I.6] Corte suministro eléctrico | 36383,73 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 3911,25 | | |
| | | | [E.4] Errores de configuración | 27287,80 | | |
| | | | [E.25] Pérdida de equipos | 873,21 | | |
| | | | [A.11] Acceso no autorizado | 5457,56 | 1091,51 | 5457,56 |
| | | | [A.25] Robo | 1091,51 | | |
| | | D1 | [E.15] Alteración accidental de la información | 90959,33 | | |
| | | | [E.18] Destrucción de información | 18191,87 | | |
| | | | [E.19] Fugas de información | 36383,73 | 36383,73 | |
| | | | [A.5] Suplantación de la identidad del usuario | 18191,87 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.6] Abuso de privilegios de acceso | 90959,33 | | |
| | | | [A.11] Acceso no autorizado | 90959,33 | 18191,87 | 90959,33 |
| | | | [A.18] Destrucción de la información | 36383,73 | 18191,87 | 36383,73 |
| | | | [A.19] Divulgación de la información | 36383,73 | 36383,73 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 363837,32 | | |
| | | | [I.6] Corte del suministro eléctrico | 363837,32 | | |
| | | | [A.6] Abuso de privilegios de acceso | 18191,87 | | |
| | | | [A.7] Uso no previsto | 18191,87 | | |
| | | | [A.11] Acceso no autorizado | 18191,87 | | |
| | | | [A.25] Robo | 2183,02 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 363837,32 | | |
| | | | [E.14] Escapes de información | 18191,87 | | |
| | | | [E.19] Fugas de información | 36383,73 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 18191,87 | 3638,37 | |
| | | | [A.15] Modificación deliberada de la información | 18191,87 | | |
| | | | [A.18] Destrucción de información | 12734,31 | 6367,15 | 12734,31 |
| | | | [A.19] Divulgación de información | 12734,31 | 12734,31 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 363837,32 | | |
| | | | [I.6] Corte del suministro eléctrico | 363837,32 | | |
| | | | [A.6] Abuso de privilegios de acceso | 18191,87 | | |
| | | | [A.7] Uso no previsto | 18191,87 | | |
| | | | [A.11] Acceso no autorizado | 18191,87 | 3638,37 | 18191,87 |
| | | | [A.25] Robo | 2183,02 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 60639,55 | | |
| | | | [I.6] Corte del suministro eléctrico | 12127,91 | | |
| | | | [A.6] Abuso de privilegios de acceso | 606,40 | | |
| | | | [A.7] Uso no previsto | 606,40 | | |
| | | | [A.11] Acceso no autorizado | 606,40 | 121,28 | 606,40 |
| | | | [A.25] Robo | 72,77 | | |

***Tabla 357. Riesgos residuales sobre activo S1***

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| S2 | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 115,17 | | |
| | | | [I.6] Corte suministro eléctrico | 24375,66 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 2620,38 | | |
| | | | [E.4] Errores de configuración | 18281,74 | | |
| | | | [E.25] Pérdida de equipos | 585,02 | | |
| | | | [A.11] Acceso no autorizado | 3656,35 | 731,27 | 3656,35 |
| | | | [A.25] Robo | 731,27 | | |
| | | D1 | [E.15] Alteración accidental de la información | 60939,15 | | |
| | | | [E.18] Destrucción de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | 24375,66 | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | | |
| | | | [A.6] Abuso de privilegios de acceso | 60939,15 | | |
| | | | [A.11] Acceso no autorizado | 60939,15 | 12187,83 | 60939,15 |
| | | | [A.18] Destrucción de la información | 24375,66 | 12187,83 | 24375,66 |
| | | | [A.19] Divulgación de la información | 24375,66 | 24375,66 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | | |
| | | | [A.25] Robo | 1462,54 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [E.14] Escapes de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | 2437,57 | |
| | | | [A.15] Modificación deliberada de la información | 12187,83 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.18] Destrucción de información | 8531,48 | 4265,74 | 8531,48 |
| | | | [A.19] Divulgación de información | 8531,48 | 8531,48 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | 2437,57 | 12187,83 |
| | | | [A.25] Robo | 1462,54 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 40626,10 | | |
| | | | [I.6] Corte del suministro eléctrico | 8125,22 | | |
| | | | [A.6] Abuso de privilegios de acceso | 406,26 | | |
| | | | [A.7] Uso no previsto | 406,26 | | |
| | | | [A.11] Acceso no autorizado | 406,26 | 81,25 | 406,26 |
| | | | [A.25] Robo | 48,75 | | |

***Tabla 358. Riesgos residuales sobre activo S2***

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| **S3** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 115,17 | | |
| | | | [I.6] Corte suministro eléctrico | 24375,66 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 2620,38 | | |
| | | | [E.4] Errores de configuración | 18281,74 | | |
| | | | [E.25] Pérdida de equipos | 585,02 | | |
| | | | [A.11] Acceso no autorizado | 3656,35 | 731,27 | 3656,35 |
| | | | [A.25] Robo | 731,27 | | |
| | | D1 | [E.15] Alteración accidental de la información | 60939,15 | | |
| | | | [E.18] Destrucción de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | 24375,66 | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | | |
| | | | [A.6] Abuso de privilegios de acceso | 60939,15 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.11] Acceso no autorizado | 60939,15 | 12187,83 | 60939,15 |
| | | | [A.18] Destrucción de la información | 24375,66 | 12187,83 | 24375,66 |
| | | | [A.19] Divulgación de la información | 24375,66 | 24375,66 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | | |
| | | | [A.25] Robo | 1462,54 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [E.14] Escapes de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | 2437,57 | |
| | | | [A.15] Modificación deliberada de la información | 12187,83 | | |
| | | | [A.18] Destrucción de información | 8531,48 | 4265,74 | 8531,48 |
| | | | [A.19] Divulgación de información | 8531,48 | 8531,48 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | 2437,57 | 12187,83 |
| | | | [A.25] Robo | 1462,54 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 40626,10 | | |
| | | | [I.6] Corte del suministro eléctrico | 8125,22 | | |
| | | | [A.6] Abuso de privilegios de acceso | 406,26 | | |
| | | | [A.7] Uso no previsto | 406,26 | | |
| | | | [A.11] Acceso no autorizado | 406,26 | 81,25 | 406,26 |
| | | | [A.25] Robo | 48,75 | | |

***Tabla 359. Riesgos residuales sobre activo S3***

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| S4 | 1218751,41 | AUX1 | [I.5] Avería de origen físico o lógico | 115,17 | | |
| | | | [I.6] Corte suministro eléctrico | 24375,03 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 2620,32 | | |
| | | | [E.4] Errores de configuración | 18281,27 | | |
| | | | [E.25] Pérdida de equipos | 585,00 | | |
| | | | [A.11] Acceso no autorizado | 3656,25 | 731,25 | 3656,25 |
| | | | [A.25] Robo | 731,25 | | |
| | | D1 | [E.15] Alteración accidental de la información | 60937,57 | | |
| | | | [E.18] Destrucción de información | 12187,51 | | |
| | | | [E.19] Fugas de información | 24375,03 | 24375,03 | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,51 | | |
| | | | [A.6] Abuso de privilegios de acceso | 60937,57 | | |
| | | | [A.11] Acceso no autorizado | 60937,57 | 12187,51 | 60937,57 |
| | | | [A.18] Destrucción de la información | 24375,03 | 12187,51 | 24375,03 |
| | | | [A.19] Divulgación de la información | 24375,03 | 24375,03 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 243750,28 | | |
| | | | [I.6] Corte del suministro eléctrico | 243750,28 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,51 | | |
| | | | [A.7] Uso no previsto | 12187,51 | | |
| | | | [A.11] Acceso no autorizado | 12187,51 | | |
| | | | [A.25] Robo | 1462,50 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 243750,28 | | |
| | | | [E.14] Escapes de información | 12187,51 | | |
| | | | [E.19] Fugas de información | 24375,03 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,51 | 2437,50 | |
| | | | [A.15] Modificación deliberada de la información | 12187,51 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.18] Destrucción de información | 8531,26 | 4265,63 | 8531,26 |
| | | | [A.19] Divulgación de información | 8531,26 | 8531,26 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 243750,28 | | |
| | | | [I.6] Corte del suministro eléctrico | 243750,28 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,51 | | |
| | | | [A.7] Uso no previsto | 12187,51 | | |
| | | | [A.11] Acceso no autorizado | 12187,51 | 2437,50 | 12187,51 |
| | | | [A.25] Robo | 1462,50 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 40625,05 | | |
| | | | [I.6] Corte del suministro eléctrico | 8125,01 | | |
| | | | [A.6] Abuso de privilegios de acceso | 406,25 | | |
| | | | [A.7] Uso no previsto | 406,25 | | |
| | | | [A.11] Acceso no autorizado | 406,25 | 81,25 | 406,25 |
| | | | [A.25] Robo | 48,75 | | |

***Tabla 360. Riesgos residuales sobre activo S4***

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| **S5** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 115,17 | | |
| | | | [I.6] Corte suministro eléctrico | 24375,66 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 2620,38 | | |
| | | | [E.4] Errores de configuración | 18281,74 | | |
| | | | [E.25] Pérdida de equipos | 585,02 | | |
| | | | [A.11] Acceso no autorizado | 3656,35 | 731,27 | 3656,35 |
| | | | [A.25] Robo | 731,27 | | |
| | | D1 | [E.15] Alteración accidental de la información | 60939,15 | | |
| | | | [E.18] Destrucción de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | 24375,66 | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.6] Abuso de privilegios de acceso | 60939,15 | | |
| | | | [A.11] Acceso no autorizado | 60939,15 | 12187,83 | 60939,15 |
| | | | [A.18] Destrucción de la información | 24375,66 | 12187,83 | 24375,66 |
| | | | [A.19] Divulgación de la información | 24375,66 | 24375,66 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | | |
| | | | [A.25] Robo | 1462,54 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [E.14] Escapes de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | 2437,57 | |
| | | | [A.15] Modificación deliberada de la información | 12187,83 | | |
| | | | [A.18] Destrucción de información | 8531,48 | 4265,74 | 8531,48 |
| | | | [A.19] Divulgación de información | 8531,48 | 8531,48 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | 2437,57 | 12187,83 |
| | | | [A.25] Robo | 1462,54 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 40626,10 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [I.6] Corte del suministro eléctrico | 8125,22 | | |
| | | | [A.6] Abuso de privilegios de acceso | 406,26 | | |
| | | | [A.7] Uso no previsto | 406,26 | | |
| | | | [A.11] Acceso no autorizado | 406,26 | 81,25 | 406,26 |
| | | | [A.25] Robo | 48,75 | | |

***Tabla 361. Riesgos residuales sobre activo S5***

| ACTIVO | VALOR | AMENAZA | | RIESGO RESIDUAL | RR2 | RR3 |
|---|---|---|---|---|---|---|
| **S6** | 1218782,98 | AUX1 | [I.5] Avería de origen físico o lógico | 115,17 | | |
| | | | [I.6] Corte suministro eléctrico | 24375,66 | | |
| | | | [I.10] Degradación de los soportes de almacenamiento de la información | 2620,38 | | |
| | | | [E.4] Errores de configuración | 18281,74 | | |
| | | | [E.25] Pérdida de equipos | 585,02 | | |
| | | | [A.11] Acceso no autorizado | 3656,35 | 731,27 | 3656,35 |
| | | | [A.25] Robo | 731,27 | | |
| | | D1 | [E.15] Alteración accidental de la información | 60939,15 | | |
| | | | [E.18] Destrucción de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | 24375,66 | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | | |
| | | | [A.6] Abuso de privilegios de acceso | 60939,15 | | |
| | | | [A.11] Acceso no autorizado | 60939,15 | 12187,83 | 60939,15 |
| | | | [A.18] Destrucción de la información | 24375,66 | 12187,83 | 24375,66 |
| | | | [A.19] Divulgación de la información | 24375,66 | 24375,66 | |
| | | HW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | | |
| | | | [A.25] Robo | 2183,02 | | |
| | | SW1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [E.14] Escapes de información | 12187,83 | | |
| | | | [E.19] Fugas de información | 24375,66 | | |
| | | | [A.5] Suplantación de la identidad del usuario | 12187,83 | 2437,57 | |
| | | | [A.15] Modificación deliberada de la información | 12187,83 | | |
| | | | [A.18] Destrucción de información | 8531,48 | 4265,74 | 8531,48 |
| | | | [A.19] Divulgación de información | 8531,48 | 8531,48 | |
| | | SRVD1 | [I.5] Avería de origen físico o lógico | 243756,60 | | |
| | | | [I.6] Corte del suministro eléctrico | 243756,60 | | |
| | | | [A.6] Abuso de privilegios de acceso | 12187,83 | | |
| | | | [A.7] Uso no previsto | 12187,83 | | |
| | | | [A.11] Acceso no autorizado | 12187,83 | 2437,57 | 12187,83 |
| | | | [A.25] Robo | 1462,54 | | |
| | | T1 | [I.5] Avería de origen físico o lógico | 40626,10 | | |
| | | | [I.6] Corte del suministro eléctrico | 8125,22 | | |
| | | | [A.6] Abuso de privilegios de acceso | 406,26 | | |
| | | | [A.7] Uso no previsto | 406,26 | | |
| | | | [A.11] Acceso no autorizado | 406,26 | 81,25 | 406,26 |
| | | | [A.25] Robo | 48,75 | | |

***Tabla 362. Riesgos residuales sobre activo S6***

## 2.2 Preparación de la auditoría

En primer lugar, la empresa auditora prepara la auditoría elaborando y redactando el alcance y las excepciones de alcance de la auditoría. Ambos se irán modificando de manera cooperativa entre la empresa auditora y la empresa auditada en la elaboración del precontrato de auditoría, para de manera iterativa conseguir el alcance detallado final del contrato de auditoría.

### 2.2.1 Alcance

A continuación, se muestra el primer alcance de auditoría elaborada por la empresa auditora. Se mencionarán cada una de las acciones que estarán dentro del alcance de auditoría.

- **Planos de las instalaciones:** Serán necesarios los planos de la empresa "Sanitaria AMS S.L." para la planificación de la auditoría y para saber cómo se encuentra distribuido el sistema de información dentro de la empresa.
- **Estado del servidor:**
  - Acceso mediante cuentas: Se estudiará como es el acceso al servidor, esto conlleva saber quién tiene acceso al mismo, a que partes tiene acceso cada cuenta, saber si hay restricciones y cuáles son dependiendo del rol de cada cuenta.
  - Conexión a la red eléctrica: Analizaremos de qué manera está conectado el servidor a la corriente eléctrica y que serie de medidas se toman para ello.
- **Acceso al SI:** Se hará un estudio igual al que se hará en el acceso al servidor, esto conlleva saber quién tiene acceso al Sistema de información desde los diferentes puntos disponibles.
- **Contraseñas:** Se estudiará si existe un sistema de contraseñas que cumpla una serie de requisitos; ya sea complejidad, renovación o control de las mismas.
- **Alarma:** Se estudiará si la empresa "Sanitaria AMS S.L." cuenta con un sistema de alarma y si este cumple con los requisitos necesarios para permitir la integridad del Sistema de información.
- **Seguros:**

  - De riesgos laborales y responsabilidad civil: Se repasarán los contratos que la empresa tenga contratados para estos casos.
- **Red Wifi: Red Wifi:** A continuación, se detallan cada uno de los aspectos que se van a estudiar para comprobar por completo el estado de la red wifi.
  - Configuración del *router:* Vamos a revisar cada uno de los siguientes aspectos de la configuración del *router.*
    - Contraseña actual acceso
    - Nombre de la red Wifi
    - Contraseña acceso a la red wifi
    - Actualizaciones del *firmware*
    - Tipo de cifrado
    - WPS
    - Red wifi para invitados
    - Filtrado MAC
    - UPnP
- **Protección frente a datos:** Estudiaremos todo lo relativo a como la empresa realiza sus copias de seguridad para proteger sus datos.
- **Cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales.** Se van a comprobar los elementos que están dentro de la aplicación de dicha Ley para ver si estos se cumplen adecuadamente dentro de nuestra empresa.

### 2.2.2 Excepciones de alcance

Las excepciones de alcance de la auditoría se refieren a todos los aspectos que no serán objetos de estudio en la auditoría “Sanitaria AMS S.L.”

- **Formación de los empleados:** No se analizarán la formación de los empleados con lo respectivo al papel que desarrolla dentro del sistema de información.
- **Estado hardware y software del servidor:** No se estudiará ni el estado hardware ni software del servidor de la empresa.
- **Estado hardware y software de los ordenadores de la empresa:** Al igual que con el servidor, no se analizará ni el estado hardware ni software de ninguno de los ordenadores de la empresa.
- **Red eléctrica:** No se estudiará la red eléctrica de la empresa “Sanitaria AMS S.L.”

- **Contratos de los trabajadores:** No se analizarán los contratos de los trabajadores, ni sueldos, ni condiciones, etc.

## 2.2.3 Precontrato de auditoría

La empresa auditora elabora y redacta un precontrato de auditoría, con los diferentes aspectos necesarios que este contiene. Este precontrato se irá modificando de manera cooperativa entre la empresa auditora y la empresa auditada, para así llegar a conseguir el contrato final de auditoría.

### 2.2.3.1 Alcance de auditoría

Después de la realización, de manera telemática, como ya hemos especificado anteriormente por medio de la aplicación Google Meet, con los dos dueños de la empresa "Sanitaria AMS S.L.", se ha acordado que la auditoría tendrá el siguiente alcance.

- **Planos de las instalaciones:** Serán necesarios los planos de la empresa "Sanitaria AMS S.L." para la planificación de la auditoría y para saber cómo se encuentra distribuido el sistema de información dentro de la empresa.
- **Estado del servidor:**
  - Acceso mediante cuentas: Se estudiará como es el acceso al servidor, esto conlleva saber quién tiene acceso al mismo, a que partes tiene acceso cada cuenta, saber si hay restricciones y cuáles son dependiendo del rol de cada cuenta.
  - Conexión a la red eléctrica: Analizaremos de qué manera está conectado el servidor a la corriente eléctrica y que serie de medidas se toman para ello.
- **Acceso al SI:** Se hará un estudio igual al que se hará en el acceso al servidor, esto conlleva saber quién tiene acceso al Sistema de información desde los diferentes puntos disponibles.
- **Contraseñas:** Se estudiará si existe un sistema de contraseñas que cumpla una serie de requisitos; ya sea complejidad, renovación o control de las mismas.
- **Alarma:** Se estudiará si la empresa "Sanitaria AMS S.L." cuenta con un sistema de alarma y si este cumple con los requisitos necesarios para permitir la integridad del Sistema de información.

- **Seguros:**
    - De riesgos laborales y responsabilidad civil: Se repasarán los contratos que la empresa tenga contratados para estos casos.
- **Red Wifi: Red Wifi:** A continuación, se detallan cada uno de los aspectos que se van a estudiar para comprobar por completo el estado de la red wifi.
    - Configuración del *router:* Vamos a revisar cada uno de los siguientes aspectos de la configuración del *router.*
        - Contraseña actual acceso
        - Nombre de la red Wifi
        - Contraseña acceso a la red wifi
        - Actualizaciones del *firmware*
        - Tipo de cifrado
        - WPS
        - Red wifi para invitados
        - Filtrado MAC
        - UPnP
- **Protección frente a datos:** Estudiaremos todo lo relativo a como la empresa realiza sus copias de seguridad para proteger sus datos.
    - Copias de seguridad: Se analizarán todos los aspectos descritos para ver cómo se hacen las copias de seguridad dentro de la empresa.
        - ¿Qué información se copia?
        - ¿Cada cuánto tiempo se hacen las copias?
        - Tipo de copias que se hacen
        - ¿Dónde se hacen?
        - Control de soportes
        - ¿Cuánto tiempo se guardan?
        - Comprobación de validez de las copias
        - Cifrado de la información
        - Documentación del proceso
        - Borrado de la información
- **Cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales.** Se van a comprobar los elementos que están dentro de la aplicación de dicha Ley para ver si estos se cumplen adecuadamente dentro de nuestra empresa.
    - Notificación de brecha de seguridad: Vamos a estudiar si se realiza el procedimiento en caso de que se produzca alguna brecha de seguridad.

- Registro de las actividades de tratamiento: Analizaremos que se lleva un registro interno de todos los datos personales que lleva a cabo la identidad.
- Consentimiento: Se estudiará si se lleva a cabo el procedimiento adecuada en cuanto al consentimiento con respecto a los datos.
- Datos de personas fallidas: Analizaremos si se realizan las acciones adecuadas en cuanto a los datos de una persona fallecida.
- Consentimiento de menores: Analizaremos si se realizan las acciones adecuadas en cuanto a los datos de un menor.
- Tratamiento de datos por obligación legal, interés público o ejercicios de poderes públicos: Estudiaremos todo lo relativo a si realizamos las acciones correctas con respecto al tratamiento de datos por obligación legal, interés público o ejercicios de poderes públicos.
- Derechos ARCO: Se analizará todo lo relativo a los derechos ARCO de las personas.
- Datos de contacto y de empresarios individuales: Estudiaremos si se cumplen todas las acciones con respecto a estos datos.
- Bloqueo de datos: Estudiaremos si se realizan las acciones adecuadas en caso de que se necesite hacer un bloqueo de datos.
- Delegado de protección de datos: Analizaremos todo lo relativo al Delegado de protección de datos.
- Derechos digitales: Analizaremos si se llevan a cabo las acciones adecuadas en cuanto a los nuevos derechos digitales.

#### 2.2.3.2 Compromiso de confidencialidad

La empresa auditora y la auditada deben firmar un contrato de confidencialidad en el cual quedará reflejado que se va a compartir material confidencial, pero se restringirá su uso público. (INCIBE, n.d.-a)

**Acuerdo de confidencialidad**

En _____ a __ de _____ de 20__

De una parte, Sanitaria AMS S.L. (en adelante, CLIENTE), con C.I.F X00000000 y domicilio social en Calle Sn, 1, representada por D. Antonio Muñoz Segura actuando en nombre y representación de esta entidad en virtud de su condición de administrador.

De otra parte, Antonio Muñoz Segura S.L. (en adelante, PROVEEDOR), con C.I.F. 53599670X y domicilio social en Calle Sargento José Martínez, 1, representada por D. Antonio Muñoz Segura actuando en nombre y representación de esta entidad en virtud de su condición de administrador.

Ambas partes acuerdas mutuamente, la capacidad legal necesaria para la suscripción del presente acuerdo y el cumplimiento y a dar cumplimiento a las siguientes obligaciones:

I. Que CLIENTE es una organización dedicada a Centro Sanitario y por tanto es responsable de la información generada y gestionada en su actividad.
II. Que PROVEEDOR es una organización dedicada a auditorías y proporciona servicios de auditoría informática a CLIENTE.
III. Que **PROVEEDOR** durante la prestación de sus servicios a CLIENTE puede recibir información confidencial de CLIENTE o disponer de acceso o de potencial acceso la misma. En este sentido se considera por información confidencial, toda información relativa a: procesos de negocio, planes de marketing, planes estratégicos, clientes, proveedores know-how, métodos, análisis funcionales, código fuente, estudios de mercado, estadísticas, datos financieros, análisis de viabilidad, especificaciones técnicas, fórmulas, diseños, estudios, aquella afectada por LOPD y toda aquella información que **CLIENTE** no haya autorizado de modo explícito a **PROVEEDOR** su libre uso o difusión.
IV. **PROVEEDOR** solo hará uso de la información facilitada por **CLIENTE** en el ámbito de los servicios prestados por **PROVEEDOR**, descritos en el apartado II. En este sentido **PROVEEDOR** se compromete a guardar el deber de secreto y mantenerla confidencialidad de la información cedida, trasladando este deber a todas aquellas personas (empleados, personal subcontratado, becarios, etc.) o entidades que dispongan de acceso a esta información en el desarrollo de sus funciones y obligaciones en relación a los servicios prestados a **CLIENTE**.

Las personas o entidades citadas en el párrafo anterior y que tengan acceso a información confidencial de **CLIENTE** en el marco de la prestación del servicio, no disponen de permiso para reproducir, modificar, publicar o difundir o comunicar a terceros dicha información sin previa autorización explícita de **CLIENTE**.

A su vez, **PROVEEDOR** se compromete a aplicar tanto las medidas de seguridad exigibles por la legislación vigente, como las medidas de seguridad

que aplicaría **PROVEEDOR** respecto a su propia información confidencial para garantizar la confidencialidad de la misma.

V. Sin perjuicio de lo reflejado en este acuerdo, tanto **CLIENTE** como **PROVEEDOR**, aceptan las siguientes exclusiones relativas al mantenimiento de la confidencialidad:
   a. Si la información es accesible a través de medios públicos en el momento de su cesión.
   b. Si la información es conocida por **PROVEEDOR** previo a la suscripción del este acuerdo, siempre y cuando no esté sujeta a la obligación de preservar su confidencialidad.
   c. Si la legislación vigente o un requerimiento judicial exige su difusión. En cuyo caso **PROVEEDOR** informará a **CLIENTE** de esta situación y tratará de preservar la confidencialidad en el tratamiento de la información.

VI. La propiedad intelectual de la información tratada en el marco de este acuerdo pertenece a **CLIENTE**.

VII. Si se produce cualquier revelación, difusión o utilización de la información facilitada por **CLIENTE** a **PROVEEDOR** en el ámbito de este acuerdo, de modo distinto a lo reflejado en este acuerdo, ya sea de forma fraudulenta o por mera negligencia, **PROVEEDOR** deberá indemnizar a **CLIENTE** por los daños y perjuicios ocasionados, con independencia de las acciones civiles o penales que se puedan derivar.

VIII. **PROVEEDOR** se compromete a devolver la información confidencial cedida por **CLIENTE** en el ámbito de la prestación del servicio, una vez finalizada la relación contractual.

IX. De acuerdo a los dispuesto en artículo 5 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, ambas partes se informan respectivamente que los datos de carácter personal intercambiados en el marco de la relación contractual serán incluidos en los ficheros de los que cada una de ellas es titular, siendo la finalidad de estos tratamientos el soporte en el desarrollo de las tareas en el ámbito de la prestación del servicio. Dichos datos no serán cedidos a terceros.
   - Adicionalmente, ambas partes se obligan a garantizar, el cumplimiento de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y de su Reglamento de Desarrollo, aprobado por el Real Decreto 1720/2007. Asimismo, para ejercer los derechos de acceso, rectificación, cancelación y oposición cualquiera de las partes deberá dirigirse mediante comunicación formal a las direcciones recogidas al inicio de este acuerdo.

X. Este acuerdo tendrá validez a partir del momento en que quede firmado por ambas partes, y se extenderá de forma indefinida, a pesar de que haya finalizado la relación contractual.

XI. Ante cualquier disputa o conflicto que pueda surgir relativa a la interpretación y/o cumplimiento del presente acuerdo, ambas partes se someten a los Juzgados y Tribunales de `Granada`, renunciando a su fuero propio.

Y en virtud de los establecido anteriormente, ambas partes firman por duplicado este acuerdo, en todas sus hojas, en el lugar y las fechas citados.

En nombre y representación del **CLIENTE**

En nombre y representación de **PROVEEDOR**

#### 2.2.3.3 Plazos

La empresa auditora se compromete a entregar un presupuesto y plan de trabajo a la empresa auditada “Sanitaria AMS S.L.” antes de pasada la fecha de tres semanas después de la firma del precontrato de auditoría.

#### 2.2.3.4 Coste

La empresa auditada debe abonar el 20 % del coste total de la auditoría cuando la empresa auditora le haga entrega del estudio previo de auditoría. Por lo tanto, como la auditoría tiene un coste total de 1840,51 € la empresa auditada deberá abonar la cantidad de 368.11 €

#### 2.2.3.5 Permisos de acceso

La empresa “Sanitaria AMS S.L” se compromete a facilitar acceso a su sistema de información, a las cuentas del mismo y a sus instalaciones a la empresa auditada “Antonio Muñoz Segura S.L”.

En nombre y representación del **CLIENTE**

En nombre y representación de **PROVEEDOR**

## 2.2.4 Plan y presupuesto

### 2.2.4.1 Adquirir conocimiento global

Para adquirir conocimiento global del SI, se han pedido datos de auditorías de complimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales, que se habían hecho anteriormente en la empresa “Sanitaria AMS S.L.”. Además, se han realizado varías videoconferencias con los dueños y empleados de la empresa para recoger información relativa a la misma.

Por último, se han revisado toda la documentación interna del sistema de información, listado de clientes, facturación, entre otros, para contrastar con los datos recogidos en las entrevistas y de esta manera ver si su veracidad.

### 2.2.4.2 Medios

En este apartado se detallan todos los medios necesarios para la realización de la auditoría, tanto los proporcionados por la empresa auditada “Sanitaria AMS S.L”, como por la empresa auditora, “Antonio Muñoz Segura”.

**Medios proporcionados por “Sanitaria AMS S.L.”:**

- Técnicos:
  - Copias de los planos de la empresa
  - Cuenta de usuario de administrador con permisos para acceder al servidor
  - Descripción detallada de cómo se conecta el servidor a la red eléctrica
  - Listado de cuentas de cada uno de los trabajadores con sus cuentas, permisos y roles en cada una de ellas.
  - Contrato del sistema de alarma
  - Pólizas de los seguros de riesgos laborales y responsabilidad civil
  - Acceso al *router* wifi de la empresa
  - Horario de trabajo de la empresa
  - Sala para reuniones, para realización de las entrevistas

**Medios proporcionados por “Antonio Muñoz Segura S.L”:**

- Técnicos:
    - 1 x ordenador portátil Lenovo IdeaPad G50
    - 1 x Ipad
    - Google Drive (almacenamiento, Documentos de Google, Hojas de cálculo de Google)
    - Microsoft Office Profesional Plus 2016
    - Coche para el transporte desde “Antonio Muñoz Segura” hasta “Sanitaria AMS S.L.”
    - Precontrato de auditoría
    - Contrato de Auditoría
    - Meet
    - TeamViewer
- Humanos:
    - Estudiante Grado en Ingeniería Informática (Auditor Junior)

Cabe destacar que la empresa auditada deberá permitir instalar el programa TeamViewer en su servidor para de esta manera la empresa auditora poder entrar mediante un escritorio remoto en sus ordenadores y poder hacer las comprobaciones pertinentes del sistema de información.

#### 2.2.4.3 Plan de trabajo

Cabe destacar que se había realizado un plan de trabajo con una planificación teniendo en cuenta la situación actual. Después de esta planificación, nos encontramos ante el suceso del virus “SARS-CoV-2”, por lo que se tuvo que realizar una nueva planificación ajustándose a las medidas que implican el estado de alarma.

En primer lugar, vamos a añadir la planificación inicial realizada por la empresa “Antonio Muñoz Segura S.L”. Vamos a detallar las tareas que se llevarán a cabo en la auditoría; fecha inicio, fecha fin, duración, medios necesarios y pequeña descripción. En cuanto a las fechas de realización, hemos tomado como inicio el día 4 de mayo de 2020.

A. **Primera visita a "Sanitaria AMS S.L." y reunión con los dueños.** En esta tarea, el estudiante, tendrá una primera reunión a modo de toma de contacto con la empresa "Sanitaria AMS S.L.".
   i. **Fecha inicio:** 4/05/2020, hora: 9:30
   ii. **Fecha fin:** 4/05/2020, hora: 11:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, dueños de "Sanitaria AMS S.L.", Ipad y Google Drive.
B. **Estudio de planos.** El estudiante estudiará los planos para saber cómo está distribuido el Sistema de información, para saber dónde está el *router*, el servidor y los demás ordenadores de la empresa.
   i. **Fecha inicio:** 4/05/2020, hora: 11:30
   ii. **Fecha fin:** 4/05/2020, hora: 13:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, planos de "Sanitaria AMS S.L", Ipad y Google Drive.
C. **Comprobación de pólizas.** El estudiante analizará las pólizas de seguros que tenga contratados la empresa para cubrir las pérdidas de diferentes tipos que puedan ocurrir en la empresa.
   i. **Fecha inicio:** 4/05/2020, hora: 17:30
   ii. **Fecha fin:** 4/05/2020, hora: 19:00
   iii. **Duración:** 1 hora y 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática y pólizas de seguros de "Sanitaria AMS S.L", Ipad y Google Drive.
D. **Estudio de contrato de alarma.** El estudiante estudiará el contrato que tenga contratado la empresa "Sanitaria AMS S.L" para su sistema de alarma.
   i. **Fecha inicio:** 4/05/2020, hora: 19:00
   ii. **Fecha fin:** 4/05/2020, hora: 20:30
   iii. **Duración:** 1 hora y 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática y contrato de alarma de "Sanitaria AMS S.L", Ipad y Google Drive.
E. **Preparación de entrevistas.** El estudiante analizará todos los datos obtenidos hasta ahora y preparará los guiones de todas las entrevistas.
   i. **Fecha inicio:** 5/05/2020, hora: 9:30
   ii. **Fecha fin:** 6/05/2020, hora: 20:30
   iii. **Duración:** 14 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.
F. **Realización de entrevistas.** El estudiante realizará las entrevistas que ha preparado con anterioridad a los correspondientes trabajadores de la empresa "Sanitaria AMS S.L".
   i. **Fecha inicio:** 7/05/2020, hora: 9:30
   ii. **Fecha fin:** 9/05/2020, hora: 13:30
   iii. **Duración:** 20 horas

   iv. **Medios necesarios:** Estudiante de Ingeniería informática, sala de reuniones, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

G. **Analizar servidor.** En esta tarea, el estudiante revisará y analizará qué cuentas tienen acceso al servidor y cuáles son sus permisos, además analizará como está realizada la conexión de este a la red eléctrica.
   i. **Fecha inicio:** 11/05/2020, hora: 9:30
   ii. **Fecha fin:** 11/05/2020, hora: 11:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, cuenta de usuario de administrador con permisos para acceder al servidor, Ipad y Google Drive.

H. **Analizar cuentas SI.** El estudiante estudiará todas las cuentas que tienen acceso a alguna parte del SI y cuáles son los roles que tiene cada una de estas.
   i. **Fecha inicio:** 11/05/2020, hora: 11:30
   ii. **Fecha fin:** 11/05/2020, hora: 13:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, listado de cuentas de cada uno de los trabajadores con sus cuentas, permisos y roles en cada una de ellas, Ipad y Google Drive.

I. **Analizar contraseñas.** El estudiante analizará qué medidas se toman en lo relativo a las contraseñas usadas para por los usuarios en sus cuentas dentro del Sistema de información.
   i. **Fecha inicio:** 11/05/2020, hora: 17:30
   ii. **Fecha fin:** 11/05/2020, hora: 19:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad y Google Drive.

J. **Analizar red Wifi.** El estudiante analizará todo lo relativo a la red wifi, configuración, seguridad, entre otros.
   i. **Fecha inicio:** 11/05/2020, hora: 19:30
   ii. **Fecha fin:** 12/05/2020, hora: 10:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Lenovo IdeaPad G50, acceso al *router* de la empresa, Ipad y Google Drive.

K. **Analizar sistema de copias de seguridad.** El estudiante estudiará todo lo relativo a como se realizan las copias de seguridad en la empresa “Sanitaria AMS S.L”.
   i. **Fecha inicio:** 12/05/2020, hora: 10:30
   ii. **Fecha fin:** 12/05/2020, hora: 13:30
   iii. **Duración:** 3 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, cuenta de usuario de administrador con permisos para acceder al servidor, Ipad y Google Drive.

L. **Analizar cumplimiento de la LOPD.** El estudiante analizará las medidas que se toman dentro de la empresa “Sanitaria AMS S.L” para el cumplimiento de la LOPD.
   i. **Fecha inicio:** 12/05/2020, hora: 17:30
   ii. **Fecha fin:** 13/05/2020, hora: 13:30
   iii. **Duración:** 7 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad y Google Drive.

M. **Comparar datos entrevista y datos obtenidos.** Se compararán todos los resultados de las entrevistas con los datos obtenidos en los análisis.
   i. **Fecha inicio:** 13/05/2020, hora: 17:30
   ii. **Fecha fin:** 14/05/2020, hora: 13:30
   iii. **Duración:** 7 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

N. **Preparar nuevos guiones de entrevistas.** Después de haber organizado y analizado los datos obtenidos en la hasta la tarea L, se preparan los guiones de las nuevas entrevistas.
   i. **Fecha inicio:** 14/05/2020, hora: 17:30
   ii. **Fecha fin:** 16/05/2020, hora: 13:30
   iii. **Duración:** 14 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

O. **Realizar nuevas entrevistas.** El estudiante realizará las entrevistas que se han preparado con anterioridad a todos los empleados de la empresa “Sanitaria AMS S.L”.
   i. **Fecha inicio:** 18/05/2020, hora: 9:30
   ii. **Fecha fin:** 19/05/2020, hora: 20:30
   iii. **Duración:** 14 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, sala de reuniones, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

P. **Realizar informe final de auditoría.** Con todos los datos recogidos en las anteriores tareas el estudiante realizará el informe final de auditoría para la empresa “Sanitaria AMS S.L”.
   i. **Fecha inicio:** 20/05/2020, hora: 9:30
   ii. **Fecha fin:** 23/05/2020, hora: 13:30
   iii. **Duración:** 25 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

Q. **Entrega y exposición del informe final de auditoría.** Después de haber realizado el informe final de auditoría, el estudiante se lo entregará a los dueños de la empresa, además, se lo explicará y expondrá de la forma más detallada posible.
   i. **Fecha inicio:** 25/05/2020, hora: 9:30
   ii. **Fecha fin:** 25/05/2020, hora: 11:30

iii. **Duración:** 2 horas
iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

A continuación, adjuntamos una tabla a modo de resumen de las tareas de la planificación.

| ID tarea | Tarea precedente | Fecha inicio | Fecha fin | Duración (horas) | Tarea |
|---|---|---|---|---|---|
| A | - | 4/05/2020 | 4/05/2020 | 2 | Primera visita a “Sanitaria AMS S.L.” y reunión con los dueños |
| B | A | 4/05/2020 | 4/05/2020 | 2 | Estudio de planos |
| C | B | 4/05/2020 | 4/05/2020 | 1 h 30 min | Comprobación de pólizas |
| D | C | 4/05/2020 | 4/05/2020 | 1 h 30 min | Estudio de contrato de alarma |
| E | D | 5/05/2020 | 6/05/2020 | 14 | Preparación de entrevistas |
| F | E | 7/05/2020 | 9/05/2020 | 20 | Realización de entrevistas |
| G | F | 11/05/2020 | 11/05/2020 | 2 | Analizar servidor |
| H | G | 11/05/2020 | 11/05/2020 | 2 | Analizar cuentas |
| I | H | 11/05/2020 | 11/05/2020 | 2 | Analizar contraseñas |
| J | I | 11/05/2020 | 12/05/2020 | 2 | Analizar red Wifi |
| K | J | 12/05/2020 | 12/05/2020 | 3 | Analizar sistema de copias de seguridad |
| L | K | 12/05/2020 | 13/05/2020 | 7 | Analizar cumplimiento de la LOPD |
| M | L | 13/05/2020 | 14/05/2020 | 7 | Comparar datos entrevista y datos obtenidos |
| N | M | 14/05/2020 | 16/05/2020 | 14 | Preparar nuevos guiones de entrevistas |
| O | N | 18/05/2020 | 19/05/2020 | 14 | Realizar nuevas entrevistas |
| P | O | 20/05/2020 | 23/05/2020 | 25 | Realizar informe final de auditoría |
| Q | P | 25/05/2020 | 25/05/2020 | 2 | Entrega y exposición del informe final de auditoría |
| | | | | TOTAL: 121 | |

***Tabla 363. Planificación tareas auditoría***

En segundo lugar, se ha realizado la nueva planificación, la cual se va a detallar a continuación, con nuevas fechas de fin, nuevos medios y nueva duración. La fecha de inicio que se ha tomado ha sido la misma que anteriormente, el 1 de mayo de 2020.

A. **Primera videoconferencia con los dueños de "Sanitaria AMS S.L".** En esta tarea, el estudiante, tendrá una primera videoconferencia a modo de toma de contacto con la empresa "Sanitaria AMS S.L.".
   i. **Fecha inicio:** 4/05/2020, hora: 9:30
   ii. **Fecha fin:** 4/05/2020, hora: 10:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, dueños de "Sanitaria AMS S.L.", Ipad, Google Drive, Lenovo IdeaPad G50 y Meet.
B. **Estudio de planos.** El estudiante estudiará los planos para saber cómo está distribuido el Sistema de información, para saber dónde está el *router*, el servidor y los demás ordenadores de la empresa.
   i. **Fecha inicio:** 4/05/2020, hora: 10:30
   ii. **Fecha fin:** 4/05/2020, hora: 11:00
   iii. **Duración:** 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, planos de "Sanitaria AMS S.L", Ipad y Google Drive.
C. **Comprobación de pólizas.** El estudiante analizará las pólizas de seguros que tenga contratados la empresa para cubrir las pérdidas de diferentes tipos que puedan ocurrir en la empresa.
   i. **Fecha inicio:** 4/05/2020, hora: 11:00
   ii. **Fecha fin:** 4/05/2020, hora: 12.30
   iii. **Duración:** 1 hora y 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática y pólizas de seguros de "Sanitaria AMS S.L", Ipad y Google Drive.
D. **Estudio de contrato de alarma.** El estudiante estudiará el contrato que tenga contratado la empresa "Sanitaria AMS S.L" para su sistema de alarma.
   i. **Fecha inicio:** 4/05/2020, hora: 12:30
   ii. **Fecha fin:** 4/05/2020, hora: 13:30
   iii. **Duración:** 1 hora
   iv. **Medios necesarios:** Estudiante de Ingeniería informática y contrato de alarma de "Sanitaria AMS S.L", Ipad y Google Drive.
E. **Preparación de entrevistas.** El estudiante analizará todos los datos obtenidos hasta ahora y preparará los guiones de todas las entrevistas.
   i. **Fecha inicio:** 5/05/2020, hora: 17:30
   ii. **Fecha fin:** 6/05/2020, hora: 20:30
   iii. **Duración:** 10 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.
F. **Realización de entrevistas.** El estudiante realizará las entrevistas de manera telemática que ha preparado con anterioridad a los correspondientes trabajadores de la empresa "Sanitaria AMS S.L".
   i. **Fecha inicio:** 7/05/2020, hora: 9:30

   ii. **Fecha fin:** 7/05/2020, hora: 13:30
   iii. **Duración:** 4 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, sala de reuniones, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016, Google Drive y Meet.

G. **Analizar servidor.** En esta tarea, el estudiante revisará y analizará qué cuentas tienen acceso al servidor y cuáles son sus permisos, además analizará como está realizada la conexión de este a la red eléctrica. Todo esto estará realizado con un escritorio remoto con la aplicación TeamViewer.
   i. **Fecha inicio:** 7/05/2020, hora: 17:30
   ii. **Fecha fin:** 7/05/2020, hora: 20:30
   iii. **Duración:** 3 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, cuenta de usuario de administrador con permisos para acceder al servidor, Ipad, Google Drive, Lenovo IdeaPad G50 y TeamViewer.

H. **Analizar cuentas SI.** El estudiante estudiará todas las cuentas que tienen acceso a alguna parte del SI y cuáles son los roles que tiene cada una de estas. Todo esto estará realizado con un escritorio remoto con la aplicación TeamViewer.
   i. **Fecha inicio:** 8/05/2020, hora: 9:30
   ii. **Fecha fin:** 8/05/2020, hora: 11:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, listado de cuentas de cada uno de los trabajadores con sus cuentas, permisos y roles en cada una de ellas, Ipad, Google Drive, Lenovo IdeaPad G50 y TeamViewer.

I. **Analizar contraseñas.** El estudiante analizará qué medidas se toman en lo relativo a las contraseñas usadas para por los usuarios en sus cuentas dentro del Sistema de información. Todo esto se realizará mediante videoconferencias con la aplicación Meet.
   i. **Fecha inicio:** 8/05/2020, hora: 11:30
   ii. **Fecha fin:** 8/05/2020, hora: 13:30
   iii. **Duración:** 2 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad y Google Drive, Lenovo IdeaPad G50 y Meet.

J. **Analizar red Wifi.** El estudiante analizará todo lo relativo a la red wifi, configuración, seguridad, entre otros. Todo esto estará realizado con un escritorio remoto con la aplicación TeamViewer.
   i. **Fecha inicio:** 8/05/2020, hora: 17:30
   ii. **Fecha fin:** 8/05/2020, hora: 19:00
   iii. **Duración:** 1 hora y 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Lenovo IdeaPad G50, acceso al *router* de la empresa, Ipad y Google Drive y Team Viewer.

K. **Analizar sistema de copias de seguridad.** El estudiante estudiará todo lo relativo a como se realizan las copias de seguridad en la empresa “Sanitaria

AMS S.L". Todo esto estará realizado con un escritorio remoto con la aplicación TeamViewer.

i. **Fecha inicio:** 8/05/2020, hora: 19:00
ii. **Fecha fin:** 9/05/2020, hora: 11:00
iii. **Duración:** 3 horas
iv. **Medios necesarios:** Estudiante de Ingeniería informática, cuenta de usuario de administrador con permisos para acceder al servidor, Ipad, Google Drive, Lenovo IdeaPad G50 y TeamViewer.

L. **Analizar cumplimiento de la LOPD.** El estudiante analizará las medidas que se toman dentro de la empresa "Sanitaria AMS S.L" para el cumplimiento de la LOPD. Todo esto se realizará mediante videoconferencias con la aplicación Meet.
   i. **Fecha inicio:** 9/05/2020, hora: 11:00
   ii. **Fecha fin:** 9/05/2020, hora: 13:30
   iii. **Duración:** 2 horas y 30 minutos
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad y Google Drive, Lenovo IdeaPad G50 y Meet.

M. **Comparar datos entrevista y datos obtenidos.** Se compararán todos los resultados de las entrevistas con los datos obtenidos en los análisis.
   i. **Fecha inicio:** 11/05/2020, hora: 9:30
   ii. **Fecha fin:** 11/05/2020, hora: 20:30
   iii. **Duración:** 7 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

N. **Preparar nuevos guiones de entrevistas.** Después de haber organizado y analizado los datos obtenidos en la hasta la tarea L, se preparan los guiones de las nuevas entrevistas.
   i. **Fecha inicio:** 12/05/2020, hora: 9:30
   ii. **Fecha fin:** 13/05/2020, hora: 20:30
   iii. **Duración:** 14 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

O. **Realizar nuevas entrevistas.** El estudiante realizará las entrevistas que se han preparado con anterioridad a todos los empleados de la empresa "Sanitaria AMS S.L". Todo esto se realizará mediante videoconferencias con la aplicación Meet.
   i. **Fecha inicio:** 14/05/2020, hora: 9:30
   ii. **Fecha fin:** 15/05/2020, hora: 20:30
   iii. **Duración:** 14 horas
   iv. **Medios necesarios:** Estudiante de Ingeniería informática, sala de reuniones, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016, Google Drive y Meet.

P. **Realizar informe final de auditoría.** Con todos los datos recogidos en las anteriores tareas el estudiante realizará el informe final de auditoría para la empresa "Sanitaria AMS S.L".
   i. **Fecha inicio:** 16/05/2020, hora: 9:30

ii. **Fecha fin:** 19/05/2020, hora: 20:30
iii. **Duración:** 20 horas
iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016 y Google Drive.

**Q. Entrega y exposición del informe final de auditoría.** Después de haber realizado el informe final de auditoría, el estudiante se lo entregará a los dueños de la empresa, además, se lo explicará y expondrá de la forma más detallada posible. Todo esto se realizará mediante videoconferencias con la aplicación Meet.

i. **Fecha inicio:** 20/05/2020, hora: 9:30
ii. **Fecha fin:** 20/05/2020, hora: 11:30
iii. **Duración:** 2 horas
iv. **Medios necesarios:** Estudiante de Ingeniería informática, Ipad, Lenovo IdeaPad G50, Microsoft Office Profesional Plus 2016, Google Drive y Meet.

*NOTA: Se entrega el informe de auditoría de manera digital por medios online (correo, Google Drive), pero queda pendiente, pasado el estado de alarma, realizar la entrega en mano del informe de auditoría a la empresa "Sanitaria AMS S.L." por parte de la empresa auditora "Antonio Muñoz Segura S.L.".*

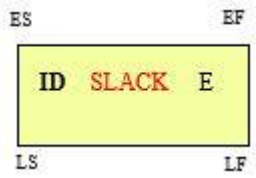
| ID tarea | Tarea precedente | Fecha inicio | Fecha fin | Duración (horas) | Tarea |
|---|---|---|---|---|---|
| A | - | 4/05/2020 | 4/05/2020 | 2 | Primera video conferencia con los dueños de "Sanitaria AMS S.L." |
| B | A | 4/05/2020 | 4/05/2020 | 30 min | Estudio de planos |
| C | B | 4/05/2020 | 4/05/2020 | 1 h 30 min | Comprobación de pólizas |
| D | C | 4/05/2020 | 4/05/2020 | 1 | Estudio de contrato de alarma |
| E | D | 5/05/2020 | 6/05/2020 | 10 | Preparación de entrevistas |
| F | E | 7/05/2020 | 7/05/2020 | 4 | Realización de entrevistas |
| G | F | 7/05/2020 | 7/05/2020 | 3 | Analizar servidor |
| H | G | 8/05/2020 | 8/05/2020 | 2 | Analizar cuentas |
| I | H | 8/05/2020 | 8/05/2020 | 2 | Analizar contraseñas |
| J | I | 8/05/2020 | 8/05/2020 | 1 h y 30 min | Analizar red Wifi |
| K | J | 8/05/2020 | 9/05/2020 | 3 | Analizar sistema de copias de seguridad |
| L | K | 9/05/2020 | 9/05/2020 | 2 h y 30 min | Analizar cumplimiento de la LOPD |

| | | | | | |
|---|---|---|---|---|---|
| M | L | 11/05/2020 | 11/05/2020 | 7 | Comparar datos entrevista y datos obtenidos |
| N | M | 12/05/2020 | 13/05/2020 | 14 | Preparar nuevos guiones de entrevistas |
| O | N | 14/05/2020 | 15/05/2020 | 14 | Realizar nuevas entrevistas |
| P | O | 16/05/2020 | 19/05/2020 | 20 | Realizar informe final de auditoría |
| Q | P | 20/05/2020 | 20/05/2020 | 2 | Entrega y exposición del informe final de auditoría |
| | | | | TOTAL: 90 | |

***Tabla 364. Planificación tareas auditoría Covid-19***

#### 2.2.4.3.1 Diagrama PDM

En cuanto al diagrama usado para describir la planificación de nuestra auditoría, se va a utilizar un diagrama de tipo PDM, ya que pensamos que es el más descriptivo. A continuación, antes de realizar el diagrama, vamos a hacer una pequeña descripción de cómo funciona.




- EF = ES + E -1
- LS = LF – E +1
- Tareas finales: LF = EF
- Camino crítico o SLACK: LF – EF = LS – ES

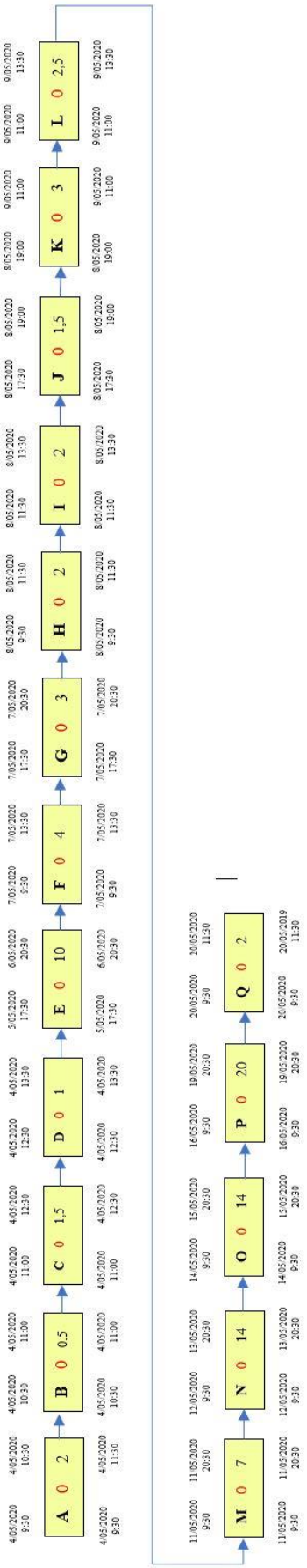



***Ilustración 351. Diagrama PDM planificación***

**Camino crítico:** A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q

Podemos observar que el diagrama tiene una estructura completamente lineal, esto es debido a que la auditoría es realizada por una única persona, por lo que no se pueden realizar tareas de forma paralela y para poder realizar una tarea, debemos haber terminado la anterior siempre.

#### 2.2.4.4 Presupuesto

En este apartado, vamos a tratar detalladamente todos los costes que conllevarán la realización de la auditoría para la empresa "Antonio Muñoz Segura S.L." Cabe destacar que vamos a añadir un 35 % sobre el valor de cada coste que será lo que corresponderá a nuestros beneficios.

- **Coste Lenovo IdeaPad G50:** Se utilizará un portátil Lenovo IdeaPad G50 con un precio de 635.59[9] €. Este equipo será utilizado los 19 días que dura la auditoría. El equipo tiene una vida útil de 6 años (en base a mi propia experiencia), 365 x 6 = 2190 días, por lo tanto, el equipo tiene un **coste de amortización,** (635.59 x 13 días) / 2190 días = 3.77 €
    - ***Coste total = Coste amortización x Beneficio =*** *3.77 x 1.35 =* ***5.08 €***
- **Coste Ipad:** Se utilizará un Ipad Air que tiene un precio de 379[10] €. Este lo vamos a usar durante los 19 días que dura la auditoría. Cada iPad tiene una vida útil de 8 años (basado en mi propia experiencia), 365 x 8 = 2920 días, por lo tanto, el iPad tiene un **coste de amortización,** (379 x 13 días) / 2920 días = 1.68 €
    - ***Coste total = Coste amortización x Beneficio =*** *1.68 x 1.35 =* ***3.61 €***
- **Coste Office Profesional 2016:** El coste del programa es 8.80[11] €/usuario x mes. Como pagamos por cada mes de uso, con pagar la subscripción para un mes ya tenemos suficiente para el tiempo que vamos a usarlo en nuestra auditoría, por lo tanto, **coste de uso =** 8.80 €
    - ***Coste total = Coste de uso x Beneficio =*** *8.80 x 1.35 =* ***11.88 €***

[9] https://www.pccomponentes.com/lenovo-ideapad-g50-70-intel-i7-4510u-8gb-1tb-r5m230-15-6-
[10] https://www.apple.com/es/shop/buy-ipad/ipad-10-2/32gb-gris-espacial-wifi
[11] https://products.office.com/es-es/compare-all-microsoft-office-products?&activetab=tab:primaryr2

- **Coste de transporte:** No hay coste de transporte ya que la auditoría se ha realizado de manera telemática, por lo tanto, no es necesario realizar transporte.
- **Coste Google Drive:** Es gratuito ya que, por ser estudiante de la UJA, podemos hacer uso de este servicio de forma gratuita.
- **Coste Meet:** Es gratuito por el mismo motivo, ya que, por ser estudiante de la UJA, podemos hacer uso de este servicio de forma gratuita.
- **Coste TeamViewer:** No tiene coste alguno, ya que es un software gratuito.

**SALARIOS:** La cantidad que cada trabajador cobrará por su trabajo en esta auditoría. Las horas de trabajo anuales en España son 1944. Por lo tanto, sabiendo el sueldo medio de cada disciplina de trabajo, podemos calcular el precio x hora del trabajador y así calcular el coste que tienen en nuestro trabajo dependiendo de las horas que desarrollen en él.

- **Auditor junior:** Sueldo medio en España: 24.000 €/anuales. Precio hora = 24.000 € / 1944 horas = 12.35 €/hora.
  - ***Coste mano de obra = (Precio hora x horas de trabajo) x Beneficio =*** *(12.35 x 90) X 1.35 =* ***1500.52 €***

Solo hay que calcular este coste de salario, puesto que la auditoría se va a realizar de manera completa por el estudiante de Ingeniería Informática (Auditor Junior).

**Resumen del presupuesto de la auditoría**

| ***Descripción*** | ***Coste (€)*** | |
|---|---|---|
| *Lenovo IdeaPad G50* | 5.08 | |
| *iPad* | 3.61 | |
| *Office Profesional 2016* | 11.88 | |
| *Google Drive* | 0 | |
| *Transporte* | 0 | |
| *Salarios* | 1500.52 | |
| | 1521.09 | **TOTAL** |
| *IVA (21 %)* | 319.42 | |
| | **1840.51** | **TOTAL, A PAGAR** |

***Tabla 365. Resumen del presupuesto de la auditoría***

## 2.3 Análisis del SI

### 2.3.1 Planificación detallada

#### 2.3.1.1 Partición del alcance

En este apartado, hacemos una partición del alcance que anteriormente hemos descrito, de esta manera conseguimos particionar el alcance en todas las tareas que se deben realizar en la auditoría.

Para realizar esta partición, se utiliza un árbol en el que partimos de un nodo inicial hacía abajo, el primer nivel son los segmentos de la auditoría, el segundo nivel las secciones, el tercer nivel subsecciones y el cuarto nivel “subsubsecciones”.

En cuanto a la manera de particionar este árbol se debe tener en cuenta que cada elemento del alcance debe ir en una parte independiente y cada parte debe ser internamente cohesiva.

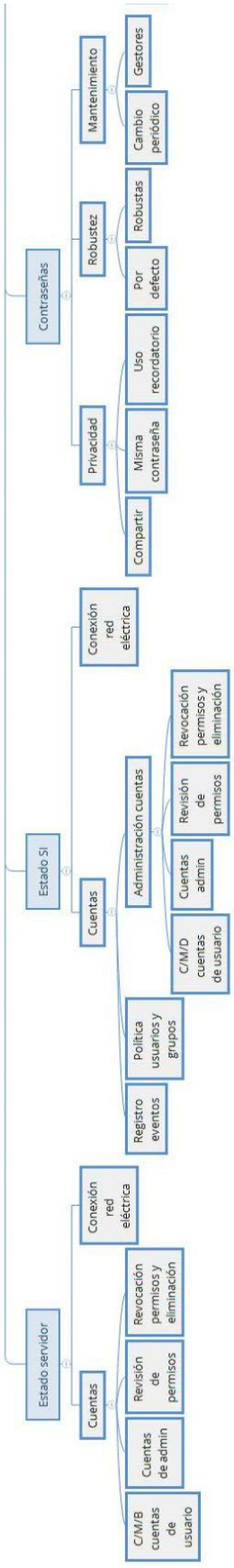



***Ilustración 352. Árbol de partición - Parte 1***

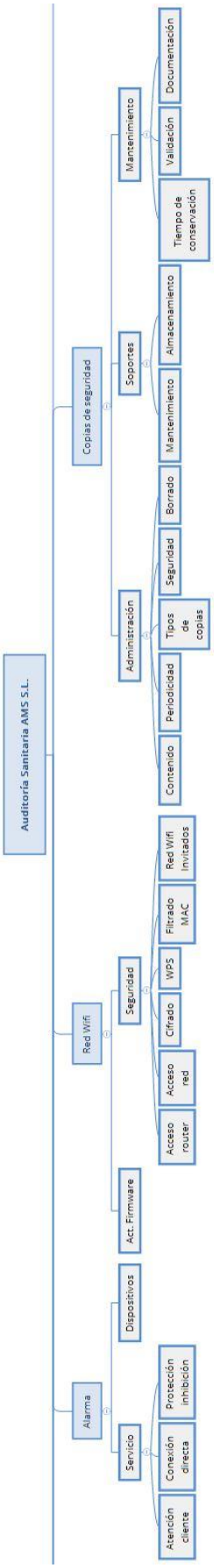



***Ilustración 353. Árbol de partición - Parte 2***

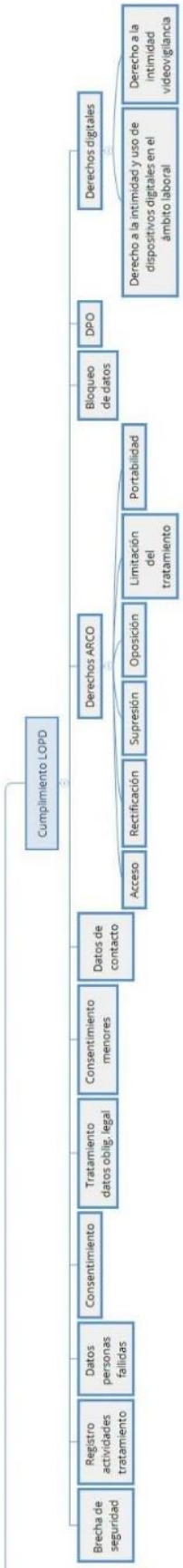



***Ilustración 354. Árbol de partición - Parte 3***

#### 2.3.1.2 Ponderación

A continuación, se debe ponderar el árbol que hemos realizado anteriormente, se ponderan todas las secciones y todos los segmentos. Hay que ponderarlos usando dos tipos de pesos, los técnicos y políticos.

En cuanto a los pesos técnicos, se dan por el equipo de auditoría y se refieren a la importancia que le damos a cada uno. Con respecto a los pesos políticos, son aquellos que le da a cada parte la empresa auditada, es decir los miembros de la empresa le dan un peso cada uno por separado y después se hace la media.

Por último, se debe hacer la media de ambos pesos para de esta manera obtener el peso ponderado del árbol de partición.

Para calcular el peso de cada nodo hoja o subsección, se utiliza la siguiente fórmula.

$$PTSS = \left(\frac{100}{NSS}\right) x\ PSC\ x\ PSG \tag{2.5}$$

Donde:

- PTSS: Peso de la subsección
- NSS: n º de secciones en esa rama
- PSC: peso de la sección en que se encuentra la subsección
- PSG: peso del segmento en el que se encuentra la subsección

Para realizar la ponderación de dichos pesos, se han utilizado las siguientes tablas.

Pesos políticos:

| **Estado servidor** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Cuentas | 60 | 70 | 50 | 60 | 60,00 |
| Conexión red eléctrica | 40 | 30 | 50 | 40 | 40,00 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

***Tabla 366. Pesos políticos***

La tabla anterior es la que se ha usado para ponderar el árbol con respecto a los besos político. En primer lugar, tenemos una tabla por cada sección del árbol y luego una final con todos los segmentos del árbol de alcance. La tabla anterior es una

de ellas, la cual vamos a utilizar para explicar el procedimiento que se ha seguido para realizar la ponderación, todas las demás las podemos consultar en el segundo apéndice.

Hay tantas filas como secciones tengamos dentro de dicho segmento y hay tantas columnas como trabajadores hay en la empresa. Para realizar la ponderación, cada trabajador debe hacerla individualmente sin ver los valores que han dado los demás trabajadores. Cada uno debe darle un peso a cada sección, dependiendo de lo importante que sea para dicho trabajador, en total deben sumar un 100 % entre todas las secciones. A continuación, calculamos la media de la ponderación de todos los trabajadores y de esta manera obtenemos los pesos políticos de cada sección.
Pesos técnicos y la media de ambos:

| **Estado servidor** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Cuentas | 65 | 65 | 60,00 | **62,50** |
| Conexión red eléctrica | 35 | 35 | 40,00 | **37,50** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

***Tabla 367. Pesos técnicos***

En cuanto a los pesos políticos, se ponderan las mismas partes del árbol de partición que para los pesos políticos, aquí tendremos tantas columnas como trabajadores vayan a realizar la auditoría, en este caso sólo hay uno porque la auditoría se realiza por un único auditor. Cuando tenemos todos los pesos técnicos de cada sección, hacemos la media de los pesos políticos y los pesos técnicas y de esta manera ya tenemos lo ponderación del árbol completada.

### 2.3.2 Listas de comprobación

Las listas de comprobación son listas que pueden ser puntuadas con una nota entre 0 y 10, y unos criterios de evaluación para cada pregunta que indica qué nota entre 0 y 10 asignar a la pregunta en función del estado del SI.

Se hacen tantas listas de comprobación como nodos hoja haya en el árbol de partición. Con la media de las notas de los criterios, conseguimos la nota de cada lista de comprobación y que usamos para puntuar cada nodo hoja del árbol de partición.

En cuanto a cómo se hacen las listas de comprobación y en que están basados los criterios de evaluación, estas se hacen basándose en los controles que se han

redactado al principio de la auditoría, en base a esos controles tendríamos la máxima nota en cada criterio y a partir de ahí escribimos los criterios de evaluación desde la máxima nota posible a la mínima.

A continuación, se muestra como es la estructura de las listas de comprobación usadas:

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 01 | | | |
| | | | |
| **Subsección:** C/M/B cuentas de usuario | | | |
| **Sección:** Cuentas | | | |
| **Segmento:** Estado servidor | | | |
| **Auditoría:** Sanitaria AMS S.L. | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Existe alguien que se encargue de la autorización de las altas/modificaciones/bajas de las cuentas de usuario? | CL 1-01 | 10 | |
| 2. ¿Se detallan los datos respectivos de las cuentas? | | 10 | |
| 3. ¿Cómo se entregan las credenciales de acceso a los dueños de las mismas? | CL 1-03 | 10 | |
| 4. ¿De qué se informa al usuario al entregarle las credenciales? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario, detallando todos los datos | 10 | | |
| Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 7 | | |
| No hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 0 | | |
| | | | |
| 2. Se detallan los datos significativos de las mismas, las acciones que se permiten y las credenciales de acceso | 10 | | |
| Se detallan los datos significativos de las mismas, las acciones que se permiten | 4 | | |
| Se detallan los datos significativos de las mismas, pero no las acciones que se permiten ni las credenciales de acceso | 4 | | |
| No se detallan los datos significativos de las mismas, ni las acciones que se permiten ni las credenciales de acceso | 0 | | |
| | | | |
| 3. Se entregan de manera confidencial, únicamente a sus dueños | 10 | | |

| | | | |
|---|---|---|---|
| Se entregan de manera conjunta con los demás trabajadores de la empresa | 0 | | |
| No se entregan a sus dueños | 0 | | |
| | | | |
| 4. Se informa de todos los requisitos relativos a su cuenta | 10 | | |
| Se informa de las credenciales de acceso y de sus permisos, pero no de la caducidad de sus contraseñas | 5 | | |
| Se informa únicamente de las credenciales de acceso | 1 | | |
| No se informa de nada al usuario de las mismas | 0 | | |

***Tabla 368. Lista de comprobación 1***

La tabla anterior muestra la estructura de nuestras listas de comprobación, aquí se hace una descripción de una de ellas y todas las demás las podemos consultar en el apéndice 3.

En cuanto a la lista de comprobación, en primer lugar, está el nombre de la empresa a la que se le realiza la lista de comprobación y un código que identifica dicha lista de comprobación.

A continuación, hay una primera parte que es la cabecera, en la cual tenemos varios aspectos, estos se refieren a la empresa, segmentos, sección, subsección, etc. para identificar a que se refiere dicha de comprobación.

Por otro lado, la zona de preguntas, aquí se redactan las preguntas que se van a comprar en la lista de comprobación.

Por último, los criterios de evaluación, aquí tenemos una serie de criterios que están dentro de cada pregunta siendo el criterio que mejor se ajusta al control el que tiene un 10 y de ahí hacía abajo se realiza una lista de criterios, a cada uno se le asigna una puntuación hasta 0 que sería el peor.

Después, una vez que se comprueben las preguntas, se le asigna una nota a cada una y se realiza la media de todas, esta media es la nota de la lista de comprobación que utilizaremos para realizar la nota de la auditoría.

### 2.3.3 Entrevistas

Cabe destacar que todas las entrevistas se han utilizado de manera telemática utilizando la aplicación que ya se especificó anteriormente, “Google Meet” que disponemos por pertenecer a la Universidad de Jaén. Cada entrevista se ha hecho de manera individual a cada persona.

Algunos aspectos a tener en cuenta a la hora de hacer las entrevistas son:

- No deben durar más de 30 minutos ya que si no se empiezan a perder detalles y no queda bien ponerse delante del entrevistado a tomar anotaciones, en este caso puede ser una excepción, ya que al haber realizado las entrevistas de manera telemática es más sencillo tomar anotaciones sin que llegue a ser violento para el entrevistado.
- Se debe conseguir que bajo la apariencia de una conversación correcta y lo menos tensa posible, el auditado conteste con precisión a las cuestiones que nos interesan.

Se pueden seguir una serie de trucos para que el entrevistado se sienta cómodo:

- Más propenso sin medir lo que dice
- Nunca grabar o tomar notas en su presencia
- No interrumpirlo, sólo si se desvía del tema
- Nunca empezar con preguntas directas, que pongan en cuestión su trabajo o conocimientos
- Mejor comenzar con preguntas genéricas que ayuden a centrar el tema, pero no se refieran 100 % al tema

A continuación, se va explicar la manera en que se deben realizar las entrevistas y los pasos que hay que seguir para hacerlas de manera correcta. Cada entrevista que se vaya a hacer tiene que estar perfectamente planificada minuciosamente antes de su realización.

En las listas de comprobación siempre hay preguntas que no se pueden comprobar por nosotros mismos, por lo tanto, todas estas preguntas se deben apuntar para añadirlas a nuestras entrevistas. Cada una de estas entrevistas tiene al lado un identificador de la forma CL XXX-YY; donde XX es la lista de comprobación a la que pertenece la pregunta y YY es el número de la pregunta dentro de esa lista de comprobación.

Una vez que se tienen todas las preguntas, estas se clasifican en base a quien se les van a hacer. Por lo tanto, se crean grupos de trabajadores dentro de la empresa y se van asignando todas las preguntas que hay.

Después de haber realizado los grupos, se deben planificar las preguntas que se van a hacer en las entrevistas. En primer lugar, las ordenamos de las más generales a las más específicas. En segundo lugar, añadimos preguntas de relleno que van a servir de introducción a las preguntas que se quieren hacer.

A continuación, se muestra una entrevista de ejemplo, la cual se va a usar para explicar la estructura que tienes y todas las demás están adjuntas en un apéndice.

| |
|---|
| **Entrevista:** Empresa <Sanitaria AMS S.L.> |
| |
| **Destinatario:** Todos los empleados |
| **Fecha:** 14/05/2020 - 12:30 |
| |
| **Preguntas:** |
| |
| 1. ¿Cuál es tu opinión sobre el sistema de cuentas de usuario de la empresa? |
| 2. ¿Dispone de cuenta de usuario específica para trabajar en la empresa? |
| **3. ¿Cómo se entregaron esas cuentas? (CL 8-03)** |
| **4. ¿De qué se informa al usuario al entregarle las credenciales? (CL 8-04)** |
| 5. ¿Esas cuentas son únicamente para uso exclusivo dentro de la empresa? |
| **6. (Si responde que no) ¿Qué uso se les da a las contraseñas? (CL 14-01)** |
| 7. ¿Cómo son esas contraseñas? |
| 8. ¿La empresa obliga a que las contraseñas cumplan algunos requisitos? |
| **9. ¿Cuál es la longitud de la contraseña? (CL 17-01)** |
| **10. ¿Qué tipo de palabras se usan en las contraseñas? (CL 17-03)** |
| **11. ¿Qué caracteres se combinan en la contraseña? (CL 17-01)** |

***Tabla 369. Entrevista 1***

La tabla anterior muestra la estructura que tienen las entrevistas, tienen una cabecera en la que se encuentra el nombre de la empresa a la que se le realiza la entrevista, el destinatario y la fecha de realización; hay una segunda parte, zona de preguntas, tenemos las preguntas introductorias y las preguntas en negrita indican que estas no son de relleno, es decir, las preguntas importantes, las que se buscan en la entrevista.

Han salido tres entrevistas, una que es para todos los empleados de la empresa, otra para el administrador del sistema de información y otra para los dueños de la empresa. Como el administrador del sistema de información es también uno de

los dueños de la empresa, se han separado la entrevista que se hace el administrador y a los dueños para que no sea demasiado larga. Además, cada parte se hace un día diferente, para que los entrevistados no se sientan agobiados con demasiadas entrevistas.

Cuando se terminan todas las entrevistas, se añaden las notas de las preguntas a las listas de comprobación, para de esta manera tener las notas de todas las listas de comprobación.

## 2.4 Examen del SI

En este punto de la auditoría, ya tenemos el árbol de partición de alcance realizado, las listas de comprobación y las entrevistas. Con todo esto hemos conseguido tener una nota por separado de cada lista de comprobación y cada entrevista. Por lo tanto, ahora se debe calcular la nota de auditoría para después emitir una valoración de auditoría.

### 2.4.1 Notas

En este apartado, utilizando todas estas notas y las ponderaciones anteriormente realizadas, se procede a calcular la nota de la auditoría. Hay una serie de fórmulas utilizadas para el cálculo de cada parte del árbol de partición, que son las siguientes.

Notas subsección:

$$N_{ssk} = \frac{\sum m\, N_{pm}}{m} \tag{2.6}$$

donde:

- $N_{ssk}$: subsección k-ésima
- $\sum m\, N_{pm}$: sumatorio notas preguntas de esa subsección
- m: todas las preguntas de la sección

Notas sección:

$$N_{sj} = \frac{\sum k\, N_{ssk}}{k} \tag{2.7}$$

donde:

- $N_{sj:}$ sección k-ésima

- $\sum k\, N_{ssk}$: sumatorio de las notas de las subsecciones de la sección
- k: total de subsecciones de la sección

Notas segmento:

$$N_{sgi} = \frac{\sum j\, N_{sj} W_{sj}}{\sum j\, W_{sj}} \tag{2.8}$$

donde:

- $N_{sgi}$: segmento
- $\sum j\, N_{sj} W_{sj}$: sumatorio de todas las secciones del segmento por su peso
- $\sum j\, W_{sj}$: suma de los pesos de las secciones

Nota de la auditoría:

$$N = \frac{\sum i\, N_{sqi} W_{sgi}}{\sum i\, W_{sqi}} \tag{2.9}$$

donde:

- $\sum i\, N_{sqi} W_{sqi}$: sumatoria de los segmentos por su peso
- $\sum i\, W_{sqi}$: sumatoria de los pesos de todos los segmentos

Después de aplicar esta fórmula obtenemos una nota que se corresponde con la nota final de la auditoría, esta nota ahora hay que interpretarla y para eso usamos unos intervalos, los cuales nos ayudan a clasificar nuestra nota y como debemos tratarla.

- 0 ≤ N < 5; zona roja: hay problemas y hay que actuar de inmediato
- 5 ≤ N < 8; zona amarilla: hay problemas y hay que actuar, pero no de inmediato
- 8 ≤ N < 10; zona verde: está bien

Por tanto, hemos calculado la nota la auditoría siguiendo todas las fórmulas y el resultado es el siguiente:

| AUDITORÍA | NOTA AUDITORÍA |
|---|---|
| "Sanitaria AMS S.L." | 7,74 |

***Tabla 370. Nota auditoría***

| Segmento | Nota Segmento |
|---|---|
| Estado servidor | 6,78 |
| Estado SI | 5,71 |
| Contraseñas | 6,04 |
| Alarma | 10,00 |
| Red Wifi | 6,06 |
| Copias de seguridad | 8,93 |
| Cumplimiento LOPD | 10,00 |

*Tabla 371. Notas de los segmentos*

| Sección | Nota sección |
|---|---|
| Cuentas | 7,25 |
| Conexión red eléctrica | 6,00 |
| Cuentas | 9,13 |
| Conexión red eléctrica | 0 |
| Privacidad | 9,67 |
| Robustez | 5,00 |
| Mantenimiento | 0,75 |
| Servicio | 10,00 |
| Dispositivos | 10 |
| Actualización firmware | 10 |
| Seguridad | 4,00 |
| Administración | 8,60 |
| Soportes | 8,38 |
| Mantenimiento | 10,00 |
| Brecha de seguridad | 10 |
| Registro actividades tratamiento | 10 |
| Datos personas fallecidas | 10 |
| Consentimiento | 10 |
| Tratamiento de datos oblig. legal | 10 |
| Consentimiento menores | 10 |
| Datos de contacto | 10 |
| Derechos ARCO | 10,00 |
| Bloqueo de datos | 10 |
| DPO | 10 |

| | |
|---|---|
| Derechos digitales | 10,00 |

*Tabla 372. Notas de las secciones*

| Subsección | Nota subsección |
|---|---|
| C/M/B cuentas de usuario | 10,00 |
| Cuentas admin | 6,00 |
| Revisión de permisos | 3,00 |
| Revocación permisos y eliminación | 10,00 |
| Política usuarios y grupos | 10,00 |
| Registro eventos | 10,00 |
| Administración cuentas | 7,40 |
| Compartir | 9,00 |
| Misma contraseña | 10,00 |
| Uso recordatorio | 10,00 |
| Por defecto | 10,00 |
| Robustas | 0,00 |
| Cambio periódico | 1,50 |
| Gestores | 0,00 |
| Atención cliente | 10,00 |
| Conexión directa | 10,00 |
| Protección inhibición | 10,00 |
| Acceso router | 5,00 |
| Acceso red | 9,00 |
| Cifrado | 10,00 |
| WPS | 0,00 |
| Filtrado MAC | 0,00 |
| Red Wifi invitados | 0,00 |
| Contenido | 10,00 |
| Periodicidad | 7,00 |
| Tipos de copias | 6,00 |
| Seguridad | 10,00 |
| Borrado | 10,00 |
| Mantenimiento | 10,00 |
| Almacenamiento | 6,75 |
| Tiempo de conservación | 10,00 |

| | |
|---|---|
| Validación | 10,00 |
| Documentación | 10,00 |
| Acceso | 10,00 |
| Rectificación | 10,00 |
| Supresión | 10,00 |
| Oposición | 10,00 |
| Limitación del tratamiento | 10,00 |
| Portabilidad | 10,00 |
| Derecho a la intimidad | 10,00 |
| Derecho a la intimidad videovigilancia | 10,00 |

*Tabla 373. Notas de las subsecciones*

| Subsubsección | Nota Subsubsección |
|---|---|
| C/M/B cuentas de usuario | 10 |
| Cuentas admin | 6,6 |
| Revisión de permisos | 3 |
| Revocación permisos y eliminación | 10 |

*Tabla 374. Notas de las subsubsecciones*

Como se ha especificado anteriormente, se han calculado cada una de las notas de la todas las partes del árbol de partición de la auditoría, basándose en las respectivas fórmulas. Además, cada nota está de un color, para de esta manera, poder identificar más fácilmente a la zona a la que pertenece la misma.

A continuación, se muestra el árbol de partición del alcance coloreado con el color correspondiente de cada nodo debido a su nota, de esta manera se tiene una forma más representativa para poder identificar las partes que tienen o no problemas dentro de la empresa.

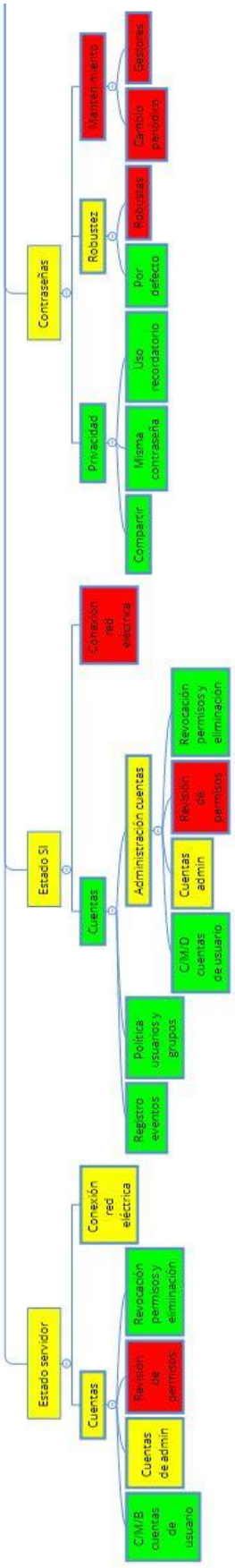



***Ilustración 355. Árbol notas - Parte 1***

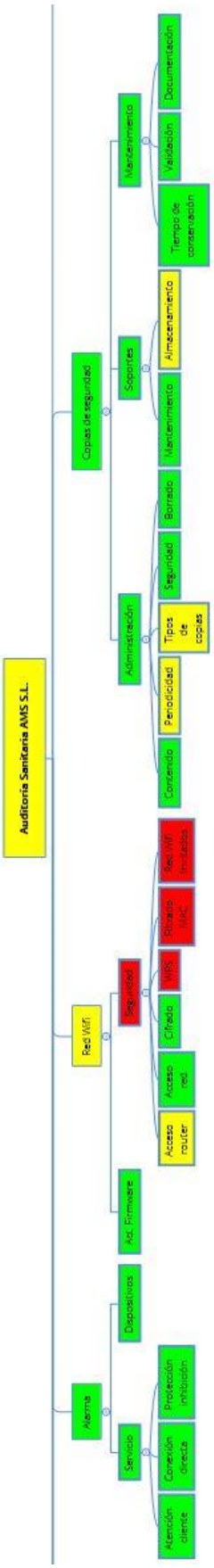



***Ilustración 356. Árbol notas - Parte 2***

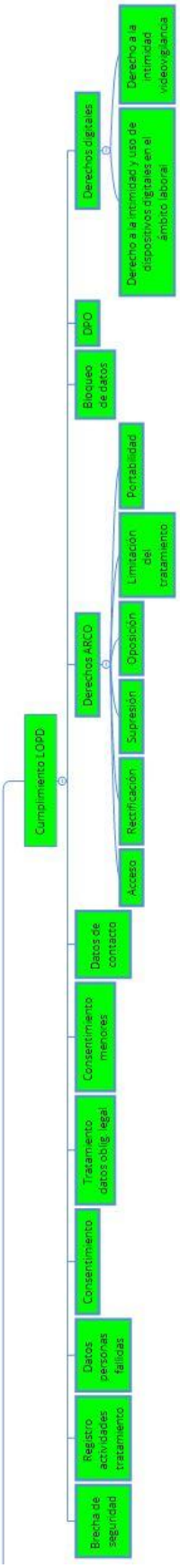



***Ilustración 357. Árbol notas - Parte 3***

## 2.5 Emitir una valoración

Cuando tenemos la nota final de auditoría, se debe emitir una valoración, la cual se hace mediante un informe de auditoría. Este informe es un documento en el que de manera clara el auditor expresa su juicio sobre el sistema de información, junto con las razones que le llevan a opinar así y recomendaciones precisas para corregir los posibles fallos.

Este documento tiene que tener algunas características que ya están predeterminadas:

- Tiene que ser a papel, firmado por la empresa auditora y por la empresa auditada. Cabe la posibilidad de enviar una copia en formato digital, pero siempre debe ser a papel.
- Debe estar la opinión de la empresa auditora de manera detallada y justificada.
- Además de decir que es lo que está mal, hay que decir como corregirlos, ¿qué hace falta?, fecha de realización, detalladamente qué poner y dónde, entre otros.

En el informe de auditoría se encuentran los hechos relevantes, esto son situaciones de mal funcionamiento o peligro para el sistema de información auditado, encontrados durante el análisis.

Además, se encuentran las recomendaciones, estas son descripciones detalladas y precisas que el equipo de auditoría hace sobre cómo se debe corregir un hecho encontrado durante el análisis.

En cuenta la estructura que debe tener el informe de auditoría es la siguiente:

1. Identificación del documento y destinatarios: breve descripción de lo que se trata en el documento y destinatario, quién encargo la auditoría.
2. Identificación de la entidad auditada: DNI de los representantes legales de la empresa auditada, esta parte suele estar hecha por abogados.
3. Alcance de la auditoría: se adjunta el mismo alcance que se había acordado en el contrato.

4. Datos técnicos de la auditoría: aquí se añade la fecha de comienzo y de finalización, equipo de la auditoría, trabajadores del sistema de información entrevistados, normativa legal aplicada.
5. Conclusiones: en este apartado, se da la opinión, esta puede ser:
    - Opinión favorable: todo el árbol de partición en zona verde
    - Opinión con salvedades: esta se da si el nodo de la auditoría está en verde, pero hay algún nodo en el árbol en zona amarilla o en zona roja.
    - Opinión desfavorable: la nota de la auditoría está en zona amarilla o roja.
    - Opinión denegada: no entra en el mismo grupo que las tres opiniones anteriores, ya que no se debe llegar a este punto. Si se da una opinión denegada es porque no puedes dar una opinión. Algunas causas pueden ser negación de permisos, de medios, no se ha podido analizar bien, entre otros.
6. Exposición de los hechos, este apartado se compone de varios puntos:
    - Descripción: en que consiste el hecho, se debe dar con muchos detalles e incluir la demostración.
    - Consecuencias: que pasa si el hecho no se corrige.
    - Tendencias: este punto es opcional, son consecuencias que se agravan con el paso del tiempo, si no soluciono rápido, se tendrán las consecuencias de antes y más.
    - Recomendaciones: como recomienda la empresa auditora que se soluciones ese hecho concreto. Tiene que ser concreto y con muchos detalles, además, la fecha en que debería llevarse a cabo, esta flecha se establece en función de la/s tendencia/s y la gravedad de las mismas. El límite temporal es importante porque te cubre de lo que pueda pasar si no lo haces dentro de este límite.

Con respecto al lenguaje que se debe usar en el informe de auditoría, tenemos que tener en cuenta que es un documento técnico, debe quedar claro y fácil de leer. Algunos aspectos a tener en cuenta pueden ser los siguientes:

- Frases cortas: no hay que enrollarse.
- Lenguaje sobrio sin adornos.
- Lenguaje no técnico: grado de precisión suficiente, pero que lo entienda quien te ha contratado.
- Omitir giros innecesarios.
- Evitar redundancias
- No cambiar verbos por nombres.

En este punto se da por finalizado el informe de auditoría, pero se suele acompañar de una carta de presentación, dentro de esta tenemos un resumen, este sirve para poner en situación a la persona o empresa, podemos hacer un resumen de las conclusiones. Además, podemos ofrecernos como empresa para realizar los cambios que hemos detallado en el informe de auditoría. Por otro lado, añadimos también un informe preliminar que sirve como una manera de adelantar lo que va a poder leer en el informe definitivo de auditoría para que pueda empezar a tomar decisiones.

Aquí se firma el informe de auditoría y ha terminado la auditoría, pero es aconsejable dar asistencia post-auditoria, esto no está dentro de la auditoría, te ofreces a realizar los cambios. Además, esto tiene ventajas para la empresa auditada, ya que ya tiene la confianza y además ya hay una planificación hecha, se conoce la empresa, entre otros; y ventajas para la empresa auditora, ya que nos ayuda a conseguir un nuevo contrato.

En último lugar, cabe destacar que este informe no se realiza en este documento y se va a realizar en un documento aparte, como ya se especificó al principio en las especificaciones del Trabajo Fin de Grado, debido a la Ley Orgánica de Protección de Datos. Por lo tanto, el informe será un documento privado entre la empresa auditora y la empresa auditada.

# 3 CONCLUSIONES Y TRABAJOS FUTUROS

En este trabajo hay dos conclusiones. Por un lado, una conclusión un poco más técnica, que se refiere al informe de auditoría que hacemos después de analizar todo el sistema de información, como final de nuestra auditoría, que en el punto anterior se han explicado detalladamente los pasos que hay que seguir para realizarlo de manera adecuada.

Por otro lado, una conclusión más personal, en la que se incluyen los motivos de la elección de este trabajo y el conocimiento aprendido después de la realización del mismo. En cuanto a los motivos de la elección de este trabajo, lo escogí debido a que la auditoría informática es una parte de esta carrera que me parece muy interesante y en la que quiero profundizar más de cara a un futuro laboral. Con respecto al conocimiento aprendido después de la realización del trabajo, me ha servido para aprender cosas nuevas que desconocía sobre auditorías informáticas y tener más referencias sobre como se debe realizar una auditoría informática.

# 4 APÉNDICES

## 4.1 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

TÍTULO I

**Disposiciones generales**

**Artículo 3. Datos de las personas fallecidas.**

1. Las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

   Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

   Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

   En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

**Principios de protección de datos**

**Artículo 6.** ***Tratamiento basado en el consentimiento del afectado.***

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.
3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

**Artículo 7.** ***Consentimiento de los menores de edad.***

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

   Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

**Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.**

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.
2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

TÍTULO III

**Derecho de las personas**

CAPÍTULO II

**Ejercicio de los derechos**

**Artículo 13. *Derecho de acceso.***

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.
4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

**Artículo 14. *Derecho de rectificación.***

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

**Artículo 15. Derecho de supresión.**

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.
2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

**Artículo 16.** ***Derecho a la limitación del tratamiento.***

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.
2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

**Artículo 17.** ***Derecho a la portabilidad.***

1. El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

**Artículo 18.** ***Derecho de oposición.***

1. El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

**Disposiciones aplicables a tratamientos concretos**

**Artículo 19. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.**

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

   a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

   b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.
3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

En resumen y con palabras menos técnicas, por ejemplo, puedes tratar datos de un electricista que va a realizarte una instalación en tu empresa

TÍTULO V

**Responsable y encargado del tratamiento**

CAPÍTULO I

**Disposiciones generales. Medidas de responsabilidad activa**

**Artículo 31. Registro de las actividades de tratamiento.**

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

   El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

   Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

**Artículo 32. Bloqueo de los datos.**

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.
2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

   Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo,

en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO III

**Delegado de protección de datos**

**Artículo 34. *Designación de un delegado de protección de datos.***

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.
4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.
5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

**Artículo 35. Cualificación del delegado de protección de datos.**

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

**Artículo 36. Posición del delegado de protección de datos.**

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá

inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.
3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.
4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

TÍTULO X

**Garantía de los derechos digitales**

**Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.**

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.
2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.
3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral: Las empresas deben establecer los criterios de uso de los dispositivos digitales junto con los representantes laborales.

**Artículo 88. Derecho a la desconexión digital en el ámbito laboral.**

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.
3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Derecho a la desconexión digital en el ámbito laboral: Las empresas no podrán contactar con sus trabajadores fuera del horario laboral o en períodos de descanso.

**Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.**

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

   En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.
2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los

trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo: Hemos dedicado un artículo completo detallando todo lo que tiene que ver con la instalación de sistemas de videovigilancia en el trabajo.

## 4.2 Pesos políticos y pesos técnicos

Pesos políticos

| **Estado servidor** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Cuentas | 60 | 70 | 50 | 60 | 60,00 |
| Conexión red eléctrica | 40 | 30 | 50 | 40 | 40,00 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Estado SI** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Cuentas | 60 | 70 | 50 | 60 | 60,00 |
| Conexión red eléctrica | 40 | 30 | 50 | 40 | 40,00 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Contraseñas** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Privacidad | 50 | 60 | 60 | 60 | 57,50 |
| Robustez | 25 | 20 | 15 | 20 | 20,00 |
| Mantenimiento | 25 | 20 | 25 | 20 | 22,50 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Alarma** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Servicio | 50 | 60 | 40 | 50 | 50,00 |
| Dispositivos | 50 | 40 | 60 | 50 | 50,00 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Red Wifi** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Actualización firmware | 30 | 50 | 40 | 35 | 38,75 |
| Seguridad | 70 | 50 | 60 | 65 | 61,25 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Copias de seguridad** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Administración | 60 | 50 | 40 | 40 | 47,50 |
| Soportes | 20 | 25 | 30 | 30 | 26,25 |
| Mantenimiento | 20 | 25 | 30 | 30 | 26,25 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Cumplimiento LOPD** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Brecha de seguridad | 5 | 10 | 10 | 10 | 8,75 |
| Registro actividades tratamiento | 10 | 10 | 10 | 10 | 10,00 |
| Datos personas fallecidas | 10 | 5 | 10 | 5 | 7,50 |
| Consentimiento | 10 | 15 | 10 | 10 | 11,25 |
| Tratamiento datos oblig. legal | 10 | 10 | 10 | 10 | 10,00 |
| Consentimiento menores | 10 | 10 | 10 | 10 | 10,00 |
| Datos de contacto | 5 | 5 | 5 | 5 | 5,00 |
| Derechos ARCO | 15 | 10 | 10 | 15 | 12,50 |
| Bloqueo de datos | 5 | 5 | 5 | 5 | 5,00 |
| DPO | 10 | 10 | 10 | 10 | 10,00 |
| Derechos digitales | 10 | 10 | 10 | 10 | 10,00 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

| **Cumplimiento LOPD** | Trabajador 1 | Trabajador 2 | Trabajador 3 | Trabajador 4 | MEDIA (%) |
|---|---|---|---|---|---|
| Estado servidor | 20 | 15 | 20 | 25 | 20,00 |
| Estado SI | 15 | 15 | 10 | 15 | 13,75 |
| Contraseñas | 10 | 15 | 5 | 10 | 10,00 |
| Alarma | 10 | 10 | 15 | 15 | 12,50 |
| Red Wifi | 10 | 15 | 15 | 10 | 12,50 |
| Copias de seguridad | 10 | 15 | 15 | 10 | 12,50 |
| Cumplimiento LOPD | 25 | 15 | 20 | 15 | 18,75 |
| TOTAL (%) | 100 | 100 | 100 | 100 | 100,00 |

Pesos políticos

| **Estado servidor** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Cuentas | 65 | 65 | 60,00 | **62,50** |
| Conexión red eléctrica | 35 | 35 | 40,00 | **37,50** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Estado SI** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Cuentas | 65 | 65 | 60,00 | **62,50** |
| Conexión red eléctrica | 35 | 35 | 40,00 | **37,50** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Contraseñas** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Privacidad | 35 | 35 | 57,50 | **46,25** |
| Robustez | 35 | 35 | 20,00 | **27,50** |
| Mantenimiento | 30 | 30 | 22,50 | **26,25** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Alarma** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Servicio | 50 | 50 | 50,00 | **50,00** |

| | | | | |
|---|---|---|---|---|
| Dispositivos | 50 | 50 | 50,00 | **50,00** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Red Wifi** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Actualización firmware | 30 | 30 | 38,75 | **34,38** |
| Seguridad | 70 | 70 | 61,25 | **65,63** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Copias de seguridad** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Administración | 40 | 40 | 47,50 | **43,75** |
| Soportes | 30 | 30 | 26,25 | **28,13** |
| Mantenimiento | 30 | 30 | 26,25 | **28,13** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **Cumplimiento LOPD** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Brecha de seguridad | 5 | 5 | 8,75 | **6,88** |
| Registro actividades tratamiento | 10 | 10 | 10,00 | **10,00** |
| Datos personas fallecidas | 5 | 5 | 7,50 | **6,25** |
| Consentimiento | 10 | 10 | 11,25 | **10,63** |
| Tratamiento datos oblig. legal | 10 | 10 | 10,00 | **10,00** |
| Consentimiento menores | 10 | 10 | 10,00 | **10,00** |
| Datos de contacto | 10 | 10 | 5,00 | **7,50** |
| Derechos ARCO | 10 | 10 | 12,50 | **11,25** |
| Bloqueo de datos | 10 | 10 | 5,00 | **7,50** |
| DPO | 10 | 10 | 10,00 | **10,00** |
| Derechos digitales | 10 | 10 | 10,00 | **10,00** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

| **SEGMENTOS** | Pesos técnicos | | Pesos políticos | Pesos |
|---|---|---|---|---|
| | Antonio Muñoz Segura | MEDIA (%) | | |
| Estado servidor | 15 | 15 | 20,00 | **17,50** |
| Estado SI | 15 | 15 | 13,75 | **14,38** |

| | | | | |
|---|---|---|---|---|
| Contraseñas | 10 | 10 | 10,00 | **10,00** |
| Alarma | 10 | 10 | 12,50 | **11,25** |
| Red Wifi | 15 | 15 | 12,50 | **13,75** |
| Copias de seguridad | 15 | 15 | 12,50 | **13,75** |
| Cumplimiento LOPD | 20 | 20 | 18,75 | **19,38** |
| TOTAL (%) | 100 | 100 | 100,00 | 100,00 |

## 4.3 Listas de comprobación

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 01 | | | |
| | | | |
| **Subsección: C/M/B cuentas de usuario** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado servidor** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Existe alguien que se encargue de la autorización de las altas/modificaciones/bajas de las cuentas de usuario? | CL 1-01 | 10 | |
| 2. ¿Se detallan los datos respectivos de las cuentas? | | 10 | |
| 3. ¿Cómo se entregan las credenciales de acceso a los dueños de las mismas? | CL 1-03 | 10 | |
| 4. ¿De qué se informa al usuario al entregarle las credenciales? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario, detallando todos los datos | 10 | | |
| Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 7 | | |
| No hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 0 | | |
| | | | |
| 2. Se detallan los datos significativos de las mismas, las acciones que se permiten y las credenciales de acceso | 10 | | |
| Se detallan los datos significativos de las mismas, las acciones que se permiten | 4 | | |
| Se detallan los datos significativos de las mismas, pero no las acciones que se permiten ni las credenciales de acceso | 4 | | |

| | | | |
|---|---|---|---|
| No se detallan los datos significativos de las mismas, ni las acciones que se permiten ni las credenciales de acceso | 0 | | |
| | | | |
| 3. Se entregan de manera confidencial, únicamente a sus dueños | 10 | | |
| Se entregan de manera conjunta con los demás trabajadores de la empresa | 0 | | |
| No se entregan a sus dueños | 0 | | |
| | | | |
| 4. Se informa de todos los requisitos relativos a su cuenta | 10 | | |
| Se informa de las credenciales de acceso y de sus permisos, pero no de la caducidad de sus contraseñas | 5 | | |
| Se informa únicamente de las credenciales de acceso | 1 | | |
| No se informa de nada al usuario de las mismas | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 02 | | | |
| | | | |
| **Subsección: Cuentas admin** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado servidor** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Para qué se utilizan este tipo de cuentas? | | 10 | |
| 2. ¿Cómo se registran las acciones de las cuentas? | | 10 | |
| 3. ¿Como se notifica del acceso como administrador? | | 0 | |
| 4. ¿Cómo son las claves de acceso de las cuentas? | CL 2-03 | 7 | |
| 5. ¿Con qué frecuencia se cambian las contraseñas? | | 3 | |
| | | 6 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Las cuentas de administrador sólo se usan para labores que requieren permisos de administración | 10 | | |
| Las cuentas de administrador se usan para labores de permisos de administración y para uso diario | 3 | | |
| Las cuentas de administrador se usan para cualquier tipo de labor | 0 | | |
| | | | |

| | | | |
|---|---|---|---|
| 2. Se registran todas las acciones en un registro log | 10 | | |
| Se registran todas las acciones en un archivo de texto | 6 | | |
| Se registran sólo las acciones de mantenimiento | 3 | | |
| Se registran sólo las acciones de instalación | 3 | | |
| No se registra ninguna acción | 0 | | |
| | | | |
| 3. Se notifica al administrador del SI | 10 | | |
| Se notifica con una ventana emergente en el servidor | 4 | | |
| No se notifica de ninguna manera | 0 | | |
| | | | |
| 4. Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas, minúsculas, números y caracteres especiales | 10 | | |
| Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas, minúsculas y números) | 7 | | |
| Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas y minúsculas) | 4 | | |
| Las contraseñas son robustas (8 caracteres mínimo) | 3 | | |
| Las contraseñas no son robustas y no tienen ningún tipo de requisito mínimo | 0 | | |
| | | | |
| 5. Las contraseñas se cambian mínimo una vez al mes | 10 | | |
| Las contraseñas se cambian una vez cada 2 meses | 5 | | |
| Las contraseñas se cambian una vez cada 6 meses | 3 | | |
| Las contraseñas no se cambian | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 03 | | | |
| | | | |
| **Subsección: Revisión de permisos** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado servidor** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cada cuanto se revisan los permisos concedidos a las cuentas de usuario? | CL 3-01 | 3 | |
| | | 3 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |

| | | | |
|---|---|---|---|
| 1. Los permisos se revisan una vez al mes | 10 | | |
| Los permisos se revisan una vez cada 2 meses | 5 | | |
| Los permisos se revisan una vez cada 6 meses | 3 | | |
| No se revisan los permisos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 04 | | | |
| | | | |
| **Subsección: Revocación permisos y eliminación** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado servidor** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se revocan los permisos de acceso a nuestros sistemas de las cuentas? | | 10 | |
| 2. ¿Qué datos de las cuentas son eliminados? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se revocan todos los permisos a nuestros sistemas | 10 | | |
| Se revocan los permisos de acceso, pero no los de consulta | 3 | | |
| No se revocan los permisos de acceso | 0 | | |
| | | | |
| 2. Se eliminan la cuenta de correo, cuentas de acceso a todo el SI | 10 | | |
| Se eliminan todas las cuentas de acceso, pero no la cuenta de correo | 6 | | |
| Se eliminan la cuenta de correo, cuentas de acceso a los repositorios y servicios, pero no a las aplicaciones | 3 | | |
| Se eliminan la cuenta de correo y cuentas de acceso a los repositorios, pero no a los servicios y a las aplicaciones | 3 | | |
| No se eliminan ni cuenta de cuenta de correo ni cuentas de acceso | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 05 | | | |
| | | | |
| **Sección: Conexión red eléctrica** | | | |

| | | | |
|---|---|---|---|
| **Segmento: Estado servidor** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se usa un SAI para conectar el servidor a la red eléctrica? | | 4,00 | |
| 2. ¿Están todos los cables conectados correctamente el SAI? | | 10,00 | |
| 3. ¿Está el software del SI instalado correctamente en el PC? | | 5,00 | |
| 4. ¿Están los ajustes realizados correctamente? | | 5,00 | |
| | | 6,00 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se usa un SAI tipo On-line | 10 | | |
| Se usa un SAI tipo In-line | 7 | | |
| Se usa un SAI tipo Off-line | 4 | | |
| No se usa SAI | 0 | | |
| | | | |
| 2. Si, todos los cables están conectados | 10 | | |
| Está conectado sólo el cable USB | 3 | | |
| No están conectados los cables | 0 | | |
| | | | |
| 3. Está instalado el software de nuestro SAI | 10 | | |
| Está instalado un software que no es de nuestro SAI | 5 | | |
| No tiene software nuestro SAI | 5 | | |
| No hay instalado ningún software | 0 | | |
| | | | |
| 4. Están ajustados el tiempo de apagado por tiempo y el tipo de apagado | 10 | | |
| Está ajustado el tiempo de apagado por tiempo, pero no el tipo | 5 | | |
| Está ajustado el tiempo de apagado, pero no el tiempo | 5 | | |
| No tiene software nuestro SAI | 5 | | |
| No está definido ningún ajuste | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 06 | | | |
| | | | |

| | | | |
|---|---|---|---|
| **Subsección: Registro eventos** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué información se registra cuando se hace manejo de la información de la empresa? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se registra quién accede a nuestra información, cuándo, cómo y con qué | 10 | | |
| Se registra quién accede a nuestra información, cuándo y cómo | 8 | | |
| Se registra quien accede a nuestra información y cuando | 8 | | |
| Se registra cuándo accede a nuestra información, cómo y con qué | 4 | | |
| No se registra nada | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 07 | | | |
| | | | |
| **Subsección: Política usuarios y grupos** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se hacen grupos dependiendo del tipo de información al que pueden acceder? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se hacen grupos en función del área o departamento al que pertenezca el empleado, en función del tipo de información a la qué accederá y en función de las operaciones permitidas | 10 | | |

| | | | |
|---|---|---|---|
| Se hacen grupos en función del área o departamento al que pertenezca el empleado y en función del tipo de información a la que accederá | 6 | | |
| Se hace grupo en función del área o departamento al que pertenezca el empleado | 3 | | |
| No se hacen grupos de ningún tipo | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 08 | | | |
| | | | |
| **Subsubsección: C/M/D cuentas de usuario** | | | |
| **Subsección: Administración cuentas** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Existe alguien que se encargue de la autorización de las altas/modificaciones/bajas de las cuentas de usuario? | CL 8-01 | 10 | |
| 2. ¿Se detallan los datos respectivos de las cuentas? | | 10 | |
| 3. ¿Cómo se entregan las credenciales de acceso a los dueños de las mismas? | CL 8-03 | 10 | |
| 4. ¿De qué se informa al usuario al entregarle las credenciales? | CL 8-04 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario, detallando todos los datos | 10 | | |
| Hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 7 | | |
| No hay un/a encargado de autorizar las altas/modificaciones/bajas de las cuentas de usuario | 0 | | |
| | | | |
| 2. Se detallan los datos significativos de las mismas, las acciones que se permiten y las credenciales de acceso | 10 | | |
| Se detallan los datos significativos de las mismas, las acciones que se permiten | 4 | | |
| Se detallan los datos significativos de las mismas, pero no las acciones que se permiten ni las credenciales de acceso | 4 | | |
| No se detallan los datos significativos de las mismas, ni las acciones que se permiten ni las credenciales de acceso | 0 | | |
| | | | |

| | | | |
|---|---|---|---|
| 3. Se entregan de manera confidencial, únicamente a sus dueños | 10 | | |
| Se entregan de manera conjunta con los demás trabajadores de la empresa | 0 | | |
| No se entregan a sus dueños | 0 | | |
| | | | |
| 4. Se informa de todos los requisitos relativos a su cuenta | 10 | | |
| Se informa de las credenciales de acceso y de sus permisos, pero no de la caducidad de sus contraseñas | 5 | | |
| Se informa únicamente de las credenciales de acceso | 1 | | |
| No se informa de nada al usuario de las mismas | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 09 | | | |
| | | | |
| **Subsubsección: Cuentas admin** | | | |
| **Subsección: Administración cuentas** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Para qué se utilizan este tipo de cuentas? | | 10 | |
| 2. ¿Cómo se registran las acciones de las cuentas? | | 10 | |
| 3. ¿Como se notifica del acceso como administrador? | | 10 | |
| 4. ¿Cómo son las claves de acceso de las cuentas? | CL 9-04 | 0 | |
| 5. ¿Con qué frecuencia se cambian las contraseñas? | CL 9-05 | 3 | |
| | | 6,6 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Las cuentas de administrador sólo se usan para labores que requieren permisos de administración | 10 | | |
| Las cuentas de administrador se usan para labores de permisos de administración y para uso diario | 3 | | |
| Las cuentas de administrador se usan para cualquier tipo de labor | 0 | | |
| | | | |
| 2. Se registran todas las acciones en un registro log | 10 | | |

| | | | |
|---|---|---|---|
| Se registran todas las acciones en un archivo de texto | 6 | | |
| Se registran sólo las acciones de mantenimiento | 3 | | |
| Se registran sólo las acciones de instalación | 3 | | |
| No se registra ninguna acción | 0 | | |
| | | | |
| 3. Se notifica al administrador del SI | 10 | | |
| Se notifica con una ventana emergente en el servidor | 4 | | |
| No se notifica de ninguna manera | 0 | | |
| | | | |
| 4. Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas, minúsculas, números y caracteres especiales | 10 | | |
| Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas, minúsculas y números) | 7 | | |
| Las contraseñas son robustas (8 caracteres mínimo, alternando mayúsculas y minúsculas) | 4 | | |
| Las contraseñas son robustas (8 caracteres mínimo) | 3 | | |
| Las contraseñas no son robustas y no tienen ningún tipo de requisito mínimo | 0 | | |
| | | | |
| 5. Las contraseñas se cambian mínimo una vez al mes | 10 | | |
| Las contraseñas se cambian una vez cada 2 meses | 5 | | |
| Las contraseñas se cambian una vez cada 6 meses | 3 | | |
| Las contraseñas no se cambian | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 10 | | | |
| | | | |
| **Subsubsección: Revisión de permisos** | | | |
| **Subsección: Administración cuentas** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cada cuanto se revisan los permisos concedidos a las cuentas de usuario? | CL 10-1 | 3 | |
| | | 3 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |

| | | | |
|---|---|---|---|
| 1. Los permisos se revisan una vez al mes | 10 | | |
| Los permisos se revisan una vez cada 2 meses | 5 | | |
| Los permisos se revisan una vez cada 6 meses | 3 | | |
| No se revisan los permisos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 11 | | | |
| | | | |
| **Subsubsección: Revocación permisos y eliminación** | | | |
| **Subsección: Administración cuentas** | | | |
| **Sección: Cuentas** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se revocan los permisos de acceso a nuestros sistemas de las cuentas? | | 10 | |
| 2. ¿Qué datos de las cuentas son eliminados? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se revocan todos los permisos a nuestros sistemas | 10 | | |
| Se revocan los permisos de acceso, pero no los de consulta | 3 | | |
| No se revocan los permisos de acceso | 0 | | |
| | | | |
| 2. No se eliminan los datos, pero se bloquean todos | 10 | | |
| Se eliminan la cuenta de correo, cuentas de acceso a todo el SI | 10 | | |
| Se eliminan todas las cuentas de acceso, pero no la cuenta de correo | 6 | | |
| Se eliminan la cuenta de correo, cuentas de acceso a los repositorios y servicios, pero no a las aplicaciones | 3 | | |
| Se eliminan la cuenta de correo y cuentas de acceso a los repositorios, pero no a los servicios y a las aplicaciones | 3 | | |
| No se eliminan ni cuenta de cuenta de correo ni cuentas de acceso | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 12 | | | |

| | | | |
|---|---|---|---|
| | | | |
| **Sección: Conexión red eléctrica** | | | |
| **Segmento: Estado SI** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se usa un SAI para conectar los ordenadores a la red eléctrica? | | 0 | |
| 2. ¿Están todos los cables conectados correctamente el SAI? | | 0 | |
| 3. ¿Está el software del SI instalado correctamente en el PC? | | 0 | |
| 4. ¿Están los ajustes realizados correctamente? | | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se usa un SAI tipo On-line | 10 | | |
| Se usa un SAI tipo In-line | 10 | | |
| Se usa un SAI tipo Off-line | 10 | | |
| No se usa SAI | 0 | | |
| | | | |
| 2. Si, todos los cables están conectados | 10 | | |
| Está conectado sólo el cable USB | 3 | | |
| No están conectados los cables | 0 | | |
| No se usa SAI | 0 | | |
| | | | |
| 3. Está instalado el software de nuestro SAI | 10 | | |
| Está instalado un software que no es de nuestro SAI | 5 | | |
| No hay instalado ningún software | 0 | | |
| No se usa SAI | 0 | | |
| | | | |
| 4. Están ajustados el tiempo de apagado por tiempo y el tipo de apagado | 10 | | |
| Está ajustado el tiempo de apagado por tiempo, pero no el tipo | 5 | | |
| Está ajustado el tipo de apagado, pero no el tiempo | 5 | | |
| No está definido ningún ajuste | 0 | | |
| No se usa SAI | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 13 | | | |
| | | | |
| **Subsección: Compartir** | | | |
| **Sección: Privacidad** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se comparten las contraseñas con alguien además del dueño? | ¿CL 13-01? | 7 | |
| 2. ¿Se usa algún método para apuntar nuestras contraseñas? | | 10 | |
| 3. ¿Se escriben las contraseñas en algún sitio distinto a los estrictamente necesario? | | 10 | |
| | | 9 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Las contraseñas no se comparten con nadie, sólo las conoce el dueño | 10 | | |
| Las contraseñas las conoce el dueño y el administrador del SI | 7 | | |
| Las contraseñas las conoce el dueño y los demás componentes del SI | 0 | | |
| | | | |
| 2. No apuntamos las contraseñas en ningún sitio y las recordamos por nosotros mismos | 10 | | |
| Las apuntamos en un archivo del ordenador | 3 | | |
| Las apuntamos en un papel | 0 | | |
| Las apuntamos en un post-it | 0 | | |
| | | | |
| 3. No se escriben en ningún sitio distinto a los estrictamente necesario | 10 | | |
| Se escriben en correo electrónicos | 0 | | |
| Se escriben en formulario web | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 14 | | | |
| | | | |
| **Subsección: Misma contraseña** | | | |
| **Sección: Privacidad** | | | |
| **Segmento: Contraseñas** | | | |

| | | | |
|---|---|---|---|
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué uso se les da a las contraseñas? | CL 14-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. La contraseña se usa para uso profesional únicamente y una para cada servicio | 10 | | |
| La contraseña se usa para uso profesional y la misma para todos los servicios | 2 | | |
| La contraseña se usa para uso profesional y uso doméstico | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 15 | | | |
| | | | |
| **Subsección: Uso recordatorio** | | | |
| **Sección: Privacidad** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se recuerda la contraseña en algún sitio? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. No se utiliza en ningún sitio, las recordamos por nosotros mismos | 10 | | |
| Las recordamos en un archivo de nuestro ordenador | 2 | | |
| Las recordamos en el navegador web | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 16 | | | |
| | | | |
| **Subsección: Por defectos** | | | |

| | | | |
|---|---|---|---|
| **Sección: Robustez** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cambiamos las contraseñas? | CL 16-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Cambiamos las contraseñas y elegimos unas por nosotros mismos | 10 | | |
| Cambiamos las contraseñas y elegimos unas predeterminadas | 2 | | |
| No cambiamos las contraseñas y usamos las contraseñas por defecto | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 17 | | | |
| | | | |
| **Subsección: Robustas** | | | |
| **Sección: Robustez** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cuál es la longitud de la contraseña? | CL 17-01 | 0 | |
| 2. ¿Qué caracteres se combinan en la contraseña? | CL 17-02 | 0 | |
| 3. ¿Qué tipos de palabras se usan en las contraseñas? | CL 17-03 | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Tienen una longitud mínima de 8 | 10 | | |
| Tienen una longitud mínima de 6 | 4 | | |
| No tienen longitud mínima | 0 | | |
| | | | |

| | | | |
|---|---|---|---|
| 2. Se combinan mayúsculas, minúsculas, números y símbolos | 10 | | |
| Se combinan mayúsculas, minúsculas y números | 5 | | |
| Se combinan mayúsculas y minúsculas | 2 | | |
| No se pide un mínimo de combinaciones | 0 | | |
| | | | |
| 3. No usamos palabras públicas o fácilmente adivinables | 10 | | |
| No usamos palabras públicas, pero si nombres propios | 3 | | |
| No usamos palabras públicas, pero si fechas de nacimiento | 3 | | |
| Usamos nombres propios + fechas de nacimiento | 0 | | |
| Sólo se usan números | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 18 | | | |
| | | | |
| **Subsección: Cambio periódico** | | | |
| **Sección: Mantenimiento** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cada cuánto tiempo se cambian las contraseñas? | CL 18-01 | 3 | |
| 2. ¿En qué nos basamos para establecer el periodo de cambio? | CL 18-02 | 0 | |
| | | 1,5 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se cambian al menos una vez al mes | 10 | | |
| Se cambian una vez cada 2 meses | 3 | | |
| Se cambian una vez cada 6 meses | 3 | | |
| No se cambian periódicamente las contraseñas | 0 | | |
| | | | |
| 2. Las contraseñas de las cuentas de administración se cambian con más asiduidad | 10 | | |
| Las contraseñas de las cuentas normales se cambian con más asiduidad | 5 | | |
| No se sigue un sistema en cuanto a la criticidad de las cuentas para cambiar las contraseñas | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 19 | | | |
| | | | |
| **Subsección: Gestores** | | | |
| **Sección: Mantenimiento** | | | |
| **Segmento: Contraseñas** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Usamos algún gestor de contraseñas? | | 0 | |
| 2. ¿De qué manera se cifran las credenciales? | | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Usamos un gestor de contraseñas | 10 | | |
| Sólo usamos un gestor de contraseñas para las cuentas de administrador | 5 | | |
| No usamos gestor de contraseñas | 0 | | |
| | | | |
| 2. Se cifran usando doble factor de autentificación | 10 | | |
| Se usa un cifrado con factor de autentificación simple | 5 | | |
| No usa ningún tipo de cifrado | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 20 | | | |
| | | | |
| **Subsección: Atención cliente** | | | |
| **Sección: Servicio** | | | |
| **Segmento: Alarma** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué horas está disponible la atención al cliente? | | 10 | |
| | | 10 | **MEDIA** |

| | | | |
|---|---|---|---|
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. La atención al cliente está disponible las 24 horas | 10 | | |
| La atención al cliente está disponible 12 horas | 4 | | |
| La atención al cliente está disponible en horario de comercio | 2 | | |
| No hay atención al cliente | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 21 | | | |
| | | | |
| **Subsección: Conexión directa** | | | |
| **Sección: Servicio** | | | |
| **Segmento: Alarma** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cómo es la conexión con la central de policía? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Tiene conexión directa con la central de policía | 10 | | |
| Hay una conexión directa con el servicio de la alarma que después este se comunica con la central de policía | 4 | | |
| No hay conexión con la central de policía | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 22 | | | |
| | | | |
| **Subsección: Protección inhibición** | | | |
| **Sección: Servicio** | | | |
| **Segmento: Alarma** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |

| | | | |
|---|---|---|---|
| 1. ¿Cómo es el sistema de protección frente a inhibición? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El sistema de protección frente a inhibición es capaz de detectar sabotajes con inhibidor de frecuencia si los ladrones encienden un inhibidor de frecuencias cerca de tu hogar o negocio. | 10 | | |
| El sistema de protección frente a inhibición es capaz de detectar sabotajes con inhibidor de frecuencia si los ladrones encienden un inhibidor dentro de tu negocio | 2 | | |
| No hay sistema de protección frente a inhibición | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 23 | | | |
| | | | |
| **Sección: Dispositivos** | | | |
| **Segmento: Alarma** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cómo es el sistema de cámaras de vigilancia? | | 10 | |
| 2. ¿Cómo es el sistema de sensores para los puntos de acceso? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Hay cámaras que pueden tomar secuencias de imágenes en cualquier momento | 10 | | |
| Hay cámaras que pueden tomar secuencias de imágenes cuando los ladrones están dentro del negocio | 4 | | |
| No hay cámaras de seguridad | 0 | | |
| | | | |
| 2. Hay sensores de detección de movimiento en todas las puertas y ventanas | 10 | | |
| Hay sensores de detección de movimiento en todas puertas | 4 | | |
| Hay sensores de detección de movimientos en todas las ventanas | 4 | | |
| No hay sensores de detección de movimientos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 24 | | | |

| | | | |
|---|---|---|---|
| | | | |
| **Sección: Actualización de firmware** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cuál es la actualización actualmente del router? | | 10 | |
| 2. ¿Cómo se realizan las actualizaciones de firmware del router? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El router tiene la última actualización de firmware | 10 | | |
| El router tiene la penúltima actualización de firmware | 5 | | |
| El router nunca se ha actualizado | 0 | | |
| | | | |
| 2. Las actualizaciones se realizan en cuanto se avisa de la disponibilidad de estas | 10 | | |
| Las actualizaciones se realizan en un periodo máximo de dos semanas desde que se avisa de la disponibilidad de estas | 7 | | |
| Las actualizaciones se realizan en un periodo máximo de un mes desde que se avisa de la disponibilidad de estas | 5 | | |
| Las actualizaciones se realizan en un periodo máximo de 6 meses desde que se avisa de la disponibilidad de estas | 2 | | |
| No se realizan actualizaciones | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 25 | | | |
| | | | |
| **Subsección:** Acceso router | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué usuario se usa para el acceso al router? | | 0 | |
| 2. ¿Qué contraseña se usa para el acceso al router? | | 0 | |

| | | | |
|---|---|---|---|
| 3. ¿Cuál es la longitud de la contraseña? | | 10 | ¿¿?? |
| 4. ¿Qué caracteres combina la contraseña? | | 10 | ¿¿?? |
| | | 5 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se usa un nombre creado por el propietario del router | 10 | | |
| Se usa un nombre proporcionado por un tercero | 5 | | |
| Se usa el nombre por defecto del router | 0 | | |
| | | | |
| 2. Se usa una contraseña creada por el propietario del router | 10 | | |
| Se usa una contraseña creado por un tercero | 5 | | |
| Se usa la contraseña por defecto del router | 0 | | |
| | | | |
| 3. La contraseña tiene una longitud de 8 caracteres | 10 | | |
| La contraseña tiene una longitud de 6 caracteres | 4 | | |
| La contraseña no tiene longitud mínima | 0 | | |
| | | | |
| 4. La contraseña combina mayúsculas, minúsculas, números y caracteres especiales | 10 | | |
| La contraseña combina mayúsculas, minúsculas y números | 6 | | |
| La contraseña combina mayúsculas y minúsculas | 3 | | |
| La contraseña no combina ningún tipo de caracteres | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 26 | | | |
| | | | |
| **Subsección:** Acceso red | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué nombre se usa para la red Wifi? | | 10 | |
| 2. ¿Qué contraseña se usa para el acceso a la red Wifi? | CL 26-02 | 10 | |

| | | | |
|---|---|---|---|
| 3. ¿Cuál es la longitud de la contraseña? | CL 26-03 | 10 | |
| 4. ¿Qué caracteres combina la contraseña? | CL 26-04 | 6 | |
| | | 9 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se usa un nombre creado por el propietario del router | 10 | | |
| Se usa un nombre proporcionado por un tercero | 5 | | |
| Se usa el nombre por defecto del router | 0 | | |
| | | | |
| 2. Se usa una contraseña creada por el propietario del router | 10 | | |
| Se usa una contraseña creada por un tercero | 5 | | |
| Se usa la contraseña por defecto del router | 0 | | |
| | | | |
| 3. La contraseña tiene una longitud de 8 caracteres | 10 | | |
| La contraseña tiene una longitud de 6 caracteres | 4 | | |
| La contraseña no tiene longitud mínima | 0 | | |
| | | | |
| 4. La contraseña combina mayúsculas, minúsculas, números y caracteres especiales | 10 | | |
| La contraseña combina mayúsculas, minúsculas y números | 6 | | |
| La contraseña combina mayúsculas y minúsculas | 3 | | |
| La contraseña no combina ningún tipo de caracteres | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 27 | | | |
| | | | |
| **Subsección:** Cifrado | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué tipo de cifrado tipo el router? | | 10 | |
| | | 10 | **MEDIA** |

| | | | |
|---|---|---|---|
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Cifrado WPA3 | 10 | | |
| Cifrado WPA2 | 10 | | |
| Cifrado WEP | 3 | | |
| No hay cifrado | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 28 | | | |
| | | | |
| **Subsección:** WPS | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cuál es el estado de este mecanismo? | | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El mecanismo está desactivado | 10 | | |
| El mecanismo se desactiva en momento puntuales | 3 | | |
| El mecanismo está activado | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 29 | | | |
| | | | |
| **Subsección:** Filtrado MAC | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |

| | | | |
|---|---|---|---|
| 1. ¿Cuál es el estado de este mecanismo? | | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El mecanismo está activado | 10 | | |
| El mecanismo se activa en ocasiones puntuales | 2 | | |
| El mecanismo está desactivado | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 30 | | | |
| | | | |
| **Subsección:** Red Wifi invitados | | | |
| **Sección: Seguridad** | | | |
| **Segmento: Red Wifi** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué redes hay en nuestro router? | | 0 | |
| 2. ¿Qué nombre tiene la red wifi de invitados? | | 0 | |
| 3. ¿Qué contraseña tiene la red wifi de invitados? | | 0 | |
| | | 0 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Tenemos una red principal y otra red wifi para invitados | 10 | | |
| Tenemos una red wifi para invitados | 5 | | |
| Tenemos una red principal | 0 | | |
| | | | |
| 2. La red wifi para invitados tiene un nombre diferente a la red principal | 10 | | |
| La red wifi para invitados tiene un nombre por defecto | 4 | | |
| La red wifi tiene el mismo nombre que la red principal | 0 | | |
| No hay red Wifi para invitados | 0 | | |
| | | | |
| 3. La red wifi para invitados tiene una contraseña diferente a la red principal | 10 | | |

| | | | |
|---|---|---|---|
| La red wifi para invitados tiene la contraseña por defecto | 4 | | |
| La red wifi tiene la misma contraseña que la red principal | 0 | | |
| No hay red Wifi para invitados | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 31 | | | |
| | | | |
| **Subsección:** Contenido | | | |
| **Sección: Administración** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué se contenido copiamos? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se copian todos los activos de la empresa | 10 | | |
| Se copian información de los pacientes, pedidos, citas, facturación y control de compra-venta | 5 | | |
| Se copian información de los pacientes, pedidos, citas y facturación | 4 | | |
| Se copian información de los pacientes, pedidos y citas | 3 | | |
| Se copian información de los pacientes y pedidos | 2 | | |
| Se copia sólo la información de los pacientes | 1 | | |
| No se hacen copias de seguridad | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 32 | | | |
| | | | |
| **Subsección:** Periodicidad | | | |
| **Sección: Administración** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |

| | | | |
|---|---|---|---|
| 1. ¿Cada cuánto tiempo se realizan las copias de seguridad? | | 7 | |
| | | 7 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Las copias se realizan como máximo cada 4 horas y media | 10 | | |
| Las copias se realizan cada 6 horas | 7 | | |
| Las copias se realizan cada 8 horas | 5 | | |
| Las copias se realizan para 12 horas | 4 | | |
| Las copias se realizan cada 24 horas | 1 | | |
| No se realizan copias | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 33 | | | |
| | | | |
| **Subsección:** Tipos de copias | | | |
| **Sección: Administración** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué tipo de copias se realizan? | | 6 | |
| | | 6 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se realizan copias de tipo diferencial | 10 | | |
| Se realizan copias de tipo completa | 6 | | |
| No se realizan copias de seguridad | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 34 | | | |
| | | | |
| **Subsección:** Seguridad | | | |
| **Sección: Administración** | | | |
| **Segmento: Copias de seguridad** | | | |

| | | | |
|---|---|---|---|
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué tipo de cifrado se hace sobre las copias? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Las copias están cifradas con una clave criptográfica asimétrica | 10 | | |
| Las copias están cifradas con una contraseña normal | 5 | | |
| Las copias no están cifradas | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 35 | | | |
| | | | |
| **Subsección:** Borrado | | | |
| **Sección: Administración** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cómo se borran las copias de seguridad? | CL 35-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Los destruye una empresa especializada | 10 | | |
| Los borra el administrador de SI | 2 | | |
| Los elimina cualquier empleado de la empresa | 1 | | |
| No se borran y se tira el soporte a la basura | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 36 | | | |
| | | | |
| **Subsección:** Mantenimiento | | | |

| | | | |
|---|---|---|---|
| **Sección: Soportes** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cada cuánto tiempo comprobamos la vida útil de nuestros soportes de almacenamiento? | CL 36-01 | 10 | |
| 2. ¿Qué versión tiene nuestro software de copias de seguridad? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. La comprobamos una vez al mes mínimo | 10 | | |
| La comprobamos una vez cada dos meses | 6 | | |
| La comprobamos una vez cada 6 meses | 4 | | |
| No la comprobamos | 0 | | |
| | | | |
| 2. La última versión disponible | 10 | | |
| La penúltima versión disponible | 4 | | |
| No se realizan actualizaciones | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 37 | | | |
| | | | |
| **Subsección:** Almacenamiento | | | |
| **Sección: Soportes** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué número de copias se realizan? | | 10,00 | |
| 2. ¿Cuántos tipos de soportes se utilizan para realizar las copias? | | 3,00 | |
| 3. ¿Qué soportes se usan para realizar las copias? | | 7,00 | |
| 4. ¿Dónde se almacenan las copias de seguridad? | | 7,00 | |
| | | 6,75 | **MEDIA** |

| | | | |
|---|---|---|---|
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se realizan 3 copias (la original y 2 secundarias) | 10 | | |
| Se realizan 2 copias (la original y 1 secundaria) | 4 | | |
| No se realizan copias | 0 | | |
| | | | |
| 2. Se utilizan 2 tipos de soportes | 10 | | |
| Se utiliza un tipo de soporte | 3 | | |
| No se realizan copias | 0 | | |
| | | | |
| 3. Una copia se realiza en un disco duro SSD y otra en un servicio de almacenamiento en la nube | 10 | | |
| Una copia se realiza en un disco duro SSD y otra en un pen drive | 7 | | |
| Las dos copias se realizan en dos discos duros SSD | 4 | | |
| Las dos copias se realizan en dos servicios de almacenamiento en la nube | 4 | | |
| Las dos copias se realizan en dos pen drive | 4 | | |
| No se realizan copias | 0 | | |
| | | | |
| 4. Una copia se almacena en la empresa y la otra en un servicio de almacenamiento en la nube | 10 | | |
| Una copia se almacena en la empresa y la otra se la lleva uno de los dueños de la empresa a su casa | 7 | | |
| Las dos copias se almacenan en la empresa | 3 | | |
| No se realizan copias | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 38 | | | |
| | | | |
| **Subsección:** Tiempo de conservación | | | |
| **Sección: Mantenimiento** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cuánto tiempo debemos conservar las copias de documentos mercantiles? | CL 38-01 | 10 | |

| | | | |
|---|---|---|---|
| 2. ¿Cuánto tiempo debemos conservar las copias de documentos fiscales? | CL 38-02 | 10 | |
| 3. ¿Cuánto tiempo debemos conservar las copias de las facturas? | CL 38-03 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se conservan de forma indefinida | 10 | | |
| Se conservan durante 6 años | 10 | | |
| Se conservan durante 4 años | 2 | | |
| Se conservan durante 2 años | 2 | | |
| No se conservan | 0 | | |
| | | | |
| 2. Se conservan durante 10 años | 10 | | |
| Se conservan durante 4 años | 10 | | |
| Se conservan durante 2 años | 2 | | |
| No se conservan | 0 | | |
| | | | |
| 3. Se conservan durante 10 años | 10 | | |
| Se conservan durante 4 años | 10 | | |
| Se conservan durante 2 años | 2 | | |
| No se conservan | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 39 | | | |
| | | | |
| **Subsección:** Validación | | | |
| **Sección: Mantenimiento** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cada cuánto tiempo comprobamos que las copias de seguridad se realizan de manera correcta? | CL 39-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |

| | | | |
|---|---|---|---|
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se revisan mínimo una vez cada dos semanas | 10 | | |
| Se revisan una vez al mes | 6 | | |
| Se revisan una vez cada 2 meses | 3 | | |
| Se revisan una vez cada 6 meses | 1 | | |
| No se revisan | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 40 | | | |
| | | | |
| **Subsección:** Documentación | | | |
| **Sección: Mantenimiento** | | | |
| **Segmento: Copias de seguridad** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué información incluye nuestra hoja de registro a la hora de hacer las copias de seguridad? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. La hoja incluye identificador de soporte, tipos de copia, fecha y hora, lugar de almacenamiento y personal a cargo de la copia | 10 | | |
| La hoja incluye identificador de soporte, tipos de copia, fecha y hora y lugar de almacenamiento | 7 | | |
| La hoja incluye identificador de soporte, tipos de copia y fecha y hora | 5 | | |
| La hoja incluye identificador de soporte y tipos de copia | 1 | | |
| La hoja incluye identificador de soporte | 1 | | |
| No existe hoja de registro | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 41 | | | |
| | | | |
| **Sección: Brecha de seguridad** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |

| | | | |
|---|---|---|---|
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cuál es el plazo para notificar en caso de que haya una brecha de seguridad? | CL 40-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se notifica en un plazo máximo de 72 horas a la Agencia Española de Datos | 10 | | |
| Se notifica en un máximo de 96 horas a la Agencia Española de Datos | 1 | | |
| No se notifica | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 42 | | | |
| | | | |
| **Sección: Registro actividades tratamiento** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Como se registra el tratamiento realizado por los responsables y encargados de los datos? | | 10 | |
| 2. ¿Qué información contiene el registro de las actividades de tratamiento? | | 10 | |
| 3. ¿Qué información contiene el registro de todas las categorías de actividades de tratamiento efectuadas? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se registran de manera escrita, inclusive en formato electrónico | 10 | | |
| Se registran de manera escrita | 5 | | |
| No se registran de ninguna manera | 0 | | |
| | | | |
| 2. Contiene nombre y datos de contacto del responsable, del corresponsable, del representante del responsable y del delegado de datos; los fines del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales; las categorías de destinatarios a quienes se comunican los datos personales; las transferencias de datos personales a un tercer país o una | 10 | | |

| | | | |
|---|---|---|---|
| organización internacional; los plazos previsto para la supresión de las diferentes categorías de datos; una descripción general de las medidas técnicas y organizativas de seguridad | | | |
| Contiene nombre y datos de contacto del responsable, del corresponsable, del representante del responsable y del delegado de datos; los fines del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales; las categorías de destinatarios a quienes se comunican los datos personales; las transferencias de datos personales a un tercer país o una organización internacional | 4 | | |
| Contiene nombre y datos de contacto del responsable, del corresponsable, del representante del responsable y del delegado de datos; los fines del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales; las categorías de destinatarios a quienes se comunican los datos personales | 4 | | |
| Contiene nombre y datos de contacto del responsable, del corresponsable, del representante del responsable y del delegado de datos; los fines del tratamiento | 3 | | |
| Contiene nombre y datos de contacto del responsable, del corresponsable, del representante del responsable y del delegado de datos | 2 | | |
| No existe un registro del tratamiento | 0 | | |
| | | | |
| 3. Contiene el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúa el encargado, del representante del responsable o del encargado y del delegado de protección de datos; las categorías de tratamientos efectuados por cuenta de cada responsable; transferencias de datos personales a un tercer país y organización internacional; descripción general de las medidas técnicas y organizativas de seguridad | 10 | | |
| 3. Contiene el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúa el encargado, del representante del responsable o del encargado y del delegado de protección de datos; las categorías de tratamientos efectuados por cuenta de cada responsable | 3 | | |
| 3. Contiene el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúa el encargado, del representante del responsable o del encargado y del delegado de protección de datos | 2 | | |
| No existe un registro del tratamiento | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 43 | | | |
| | | | |
| **Sección: Datos personas fallecidas** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Que se permite hacer con los datos de las personas fallecidas? | | 10 | |
| 2. ¿Quién puede acceder a los datos de las personas fallecidas? | | 10 | |
| 3. ¿Quién no puede acceder a los datos de las personas fallecidas? | | 10 | |

| | | | |
|---|---|---|---|
| 4. ¿Qué sucede con los datos de los fallecidos menores? | | 10 | |
| 5. ¿Qué sucede con los datos de los fallecidos con discapacidad? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se puede tener acceso a los datos, rectificación y supresión por los representantes legales | 10 | | |
| Se puede tener acceso a los datos y rectificación por los representantes legales | 1 | | |
| Se puede tener acceso a los datos por los representantes legales | 1 | | |
| No se puede tener acceso a los datos | 0 | | |
| | | | |
| 2. Podrán solicitar acceso las personas vinculadas por razones familiares, los herederos, las personas o instituciones a las que el fallecido hubiese designado expresamente para ello | 10 | | |
| Podrán solicitar acceso las personas vinculadas por razones familiares y los herederos | 5 | | |
| Podrán solicitar acceso las personas vinculadas por razones familiares | 1 | | |
| No podrá solicitar acceso nadie | 0 | | |
| | | | |
| 3. No podrán acceder las personas a las que el fallecido se lo haya prohibido expresamente | 10 | | |
| No podrán acceder a las personas las personas vinculadas por razones familiares ni los herederos | 1 | | |
| Podrá acceder quien quiera a los datos | 0 | | |
| | | | |
| 4. Podrán tener acceso, rectificación y supresión, los representantes legales o el Ministerio Fiscal | 10 | | |
| Podrán tener acceso, rectificación y supresión los representantes legales | 3 | | |
| Podrán tener acceso, rectificación y supresión el Ministerio Fiscal | 3 | | |
| Podrán tener acceso, rectificación y supresión cualquier persona | 0 | | |
| Nadie podrá tener acceso | 0 | | |
| | | | |
| 5. Podrán tener acceso, rectificación y supresión, los representantes legales, el Ministerio Fiscal o las personas designadas para el ejercicio de funciones de apoyo | 10 | | |
| Podrán tener acceso, rectificación y supresión, los representantes legales o el Ministerio Fiscal | 3 | | |
| Podrán tener acceso, rectificación y supresión los representantes legales | 3 | | |
| Podrán tener acceso, rectificación y supresión el Ministerio Fiscal | 3 | | |
| Podrán tener acceso, rectificación y supresión cualquier persona | 0 | | |
| Nadie podrá tener acceso | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 44 | | | |
| | | | |
| **Sección: Consentimiento** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cómo guardamos y recogemos el consentimiento de los afectados? | CL 44-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se rellena un documento específico para dejar constancia de manera expresa del consentimiento | 10 | | |
| Se pregunta de manera verbal al afectado para asegurarnos de su consentimiento | 2 | | |
| No se pregunta por el consentimiento al afecta | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 45 | | | |
| | | | |
| **Sección: Tratamiento datos oblig. legal** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Es ilícito el tratamiento? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos | 10 | | |
| El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales | 10 | | |

| | | | |
|---|---|---|---|
| El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento | 10 | | |
| El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física | 10 | | |
| El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero | 10 | | |
| El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero | 10 | | |
| No es lícito | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 46 | | | |
| | | | |
| **Sección: Consentimiento menores** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿A qué edad se permite el consentimiento por parte de los menores? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El consentimiento se permite a partir de los 14 años | 10 | | |
| El consentimiento se permite a partir de 12 años | 1 | | |
| El consentimiento se permite a partir de los 11 años | 1 | | |
| El consentimiento se permite a cualquier edad | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 47 | | | |
| | | | |
| **Sección: Datos de contacto** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Se permite el interés legítimo de los esos datos? | | 10 | |
| | | 10 | **MEDIA** |

| | | | |
|---|---|---|---|
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se permite siempre que su finalidad sea profesional | 10 | | |
| Se permite siempre independientemente de su finalidad | 1 | | |
| No se permite nunca | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 48 | | | |
| | | | |
| **Subsección**: Acceso | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Como se permite el acceso a los datos al afectado? | | 10 | |
| 2. ¿A qué información se le permite acceder al interesado? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se facilitará un sistema de acceso remoto, directo y seguro | 10 | | |
| Se facilitará un sistema de acceso remoto | 1 | | |
| Se facilitará un sistema de acceso directo | 1 | | |
| No se facilitará un sistema de acceso | 0 | | |
| | | | |
| 2. Los fines de tratamiento; las categorías de datos personales que se trate; los destinatarios o las categorías de destinatarios a los que se comunicaron o será comunicados los datos personales; el plazo previsto de conservación de los datos personales; la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; cualquier tipo de información disponible sobre el origen de los datos del interesado; la existencia de decisiones automatizadas | 10 | | |
| No se ofrecen todos los datos descritos anteriormente | 1 | | |
| No se permite el derecho al acceso | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 49 | | | |
| | | | |
| **Subsección**: Rectificación | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Cómo se permite que el afectado rectifique sus datos? | CL 49-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se le facilita una solicitud al afectado para que indique que datos se refiere y la corrección que haya de realizarse | 10 | | |
| Se le pregunta de forma verbal al afectado para que indique que datos se refiere y la corrección que haya de realizarse | 1 | | |
| No se le pregunta al afectado por los datos ni por la corrección | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 50 | | | |
| | | | |
| **Subsección**: Supresión | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué se hace cuando los datos no son necesarios en relación con los fines para los que fueron recogidos? | CL 49-01 | 10 | |
| 2. ¿Qué se hace cuando se retira el consentimiento en que se basa el tratamiento? | CL 49-02 | 10 | |
| 3. ¿Qué se hace cuando el afectado se opone al tratamiento de los datos? | CL 49-03 | 10 | |
| 4. ¿Qué se hace cuando los datos han sido tratados ilícitamente? | CL 49-04 | 10 | |
| | | 10 | **MEDIA** |
| | | | |

| | | | |
|---|---|---|---|
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El responsable del tratamiento de los datos realizará la supresión de los datos sin dilación | 10 | | |
| El responsable del tratamiento de los datos realizará la supresión de los datos cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no realizará la supresión de los datos | 0 | | |
| No se permite la supresión de los datos | 0 | | |
| | | | |
| 2. El responsable del tratamiento de los datos realizará la supresión de los datos sin dilación | 10 | | |
| El responsable del tratamiento de los datos realizará la supresión de los datos cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no realizará la supresión de los datos | 0 | | |
| No se permite la supresión de los datos | 0 | | |
| | | | |
| 3. El responsable del tratamiento de los datos realizará la supresión de los datos sin dilación | 10 | | |
| El responsable del tratamiento de los datos realizará la supresión de los datos cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no realizará la supresión de los datos | 0 | | |
| No se permite la supresión de los datos | 0 | | |
| | | | |
| 4. El responsable del tratamiento de los datos realizará la supresión de los datos sin dilación | 10 | | |
| El responsable del tratamiento de los datos realizará la supresión de los datos cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no realizará la supresión de los datos | 0 | | |
| No se permite la supresión de los datos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 51 | | | |
| | | | |
| **Subsección**: Oposición | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |

| | | | |
|---|---|---|---|
| 1. ¿Cómo se actúa en caso de que el afectado se oponga al tratamiento de los datos? | CL 50-1 | 10 | |
| 2. ¿Cuánto tiempo tarda el responsable de tratamiento en contestar a la solicitud? | CL 50-2 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El responsable de tratamiento estudia la solicitud y responde al afectado dentro de los plazos | 10 | | |
| El responsable de tratamiento estudia la solicitud y responde al afectado fuera de los plazos | 1 | | |
| El responsable de tratamiento estudia la solicitud y no responde | 1 | | |
| El responsable no estudia la solicitud | 0 | | |
| | | | |
| 2. El responsable de tratamiento contesta en un plazo máximo de 10 días | 10 | | |
| El responsable de tratamiento contesta en un plazo máximo de 20 días | 1 | | |
| El responsable de tratamiento contesta en un plazo máximo de 2 meses | 1 | | |
| El responsable de tratamiento contesta en un plazo máximo de 6 meses | 1 | | |
| El responsable de tratamiento no contesta | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 52 | | | |
| | | | |
| **Subsección**: Limitación del tratamiento | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Qué se hace cuando la exactitud de los datos no es la adecuada? | CL 52-01 | 10 | |
| 2. ¿Qué se hace cuando el tratamiento de los datos es ilícito? | CL 52-02 | 10 | |
| 3. ¿Qué se hace cuando el interesado se opone a la supresión de sus datos personales y solicita la limitación de su uso? | CL 52-03 | 10 | |
| 4. ¿Qué se hace cuando los datos no son necesarios para los fines, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones? | CL 52-04 | 10 | |
| 5. ¿Cómo se informa de que el tratamiento de datos está limitado? | CL 52-05 | 10 | |

| | | 10 | MEDIA |
|---|---|---|---|
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El responsable del tratamiento de los datos limita su tratamiento sin dilación | 10 | | |
| El responsable del tratamiento de los datos limita su tratamiento cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no limita el tratamiento | 1 | | |
| No se permite la limitación de los datos | 0 | | |
| | | | |
| 2. El responsable del tratamiento de los datos limita su tratamiento sin dilación | 10 | | |
| El responsable del tratamiento de los datos limita su tratamiento cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no limita el tratamiento | 1 | | |
| No se permite la limitación de los datos | 0 | | |
| | | | |
| 3. El responsable del tratamiento de los datos limita su tratamiento sin dilación | 10 | | |
| El responsable del tratamiento de los datos limita su tratamiento cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no limita el tratamiento | 1 | | |
| No se permite la limitación de los datos | 0 | | |
| | | | |
| 4. El responsable del tratamiento de los datos limita su tratamiento sin dilación | 10 | | |
| El responsable del tratamiento de los datos limita su tratamiento cuando estime oportuno | 1 | | |
| El responsable del tratamiento de los datos no limita el tratamiento | 1 | | |
| No se permite la limitación de los datos | 0 | | |
| | | | |
| 5. El responsable del tratamiento de los datos informa expresamente al afectado de manera formal | 10 | | |
| El responsable del tratamiento de los datos informa al afectado de manera verbal | 1 | | |
| El responsable del tratamiento de los datos no informa al afectado | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 53 | | | |
| | | | |
| **Subsección**: Portabilidad | | | |
| **Sección: Derechos ARCO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |

| | | | |
|---|---|---|---|
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿En qué formato se le facilitan los datos cuando el interesado solicita la portabilidad de estos? | | 10 | |
| 2. ¿Cómo se ejerce la portabilidad de los datos? | CL 53-01 | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se le facilitan los datos en un formato estructurado, de uso común y lectura mecánica | 10 | | |
| Se le facilitan los datos de manera que el encargado de tratamiento de los datos vea oportuno | 1 | | |
| No se facilitan los datos | 0 | | |
| | | | |
| 2. Los datos personales se transmiten de responsable a responsable | 10 | | |
| Los datos se transmiten como el responsable que los tiene estime oportuno | 1 | | |
| No se permite la portabilidad de los datos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 54 | | | |
| | | | |
| **Sección: Bloqueo datos** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Quién realiza el bloqueo de los datos? | CL 54-01 | 10 | |
| 2. ¿Cómo se realiza el bloqueo de los datos? | | 10 | |
| 3. ¿Qué está permitido hacer con los datos bloqueados? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |

| | | | |
|---|---|---|---|
| 1. El responsable del tratamiento realiza el bloqueo de los datos? | 10 | | |
| Cualquier trabajador realiza el bloqueo de los datos | 1 | | |
| No se realiza el bloqueo de los datos | 0 | | |
| | | | |
| 2. Se identifican y reservan los datos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueves y tribunales, el Ministerio Fiscal o las Administraciones Públicas | 10 | | |
| Se identifican y reservan los datos, permitiendo su visualización | 1 | | |
| No se realiza el bloqueo de datos | 0 | | |
| | | | |
| 3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior | 10 | | |
| Los datos bloqueados no se podrán modificar, pero si consultar | 1 | | |
| No se realiza el bloqueo de datos | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 55 | | | |
| | | | |
| **Sección: DPO** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿De qué manera se ha designado un DPO? | CL 55-01 | 10 | |
| 2. ¿Cuánto tiempo se tarda en informar a la Agencia Española de Protección de Datos de designaciones, nombramientos y ceses de delegados? | | 10 | |
| 3. ¿Cuál es la posición del DPO? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. El responsable y encargado del tratamiento han designado un DPO | 10 | | |
| Los trabajadores han designado un DPO | 1 | | |
| No hay DPO | 0 | | |
| | | | |
| 2. Se comunica en un plazo de 10 días | 10 | | |

| | | | |
|---|---|---|---|
| Se comunica en un plazo de 1 mes | 1 | | |
| Se comunica en un plazo de 6 meses | 1 | | |
| No se comunica | 0 | | |
| | | | |
| 3. El DPO deberá actuar como interlocutor responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos | 10 | | |
| El DPO actuará siempre en beneficio a la empresa que hace el tratamiento de los datos | 1 | | |
| EL DPO actuará siempre en beneficio al afectado | 1 | | |
| El DPO no actuará | 1 | | |
| No existe DPO | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 56 | | | |
| | | | |
| **Subsección**: Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral | | | |
| **Sección: Derechos digitales** | | | |
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿De qué modo se especifican los fines para los que se han definido los dispositivos digitales? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Se informa de manera detallada de los derechos de utilización a los que se refiere este apartado | 10 | | |
| Se informa de manera poco detallada de los derechos de utilización a los que se refiere este apartado | 4 | | |
| No se informa de ninguna manera | 0 | | |

| | | | |
|---|---|---|---|
| **Lista de comprobación:** Empresa <Sanitaria AMS S.L.> **Código:** 57 | | | |
| | | | |
| **Subsección**: Derecho a la intimidad videovigilancia | | | |
| **Sección: Derechos digitales** | | | |

| | | | |
|---|---|---|---|
| **Segmento: Cumplimiento LOPD** | | | |
| **Auditoría: Sanitaria AMS S.L.** | | | |
| | | | |
| **Preguntas:** | | | |
| | | | |
| 1. ¿Para qué son usadas las imágenes obtenidas a través de sistemas de videocámaras? | | 10 | |
| 2. ¿Dónde están instaladas las cámaras de videovigilancia? | | 10 | |
| | | 10 | **MEDIA** |
| | | | |
| **Criterios de evaluación:** | | | |
| | | | |
| 1. Para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública. | 10 | | |
| Para lo que deseen los dueños de la empresa | 1 | | |
| Para lo que desee cualquier empleado de la empresa | 0 | | |
| | | | |
| 2. En las zonas de venta y de entrada de la empresa | 10 | | |
| En las zonas de venta de la empresa | 7 | | |
| En las zonas de entrada de la empresa | 7 | | |
| En las zonas de descanso y esparcimiento de la empresa | 0 | | |

## 4.4 Entrevistas

| |
|---|
| **Entrevista:** Empresa <Sanitaria AMS S.L.> |
| |
| **Destinatario:** Dueño de la empresa |
| **Fecha:** 14/05/2020 - 9:30 |
| |
| **Preguntas:** |
| |
| 1. ¿Como se distribuyen las cuentas dentro de la empresa? |
| 2. ¿Hay cuentas específicas para uso dentro de la empresa? |
| **3. (Si dice que sí) ¿Existe alguien que se encargue de la autorización de las altas/modificaciones/bajas de las cuentas de usuario? (CL 1-01)** |
| 4. ¿Se realizan copias de seguridad en la empresa? |

| |
|---|
| 5. ¿Cuánto tiempo se conservan las copias de seguridad? |
| **6. ¿Cuánto tiempo se conservan las copias de documentos mercantiles? (CL 38-01)** |
| **7. ¿Cuánto tiempo se conservan las copias de documentos fiscales? (CL 38-02)** |
| **8. ¿Cuánto tiempo se conservan las copias de las facturas? (CL 38-03)** |
| 9. ¿Conoce la LOPD? |
| 10. ¿Alguna vez ha tenido algún problema la empresa con respecto a esta ley? |
| **11. En caso de que haya una brecha de seguridad, ¿Cuál es el plazo para notificar en caso de que haya una brecha de seguridad? (CL 40-01)** |
| 12. ¿La empresa recoge el consentimiento de los afectados? |
| **13. ¿Cómo guardamos y recogemos el consentimiento de los afectados? (CL 44-01)** |
| 14. ¿Si una persona tiene un problema o fallo con sus datos, este puede rectificarlos? |
| **15. ¿Cómo se permite que el afecta rectifique sus datos? (CL 49-01)** |
| 16. ¿Alguna vez la empresa ha recogido datos que no eran necesarios? |
| **17. ¿Qué se hace cuando los datos no son necesarios en relación con los fines para los que fueron recogidos? (CL 49-01)** |
| **18. ¿Qué se hace cuando se retira el consentimiento en que se basa el tratamiento? (CL49-02)** |
| 19. ¿Ha habido en la empresa algún problema con los datos de algún cliente? |
| **20. ¿Qué se hace cuando el afectado se opone al tratamiento de los datos? (CL 49-03)** |
| **21. ¿Qué se hace cuando los datos han sido tratados ilícitamente? (CL 49-04)** |

| |
|---|
| **Entrevista:** Empresa <Sanitaria AMS S.L.> |
| |
| **Destinatario:** Administrador del SI |
| **Fecha:** 14/05/2020 - 17:30 |
| |
| **Preguntas:** |
| |
| 1. ¿Cuál es tu opinión sobre el sistema de cuentas de usuario de la empresa? |
| 2. ¿Dispone de cuenta de usuario específica para trabajar en la empresa? |
| **3. ¿Cómo se entregaron esas cuentas? (CL 1-03)** |
| 4. ¿De qué se informa al usuario al entregarle las credenciales? (CL 8-04) |
| 5. ¿Todas las cuentas son iguales, es decir, tienen los mismos permisos? |
| **6. (Si dice que sí) ¿Cada cuanto se revisan los permisos concedidos a las cuentas de usuario? (CL 3-01)** |
| 7. ¿Dispones de una cuenta de usuario dentro de la empresa? |
| 8. (Si dice que sí) ¿Cómo son esas cuentas? |
| 10. Esas cuentas se usan únicamente dentro de la empresa? |

| |
|---|
| **11. ¿Cómo son las claves de acceso de las cuentas? (CL 9-04)** |
| **12. ¿Se usan únicamente dentro de la empresa? (CL 14-01)** |
| 13. ¿La empresa obliga a renovar las contraseñas cada cierto tiempo? |
| **14. (Si dice que sí) ¿Con qué frecuencia se cambian las contraseñas? (CL 9-05)** |
| 15. ¿La empresa pone algún tipo de restricción a la hora de crear las contraseñas? |
| **15. (Si dice que sí) ¿Cuál es la longitud de la contraseña? (CL 17-01)** |
| **16. ¿Qué caracteres se combinan en la contraseña? (CL 17-01)** |
| **17. ¿Qué tipos de palabras se usan en las contraseñas? (CL 17-03)** |
| 19. ¿La empresa obliga a cambiar las contraseñas cada cierto tiempo? |
| **20. (Si dice que sí) ¿Cada cuánto tiempo se cambian las contraseñas? (CL 18-01)** |
| 21. ¿Todas las contraseñas se cambian en el mismo tiempo? |
| **22. (Si dice que no) ¿En qué nos basamos para establecer el periodo de cambio? (CL 18-02)** |

| |
|---|
| **Entrevista:** Empresa <Sanitaria AMS S.L.> |
| |
| **Destinatario:** Dueño de la empresa |
| **Fecha:** 15/05/2020 - 9:30 |
| |
| **Preguntas:** |
| |
| 1. Alguna vez la empresa ha tenido un problema con los datos de un cliente? |
| **2. ¿Cómo se actúa en caso de que el afectado se oponga al tratamiento de los datos? (CL 50-1)** |
| 3. ¿El cliente presentó una solicitud para el tratamiento de sus datos? |
| **4. (En caso de que diga que sí) ¿Cuánto tiempo tarda el responsable de tratamiento en contestar a la solicitud? (CL 50-2)** |
| **5. ¿Qué se hace cuando la exactitud de los datos no es la adecuada? (CL 52-01)** |
| **6. ¿Qué se hace cuando el tratamiento de los datos es ilícito? (CL 52-02)** |
| **7. ¿Qué se hace cuando el interesado se opone a la supresión de sus datos personales y solicita la limitación de su uso? (CL 52-03)** |
| **8. ¿Qué se hace cuando los datos no son necesarios para los fines, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones? (CL 52-04)** |
| **9. ¿Cómo se informa de que el tratamiento de datos está limitado? (CL 52-05)** |
| 10. ¿Alguna vez un paciente ha pedido una recopilación de sus datos? |
| **11. (Si dice que sí) ¿Cómo se ejerce la portabilidad de los datos? (CL 53-01)** |
| 12. ¿Alguna vez un paciente ha pedido un bloque de sus datos? |
| **13. (SI dice que sí) ¿Quién realiza el bloqueo de los datos? (CL 54-01)** |
| 14. ¿Conoce que es un Delegado de Protección de Datos? |

| |
|---|
| 15. (Si dice que sí) ¿Dispone la empresa de uno? |
| **16. (Si dice que sí) ¿De qué manera se ha designado un DPO? (CL 55-01)** |

| |
|---|
| **Entrevista:** Empresa <Sanitaria AMS S.L.> |
| |
| **Destinatario:** Administrador del SI |
| **Fecha:** 15/05/2020 - 17:30 |
| |
| **Preguntas:** |
| |
| 1. ¿Qué uso haces de la red Wifi de la empresa? |
| 2. ¿Quién te proporcionó la contraseña? |
| **3. ¿Quién definió la contraseña de acceso al router? (CL 26-02)** |
| 4. ¿La empresa pone algún tipo de restricción a la hora de definir la contraseña del router? |
| **5. (Si dice que sí) ¿Cuál es la longitud de la contraseña? (CL 26-03)** |
| **6. ¿Qué caracteres combina la contraseña? (CL 26-04)** |
| 7. ¿Alguna vez ha habido algún problema de pérdidas de datos en la empresa? |
| 8. ¿En la empresa se realizan copias de seguridad? |
| **9. (Si dice que sí) ¿Cómo se borran las copias de seguridad? (CL 35-01)** |
| 10. ¿Se comprueba que las copias de seguridad se realizan de manera adecuada? |
| **11. ¿Cada cuánto tiempo comprobamos que las copias de seguridad se realizan de manera correcta? (CL 39-01)** |
| 12. ¿Qué soportes se utilizan para realizar las copias de seguridad? |
| **13. ¿Cada cuánto tiempo comprobamos la vida útil de nuestros soportes de almacenamiento? (CL 36-01)** |

# 5 DEFINICIONES Y ABREVIATURAS

- Auditoría: proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.
- Alcance de una auditoría: extensión y límites de una auditoría.
- Plan de auditoría: descripción de las actividades y de los detalles acordados de una auditoría.
- Criterios de auditoría: conjunto de requisitos usados como referencia frente a la cual se compara la evidencia objetiva.
- Evidencia objetiva: datos que respaldan la existencia o veracidad de algo.
- Evidencia de la auditoría: registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable.
- Hallazgos de la auditoría: resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.
- Conclusiones de la auditoría: resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.
- Cliente de la auditoría: organización o empresa que solicita una auditoría.
- Auditado: organización que es auditada en su totalidad o partes.
- Equipo auditor: una o más personas que llevan a cabo una auditoría con el apoyo, si es necesario de expertos técnicos.
- Auditor: persona que lleva a cabo una auditoría.
- Sistema de gestión: conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.
- Riesgo: efecto de la incertidumbre.
- Conformidad: cumplimiento de un requisito.
- No conformidad: incumplimiento de un requisito.

- Competencia: capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.
- Requisito: necesidad o expectativa establecida, generalmente implícita u obligatoria.
- Proceso: conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto.
- Desempeño: resultado medible.
- Eficacia: grado en el que se realizan las actividades planificadas y se logran los resultados planificados.
- Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

# 6 BIBLIOGRAFÍA

BOE. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). *Boletín Oficial Del Estado (BOE)*, (294), 119778–119857. https://doi.org/BOE-A-2012-5403

INCIBE. (n.d.-a). *Acuerdo de confidencialidad*.

INCIBE. (n.d.-b). *Guía de almacenamiento seguro de la información*.

INCIBE. (n.d.-c). *Políticas de seguridad para la pyme: contraseñas*.

INCIBE. (n.d.-d). *Políticas de seguridad para la pyme: control de acceso*.

INCIBE. (2018a). *Copias de seguridad una guía de aproximación para el empresario*. Retrieved from https://www.incibe.es/protege-tu-empresa/guias/copias-seguridad-guia-aproximacion-el-empresario

INCIBE. (2018b, May 18). Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario. Retrieved May 27, 2020, from https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

INCIBE. (2019, May 14). Seguridad en redes wifi: una guía de aproximación para el empresario. Retrieved May 27, 2020, from https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

ISO. (2008). *ISO 19011. Sistemas de gestiónd e calidad*. *2008*, 42. Retrieved from http://farmacia.unmsm.edu.pe/noticias/2012/documentos/ISO-9001.pdf

Magerit. (n.d.). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II : Catálogo de elementos. Retrieved May 27, 2020, from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Magerit. (2012a). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*. 42. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Magerit. (2012b, October). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I : Método. Retrieved May 27, 2020, from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

SI, S. (2017, June 8). Configurar SAI SALICRU - Mantenimiento informático para empresas. Retrieved June 1, 2020, from https://www.soluciones.si/blog/2017/06/08/configurar-sai-salicru/

UNE-ISO 31000-2010. Gestión del riesgo. Principios y directrices

UNE-ISO 31010-2011. Gestión del riesgo. Técnicas de apreciación del riesgo.

UNE-ISO 19011-2018. Directrices para la auditoría de los sistemas de gestión.