UNIVERSIDAD EUROPEA DE MADRID

Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones

PROYECTO FIN DE MASTER

Gobierno y Gestión de la Seguridad de la Información de la PYME Congelados Madrid

JAZMÍN PARELLADA MARTÍN

JHONNY DE FREITAS GOMES

Dirigido por

CARLOS BACHMAIER JOHANNING

CURSO 2021-2022

TÍTULO: Gobierno y Gestión de la Seguridad de la Información de la PYME Congelados Madrid

AUTOR: Jazmín Parellada Martín y Jhonny De Freitas Gomes

TITULACIÓN: Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones

DIRECTOR DEL PROYECTO: Doctor Ingeniero Carlos Bachmaier Johanning

FECHA: Julio del 2022

RESUMEN

El presente proyecto de fin de master consiste una elaboración de un sistema de gobierno y gestión de seguridad de la información de una empresa con el fin asegurar que la empresa gestione el riesgo mediante los controles adecuados sobre confidencialidad, integridad y disponibilidad para proteger la información de todas las partes interesadas.

El proyecto desarrollado se ha llevado a cabo en una empresa real. Con el objetivo de mantener información confidencial, se utilizará el nombre de Congelados Madrid.

Congelados Madrid es un mayorista de distribución de congelados que tiene sus oficinas y puestos en MercaMadrid. Es importante tener en cuenta que tiene informatizado todo el proceso diario de compras, ventas, trazabilidad, control de almacenes, repartos, etc.

Este trabajo va a ser un proyecto de tipo industrial en el que buscamos resolver un problema típico de un sector de la actividad económica empresarial privada, es decir, los integrantes han aplicado sus conocimientos para resolver un problema en el ámbito de seguridad de la información de una empresa determinada.

Palabras clave: SGSI, Análisis de riesgos, Ciberseguridad, Vulnerabilidad, Amenaza, ISO/IEC 27001 y Magerit V3.

ABSTRACT

This master's final project consists of an elaboration of a system of governance and information security management of a company in order to ensure that the company manages its risk using appropriate controls on confidentiality, integrity and availability to protect the information of all parties. concerned parties.

The project developed has covered a real company. In order to keep information confidential, the name of Congelados Madrid will be used.

Congelados Madrid is a frozen food distribution wholesaler that has its offices and stalls in MercaMadrid. It is important to bear in mind that the entire daily process of purchases, sales, traceability, warehouse control, distribution, etc. is computerized.

This work is going to be an industrial-type project in which we seek to solve a typical problem in a sector of economic activity of private business, that is, the members who developed the project applied their knowledge to solve a problem in the field of information security of a given company.

Keywords: SGSI, Risk Analysis, Cybersecurity, Vulnerability, Threat, ISO/IEC 27001 and Magerit V3.

AGRADECIMIENTOS

Transmitir nuestro más sincero agradecimiento a todos aquellos que nos han acompañado a lo largo de nuestra etapa universitaria y han colaborado para que podamos llevar a cabo el desarrollo del presente Trabajo de Fin de Master.

En primer lugar, a nuestros familiares más cercanos. En segundo lugar a nuestro tutor Carlos, por haber fomentado el desarrollo de nuestra curiosidad y conocimiento.

Por último agradecer a nuestro compañera/compañero de TFM por haber llevado a cabo este proyecto de forma conjunta en el que compartimos una experiencia única de aprendizaje.

TABLA RESUMEN

	DATOS
Nombre y apellidos:	Jazmín Parellada Martín Jhonny De Freitas Gomes
Título del proyecto:	Gobierno y Gestión de la Seguridad de la Información de la PYME Congelados Madrid
Directores del proyecto:	CARLOS BACHMAIER JOHANNING
Tipo de proyecto:	Proyecto de tipo industrial
Objetivo general del proyecto:	El objetivo principal del presente proyecto de fin de master es establecer los mecanismos de gestión de la seguridad y las salvaguardas necesarias con el fin de permitir definir, alcanzar y mantener los objetivos de seguridad de la información de la empresa Congelados Madrid.
Versión:	V1

Capítulo 1. Contenido

Índice de Gráficos

Índice de ilustraciones

Índice de Tablas

Capítulo 1. RESUMEN DEL PROYECTO

1.1 Contexto y justificación

En la actualidad se multiplican exponencialmente los ataques informáticos, especialmente los de suplantación de identidad, ransomware y otros malware. Adicional a esto existe el robo de información y los daños reputacionales. La mayoría de estos ataques son realizados valiéndose de vulnerabilidades existentes en las infraestructuras informáticas o por uso inadecuado de los equipos y software por parte de los usuarios.

La importancia del presente proyecto es mostrar una aproximación real a minimizar o mitigar los ataques cibernéticos analizando la red y los activos de un cliente real, en nuestro caso la empresa Congelados Madrid. Este proyecto puede ser desarrollado igualmente en otras PYMES digitalizadas que tengan la necesidad de conocer y contener el nivel de riesgo de sus sistemas.

El ajustar los riesgos pasa por dos aspectos importantes. Primeramente, está el actualizar y optimizar los sistemas para corregir vulnerabilidades detectadas y segundo, y no menos importante, está en la formación, capacitación y concienciación de los usuarios de los sistemas.

1.2 Planteamiento del problema

Con el desarrollo del presente documento hemos buscado crear una propuesta y estudio que establezca los mecanismos necesarios de gestión de la seguridad de la información en todos los niveles de la empresa Congelados Madrid.

1.3 Objetivos del proyecto

El objetivo principal del presente proyecto de fin de master es establecer los mecanismos de gestión de la seguridad y las salvaguardas necesarias con el fin de permitir definir, alcanzar y mantener los objetivos de seguridad de la información de la empresa Congelados Madrid.

Estructura de la memoria

Estructura de la memoria:

- En el segundo capítulo se lleva a cabo un estudio del estado del arte, donde explicaremos diferentes alternativas de gobierno y gestión de la seguridad de la información. En base a esto se explicará por qué se ha tomado la decisión de seleccionar del Sistema de Gestión de la Seguridad de la Información conforme con la ISO/IEC 27001.
- En el tercer capítulo se explican los objetivos que se han desarrollado para llevar a cabo el desarrollo del Sistema de Gestión de la Seguridad de la Información conforme con la ISO/IEC 27001 para la empresa Congelados Madrid.
- En el cuarto capítulo se explica el desarrollo del Sistema de Gestión de la Seguridad de la Información conforme con la ISO/IEC 27001 para la empresa Congelados Madrid.
- En el quinto capítulo se obtienen las conclusiones tras la realización del desarrollo del Sistema de Gestión de la Seguridad de la Información.

- En el sexto capitulo se habla sobre las posibles líneas de trabajo futuro que se podrían llevar a cabo a continuación de lo realizado en este Proyecto de Fin de Master.
- En el séptimo capitulo encontraremos las referencias utilizadas para el desarrollo de la memoria.
- En el octavo capítulo (anexo) encontraremos un glosario, tablas de datos (activos detectados, valoración de los activos, cálculo del riesgo, etc.), manual de instalación y el manual de usuario de la aplicación desarrollada para la identificación de los activos que existen en la red, sistemas operativos que utilizan, puertos abiertos y servicios en ejecución más comunes.

Capítulo 2. ANTECEDENTES / ESTADO DEL ARTE

2.1 Estado del arte

Actualmente existen diversas alternativas para que poder realizar el gobierno y la gestión de la seguridad de la información.

Para la realización del presente proyecto, ha sido necesario conocer varias de estas herramientas, estándares o metodologías para poder seleccionar la más adecuada para lograr los objetivos establecidos para la investigación y desarrollo de un análisis de la seguridad de la información en la empresa Congelados Madrid.

A continuación, revisaremos algún de estas herramientas a considerar:

- **PILAR:** es un software, una aplicación informática que se basa en la reunión y registro de activos electrónicos de forma tal que luego, a través de cálculos matemáticos y algoritmos, poder ser capaz de arrojar indicadores de riesgo para su posterior análisis y propuestas de mejora. Su fuerte son sus métricas y los enfoques que permiten establecer nuevos cumplimientos bien sean normativos o de seguridad.
- **NIST Cybersecurity Framework:** es un estándar de tecnología orientado a las buenas prácticas sobre la seguridad de la información ayudando a dar una mejor visibilidad sobre los riesgos de ciberseguridad que pueda tener una empresa y aportando soluciones para reducir los mismos. NIST Cybersecurity Framework guía al usuario a determinar donde enfocarse e invertir de la forma más efectiva el tiempo y presupuesto dirigido al apartado de ciberseguridad. Al igual que en Pilar, NIST Cybersecurity Framework identifica todos los equipos, pero adicionalmente el software y los datos para luego crear un esquema de protección, detección, respuesta y recuperación.
- **COBIT5:** es una herramienta excelente para la creación de políticas que busquen establecer una brecha menor entre una larga lista de requerimientos que permitan realizar controles en cara a los temas técnicos y lo más importante, los riesgos del negocio. Se vale una lista de controles con alcances y limitaciones específicos y es precursor de varios principios entre ellos, la satisfacción de necesidades a nivel de accionistas o dueños de la empresa, el tomar en cuenta toda la empresa y no solo una parte de esta, la utilización de un único marco referencial que permita la integración de herramientas de control y auditoria o modelos de negocio.
- **MAGERIT:** es una metodología que principalmente gestiona la seguridad en base a riesgos existentes. En general MAGERIT tiene como propósito el crear conciencia en los responsables del manejo de la información a través de métodos sistemáticos que ayuden a descubrir riesgos para finalmente establecer controles que sirvan para mitigarlos. Para alcanzar los objetivos de la organización utiliza el Esquema Nacional de Seguridad, la gestión basada en riesgos, su análisis y gestión.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** es una metodología que tiene como objetivo gestionar los procesos para mantener seguros los datos.

Al utilizar SGSI es fundamental definir el alcance, tener claro que metodología se utilizará para identificar los riesgos, la evaluación de cuales riesgos aplican en un negocio para finalmente establecer controles y documentación de las tareas que tienen como finalidad la mitigación del riesgo. Este sistema tiene continuidad en el tiempo ya que se agendan revisiones y nuevas evaluaciones.

- **ISO/IEC 27001:** Indica los requisitos para gestionar la seguridad conforme la norma. Pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización.
  La norma define de manera genérica cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002**: es un estándar de la organización internacional de normalización y la comisión electrotécnica internacional y se basa es una serie de recomendaciones de buenas y mejores prácticas en todo a lo que a la seguridad de la información se refiere. La finalidad fundamental es preservar la confidencialidad, integridad y la disponibilidad de los datos. Una vez identificados los riesgos, podemos detectar los controles que pueden aplicar sobre estos riesgos y establecer políticas con objetivos claros, sus responsables de cumplimiento y los resultados esperados que mitiguen el riesgo y velen por el cumplimiento de la norma.

Adicional a la mencionadas anteriormente existen más herramientas más fundamentadas en la identificación del riesgo, alguna reseñables serian:

- **APR:** es una herramienta que es utilizada para realizar un análisis preliminar de riesgos al inicio de un proyecto. Estudia las fases de los procesos profundizando en cada una de sus partes para facilitar la identificación de un riesgo.
- **FMEA:** sus siglas son de Failure Mode and Effect Analysis y su finalidad es la identificación de fallos para posteriormente clasificarlos y eliminarlos. Se abordan aquellas fallas que se consideran más graves y luego las menos prioritarias.

Por último, para la medición de riesgos se puede recurrir a métodos cuantitativos o cualitativos.

Por un lado, entre los métodos cualitativos podemos encontrar algunos ejemplos como:

- Listas de chequeo o de comprobación (check list).
- Análisis de seguridad de tareas.
- Observación.
- Entrevistas.

Por otro lado, entre los métodos cuantitativos podemos encontrar algunos ejemplos como:

- Métodos numéricos para la valoración de los activos.
- Cálculo o estimación de la probabilidad de ocurrencia.
- Métodos de valoración del riesgo.

De las herramientas para gestionar el riego son utilizadas las listas de chequeo que buscan detectar los focos de riesgo, formular preguntas cuyas respuestas ayuden a detectar posibles

problemas potenciales para luego al final del ejercicio poder tomar decisiones orientadas a la mitigación de los riesgos detectados.

También existen matrices de riesgo o control también basadas en probabilidad en que ocurra un impacto en la empresa en base a un riesgo. Estas matrices que evalúan los riesgos del 1 al 5 siendo el 5 el valor de riesgo mayor ayuda a reconocer amenazas para tomar medidas de prevención a tiempo. Para concretar la matriz se realiza la consulta a expertos en torno al contexto que se está revisando, tomando en cuenta los componentes y recursos que se podrían encontrar bajo amenaza.

2.2 Planteamiento del problema

Para el contexto actual de la PYME Congelados Madrid, donde todo el tratamiento de la información para la gestión del negocio se encuentra informatizado y teniendo en cuenta que en la actualidad las bases de datos y el manejo comercial contienen información sensible de terceros y de la propia empresa, nace la necesidad de proteger esta información y utilizar las mejores herramientas para lograrlo.

Tomando en cuenta lo indicado anteriormente debemos contar con una propuesta y estudio que garantice la seguridad de la información en todos los niveles de la empresa tanto en los repositorios como en la transferencia y manejo de los datos. El uso del estándar ISO/IEC 27001 es un aliado para lograr los objetivos planteados que finalmente puedan asegurar la integridad, confidencialidad y disponibilidad de la información en una infraestructura segura.

Considerando las herramientas para el presente proyecto, SGSI ofrece una gestión centralizada destinada a proteger la seguridad de los datos de toda la organización. El despliegue en Congelados Madrid de políticas, procedimientos, controles, bien sean físicos o lógicos con un alcance definido bien sea general o local, es bastante útil para que la empresa pueda defenderse de los riesgos IT ofreciendo, además, herramientas de ayuda en lo que la administración de la información se refiere.

La cultura empresarial y los procesos que involucran a todos los empleados, las mejoras y el poder monitorizar la infraestructura informática, se verán reforzados y controlados ofreciendo una visión amplia y una gestión auditable. Estas características de un SGSI se implican de forma directa con las necesidades actuales de Congelados Madrid.

La necesidad de un enfoque que de forma general se despliegue en toda la empresa y no únicamente en el departamento de tecnología es necesario para poder evaluar los riesgos actuales presentes en la empresa.

En Congelados Madrid urge que se revise y acredite que sus sistemas previenen las amenazas y que cuenta con los controles necesarios para gestionar las mismas.

Es evidente la necesidad de minimizar los riesgos actuales a través de un sistema de gestión estructurado que, adicionalmente, aporte al cumplimiento de la legislación que aplica a estos puntos.

Como toda empresa, el prestigio y la confianza de los clientes como negocio de compra y venta de alimentos congelados que se distribuyen desde un punto comercial tan importante como lo es MercaMadrid, es fundamental.

Por todo lo expuesto anteriormente se ha decidido utilizar el estándar ISO/IEC 27001 que requiere la definición de un Sistema de Gestión de la Seguridad de la Información (SGSI) para asegurar de forma eficaz la integridad, confidencialidad y disponibilidad de la información de la empresa Congelados Madrid.

Capítulo 3. OBJETIVOS

3.1 Objetivos generales

El objetivo principal del presente proyecto de fin de master es establecer los mecanismos de gestión de la seguridad y las salvaguardas necesarias con el fin de permitir definir, alcanzar y mantener los objetivos de seguridad de la información de la empresa Congelados Madrid.

3.2 Objetivos específicos

En la siguiente tabla se muestran los objetivos específicos detectados para conseguir llevar a cabo el objetivo principal:

ID	Descripción	Líder
OE1	Revisar las alternativas existentes de gobierno y gestión de la seguridad de la información.	Ambos integrantes
OE2	Justificar la selección de SGSI e ISO/IEC 27001 en el contexto de la PYME	Ambos integrantes
OE3	Detectar y analizar la situación actual de la empresa en el ámbito de la gestión y protección de la seguridad de la información	Ambos integrantes
OE4	Desarrollar un programa para la identificación de los activos que existen en la red, sistemas operativos que utilizan, puertos abiertos y servicios en ejecución más comunes	Jazmín Parellada Martín
OE5	Definir el SGSI de la empresa conforme con la ISO/IEC 27001	Ambos integrantes
OE6	Establecer los diversos procesos, procedimientos y prácticas a seguir	Jhonny de Freitas Gomes

Tabla 1: Objetivos específicos – Elaboración propia

Cuando en la tabla anterior se hace referencia al estudiante como líder lo que se busca es dejar constancia de quien será el encargado principal del desarrollo de ese objetivo, mientras que el otro integrante será el revisor.

3.3 Fuera del alcance del proyecto

No se contempla dentro del alcance la implementación y el mantenimiento del SGSI. Adicionalmente no se contempla la certificación porque no existe una necesidad real que justifique la misma.

3.4 Beneficios del proyecto para Congelados Madrid

Los beneficios más significativos que podemos destacar son los siguientes:

- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Asegurar la continuidad del negocio, que las operaciones y el servicio no se vean interrumpidos ante un ataque informático.
- Establecer un marco de gestión de la seguridad de la información.
- Contar con respaldos de información que aseguren que existe baja probabilidad de que existan pérdidas de datos que puedan comprometer a la empresa a nivel legal y reputacional. Igualmente, esta medida aporta una recuperación más rápida en caso de pérdida de información causada por un ataque.
- Implementar de medias correctoras que actualicen los sistemas haciéndolos más seguros y de menor o ningún riesgo
- Concienciar y formar a los usuarios logrando el uso responsable de los sistemas y aportando a que sean capaces de detectar posibles intentos de fraude en sitios web, correo electrónico o en sus aplicaciones de uso diario.
- Afianzar la confianza de los clientes al ofrecerles garantías de que la información con la que interactúan, los procesos y el atendimiento en general es seguro y disponible.
- Establecer salvaguardas y políticas que garanticen los objetivos de minimizar el impacto de un siniestro informático.

Capítulo 4. DESARROLLO DEL PROYECTO

4.1 Planificación y ejecución del proyecto

4.1.1 Etapa 1: Elaboración del anteproyecto

En esta primera etapa se elaboró el anteproyecto.

En esta se estimó el tiempo que se iba a tardar en desarrollar el proyecto con el siguiente diagrama de Gantt.

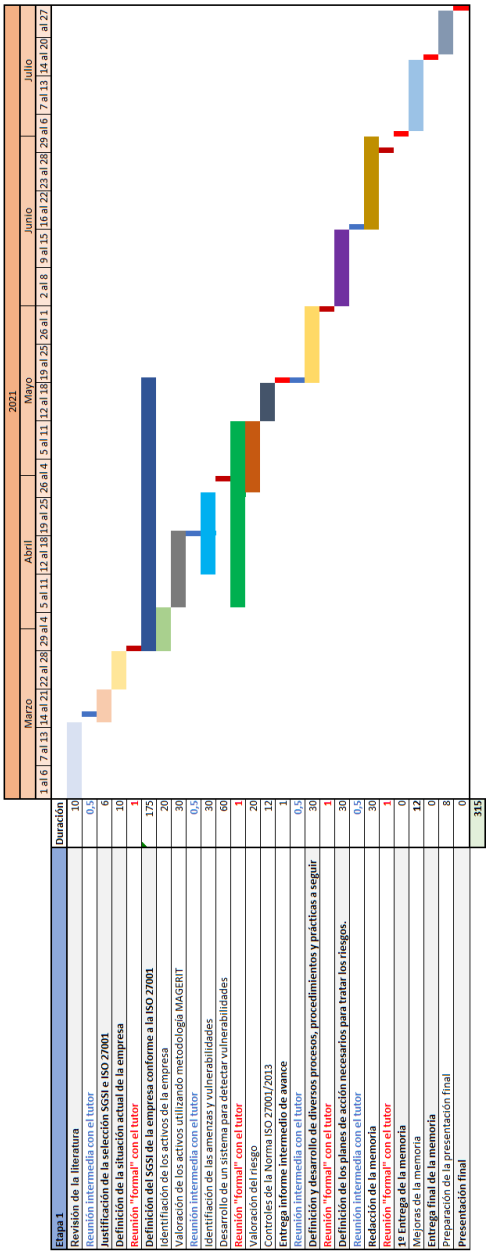


Ilustración 1: Anteproyecto: Diagrama de Gantt – Elaboración propia

4.1.2 Etapa 2: Revisión de la literatura y justificación de la selección de ISO/IEC 27001

4.1.3 Etapa 3: Contexto de la organización conforme a la ISO/IEC 27001

Ha sido necesario desarrollar la situación actual de la empresa para poder desarrollar los correctamente el SGSI de la empresa Congelados Madrid.

Para llevar a cabo este punto se ha realizado una serie de entrevistas a diversas personas que se han considerado necesarias con el fin de definir correctamente la estructura de la empresa, sus diferentes oficinas y distribución, un organigrama de la organización, etc.

4.1.4 Etapa 4: Definición del SGSI de la empresa conforme a la ISO/IEC 27001

Para definir de forma correcta un SGSI hemos definido esta etapa en las siguientes fases:

- Liderazgo y compromiso
- Política general (véase en "Política general de la empresa Congelados Madrid" en anexos)
- Identificación de los activos de la empresa.
- Dentro de este apartado se desarrolló un programa para la identificación de los activos que existen en la red, sistemas operativos que utilizan, puertos abiertos y servicios en ejecución más comunes.
- Valoración de los activos utilizando la metodología MAGERIT.
- Identificación de las vulnerabilidades y amenazas
- Valoración del riesgo: El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad causando un impacto.
- Valoración del riesgo con salvaguardas: Utilizando las salvaguardas con las que cuenta la empresa se ha minimizado la probabilidad de que una amenaza explote una vulnerabilidad, y por lo tanto el riesgo de determinados activos ha disminuido.
- Definición y desarrollo de diversos procesos, procedimientos y prácticas a seguir para disminuir los riesgos más peligrosos.

4.1.5 Diagrama de Gantt

En la siguiente imagen se muestra el cálculo final de ejecución realizada mediante un Diagrama de Gantt.

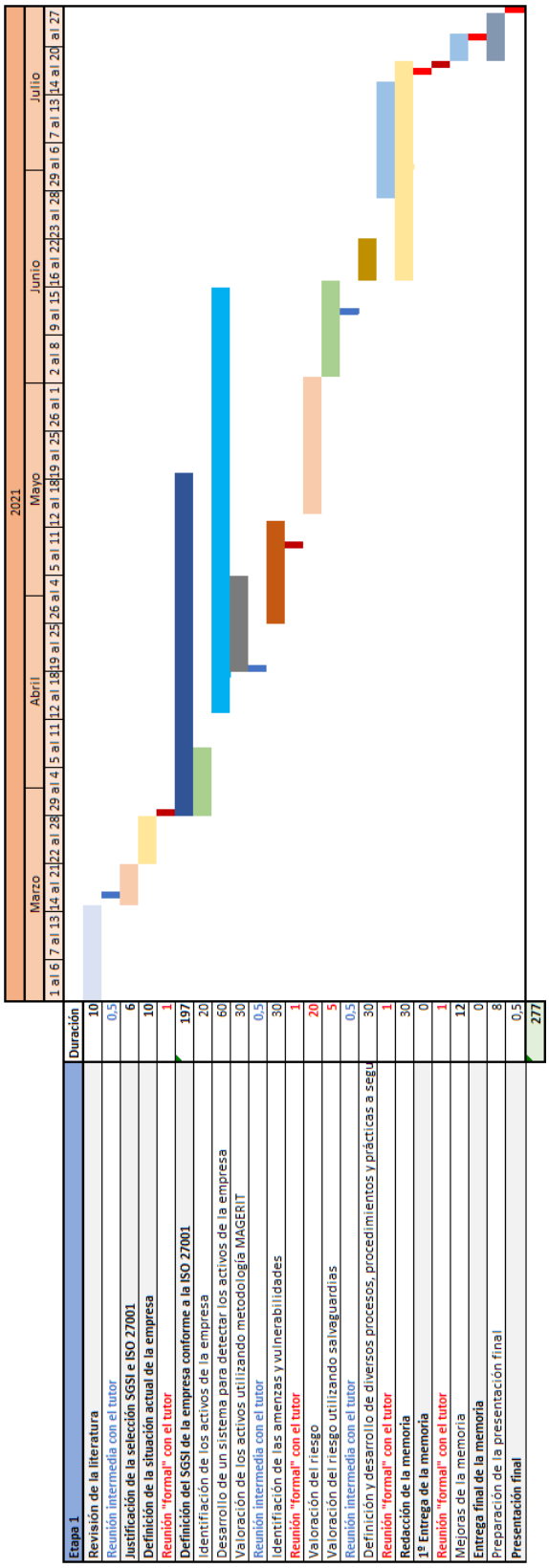


Ilustración 2: Cálculo final de ejecución del proyecto: Diagrama de Gantt – Elaboración propia

4.2 Descripción de la solución, metodologías y herramientas empleadas

4.2.1 Contexto de la organización conforme a la ISO/IEC 27001

4.2.1.1 Compresión de la organización y de su contexto

La empresa Congelados Madrid es un mayorista distribuidor de alimentos congelados y ultracongelados que nace en el año 1992 con la adquisición de un puesto en el Mercado de Pescados de la Puerta de Toledo. A lo largo de esos mismos años 90 da un gran crecimiento y ante la necesidad de contar con mayores espacios físicos para la gestión y transporte de sus productos terminan ubicándose en el mercado de MercaMadrid. En el año 2002 amplía aún más sus almacenes y oficinas centrales para lograr cubrir la demanda de sus servicios que se encontraban en constante aumento. Para el año 2012 se proyecta más allá del mercado nacional y da un salto abriéndose al mercado internacional con la distribución de sus productos en diversos países de Europa, Asia y África.

Actualmente, la empresa cuenta con diversos clientes dentro del mundo de la alimentación. Los tipos de negocio de sus clientes pueden ser: restauración, hostelería, supermercados, tiendas de alimentación, empresa de catering y eventos, colegios, y colectividades, residencias y centros con necesidades, hospitales, clientes finales, otros mayoristas y distribuidores.

Congelados Madrid ha hecho del mundo del congelado su ámbito de negocio, entre otras razones, por la consideración que le merece la aplicación del método de congelación en la preservación de alimentos.

La empresa tiene como misión principal ofrecer a un precio competitivo una gran variedad de productos congelados (pescados, mariscos, moluscos, precocinados, cárnicos, verduras, frutas y postres), presentados en diferentes formatos y adaptados a cada modelo de negocio. Además, tiene en cuenta las necesidades de sus diversos clientes en todo momento, ofreciéndoles un servicio cercano, personalizado y con productos de altísima calidad.

Por último, Congelados Madrid tiene como visión continuar expandiéndose a nivel geográfico en España y Europa lo cual vendrá acompañado del aumento de su capacidad de gestión, almacenamiento y distribución.

4.2.1.2 Comprensión de las necesidades y expectativas de las partes interesadas

Dirección

Los recursos y controles económicos en Congelados Madrid están orientados a productividad generadora de rentabilidad como todo negocio, pero en el caso actual como meta de negocio está definido el crecimiento.

Clientes

En Congelados Madrid es fundamental el cuidado de los productos congelados que disponen en su catálogo, de ello depende de forma directa la calidad del servicio. La calidad de estos servicios está compuesta de varios ítems, como puede ser el sistema de congelado, la trazabilidad, el transporte y las fechas de caducidad, etc.

Empleados

El desarrollo y satisfacción del personal deriva del interés del negocio en mantener políticas, ambiente de trabajo y las herramientas necesarias para la realizar las gestiones propias de Congelados Madrid. Ciertamente la seguridad laboral y la posibilidad de que el empleado pueda desarrollarse profesionalmente es clave y nuevamente los equipos IT están dentro del esquema.

Proveedores

En el aspecto de los proveedores para la presente práctica, la parte de negocio en general toma fuerza en lo que respecta a las alianzas y sus estrategias en los suministros de los diferentes productos que comercializan. La directriz de la empresa es mantener la calidad de los productos y servicios por lo que los sistemas de información forman parte del todo.

IT

La dirección de la empresa es consiente que el crecimiento general debe estar acompañado en dimensión y alcance por el crecimiento del área IT

Los presupuestos y proyecciones económicas son parte activa de la dirección.

Es determinante el buen funcionamiento de los sistemas de información que aseguren el servicio que originará a corto plazo cumplir con las expectativas y satisfacción del cliente con el objetivo de que finalmente se fidelice con la empresa, y teniendo que cuidar luego esa permanencia.

Para Congelados Madrid es vital para sus operaciones la disponibilidad de la información ya de ello depende en un gran porcentaje que sea exitoso. Están claras las necesitades de que IT vele por el cumplimiento de esta expectativa de la empresa.

Así como los proveedores de servicios, la necesidad de contar con un soporte informático a nivel de suministro de equipos necesarios bien sea de hardware y software es nuevamente fundamental ya que a todos los niveles de la organización la disponibilidad de los datos y correcto funcionamiento de los sistemas IT son necesarios para cumplir con las tareas de gestión.

4.2.1.3 Definición del alcance del sistema de gestión de la seguridad de la información

4.2.1.3.1 Organigrama

A continuación, se muestra un organigrama que muestra como está organizada la empresa Congelados Madrid.

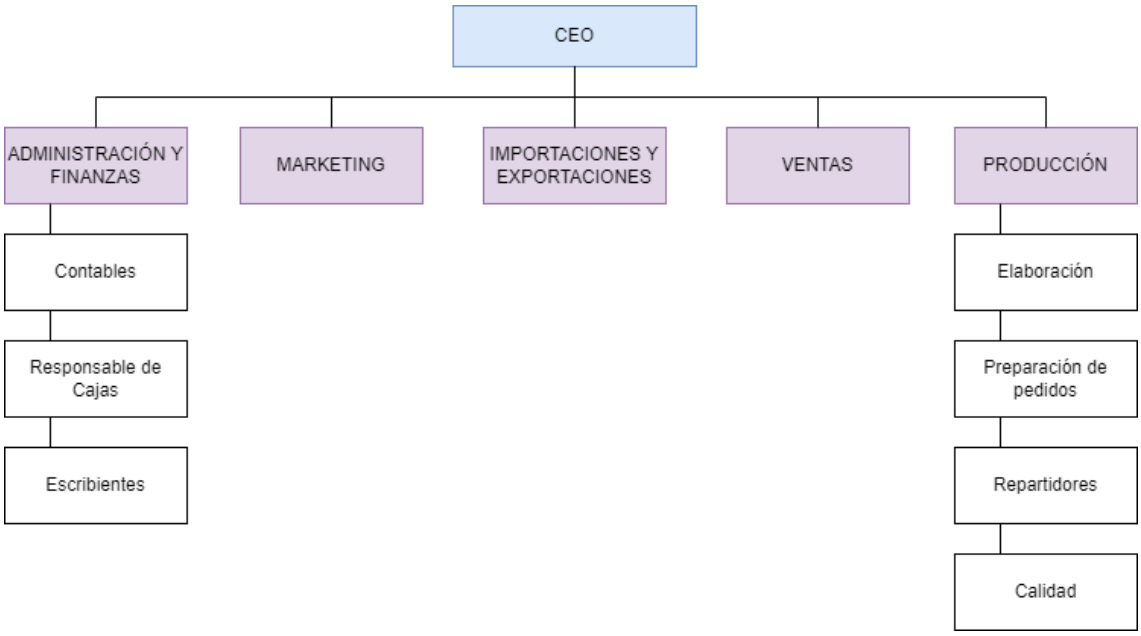


Ilustración 3: Organigrama de Congelados Madrid – Elaboración propia

En la parte superior del Organigrama podemos ver al CEO de la empresa. En este caso existen dos socios que desarrollan el papel de CEO y se encargan de tomar decisiones, definir estrategias globales, etc.

En la segunda escala de la imagen podemos ver varios departamentos en color morado. Cada departamento desarrolla una función diferente dentro de la empresa.

A continuación se explica el desempeño que realiza cada departamento con los sistemas de información de la empresa:

- Administración y finanzas: Este departamento es el encargado de gestionar los medios financieros de la empresa. Se encargan de elaborar presupuestos, gestionar la contabilidad, introducir las ventas y asignarles trazabilidad, etc.
  Dentro de este departamento podemos definir diferentes tipos de empleados que desempeñan las siguientes funcionalidades:
  - Contables: Personal encargado de registrar en el sistema de gestión todas las operaciones económicas (ingresos y gastos) que se lleven a cabo en la empresa según la legalidad vigente.
  - Escribientes: Personal encargado introducir las ventas realizadas en los puestos de MercaMadrid.
  - Responsable de cajas: Además de desempeñar funciones cómo escribiente existe una persona encargada de que cuadren las cajas al finalizar la venta.
- Marketing: Este departamento está formado por una persona encargada de llevar la publicidad de la empresa y además, también la encargada de comunicarse con los proveedores que han realizado la página web y el eCommerce a la empresa.

- Importaciones: Este departamento está formado por una persona encargada de la importación de mercancía comprada a diversos proveedores.
- Ventas: Este departamento está formado por un conjunto de vendedores que se encargan de captar nuevos clientes para el negocio.
- Producción: Este departamento se basa en la recepción, elaboración y distribución de los productos de la organización.
  Dentro de este departamento podemos definir diferentes tipos de empleados que desempeñan las siguientes funcionalidades:
  - Elaboración: Personal encargado de manipular la mercancía (envasar, etiquetar, etc.).
  - Preparación de pedidos: Personal encargado de preparar y cargar los camiones con los pedidos introducidos en el sistema de gestión de la empresa.
  - Calidad: Personal encargado de verificar que los productos sean vendidos en perfecto estado. Se encargan de validar diversas condiciones que deben cumplir los alimentos según la normativa vigente. Por ejemplo, controlan que los productos se mantengan a una temperatura adecuada, que tengan una trazabilidad correcta, verifican su estado, etc.
  - Repartidores: Personal encargado de distribuir la mercancía vendida a los diferentes puntos de venta.
    No utilizan ningún sistema informático para realizar el reparto.

4.2.1.3.2 Planos

La empresa tiene una nave en MercaMadrid de dos plantas.

En la primera planta la empresa se dedica a preparar los productos, cargarlos en camiones, etc.

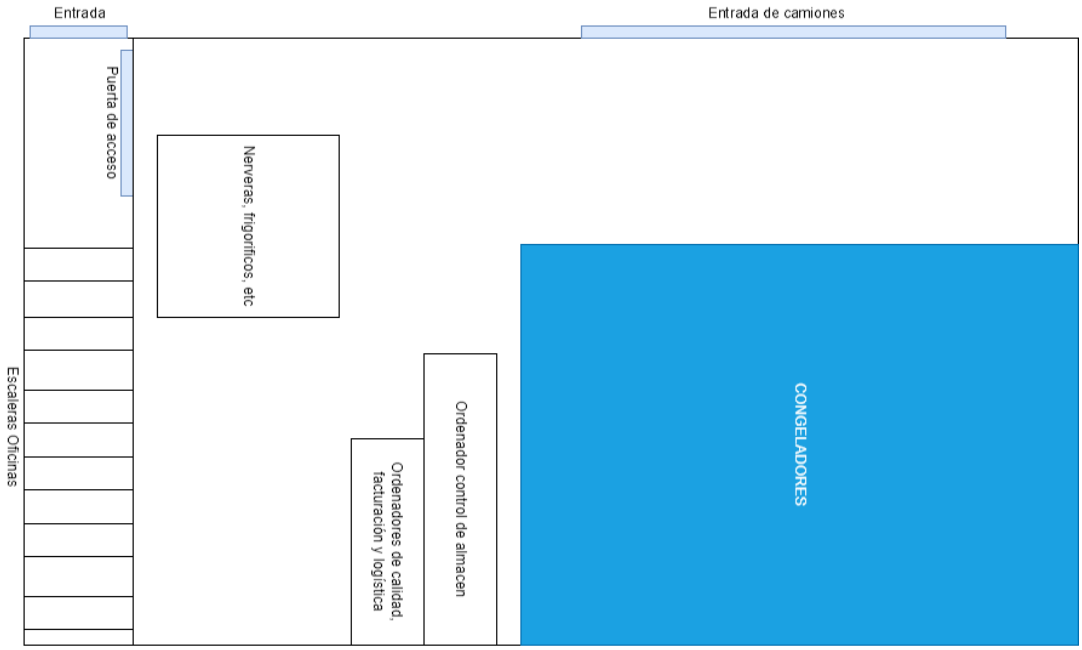


Ilustración 4: Plano de la nave de la empresa – Elaboración propia

La mitad de la segunda planta está alquilada a otra empresa que se dedica a la distribución de pescado.

En el resto de la segunda planta encontramos las oficinas distribuidas de la siguiente forma:

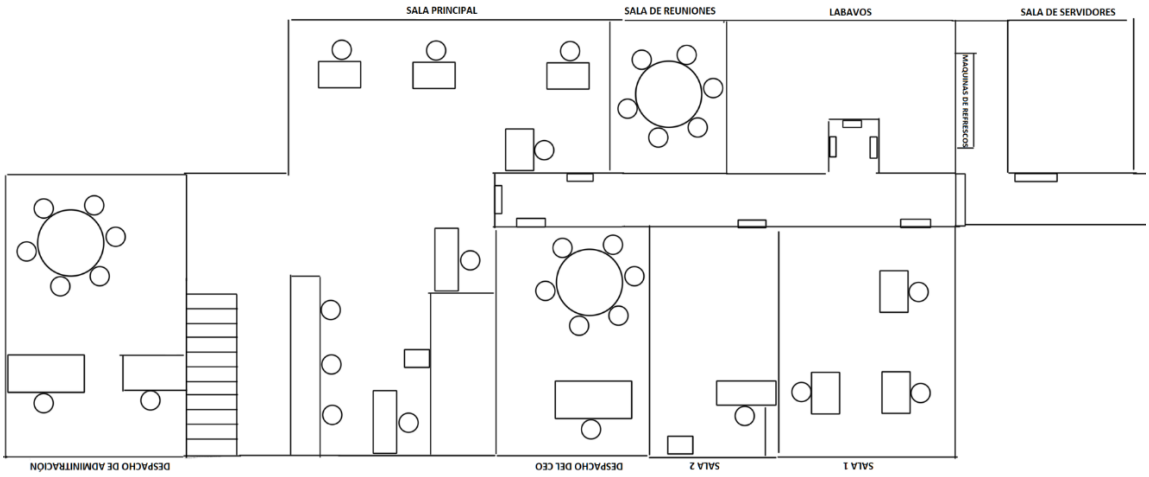


Ilustración 5: Plano de la Oficina – Elaboración propia

Además de la nave, la empresa tiene 4 puestos abiertos en la Nave de Pescados de MercaMadrid.

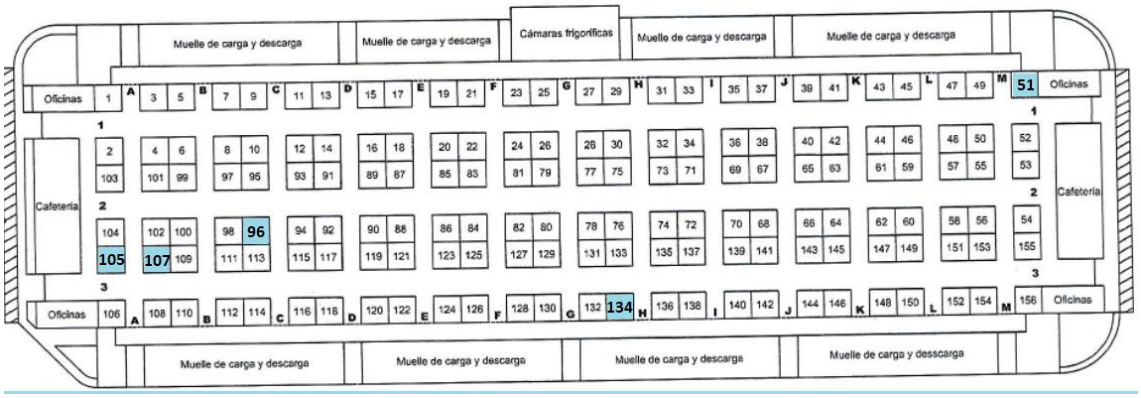


Ilustración 6: Plano de puestos de la nave de pescados de MercaMadrid- Elaborado por ADEPESCA

En la imagen anterior podemos ver resaltado en color azul la distribución de puestos que tiene la empresa Congelados Madrid en la Nave de Pescados.

Todos los puestos tienen un ordenador que se conecta por Escritorio Remoto al ordenador central (FrontEnd) para realizar las ventas desde la madrugada. El puesto 105 tiene dos ordenadores porque desde el realizan un mayor volumen de ventas que en el resto de los puestos.

4.2.1.3.3 Estructura de la red

Actualmente la compañía cuenta con la siguiente estructura de red.

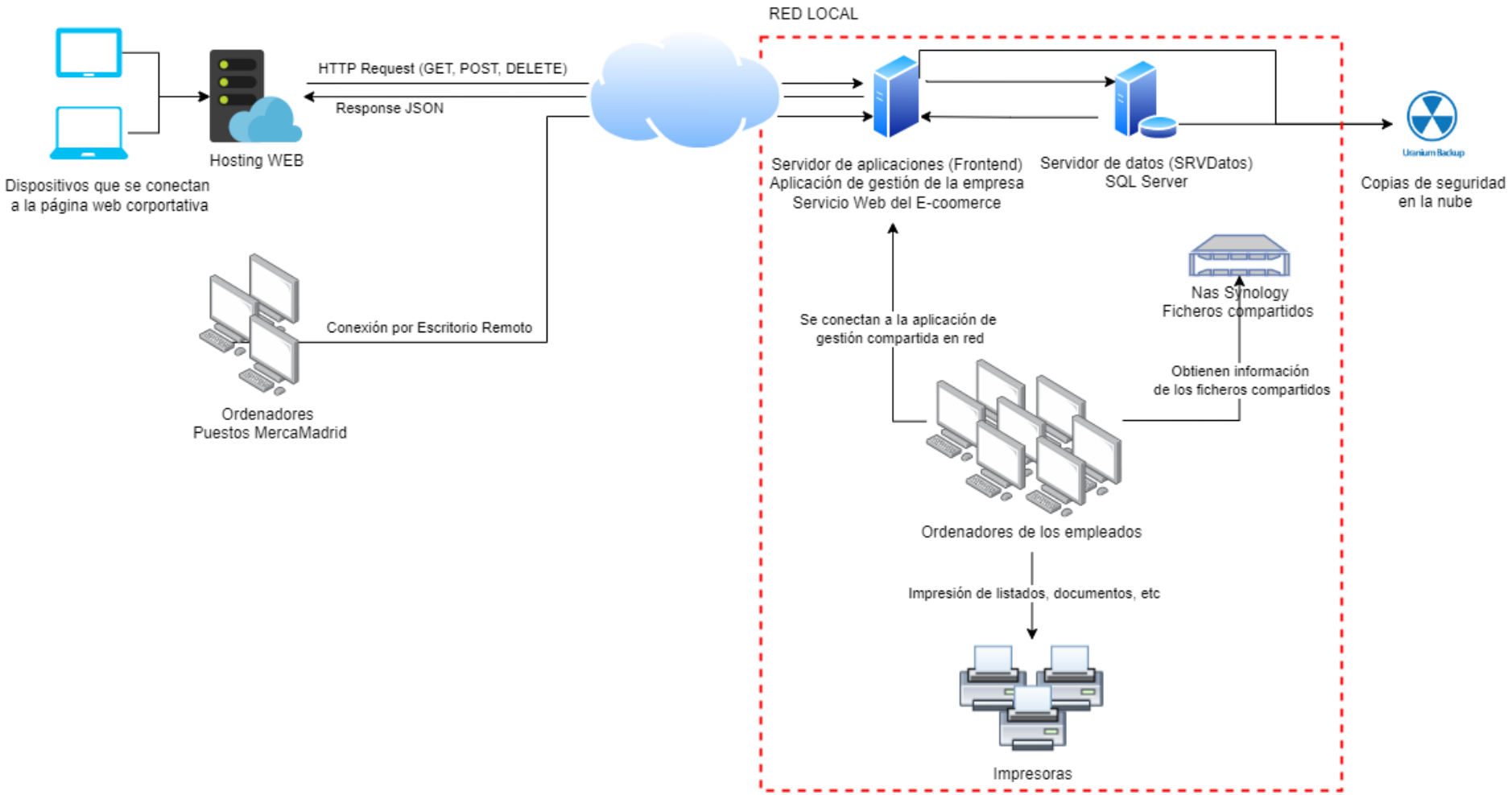


Ilustración 7: Estructura de la red: Elaboración propia

En la imagen anterior podemos ver un cuadrado rojo que contiene los diversos dispositivos conectados dentro de la red local.

La empresa cuenta con los siguientes tres dispositivos principales para el desarrollo de su actividad diaria:

1. Servidor de datos (SrvDatos): Este servidor contiene la base de datos (SQL Server) de la empresa. Esta base de datos está conectada con el sistema de gestión de la empresa y el servicio web para la venta a particulares. Contiene información de los clientes, proveedores, mercancías, pedidos, ventas, trazabilidad, contabilidad, empleados, almacenes, etc.
2. Servidor de aplicaciones (FrontEnd): Contiene la aplicación del sistema de gestión de la empresa y el servicio web para el eCommerce.
   Es importante destacar que la carpeta que contiene el ejecutable del sistema de gestión esta compartida en red para que cualquier usuario pueda utilizarlo desde su dispositivo. Además los diversos puestos de MercaMadrid se conectan directamente a este servidor, a través de la herramienta de escritorio remoto, para realizar la venta diaria.
3. NAS Synology: NAS donde se comparten diversos tipos de ficheros dentro de la red local de la organización.

Se realiza una copia diaria en la nube con Uranium Backup de la información contenida dentro del servidor de aplicaciones y el servidor de datos.

La empresa tiene contratado un Hosting Web que contiene la página web de la empresa y el eCommerce.

4.2.2 Diseño y desarrollo de un programa para la identificación de los activos que existen en la red, sistemas operativos que utilizan, puertos abiertos y servicios en ejecución más comunes

Se ha diseñado y desarrollado un programa con el objetivo de ayudar a la empresa a detectar los activos que están conectados a la red, los sistemas operativos que utilizan, el estado de sus puertos y los servicios en ejecución.

4.2.2.1 Análisis de requisitos

4.2.2.1.1 Requisitos funcionales

En este apartado encontramos una matriz con los requisitos funcionales detectados para el desarrollo del prototipo.

Id	Nombre	Categoría	Descripción
RF-01	Visualización de los activos	Visualización de información	El sistema deberá mostrar el conjunto de activos conectados a una red filtrados por un rango de direcciones IPs introducidas por el usuario.

Id	Nombre	Categoría	Descripción
RF-02	Visualización del estado de los puertos de los activos	Visualización de información	El sistema deberá mostrar el estado de los puertos más comunes dentro de cada dispositivo indicado por un rango de direcciones IPs introducidas por el usuario.
RF-03	Visualización de detalles del activo	Visualización de información	El sistema deberá mostrar información más detallada del sistema operativo y los saltos a los que se encuentra cada dispositivo indicado por un rango de direcciones IPs introducidas por el usuario.

Tabla 2: Requisitos funcionales de la aplicación: Elaboración propia

4.2.2.1.2 Requisitos no funcionales

En este apartado encontramos una matriz con los no funcionales detectados para el desarrollo del prototipo.

Id	Nombre	Categoría	Descripción
RNF-01	Mensajes de ayuda	Usabilidad	El sistema deberá proporcionar mensajes de error orientativos.
RNF-02	Movilidad de la aplicación	Usabilidad	La aplicación web debe poseer un diseño Responsive a fin de garantizar la adecuada visualización en múltiples ordenadores, tablets y teléfonos móviles.
RNF-03	Estilo e interfaces	Usabilidad	El sistema debe poseer interfaces gráficas bien formadas y con un estilo moderno.

Tabla 3: Requisitos no funcionales de la aplicación: Elaboración propia

4.2.2.2 Elección tecnológica

En este punto se va a explicar justificadamente la elección de las tecnologías, librerías y herramientas para el desarrollo de la aplicación.

Por un lado, la aplicación web se ha desarrollado con Angular y el servicio web con Asp Net Core de Visual Studio. Pero ¿por qué se han elegido estos frameworks?

- **Angular**: Es un framework opensource para facilitar la creación y programación de aplicaciones web. Entre las ventajas por las cuales se ha decidido utilizar este framework encontramos: Typescript7 como lenguaje de programación; diseño MVC, reusabilidad de componentes y flexibilidad en cuanto a la plataforma para la que desarrollar.
- **Asp Net Core**: Es un framework opensource para el desarrollo web.
  Se ha seleccionado este framework porque es el que utiliza actualmente la empresa que desarrolla los sistemas informáticos al cliente.

Para el control de versiones se ha utilizado Git. Este es un sistema de control de versiones de código abierto y gratuito para el desarrollo software.

4.2.2.3 Arquitectura de la aplicación

En este apartado se va a llevar a realizar la definición de la arquitectura general de la solución desarrollada. Esta está basada en un modelo cliente/servidor.

El esquema de funcionamiento de la presente aplicación es el siguiente:

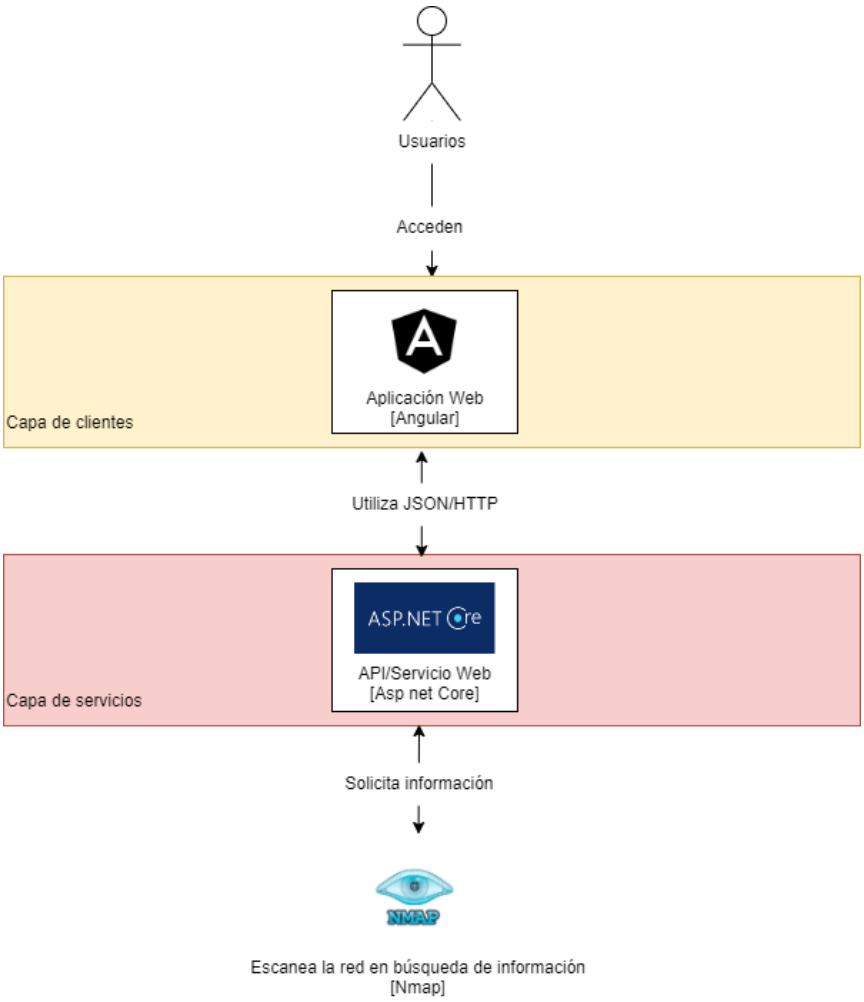


Ilustración 8: Arquitectura de la aplicación: Elaboración propia

Donde:

1. El usuario interactúa con la capa de clientes.
2. La capa de clientes maneja las solicitudes del usuario y realiza peticiones de información al servidor.
3. El servidor procesa la solicitud y utiliza NMAP para recopilar la información necesaria.
4. El servidor responde al cliente con el resultado de la petición en formato JSON.
5. El cliente procesa el resultado recibido.

4.2.2.4 Documentación de la API

Para la documentación de la API creada con Laravel se ha optado por el uso de *Swagger*.

Swagger es un conjunto de herramientas de código abierto creadas en torno a la especificación OpenApi que nos ha ayudado a documentar y consumir Apis REST de manera sencilla.

4.2.2.5 Resultados

En este apartado se va a explicar las diferentes pruebas realizadas para comprobar que la aplicación funcione correctamente.

Para lograr un software eficaz es necesario realizar un buen diseño de casos de prueba. Las pruebas son un conjunto de actividades planeadas con anticipación y que se realizan de manera sistemática. Estas son partes de la verificación y validación incluidas en el aseguramiento de la calidad del software.

- Verificación: Comprobar que el software está de acuerdo con su especificación, donde se debe comprobar que satisface tanto los requerimientos funcionales como los no funcionales.
- Validación: El objetivo es asegurar que el software satisface las expectativas del cliente.

4.2.2.5.1 Pruebas realizadas

4.2.2.5.1.1 Pruebas de código

Cada vez que se ha creado o modificado una nueva función en Asp.net Core se ha comprobado que esta devolviese el resultado esperado con Swagger y una vez que estuviésemos seguros de que funcionaba correctamente se comprobaba que al unirlo al resto de código de la aplicación la funcionalidad de este continuase siendo el mismo.

Además, todas las solicitudes disponibles piden de entrada un rango de direcciones IPs privadas con el siguiente formato: 192.168.1.10-200. Se ha validado la información introducida por el usuario para evitar posibles errores o ataques de Command Injection (ya que Nmap se ejecuta a través de la terminal). La validación se ha realizado teniendo en cuenta las siguientes condiciones:

1. **Es una dirección privada: Información** validada con la siguiente expresión regular:

```
(
      10.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}([\\-][0-9]{1,3})?|
      192.168.[0-9]{1,3}.[0-9]{1,3}([\\-][0-9]{1,3})?|
      172.((16|17|18|30|31)|(2[0-9]{1})){1}.[0-9]{1,3}.[0-9]{1,3}([\\-][0-9]{1,3})?
){1}
```

2. **Es un rango de direcciones válidas:** No puede ser que el último número después del guion sea mayor o igual al último número de la dirección IP y tampoco puede existir ningún número mayor a 255.

4.2.2.5.1.2 Pruebas en la aplicación

La siguiente tabla muestra una breve descripción de las pruebas realizadas, en base a los requisitos funcionales y no funciones, e indica si el resultado ha sido satisfactorio o no.

Id	Descripción	Resultado
RF-01	El sistema deberá mostrar el conjunto de activos conectados a una red filtrados por un rango de direcciones IPs introducidas por el usuario.	☺
RF-02	El sistema deberá mostrar el estado de los puertos más comunes dentro de cada dispositivo indicado por un rango de direcciones IPs introducidas por el usuario.	☺
RF-03	El sistema deberá mostrar información más detallada del sistema operativo y la distancia a la que se encuentra cada dispositivo indicado por un rango de direcciones IPs introducidas por el usuario.	☺

Tabla 4: Pruebas en la aplicación: Elaboración propia

4.2.2.5.2 Explicación de los resultados obtenidos

El resultado de esta aplicación ha sido satisfactorio. Cómo se puede ver en la fase de pruebas se han podido realizar todos los requisitos funcionales.

4.2.3 Definición del SGSI de la empresa conforme a la ISO/IEC 27001

4.2.3.1 Identificación de los activos a proteger

Para la identificación de los activos a proteger se ha realizado una serie de entrevistas en la empresa para conocer la estructura de la organización y los diferentes activos disponibles y se ha contrastado dicha información con la aplicación desarrollada explicada en el punto anterior.

Por un lado, la aplicación desarrollada detectó que durante las horas de trabajo existían un total de 35 dispositivos en funcionamiento conectados a la misma red que el servidor de aplicaciones (ver "Resultados obtenidos de la búsqueda de activos" en Anexos).

Por otro lado, los empleados de la empresa nos mostraron los diferentes dispositivos que tenían operativos, así como sus instalaciones y personal.

Con toda esta información hemos obtenido la siguiente tabla organizada según la clasificación de activos de Magerit V3.

Esta contiene todos los activos de la empresa y una breve descripción del desempeño que lleva a cabo cada uno.

ID	Nombre	Descripción
Datos/Información		
Act-DA-001	Fichero de importaciones	Documentos Excel con datos referentes a las importaciones de la empresa.
Act-DA-002	Fichero con tarifas	Documentos Excel con datos referentes a las tarifas de la empresa.
Act-DA-003	Ficheros compartidos	Documentos varios que se comparte entre el personal de la empresa por la red.
Act-DA-004	Datos de albaranes	Información relativa a las ventas de las empresa.
Act-DA-005	Datos de facturación	Información relativa a los datos utilizados para la facturación diría.
Act-DA-006	Datos de pedidos	Información relativa a los pedidos realizados por los clientes que se deben ser preparados.
Act-DA-007	Datos de almacenes	Información relativa al inventario (ubicación, stock, etc.).
Act-DA-008	Datos de trazabilidad	Información relativa al seguimiento de la compra/venta de los productos.
Act-DA-009	Datos contables	Información relativa a la contabilidad de la empresa (apuntes, cobros, etc.).
Act-DA-010	Datos de productos	Información relativa a la codificación de los productos vendidos (nombre, características, información nutricional, etc.).
Act-DA-011	Datos de clientes	Información relativa a los clientes de la empresa.
Act-DA-012	Datos de empleados	Información relativa a los empleados de la empresa.
Act-DA-013	Datos de proveedores	Información relativa a los proveedores de la empresa.
Act-DA-014	Datos tarifas	Información relativa a los precios de los productos.
Act-DA-015	Datos de usuarios del sistema de gestión	Información relativa a los usuarios que tienen acceso al sistema de gestión y sus privilegios.

ID	Nombre	Descripción
Servicios		
Act-SE-001	Acceso remoto de Windows	Utilizado por los puestos comerciales para utilizar la aplicación a través de la herramienta nativa del sistema operativo.
Act-SE-002	Anydesk	Utilizado por el proveedor del sistema de gestión y personal interno para conectarse al sistema de forma remota.
Act-SE-003	Correo electrónico	Utilizado para las comunicaciones internas y externas de la empresa.
Act-SE-004	Almacenamiento de ficheros	NAS donde comparten documentos en diversos directorios: - Directorio de importaciones: solo tiene acceso el personal de importaciones y la jefa de administración. - Directorio de tarifas: solo tienen acceso el personal de contabilidad. Directorio de documentos generales: tienen acceso todos los empleados que utilicen sistemas informáticos en la empresa
Software		
Act-SO-001	Página web de la empresa	Página web utilizada para dar visibilidad a la empresa y vender a clientes particulares.
Act-SO-002	Servicio Web	API utilizada por la página web de la empresa para la venta a particulares. Está ubicada en el IIS del servidor de aplicaciones y se ha abierto un puerto para su uso.
Act-SO-003	Internet Information Services (IIS)	Utilizado para publicar el servicio web.
Act-SO-004	Sistema de Gestión	Software de gestión general de la empresa.
Act-SO-005	Google Chrome	Navegador predeterminado para consultas web.

ID	Nombre	Descripción
Act-SO-006	SQL Server	Sistema de gestión de la base de datos de la empresa.
Act-SO-007	Office 365	Software Office 365 para desarrollar diversas tareas en la empresa.
Act-SO-008	Antivirus	Software de protección de virus informáticos.
Act-SO-009	Firewall	Se utiliza el firewall del sistema operativo nativo.
Act-SO-010	Licencias Windows 7 Pro	Product Key de software original.
Act-SO-011	Licencias Windows 8	Product Key de software original.
Act-SO-012	Licencias Windows 10 Home	Product Key de software original.
Act-SO-013	Licencias Windows 10 Pro	Product Key de software original.
Act-SO-014	Sistema de BackUp del servidor de aplicaciones	Se utiliza Uranium BackUp para realizar copias diarias.
Act-SO-015	Sistema de BackUp de la base de datos	Se utiliza Uranium BackUp para realizar copias diarias.
Equipos informáticos		
Act-EI-001	Servidor de base de datos	Equipo informático que contiene la base de datos.
Act-EI-002	Servidor de aplicaciones	Equipo informático que contiene la aplicación del sistema de gestión y el servicio web.
Act-EI-003	Ordenador del departamento de importaciones	Equipo informático que se utiliza para la gestión de las importaciones.
Act-EI-004	Ordenadores del departamento de contabilidad	Equipos informáticos utilizados por el departamento contable.

ID	Nombre	Descripción
Act-EI-005	Portátiles del departamento de Marketing	Equipos informáticos utilizados por el departamento Marketing.
Act-EI-006	Portátiles del departamento de ventas	Equipos informáticos utilizados por el departamento ventas.
Act-EI-007	Ordenadores de los escribientes	Equipos informáticos utilizados por los escribientes para introducir pedidos/cuadrar cajas.
Act-EI-008	Portátil del CEO	Equipo informático utilizado por el CEO.
Act-EI-009	Ordenadores de los puestos comerciales	Equipo informático utilizado en los puestos comerciales de Mercamadrid para realizar las ventas diarias.
Act-EI-010	Impresora Samsung	Utilizada por los comerciales para imprimir
Act-EI-011	Impresora HP	Utilizada por los comerciales. Se puede utilizar únicamente para realizar fotocopias.
Act-EI-012	Impresora HP	Ubicada en la sala principal. Cualquier persona en la red puede imprimir.
Act-EI-013	Switches	Ubicado en la sala de servidores.
Act-EI-014	Router Huawei	Ubicado en la sala de servidores.
Act-EI-015	Access Point	No es utilizado actualmente por la empresa y se desconoce su finalidad. No se retiene en análisis posterior. (PIE DE PÁGINA)
Redes de comunicaciones		
Act-RC-001	WiFi	Red inalámbrica de la empresa.
Act-RC-002	LAN	Red cableada de la empresa.
Soportes de información		
Act-SI-001	Memorias USB	Dispositivos de almacenamiento multiuso.

ID	Nombre	Descripción
Act-SI-002	Almacenamientos en RED	Utilizado para compartir información por la red de la empresa.
Act-SI-003	Material impreso	Documentos almacenados en carpetas (facturas, albaranes, datos contables, etc.).
Equipamiento auxiliar		
Act-EA-001	Sistema de suministro eléctrico ininterrumpido (UPS)	El ordenador con la base de datos y el ordenador con las aplicaciones se encuentran conectados a una SAI.
Act-EA-002	Aire acondicionado (CPD)	Utilizado para mantener la correcta temperatura del CPD.
Act-EA-003	Cableado	Cableado categoría CAT5e utilizado para realizar las conexiones entre los equipos.
Act-EA-004	Fibra óptica	Cableado de alta velocidad para la entrada del servicio de internet.
Act-EA-005	Red eléctrica	Suministro eléctrico distribuido en las instalaciones para proveer de corriente eléctrica a los equipos necesarios.
Act-EA-006	Router de Movistar (ISP)	Proveedor de servicio de internet.
Instalaciones		
Act-IN-001	Puestos comerciales de MercaMadrid	Se encuentran dentro de la nave de pescados de MercaMadrid y son utilizados para las ventas diarias.
Act-IN-002	Nave	Instalación principal de la empresa.
Act-IN-003	CPD	Centro de procesamiento de datos donde están ubicados el servidor de base de datos, el servidor de aplicaciones, Router, switch y otros activos.
Act-IN-004	Despacho CEO	Oficina destinada a el desempeño de las actividades del CEO.

ID	Nombre	Descripción
Act-IN-005	Sala Principal	Se encuentran los puestos de trabajo de diversos empleados (contabilidad, marketing, importaciones, responsable de cajas y comerciales).
Act-IN-006	Despacho de Administracion	Se encuentra el puesto de los responsables de área.
Act-IN-007	Sala 1	Existen tres puestos de trabajo con sus respectivos dispositivos, pero actualmente se utilizan dos por parte de un comercial y un escribiente.
Act-IN-008	Sala 2	Sala donde trabaja un comercial y están ubicadas las dos impresoras.
Personal		
Act-PE-001	Personal de Contabilidad	Personas destinadas a la desempeñar funciones de contabilidad.
Act-PE-002	Empleado de Marketing	Personas destinadas a la desempeñar funciones de Marketing.
Act-PE-003	Personal de Ventas	Personas destinadas a la desempeñar funciones de ventas.
Act-PE-004	Escribientes	Personas destinadas a realizar las ventas.
Act-PE-005	Responsable de Cajas	Persona responsable de cuadrar las ventas de los puestos de MercaMadrid.
Act-PE-006	Empleado de Importaciones	Persona destinadas a realiza la gestión de las importaciones de la empresa.
Act-PE-007	Clientes de la página WEB	Usuarios que acceden a la página web para realizar/consultar compras.
Act-PE-008	CEO	Líder y responsable de todas las operaciones de la empresa.
Act-PE-09	Proveedor del sistema de gestión	Empresa externa encargada de suministrar y mantener las necesidades del sistema de gestión.

Tabla 5: Identificación de los activos a proteger

4.2.3.2 Valoración de los activos de la empresa

Para valorar los activos se ha tenido en cuenta la información proporcionada por parte del CEO sobre el funcionamiento y las necesidades de la empresa Congelados Madrid.

Una vez recopilada la información necesaria se ha procedido a la valoración de los activos teniendo en cuenta la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de la información de estos. Esta valoración se ha realizado a través del uso de la tabla ACIDA (ver "¿Cómo valoramos los activos?" en Anexos).

En el siguiente gráfico podemos ver el resultado obtenido tras calcular el valor de los diferentes activos (ver "Valoración de los activos de la empresa" en Anexos).

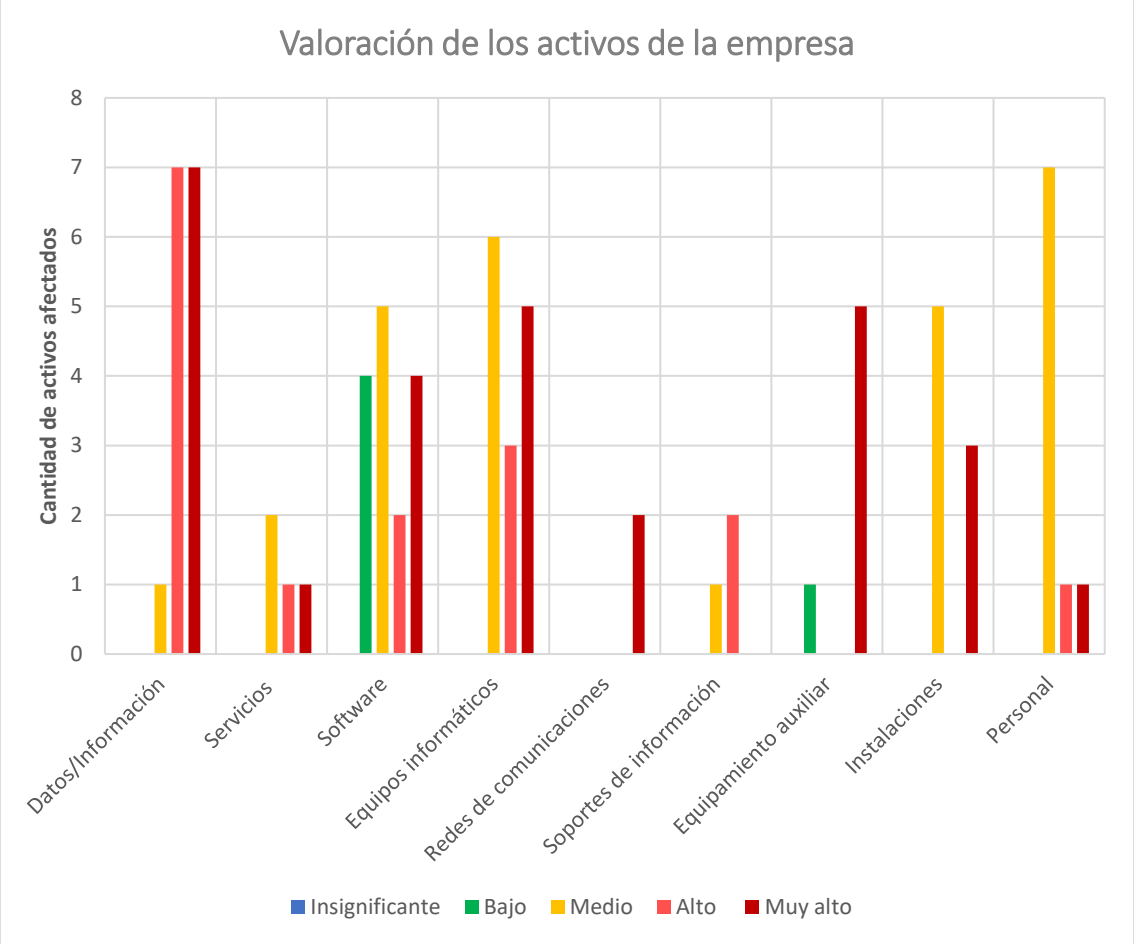


Gráfico 1: Representación del valor del activo dependiendo de la clasificación del tipo activo: Valoración propia

El gráfico de barras anterior muestra el valor de los activos en función de la clasificación del tipo de activo según Magerit V3.

Como podemos observar, según el cálculo realizado, el conjunto de activos que son clasificados como activos de datos, software, equipos informáticos, redes de comunicaciones y equipamiento auxiliar tienen un mayor valor en términos de la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad para la empresa.

4.2.3.3 Selección de activos para ser valorados en el presente SGSI

Debido al gran número de activos que tiene la organización hemos entrevistado al CEO y hemos decidido que para esta primera aproximación del SGSI se valoren 23 activos que tienen relación con el Sistema de Gestión de la Empresa y el correo electrónico.

Podemos observar que los valores más altos representados en el gráfico calculado en el punto anterior coinciden en una gran parte con los utilizados en el Sistema de Gestión de la Empresa y en el correo electrónico. Es por esto y por la preocupación del CEO por lo que en esta primera aproximación del SGSI se han tenido en cuenta los activos mostrados en la siguiente tabla:

ID	Nombre	Descripción
Datos/Información		
Act-DA-004	Datos de albaranes	
Act-DA-005	Datos de facturación	
Act-DA-006	Datos de pedidos	
Act-DA-007	Datos de almacenes	
Act-DA-008	Datos de trazabilidad	
Act-DA-009	Datos contables	
Act-DA-010	Datos de productos	
Act-DA-011	Datos de clientes	
Act-DA-013	Datos de proveedores	
Act-DA-014	Datos tarifas	
Act-DA-015	Datos de usuarios del sistema de gestión	
Servicios		
Act-SE-001	Acceso remoto de Windows	
Act-SE-003	Correo electrónico	
Software		
Act-SO-004	Sistema de Gestión	

ID	Nombre	Descripción
Act-SO-006	SQL Server	
Equipos informáticos		
Act-EI-001	Servidor de base de datos	
Act-EI-014	Router Huawei	
Redes de comunicaciones		
Act-RC-001	Wifi	
Soportes de información		
Act-SI-002	Almacenamientos en RED	
Equipamiento auxiliar		
Act-EA-005	Red eléctrica	
Act-EA-006	Router de Movistar (ISP)	
Instalaciones		
Act-IN-001	Puestos comerciales de MercaMadrid	
Act-IN-003	CPD	

Tabla 6: Activos seleccionados: Elaboración propia

4.2.3.4 ¿Cómo se calcula el riesgo?

Según Magerit, versión 3.0 un riesgo es la "estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización". La fórmula que se ha utilizado en el presente trabajo es la siguiente:

$$Valor\ riesgo = Valor\ del\ activo * Valor\ probabilístico$$

Siendo:

- Valor del activo: Es la consecuencia que sobre un activo se materialice en una amenaza. Este valor ha sido calculado anteriormente (ver "Valoración de los activos de la empresa") con el uso de la tabla ACIDA.
- Valor probabilístico: Es un valor cualitativo por medio de una escala nominal (1 al 4) que hemos determinado para medir la probabilidad de ocurrencia de que una vulnerabilidad explote una amenaza causando un impacto.

4.2.3.4.1 ¿Cómo se calcula el valor probabilístico?

En este caso, para medir la probabilidad de ocurrencia se ha definido un valor cualitativo por medio de una escala nominal que representa la frecuencia de tiempo con la que una vulnerabilidad explota una amenaza causando un impacto.

Se ha decidido medir la probabilidad de ocurrencia en base a la siguiente tabla:

Probabilidad de riesgo	Valor probabilístico	Descripción
Rara vez	1	Probabilidad muy baja de ocurrencia (puede ocurrir una vez cada 3-4 años). Debería causar un impacto despreciable.
Moderada	2	Probabilidad de que ocurra entre un intervalo de dos a tres años. Tiene un impacto moderado, puede haber pérdidas económicas y de información.
Probable	3	Probabilidad de que ocurra como mucho en un intervalo de uno a dos años. Tiene un impacto significante en la organización que puede conllevar a pérdidas económicas altas y posible pérdida de clientes.
Muy probable	4	Probabilidad de que ocurra más de una vez al año. Tiene un impacto muy alto que conlleva a pérdidas económicas altas y posible pérdida de clientes.

Tabla 7: Valor probabilístico: Elaboración propia

4.2.3.4.2 Niveles de riesgo

Una vez aplicada la fórmula para calcular el riesgo se ha establecido la siguiente escala para medir el riesgo en cinco niveles:

Riesgo	Valor	Intervalo	Descripción
Bajo	1	0-4	Actualmente el activo tiene un control de seguridad. La oportunidad de explotar la vulnerabilidad es baja. Requiere monitoreo.
Moderado	2	5-9	Hay posibilidad de que ocurra una vulnerabilidad.

Riesgo	Valor	Intervalo	Descripción
			Probabilidad de ocurrencia media. Puede dañar solo a aplicaciones que no son críticas para la organización. Impacto no importante pero es necesario un control activo del riesgo.
Alto	3	10-14	Hay muchas posibilidades de que ocurra una vulnerabilidad. Probabilidad de ocurrencia alta. Tiene impacto en aplicaciones críticas del negocio o servicios. Alto impacto en las operaciones del negocio y es necesario monitorear el riesgo de forma frecuente.
Muy Alto	4	15-20	Hay muchas posibilidades de que ocurra una vulnerabilidad. Probabilidad de ocurrencia muy alta. Tiene un mal impacto en aplicaciones críticas del negocio o servicios dejándolas sin funcionamiento durante bastante tiempo. Alto impacto en las operaciones del negocio y es necesario monitorear el riesgo de forma frecuente.

Tabla 8: Valoración del riesgo: Elaboración propia

4.2.3.5 Valoración del riesgo sin Salvaguardias

4.2.3.5.1 Mapa de calor

Una vez calculado el riesgo (ver "Valoración del riesgo sin Salvaguardias" en los Anexos) podemos reflejarlo en un mapa de calor. En el eje y encontramos el valor del activo y en el eje x la probabilidad de ocurrencia.

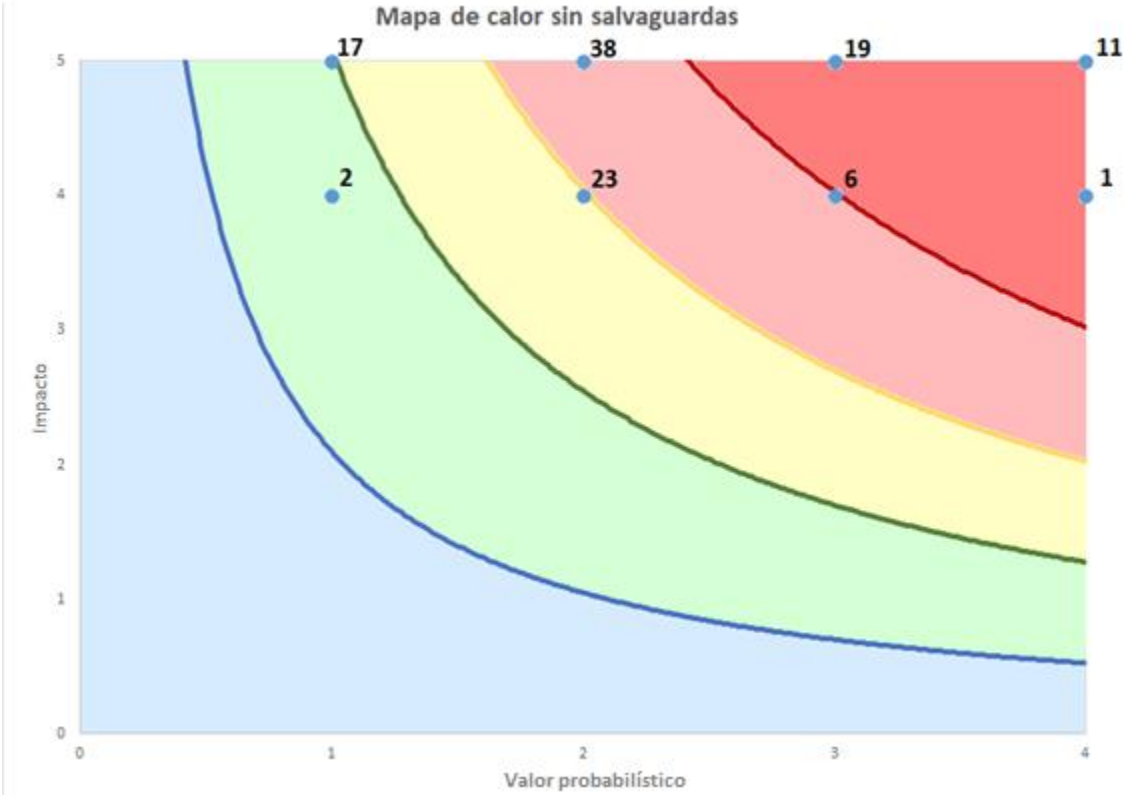


Gráfico 2: Mapa de calor sin aplicar salvaguardas: Elaboración propia

En la imagen anterior vemos reflejado el mapa de calor donde:

- El color azul claro representa una franja donde se encuentran aquellos activos expuestos a un riesgo inferior al mínimo aceptable.
- El color verde representa una franja donde se encuentran aquellos activos expuestos a un riesgo aceptable para la empresa.
  El nivel de tolerancia ha sido propuesto por los consultores del presente proyecto y aprobado por el CEO.
- El color amarillo representa una franja donde se encuentran aquellos activos expuestos a un riesgo moderado para la empresa.
- El color rojo claro representa una franja donde se encuentran aquellos activos expuestos a un riesgo alto para la empresa.
- El color rojo oscuro representa una franja donde se encuentran aquellos activos expuestos a un riesgo crítico para la empresa.

Además, podemos ver reflejado un número al lado superior derecho de los puntos que indica la cantidad de riesgos en ese punto.

Como podemos observar los activos elegidos en general tienen riesgo alto/crítico que tiene correlación con el valor del activo calculado en la tabla ACIDA. Es de vital importancia para la empresa tratar de mitigar el riesgo de estos activos aplicando salvaguardas.

4.2.3.6 Valoración del riesgo con salvaguardas

En el punto anterior valoramos el riesgo de los activos seleccionados y creamos un mapa de calor para delimitar los riesgos en cinco escalas (bajo, aceptable, moderado, alto y crítico).

En este apartado se van a tratar de mitigar los riesgos sobre dichos activos teniendo en cuenta las salvaguardas con las que cuenta la empresa actualmente. Los activos definidos anteriormente que actúan como salvaguardas son:

ID	Nombre	Descripción
Software		
Act-SO-008	Antivirus	Software de protección de virus informáticos.
Act-SO-009	Firewall	Se utiliza el firewall del sistema operativo nativo.
Act-SO-014	Sistema de BackUp del servidor de aplicaciones	Se utiliza Uranium BackUp para realizar copias diarias.
Act-SO-015	Sistema de BackUp de la base de datos	Se utiliza Uranium BackUp para realizar copias diarias.
Equipamiento auxiliar		
Act-EA-001	Sistema de suministro eléctrico ininterrumpido (UPS)	El ordenador con la base de datos y el ordenador con las aplicaciones se encuentran conectados a un sistema de alimentación interrumpida (SAI).

Tabla 9: Salvaguardas: Elaboración propia

Dentro de las salvaguardas debemos de diferenciar entre:

- Salvaguardas que reducen la probabilidad de amenazas que son ideales para impedir que la amenaza se materialice (antivirus, firewall).
- Salvaguardas que limitan el daño causado, es decir, limitan la posible degradación (UPS) o permiten la pronta recuperación del sistema cuando una amenaza lo destruye (BackUps).

4.2.3.6.1 Mapa de calor con salvaguardas

Una vez definidas las salvaguardas con las que cuenta la empresa se han procedido a calcular los nuevos riesgos (ver "Cálculo del riesgo con salvaguardas" en el Anexo).

Para entender cómo afecta el uso de salvaguardas al mapa de calor se va a utilizar el siguiente ejemplo:

- Datos de albaranes: inicialmente teníamos una vulnerabilidad podía provocar la interrupción indefinida de los procesos del negocio al no realizar copias de seguridad. Como podemos ver en la siguiente imagen, el riesgo inicial en este caso había sido valorado en 15 (franja roja) y al realizar copias de seguridad el riesgo anterior disminuye notablemente y pasa a ser de un riesgo crítico a un riesgo aceptable para la empresa.

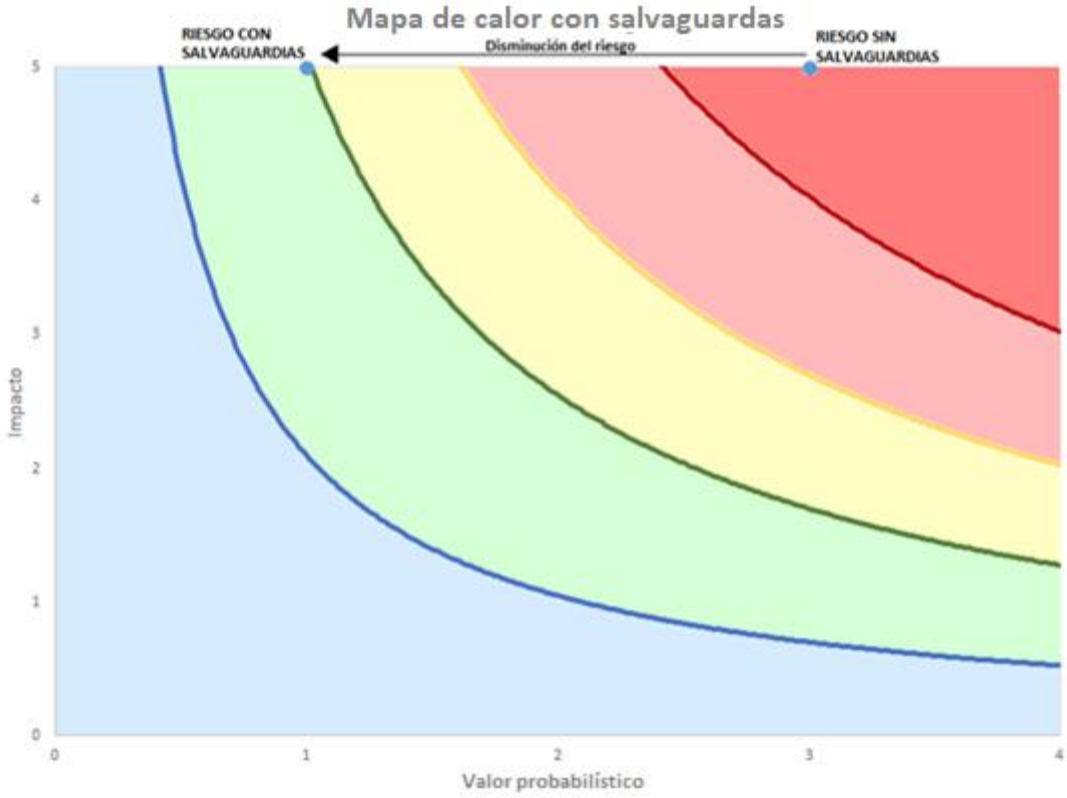


Gráfico 3: Ejemplo de disminución del riesgo aplicando una salvaguarda: Elaboración propia

Una vez calculado el nuevo valor del riesgo para cada activo en el punto anterior podemos reflejar cómo quedaría el nuevo mapa de calor con las salvaguardas.

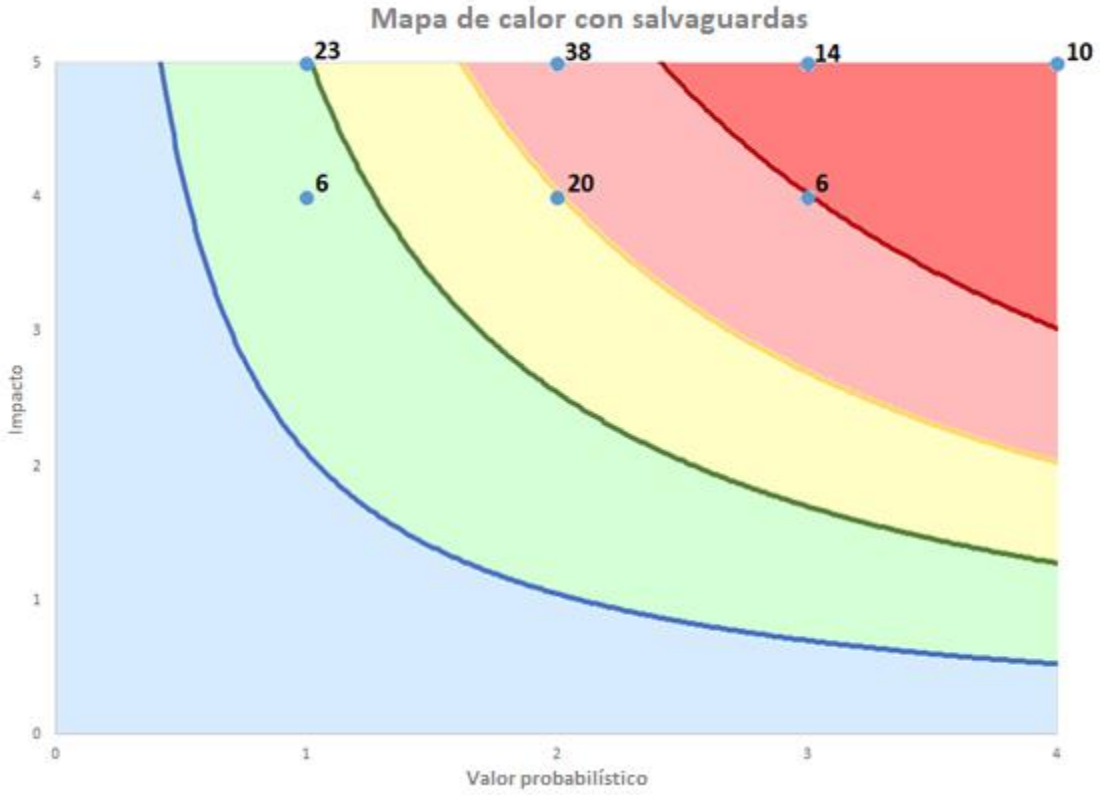


Gráfico 4: Mapa de calor con salvaguardas: Elaboración propia

En la imagen anterior vemos reflejado el mapa de calor donde:

- El color azul claro representa una franja donde se encuentran aquellos activos que tienen un riesgo bajo.
- El color verde representa una franja donde se encuentran aquellos activos que tienen un riesgo aceptable para la empresa.
- El color amarillo representa una franja donde se encuentran aquellos activos que tienen un riesgo moderado para la empresa.
- El color rojo claro representa una franja donde se encuentran aquellos activos que tienen un riesgo alto para la empresa.
- El color rojo oscuro representa una franja donde se encuentran aquellos activos que tienen un riesgo crítico para la empresa.

Además, podemos ver reflejado un número al lado superior derecho de los puntos que indica la cantidad de riesgos en ese punto.

Como podemos observar aplicando las salvaguardas ya existentes de la empresa hemos conseguido "bajar" múltiples riesgos que se encontraban en la franja roja a una franja moderada o aceptable del riesgo. A pesar de lo anterior siguen existiendo múltiples riesgos por encima de la franja verde.

4.2.3.7 Valor del riesgo aplicando diversos procesos, procedimientos y prácticas a seguir

En el punto anterior valoramos el riesgo teniendo en cuenta las salvaguardias con las que cuenta la empresa y además creamos un mapa de calor para delimitar los riesgos en cinco escalas (bajo, aceptable, moderado, alto y crítico).

En este apartado se van a tratar de mitigar los riesgos que continúan siendo altos o críticos, tras aplicar las salvaguardas, a través de la implementación y uso de las siguientes políticas y procedimientos definidas en el apartado "Políticas de seguridad y procedimientos" que encontramos en el Anexo.

- Política de Seguridad de Acceso a los ordenadores y Servidores
- Política de concienciación y formación del personal
- Procedimiento de pruebas o actualización del software
- Políticas de segregación de funciones de documentos y aplicaciones compartidos en red
- Políticas de segregación de funciones orientado al Sistema de Gestión de la empresa
- Políticas de monitorización de los sistemas informáticos
- Políticas de herramientas de seguridad

4.2.3.7.1 Mapa de calor aplicando las políticas de seguridad

Una vez definidas las políticas y procedimientos se han procedido a calcular los nuevos riesgos (ver "Cálculo del riesgo utilizando las políticas y procedimientos" en el Anexo) obteniendo finalmente el siguiente mapa de calor:

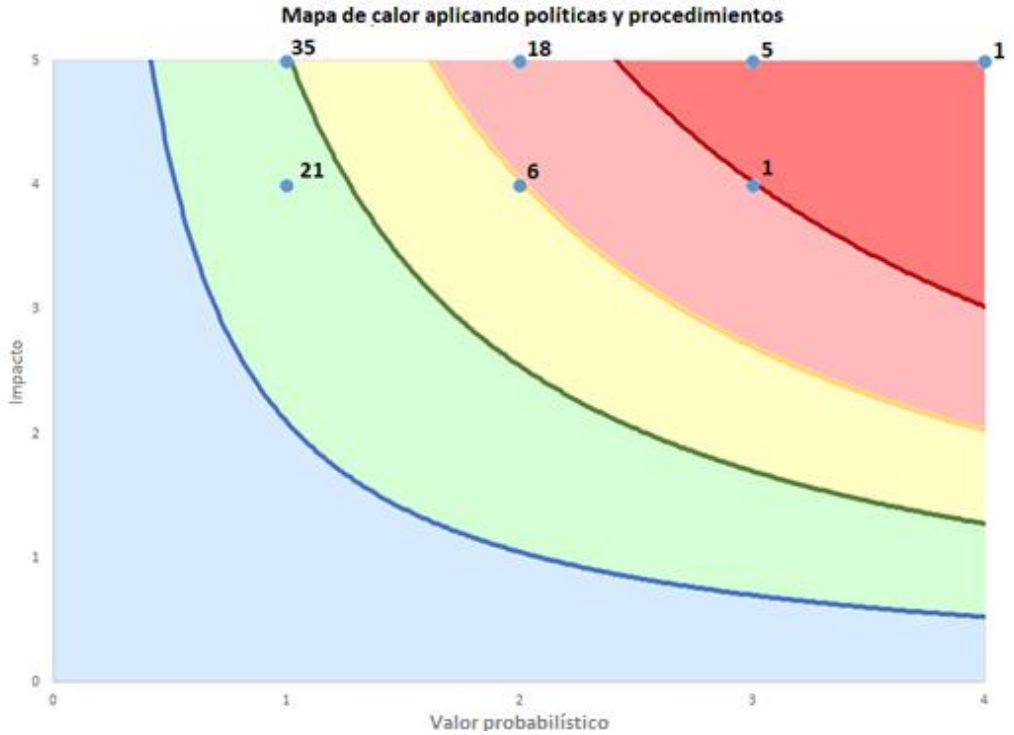


Gráfico 5: Mapa de calor aplicando políticas y procedimientos

En este último mapa de calor se puede comprobar cómo al aplicar una serie de políticas y procedimientos se va a poder disminuir los riesgos de seguridad notablemente, pasando de tener inicialmente 31 riesgos críticos a 6 y de tener 19 riesgos dentro de la franja tolerable a 56.

Es importante destacar que por el momento el riesgo crítico con valor (4, 5) se ha decidido asumir y no mitigar. Esto se debe a que para mitigar este riesgo es necesario obligar a seguir a la empresa proveedora de la Aplicación de Gestión políticas y procedimientos a la hora de probar los programas. En este punto la empresa prefiere seguir recibiendo las actualizaciones a pesar de que estás pueden afectar a la continuidad del negocio.

Por otro lado, la empresa ha decidido asumir los 31 riesgos altos o críticos restantes en esta primera aproximación del SGSI por motivos económicos.

Capítulo 5. CONCLUSIONES

5.1 Conclusiones del trabajo

El objetivo que perseguía el presente TFM era establecer los mecanismos de gestión de la seguridad y las salvaguardas necesarias con el fin de permitir definir, alcanzar y mantener los objetivos de seguridad de la información de la empresa Congelados Madrid.

Dentro del objetivo del proyecto quedó fuera la implementación y el mantenimiento del SGSI. Adicionalmente no se ha contemplado la certificación porque no existe una necesidad real que justifique la misma.

La planificación ha estado estructurada en una serie de etapas que se han ido realizando secuencialmente por ambos estudiantes.

El diseño y desarrollo del presente SGSI se ha realizado conforme al estándar ISO/IEC 27001 utilizando la metodología de Magerit V3. Además, la aplicación informática desarrollada con la finalidad de ayudar a detectar los dispositivos conectados a la red se ha desarrollado con una arquitectura cliente/servidor.

El equipo de trabajo ha estado formado por dos estudiantes que han trabajado de forma conjunta en todas las etapas en el desarrollo del presente trabajo.

Por último, cabe destacar que, no solo se han cumplido satisfactoriamente las metas planteadas en el anteproyecto, si no, que se han superado las expectativas iniciales y se han agregado más funcionalidades obteniendo un mejor resultado del que se esperaba inicialmente por parte de ambos estudiantes.

5.2 Conclusiones personales

En la actualidad existe bastante información sobre los riesgos de seguridad de la información que pueden afectar a una empresa y a su continuidad de negocio. Al estudiar y analizar un escenario real de una PYME, como lo ha sido Congelados Madrid, está claro que aún no se están tomando las medidas necesarias para minimizar los riesgos.

Hoy en día, todavía existen muchas empresas que no tienen definidas políticas y procedimientos de seguridad para minimizar los riesgos a los que se ven expuestos la información. Por ejemplo, en este caso hemos podido validar que no existe ninguna política y procedimiento de seguridad entregado al personal, lo que provoca que la empresa esté expuesta a todo tipo de amenazas que pueden explotar vulnerabilidades por culpa de la incorrecta interacción humana con los equipos informáticos.

Conociendo los activos e informándonos sobre las actividades y tareas que nos explican los responsables de departamentos existen diferentes técnicas y herramientas para detectar las vulnerabilidades en un entorno informático y las medidas a aplicar para mitigarlas. Tras aplicar nuestro SGSI apoyado en el estándar ISO/IEC 27001 y con el desarrollo de una herramienta de

red para escaneo de activos, puertos y servicios hemos podido conocer la situación real de la empresa en el ámbito de gestión de seguridad.

Por último, ambos integrantes queremos destacar como los conocimientos adquiridos durante el desarrollo del master, tanto del gobierno y gestión de la información como de las salvaguardas para gestionar el riesgo, nos han sido de gran utilidad para realizar exitosamente el presente trabajo. Esperamos continuar aprendiendo y poder aplicar nuestros conocimientos en más escenarios reales.

Capítulo 6. FUTURAS LÍNEAS DE TRABAJO

El primer paso a seguir tras acabar el presente trabajo sería implementar en la empresa las diversas políticas y procedimientos desarrollados para mitigar los riesgos detectados.

A continuación buscaríamos evaluar la introducción de salvaguardas adicionales y estructurar el proceso de gestión del riesgo.

Tras implementar las políticas y procedimientos y evaluar las introducción de nuevas salvaguardas se debería definir un plan de mejora continua del Sistema de Gestión de Seguridad de la Información para mitigar, eliminar o aceptar las no conformidades identificadas. Para este plan de mejora continua la empresa deberá tener en cuenta los recursos necesarios con los que cuenta y realizar las acciones correctivas correspondientes para mitigar el riesgo de forma efectiva.

En la fase de mejora continua se puede utilizar la aplicación desarrollada para detectar posibles vulnerabilidades a raíz de tener sistemas operativos obsoletos, puertos abiertos o servicios innecesarios en ejecución.

Finalmente queremos destacar la importancia de que, en general, se tomen todas las medidas necesarias que garanticen la continuidad del negocio.

Capítulo 7. BIBLIOGRAFÍA

CTN 71 Tecnología de la Información. (2017, mayo). *UNE-EN ISO/IEC 27002*. UNE.

Cybersecurity Framework. (2022, 19 julio). NIST. https://www.nist.gov/cyberframework

de Luz, S. (2022, 5 mayo). *Realiza escaneos de puertos con Nmap a cualquier servidor o sistema*. RedesZone. https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

E. (2019, 14 noviembre). *Listado de amenazas y vulnerabilidades en ISO 27001*. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

EditorR. (2019, 25 enero). *¿Cómo llevar a cabo la mejora continua del SGSI?* Software ISO. https://www.isotools.org/2019/01/24/como-llevar-a-cabo-la-mejora-continua-del-sgsi/#:%7E:text=El%20principal%20elemento%20del%20proceso,dichas%20acciones%20correctivas%20sean%20efectivas .

G.E. (2012, octubre). *PAe - Magerit V3*. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. https://administracionelectronica.gob.es/general/error.htm;jsessionid=0834879DC860C000CBE5EB1DCE83D1EA.node2_paeaplic

ISO/IEC. (2018, febrero). *ISO/IEC 27000*. https://www.iso.org

ISO/IEC. (2018, febrero). *ISO/IEC 27001*. https://www.iso.org

Lara, D. R. (2020, 19 octubre). *Diferencias entre amenazas y vulnerabilidades*. OpenWebinars.net. https://openwebinars.net/blog/diferencias-entre-amenazas-y-vulnerabilidades/#:%7E:text=Qu%C3%A9%20es%20una%20vulnerabilidad%20y%20qu%C3%A9%20es%20una%20amenaza&text=Estos%20agujeros%20pueden%20tener%20distintos,de%20un%20sistema%20de%20informaci%C3%B3n

M. (2022, 18 enero). *Análisis de Modos de Fallas y Efectos (FMEA)*. Blogdelacalidad. https://blogdelacalidad.com/analisis-de-modos-de-fallas-y-efectos-fmea/#:%7E:text=El%20an%C3%A1lisis%20de%20modos%20de,utilizaran%20para%20inhibir%20las%20fallas.

Subdirección General de Información, Documentación y Publicaciones (Jesús González Barroso). (2012, octubre). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (Libro I). https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YtP-UnZBxhE

Unir, V. (2020, 28 septiembre). *¿Qué es la certificación ISO 27001 y para qué sirve?* UNIR. https://www.unir.net/ingenieria/revista/iso-27001/

Warden, J. G. (2019, 4 diciembre). *Riesgos en el desarrollo de aplicaciones web y móviles*. Desafío Latam. https://blog.desafiolatam.com/riesgos-en-app-web-y-moviles/

Capítulo 8. ANEXOS

8.1 Declaración de la política General de Congelados Madrid

Tenemos como como política general en Congelados Madrid la prioridad de vender y distribuir productos congelados de alta calidad, por lo que todos nuestros proveedores, personal interno (administrativo o de logística) y empleados deben respetar, seguir y atender todas las acciones necesarias para que todos nuestros clientes sean beneficiados en todas nuestras transacciones comerciales con una amplia gama de alimentación congelada en perfecto estado de calidad.

Nuestra alta dirección vela por nuestra prioridad principal a través de herramientas de evaluación continua y atendiendo a todas las incidencias que puedan afectar de forma directa o indirecta los procesos de congelación y distribución de los alimentos congelados. Existen además políticas generales que garantizan el tratamiento y funcionamiento de los equipos dentro de las instalaciones de los cuales depende mantener a temperaturas optimas.

Para lograr una máxima competitividad ofrecemos precios comprensibles que acompañen a la calidad de nuestros productos para que sean lo suficientemente atractivos para captar a nuevos clientes y para mantener a aquellos que en la actualidad ya pertenecen a nuestra red de distribución.

Nuestro ambiente laboral facilita a todos los trabajadores cordialidad, seguridad y apoyo en todas sus labores cotidianas. Es fundamental para Congelados Madrid que todo el personal interno desarrolle sus actividades en un ambiente de armonía y colaboración. Sumando a lo anterior, es importante fomentar el incentivo laboral a través de beneficio s que acompañen al esfuerzo individual o colectivo dentro de cada área de trabajo.

Seguir el crecimiento continuo, establecer una visión de futuro basada en la inversión de los beneficios para que aporten crecimiento y expansión de las operaciones, que esto nos permita llegar a un entorno geográfico mayor a la vez que se puede contratar y dar oportunidades de trabajo a una cantidad mayor de personas.

En ningún momento se tolerarán las malas prácticas humanas comerciales, laborales o económicas que atenten contra los reglamentos y leyes establecidas interna o externamente y se tomaran las medidas necesarias y aplicaran según la normativa y procedimientos del ente encargado de evaluarlas o sancionarlas.

La dirección de la empresa declara la importancia de la seguridad de la información y dicta que todo el personal de la empresa debe cumplir con las normas y políticas.

8.2 Manual de instalación de la aplicación desarrollada para la identificación de los activos que existen en la red, sistemas operativos que utilizan, puertos abiertos y servicios en ejecución más comunes

El Manual de Instalación tiene como objetivo servir de guía en la instalación del sistema.

Para ello, en primer lugar, deberá especificar los requerimientos hardware y software necesarios para el correcto funcionamiento del sistema y posteriormente describir cada uno de los pasos necesarios para la configuración, compilación e instalación del sistema.

8.2.1 Recursos Hardware

A continuación, enumeramos una serie de valores mínimos y recomendados que deberá tener tu equipo, con el fin de poder hacer la instalación y ejecución del sistema correctamente.

Componente	Valor mínimo	Valor recomendado
Procesador	32-bit	64-bit
Memoria RAM	8GB	8GB
Tamaño almacenamiento	128GB	512GB

Tabla 10: Manual de instalación - Recursos hardware: Elaboración propia

8.2.2 Recursos Software

8.2.2.1 Restricciones técnicas del sistema de desarrollo

Elemento	Descripción
Sistema operativo	La programación del servicio web está disponible únicamente para dispositivos con sistema operativo Windows.
Compilador	Sirve cualquier IDE (entorno de desarrollo integrado) para la página web. Recomendamos PhpStorm o Visual Studio Code. Para el desarrollo del servicio web es necesario Visual Studio 2019

Ilustración 9: Manual de instalación - Restricciones técnicas del sistema en desarrollo: Elaboración propia

8.2.2.2 Restricciones técnicas del sistema de producción

Elemento	Descripción
Sistema operativo	Disponible para cualquier tipo de SO, Windows, MacOS y Linux.
Compilador	Para hospedar el programa en una máquina con sistema operativo Windows es necesario tener instalado IIS. Para hospedar el programa en una máquina con sistema operativo Linux es necesario realizarlo con Nginx.

Tabla 11: Manual de instalación - Restricciones técnicas del sistema de producción: Elaboración propia

8.2.3 Descarga del del prototipo

Paso	Descripción
Paso 1	Acceder al siguiente enlace: https://github.com/Jazminpm/analisisVulnerabilidadesTFM
Paso 2	Pulsar en el siguiente botón de “Code” de color verde.
Paso 3	Seleccionar la opción “Download Zip”.
Paso 4	Descomprimir la carpeta en la ruta seleccionada.

Tabla 12: Manual de instalación - descarga del prototipo: Elaboración propia

8.2.4 Configurar el entorno y el espacio de desarrollo locales

Paso	Descripción
Paso 1	Abrir entorno de desarrollo de la carpeta “BackVulnerabilidades” con Visual Studio.
Paso 2	Abrir Visual Studio 2019 e instalar: • Desarrollo de ASP.NET y Web. • Desarrollo de Node.js .
Paso 3	Abrir el entorno de desarrollo de la carpeta “FrontVulnerabilidades”.
Paso 4	Escribir en el terminal el comando: *npm install.*

Tabla 13:Manual de instalación - Configurar el entorno y el espacio de desarrollo locales: Elaboración propia

8.2.5 Compilación de la aplicación

8.2.5.1 Compilación de la aplicación web

Paso	Descripción
Paso 1	Abrir entorno de desarrollo de la carpeta “BackVulnerabilidades” con Visual Studio.
Paso 2	Ejecutar la aplicación con IIS Express.
Paso 3	Abrir el entorno de desarrollo de la carpeta “front-angular”.
Paso 4	Escribir en el terminal el comando: npm start.

Tabla 14: Manual de instalación: Compilación de la aplicación web

8.3 Manual de usuario

8.3.1 Manual de usuario del servicio web

Se ha desarrollado con Swagger la documentación de las diferentes llamadas a la API que realiza el sistema. Esto se ha realizado con la finalidad de que cualquier desarrollador pueda utilizar el servicio web para su propia finalidad sin la necesidad de utilizar la aplicación web desarrollada.

Para acceder a la documentación debemos de ejecutar el programa y realizar lo siguiente:

- Desarrollo local: Acceder a la siguiente url:
  http://localhost/BackVulnerabilidades/swagger/index.html
- Aplicación publicada: Acceder a el dominio o dirección IP donde se esté ejecutando la aplicación y añadir /swagger/index.html.
  Error! Hyperlink reference not valid.

Una vez abierto el buscador web nos encontramos la siguiente pestaña:

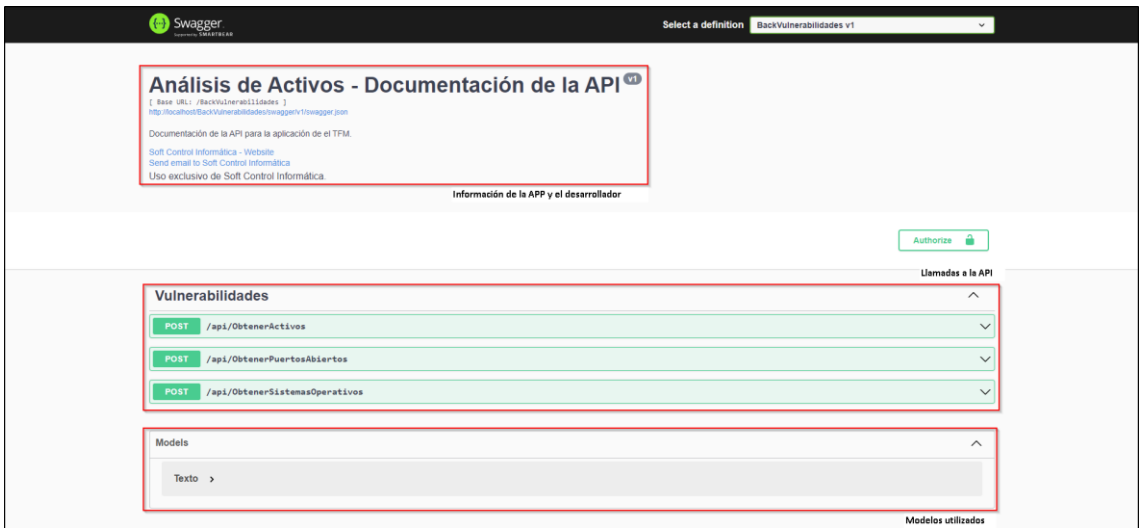


Ilustración 10: Manual de la documentación de la API - Panel inicial: Elaboración propia

En la parte superior de la pantalla anterior podemos visualizar:

1. La información de la aplicación y el desarrollador
2. Una serie de peticiones POST para obtener la información deseada.
3. Los modelos utilizados en las peticiones.

Si abrimos cualquiera de las peticiones POST disponibles veremos que se nos solicita un rango de direcciones IPS e indica el tipo de respuesta que puede dar la petición (200 → respuesta correcta, 400 → Modelo introducido inválido, 500 →Error interno del servidor).

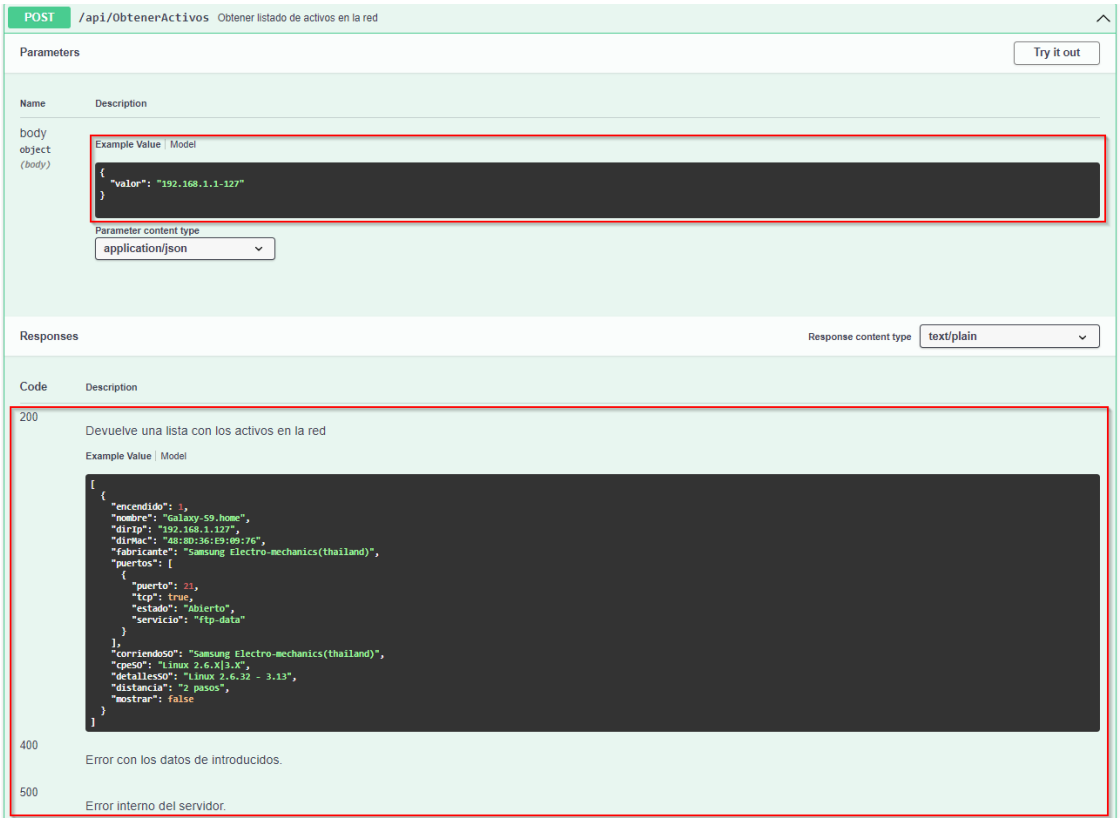


Ilustración 11: Manual de la documentación de la API –Petición POST: Elaboración propia

Para probar la petición POST debemos:

1. Pulsar encima de la petición que deseemos ejecutar.

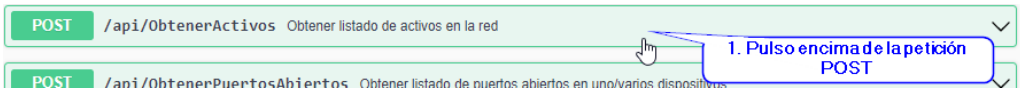


Ilustración 12: Manual de la documentación de la API– Ejemplo petición POST 1: Elaboración propia

2. Pulsar el botón “Try it Out”

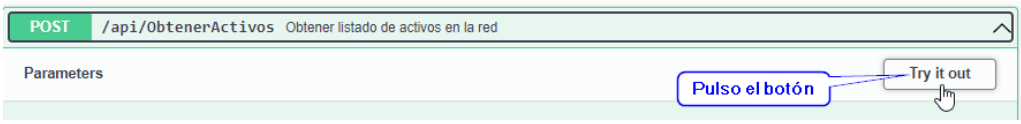


Ilustración 13: Manual de la documentación de la API – Ejemplo petición POST 2: Elaboración propia

3. Indicar el rango de direcciones IPS.

Ilustración 14: Manual de la documentación de la API – Ejemplo petición POST 3: Elaboración propia

4. Pulsar el botón "Execute".

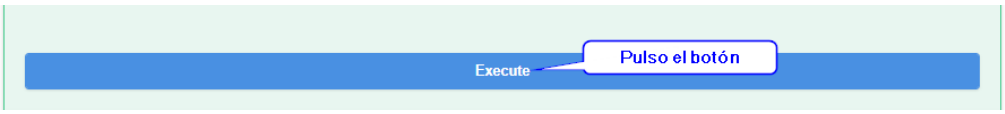


Ilustración 15: Manual de la documentación de la API – Ejemplo petición POST 4: Elaboración propia

Una vez ejecutada la petición obtenemos la respuesta en formato JSON.

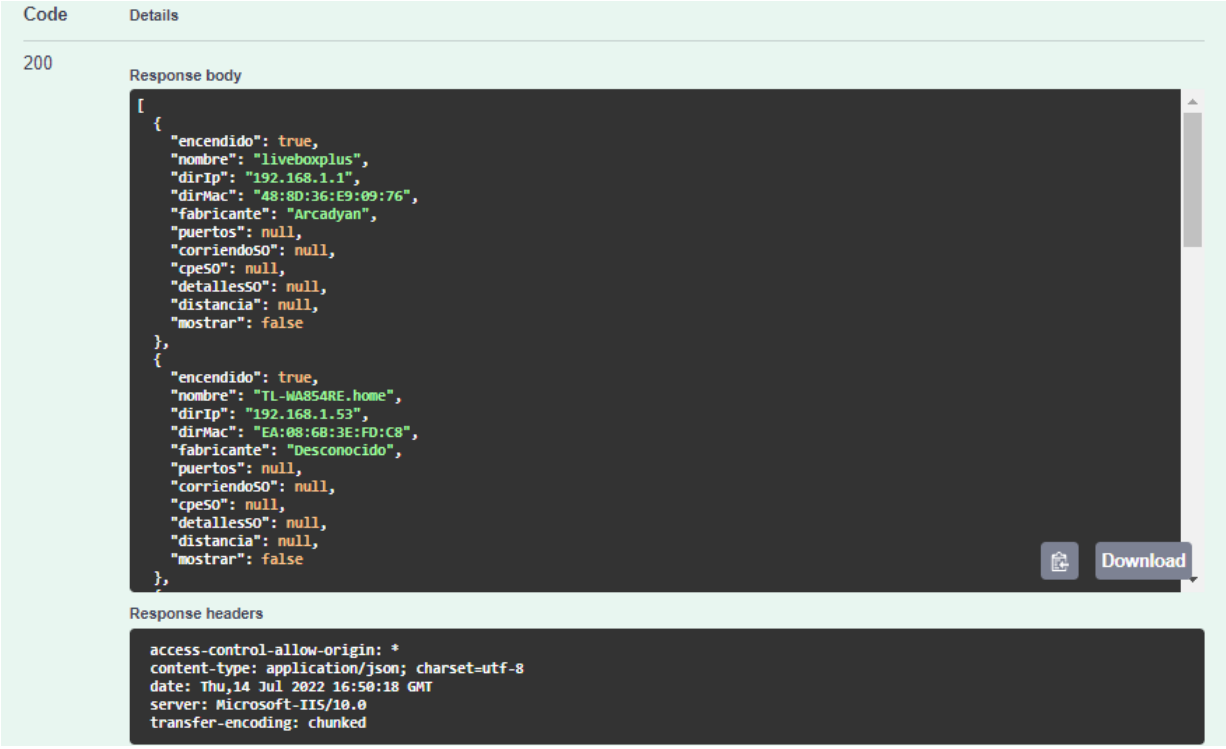


Ilustración 16: Manual de la documentación de la API – Ejemplo petición correcta: Elaboración propia

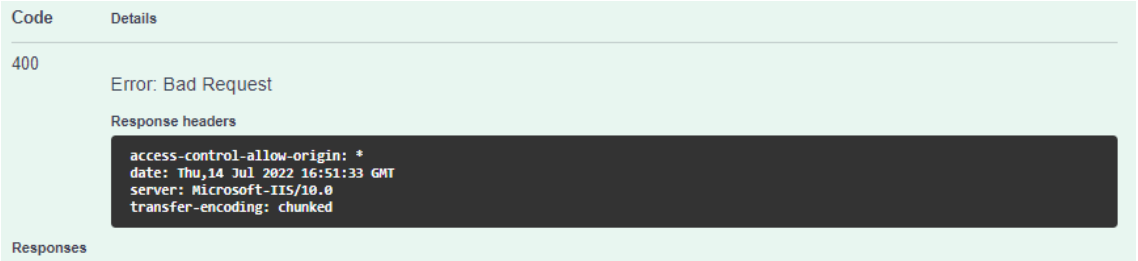


Ilustración 17: Manual de la documentación de la API – Ejemplo petición incorrecta: Elaboración propia

8.3.2 Manual de usuario de la aplicación

El presente manual está organizado de acuerdo con la secuencia de ingreso a las pantallas del sistema.

Para hacer el manual se ha optado por el uso de una pantalla de ordenador. De esta forma se va a poder mostrar con claridad los diferentes procesos que se van a ir ejecutando.

8.3.3 Menú inicial

Desde el menú inicial el usuario se podrá mover entre las tres posibles funcionalidades que ofrece el sistema. Siendo estas:

- Listado de activos: muestra el conjunto de activos conectados a una red.
- Listado de puertos: muestra el estado de los puertos más comunes dentro de cada dispositivo.
- Listado del sistema operativo: muestra información más detallada del sistema operativo y la distancia a la que se encuentra cada dispositivo buscado.

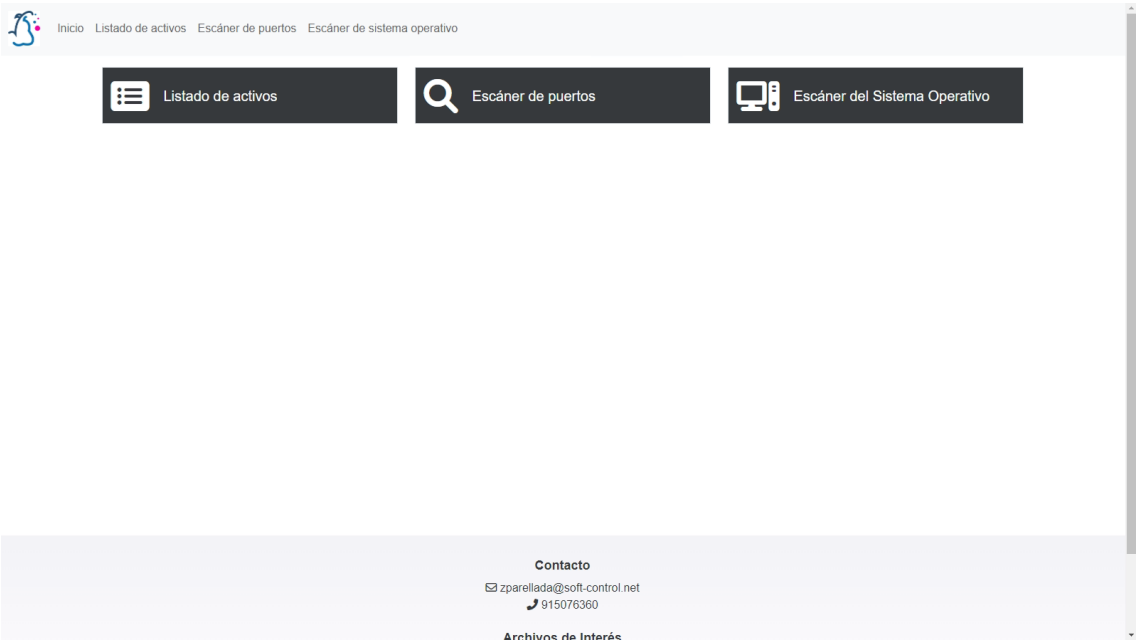


Ilustración 18: Menú de usuario - Panel inicial: Elaboración propia

8.3.4 Listado de activos

En esta pestaña se muestra el conjunto de activos conectados a una red.

Inicialmente la pestaña muestra un mensaje donde indica que es necesario indicar el rango de IPS internas para realizar la búsqueda.

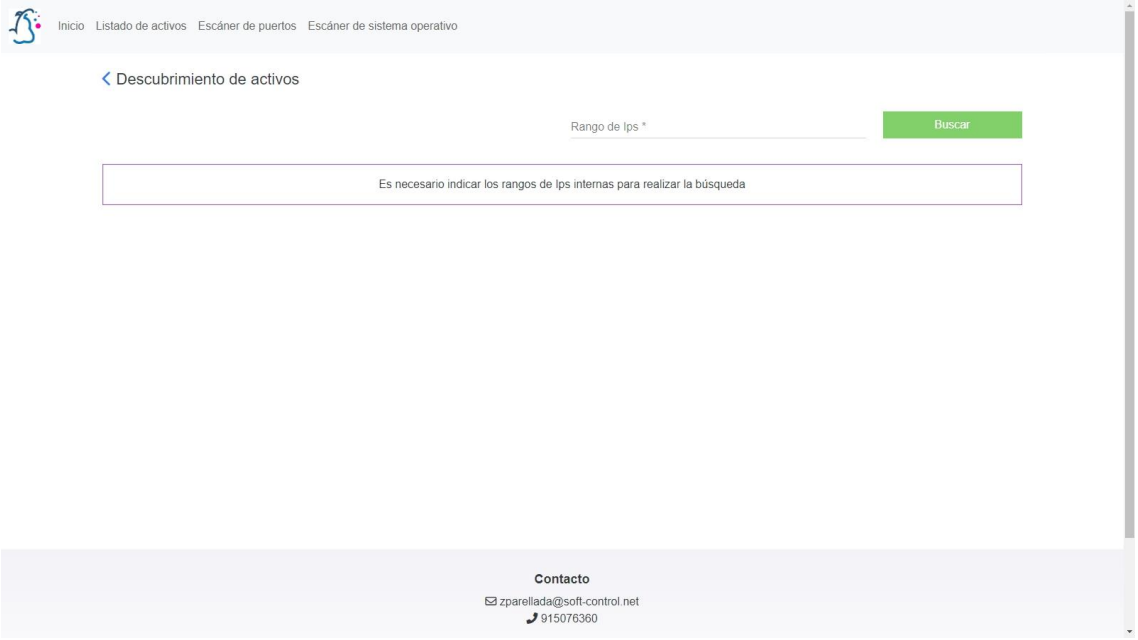


Ilustración 19: Menú de usuario – Panel inicial del listado de activos: Elaboración propia

Para evitar ataques de Command Injection se comprueba tanto en la parte visual cómo en el servicio web que los datos introducidos por el usuario sean válidos, es decir, debe introducir un rango de IPS con el siguiente formato: 192.168.1.1-255.

Ilustración 20: Menú de usuario - Formato incorrecto de búsqueda: Elaboración propia

Ilustración 21: Menú de usuario - Formato correcto de búsqueda: Elaboración propia

Una vez introducido el rango de IPS correctos procedemos a pulsar el botón de “Buscar” para que el programa nos liste los activos comprendidos dentro de nuestra búsqueda.

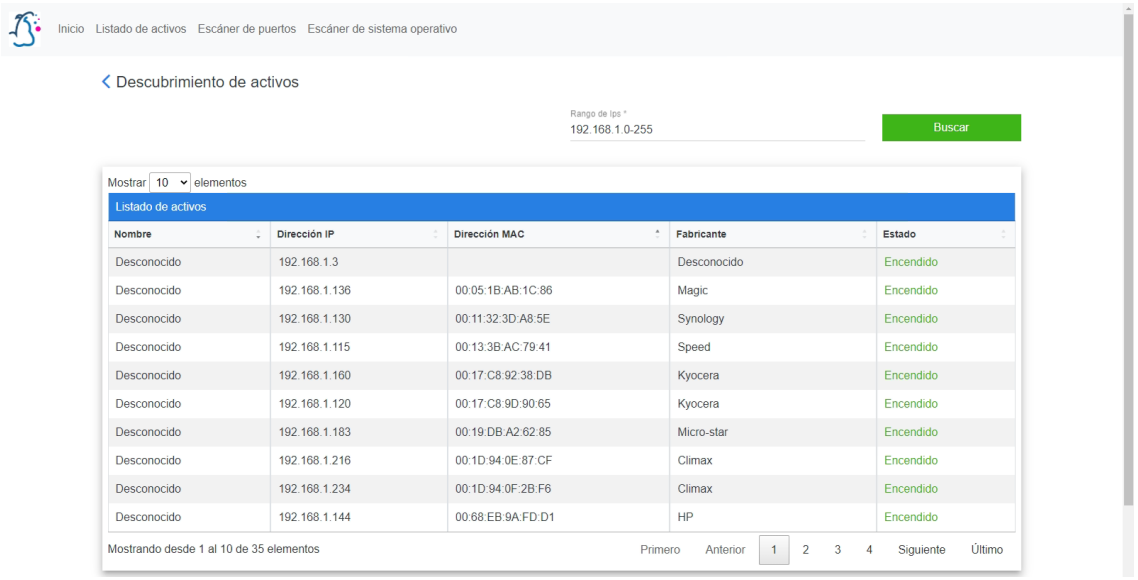


Ilustración 22: Menú de usuario – Listado de activos: Elaboración propia

Una vez listado los activos podemos ver en formato tabla la información detallada (nombre, dirección IP, dirección MAC, fabricante y estado) de cada uno.

En caso de abrir esta pestaña con un dispositivo móvil para ver toda la información detallada del activo se deberá pulsar encima del mismo.

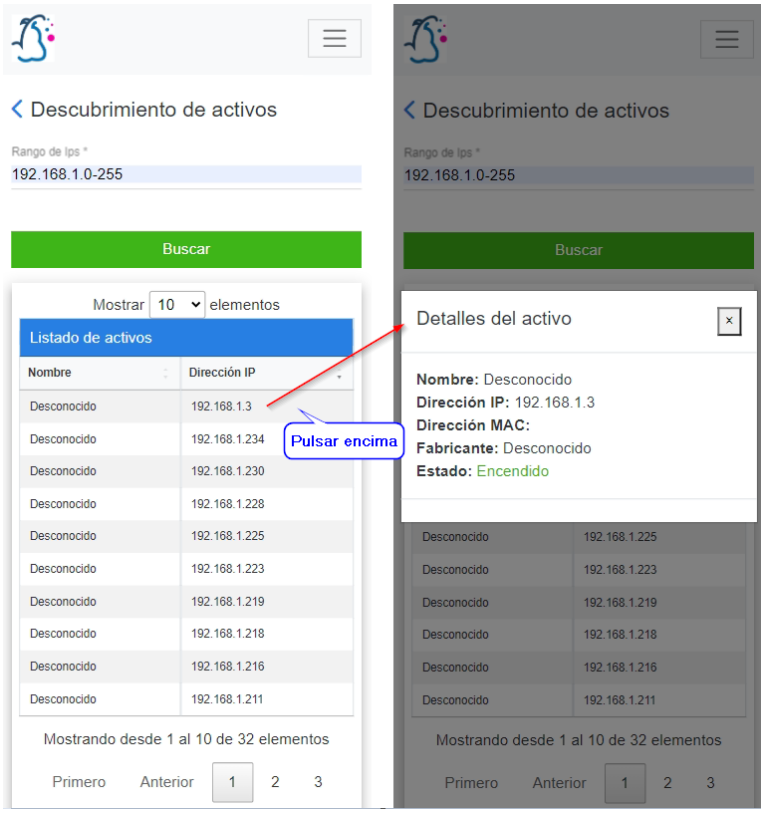


Ilustración 23: Menú de usuario - Información detallada de un activo en vista móvil: Elaboración propia

8.3.5 Listado de puertos

En esta pestaña se muestra el estado de los puertos más comunes de cada dispositivo conectado a una red.

Al igual que en la pestaña anterior, inicialmente se muestra un mensaje donde indica que es necesario indicar el rango de IPS internas para realizar la búsqueda.

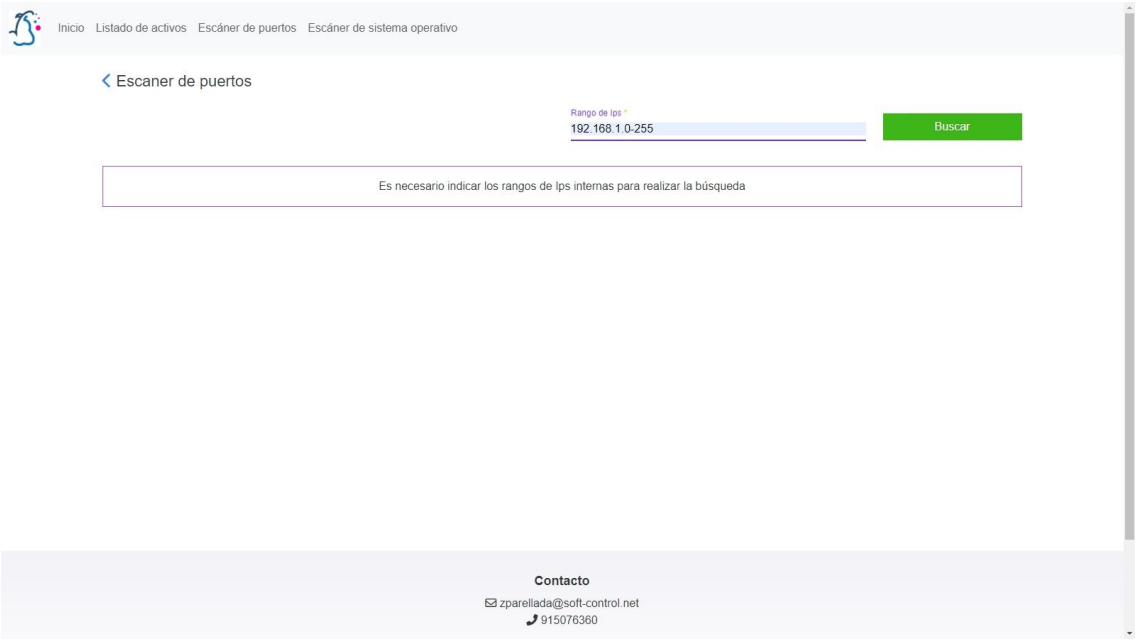


Ilustración 24: Menú de usuario – Panel inicial del listado de puertos: Elaboración propia

Para evitar ataques de Command Injection se comprueba tanto en la parte visual cómo en el servicio web que los datos introducidos por el usuario sean válidos, es decir, debe introducir un rango de IPS con el siguiente formato: 192.168.1.1-255.

Ilustración 25: Menú de usuario - Formato correcto de búsqueda: Elaboración propia

Una vez introducido el rango de IPS correctos procedemos a pulsar el botón de “Buscar” para que el programa nos liste el estado de los puerto de cada activo comprendido dentro de nuestra búsqueda.

Tras pulsar el botón de “Buscar” nos saldrá una lista de direcciones IPS que coincidirá con los dispositivos encontrados en nuestra red.

Ilustración 26:: Menú de usuario – Listado de dispositivos detectados en el escáner de puertos: Elaboración propia

Para ver información detallada de cualquier activo debemos pulsar encima del mismo y nos listará el estado (abierto, cerrado, filtrado, sin filtrar, abierto/filtrado y cerrado/filtrado) de todos los puertos.

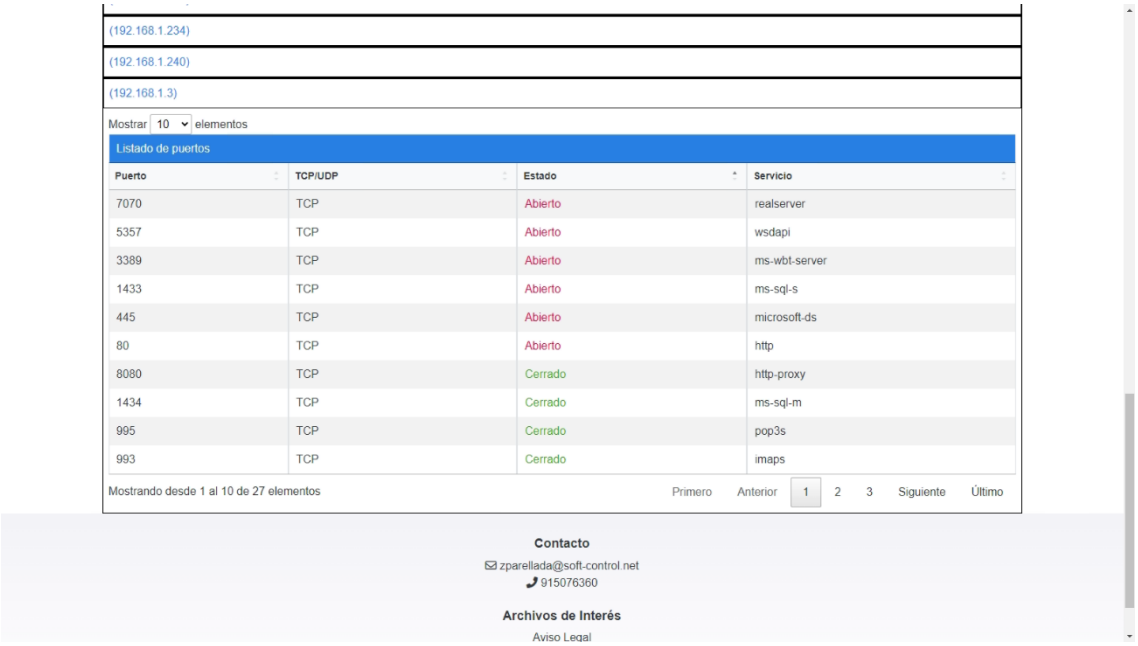


Ilustración 27: Menú de usuario - Listado de puertos de un dispositivo: Elaboración propia

En el caso de que todos los puertos del dispositivo estén cerrados se nos mostrará lo siguiente:

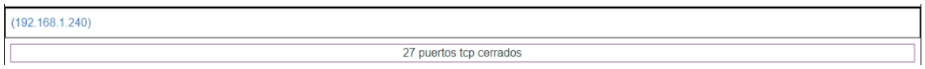


Ilustración 28: Menú de usuario - Todos los puertos de un dispositivo cerrados: Elaboración propia

8.3.6 Listado de Sistemas operativos

En esta pestaña se muestra información detallada de un dispositivo () y el estado de sus puertos. Es importante destacar que realizar esta búsqueda consume bastantes recursos y por ello es recomendable hacerlo cuando exista poco volumen de trabajo.

Al igual que en la pestaña anterior, inicialmente se muestra un mensaje donde indica que es necesario indicar el rango de IPS internas para realizar la búsqueda.

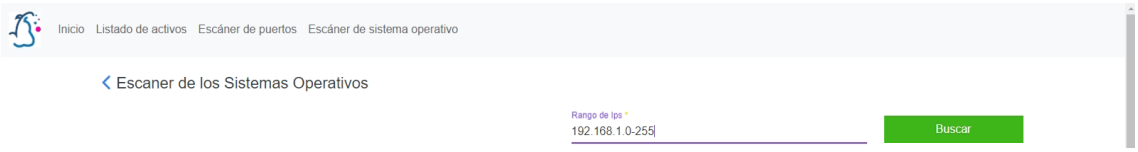


Ilustración 29: Menú de usuario - Formato correcto de búsqueda: Elaboración propia

Una vez introducido el rango de IPS correctos procedemos a pulsar el botón de “Buscar” para que el programa nos liste el estado de los puerto de cada activo comprendido dentro de nuestra búsqueda.

Tras pulsar el botón de “Buscar” nos saldrá una lista de direcciones IPS junto a su sistema operativo que coincidirá con los dispositivos encontrados en nuestra red.

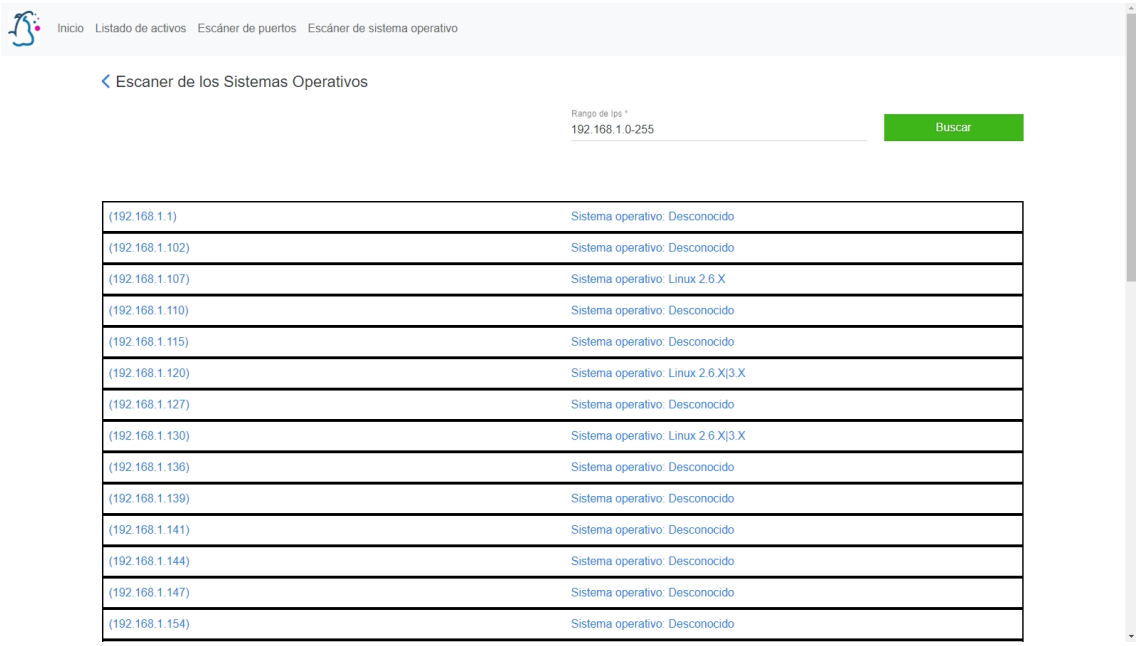
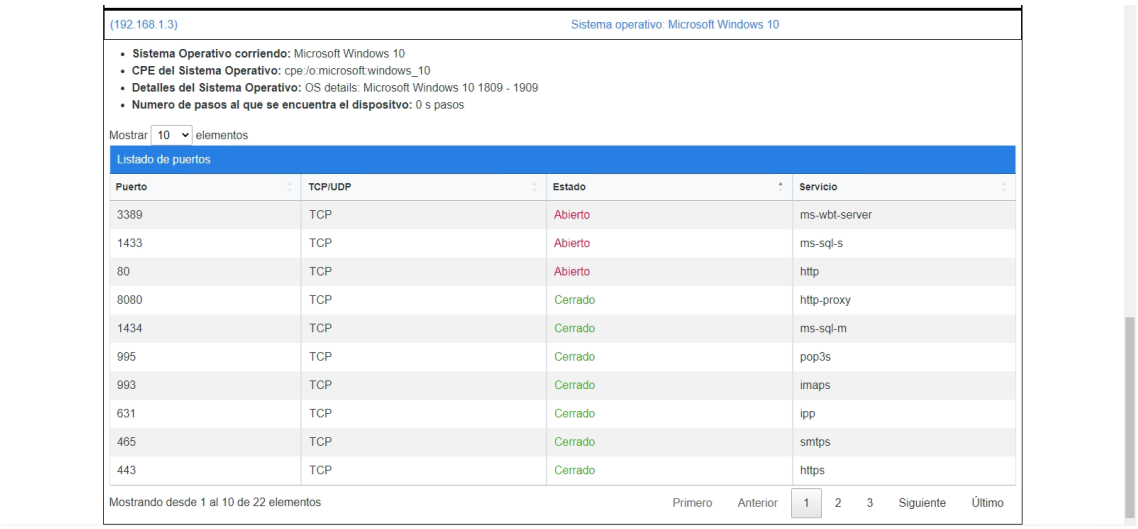


Ilustración 30: Menú de usuario – Listado de dispositivos detectados en el escáner de Sistemas Operativos: Elaboración propia

Para ver información detallada de cualquier activo debemos pulsar encima del mismo y nos listará el sistema operativo que está corriendo, el CPE del Sistema Operativo, los detalles del sistema operativo, la distancia a la que se encuentra el activo del dispositivo que ha ejecutado el escáner y el estado (abierto, cerrado, filtrado, sin filtrar, abierto/filtrado y cerrado/filtrado) de todos los puertos.



(192.168.1.3) Sistema operativo: Microsoft Windows 10

- **Sistema Operativo corriendo:** Microsoft Windows 10
- **CPE del Sistema Operativo:** cpe:/o:microsoft:windows_10
- **Detalles del Sistema Operativo:** OS details: Microsoft Windows 10 1809 - 1909
- **Numero de pasos al que se encuentra el dispositvo:** 0 s pasos

Mostrar 10 elementos

Listado de puertos

Puerto	TCP/UDP	Estado	Servicio
3389	TCP	Abierto	ms-wbt-server
1433	TCP	Abierto	ms-sql-s
80	TCP	Abierto	http
8080	TCP	Cerrado	http-proxy
1434	TCP	Cerrado	ms-sql-m
995	TCP	Cerrado	pop3s
993	TCP	Cerrado	imaps
631	TCP	Cerrado	ipp
465	TCP	Cerrado	smtps
443	TCP	Cerrado	https

Mostrando desde 1 al 10 de 22 elementos — Primero Anterior 1 2 3 Siguiente Último

Ilustración 31: Menú de usuario - Información detallada de cada activo: Elaboración propia

8.4 Resultados obtenidos de la búsqueda de activos

Se ha ejecutado la aplicación en el Servidor de Aplicaciones (FrontEnd) del cliente y se han obtenido los siguientes resultados tras realizar la búsqueda de los dispositivos conectados según el rango de IPs: 192.168.1.1-255.

Mostrar 10 elementos

Listado de activos

Nombre	Dirección IP	Dirección MAC	Fabricante	Estado
Desconocido	192.168.1.3		Desconocido	Encendido
Desconocido	192.168.1.136	00:05:1B:AB:1C:86	Magic	Encendido
Desconocido	192.168.1.130	00:11:32:3D:A8:5E	Synology	Encendido
Desconocido	192.168.1.115	00:13:3B:AC:79:41	Speed	Encendido
Desconocido	192.168.1.160	00:17:C8:92:38:DB	Kyocera	Encendido
Desconocido	192.168.1.120	00:17:C8:9D:90:65	Kyocera	Encendido
Desconocido	192.168.1.183	00:19:DB:A2:62:85	Micro-star	Encendido
Desconocido	192.168.1.216	00:1D:94:0E:87:CF	Climax	Encendido
Desconocido	192.168.1.234	00:1D:94:0F:2B:F6	Climax	Encendido
Desconocido	192.168.1.144	00:68:EB:9A:FD:D1	HP	Encendido

Mostrando desde 1 al 10 de 35 elementos — Primero Anterior 1 2 3 4 Siguiente Último

Tabla 15: Dispositivos encontrados en la búsqueda de activos: Elaboración propi

Mostrar 10 elementos

Listado de activos

Nombre	Dirección IP	Dirección MAC	Fabricante	Estado
Desconocido	192.168.1.211	06:3D:41:AE:0C:60	Desconocido	Encendido
Desconocido	192.168.1.102	08:55:31:86:A4:C2	Routerboard.com	Encendido
Desconocido	192.168.1.141	1C:66:6D:93:CC:29	Hon	Encendido
Desconocido	192.168.1.225	3C:D9:2B:5F:57:AD	Hewlett	Encendido
Desconocido	192.168.1.167	40:8D:5C:10:65:60	Giga-byte	Encendido
Desconocido	192.168.1.184	40:8D:5C:1B:AC:A8	Giga-byte	Encendido
Desconocido	192.168.1.204	40:8D:5C:B3:41:9F	Giga-byte	Encendido
Desconocido	192.168.1.127	4C:CC:6A:E3:A1:53	Micro-star	Encendido
Desconocido	192.168.1.228	54:E1:40:51:1E:6A	Ingenico	Encendido
Desconocido	192.168.1.161	72:0B:47:25:00:EB	Desconocido	Encendido

Mostrando desde 11 al 20 de 35 elementos Primero Anterior 1 2 3 4 Siguiente Último

Tabla 16: Dispositivos encontrados en la búsqueda de activos: Elaboración propia

Mostrar 10 elementos

Listado de activos

Nombre	Dirección IP	Dirección MAC	Fabricante	Estado
Desconocido	192.168.1.154	74:D4:35:DC:71:31	Giga-byte	Encendido
Desconocido	192.168.1.218	74:D4:35:DC:71:73	Giga-byte	Encendido
Desconocido	192.168.1.147	74:D4:35:DC:71:CB	Giga-byte	Encendido
Desconocido	192.168.1.110	74:D4:35:DC:71:CC	Giga-byte	Encendido
Desconocido	192.168.1.209	74:D4:35:DC:71:CE	Giga-byte	Encendido
Desconocido	192.168.1.223	74:D4:35:EF:91:1D	Giga-byte	Encendido
Desconocido	192.168.1.139	7A:49:49:6D:3B:29	Desconocido	Encendido
Desconocido	192.168.1.230	80:C1:6E:ED:19:AC	Hewlett	Encendido
Desconocido	192.168.1.195	84:25:19:94:60:C2	Samsung	Encendido
Desconocido	192.168.1.201	9C:2E:A1:22:C6:B5	Xiaomi	Encendido

Mostrando desde 21 al 30 de 35 elementos Primero Anterior 1 2 3 4 Siguiente Último

Tabla 17: Dispositivos encontrados en la búsqueda de activos: Elaboración propia

Mostrar 10 elementos

Listado de activos

Nombre	Dirección IP	Dirección MAC	Fabricante	Estado
Desconocido	192.168.1.166	AA:63:58:53:0E:71	Desconocido	Encendido
Desconocido	192.168.1.1	C4:FF:1F:75:55:82	Huawei	Encendido
Desconocido	192.168.1.219	C8:5A:CF:AC:DC:06	Desconocido	Encendido
Desconocido	192.168.1.107	E4:AB:89:10:21:15	MitraStar	Encendido
Desconocido	192.168.1.174	F0:79:59:81:3A:CF	Asustek	Encendido

Mostrando desde 31 al 35 de 35 elementos Primero Anterior 1 2 3 4 Siguiente Último

Tabla 18: Dispositivos encontrados en la búsqueda de activos: Elaboración propia

8.5 Valoración de los activos utilizando la metodología MAGERIT

8.5.1 ¿Cómo valoramos los activos?

Para valorar el activo tomamos el dato más alto de los valores de autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad. Esto se ha decidido debido a que consideramos que es una forma de tener en cuenta todos aquellos valores críticos en activos en los que además existen valoraciones bajas.

La valoración de la información se ha realizado utilizando los valores numéricos (del 1 al 5) de la siguiente tabla ACIDA:

Nivel	Autenticidad Garantía de la identidad de los datos		Confidencialidad Grado de restricción en cuanto al acceso y la divulgación		Integridad Grado de veracidad, consistencia y fiabilidad de la información		Disponibilidad Necesidad de tener la información siempre lista para su uso		Auditabilidad Registro de las acciones u operaciones del usuario	
	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto
1	**ANÓNIMA: Información que no requiere conocer el origen/autor, ni el responsable de esta.**	Ningún efecto	**PÚBLICA: Información sin restricciones en su difusión.**	No existe impacto.	**BAJA: Informacion cuya modificación no implica ningún riesgo y puede realizarla cualquier persona.**	No causa impacto alguno.	**REGENRABLE: Se puede volver a disponer de la información en un periodo inferior a medio mes.**	Afecta mínimamente las actividades de personas concretas.	**LIBRE: No hay necesidad de registrar ninguna acción o evento.**	Efecto nulo.
2	**REMITIDA: Información que requiera conocer los datos del emisor y el origen de esta.**	Pérdidas mínimas de imagen como consecuencia de confiar en un emisor equivocado.	**USO INTERNO: Información que puede ser conocida por cualquier persona de la organización.**	Posible publicidad negativa.	**FIABLE: Información restringida en su actualización a cualquier persona de la organización con acceso permitido.**	Pérdida de imagen.	**RECUPERABLE: La información debe recuperarse en un tiempo inferior a una semana.**	Afecta a las actividades/objetivos de un grupo de personas.	**GENÉRICA: Solo se registran datos de forma genérica.**	Desconocimiento de cuando se realizan modificaciones sobre la información.

Nivel	Autenticidad Garantía de la identidad de los datos		Confidencialidad Grado de restricción en cuanto al acceso y la divulgación		Integridad Grado de veracidad, consistencia y fiabilidad de la información		Disponibilidad Necesidad de tener la información siempre lista para su uso		Auditabilidad Registro de las acciones u operaciones del usuario	
	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto
3	**CONFIRMADA: Información que precise confirmar el origen y el destino, así como la necesidad de verificar la recepción.**	Posibles pérdidas monetarias como consecuencia de enviar información a terceros no contrastados.	**RESTRINGIDA: Información cuyo conocimiento y difusión se debe limitar a un determinado grupo organizativo.**	Publicidad negativa y posible pérdida de clientes.	**GARANTIZADA: Información que exige disponer de medidas que garanticen su veracidad.**	Pérdidas económicas por posible pérdida de clientes.	**NECESARIA: Recuperación de la información en un plazo inferior a tres días.**	Disminución de actividades en algún área.	**PARTICULAR: Se debe registrar a nivel de usuarios las acciones críticas de alta, baja y modificación.**	Incapacidad de persecución de delitos.
4	**CERTIFICADA: Información que requiera certificación por una tercera parte del origen y el destino.**	Pérdidas económicas e implicaciones legales por desconfianza de autor.	**CONFIDENCIAL: Información que debe tener accesos restringidos a un grupo muy reducido y controlado de personas.**	Pérdida económica alta e importantes daños en la imagen y posibles repercusiones legales.	**SENSIBLE: Información que debe tener alto nivel de exactitud.**	Fuertes pérdidas financieras y de clientes.	**CRÍTICA: Recuperación de la información en un plazo inferior de un día.**	Alteración de actividades internas-	**RESTRINGIDA: Se debe registrar a nivel de usuarios las acciones críticas de alta, baja, modificación y lectura.**	Fraude
5	**CRÍTICA: Información que requiera certificación por una tercera parte del origen, del destino, así como el contenido de la**	Graves implicaciones legales y pérdidas económicas.	**SECRETA: Información de suma importancia y de carácter crítico para la organización a la que tendrán**	Graves problemas estratégicos y patrimoniales.	**CRUCIAL: Información de suma importancia desde el punto de vista de la veracidad, coherencia y**	Graves problemas estratégicos y patrimoniales.	**VITAL: La información debe recuperarse inmediatamente.**	Interrupción elevada de actividades del negocio.	**TRAZA TOTAL: Se debe registrar a nivel de usuarios las acciones de alta, baja, modificación, lecturas e**	Incumplimiento de obligaciones legales.

Nivel	Autenticidad Garantía de la identidad de los datos		Confidencialidad Grado de restricción en cuanto al acceso y la divulgación		Integridad Grado de veracidad, consistencia y fiabilidad de la información		Disponibilidad Necesidad de tener la información siempre lista para su uso		Auditabilidad Registro de las acciones u operaciones del usuario	
	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto	Descripción	Impacto
	información enviada.		**acceso personas muy concretas.**		**exactitud para la organización.**				**intentos de lecturas.**	

Tabla 19: Definición de la tabla ACIDA – Elaboración Propia

Cada valor numérico obtenido al final estará comprendido en un número del 1 al 5. Estos números corresponderán con la siguiente escala:

Valor	Valor del activo
1	Insignificante
2	Bajo
3	Medio
4	Alto
5	Muy alto

Tabla 20: Valoración de los activos: Elaboración propia

8.5.2 Valoración de los activos de la empresa

En la siguiente tabla se muestra la valoración de los activos de la empresa siguiendo la estructura de la tabla ACIDA.

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Fichero de importaciones	2	3	4	3	3	**4**	Alto
Fichero con tarifas	2	3	5	3	3	**5**	Muy Alto
Ficheros compartidos	2	2	3	1	2	**3**	Medio
Datos de albaranes	3	4	5	5	3	**5**	Muy Alto
Datos de facturación	3	4	5	5	3	**5**	Muy Alto
Datos de pedidos	2	3	5	5	3	**5**	Muy Alto
Datos de almacenes	2	3	4	4	3	**4**	Alto
Datos de trazabilidad	3	3	5	5	3	**5**	Muy Alto
Datos contables	5	3	5	4	3	**5**	Muy Alto
Datos de productos	2	1	3	4	3	**4**	Alto
Datos de clientes	2	3	4	4	3	**4**	Alto
Datos de empleados	2	4	3	2	3	**4**	Alto
Datos de proveedores	3	3	4	3	3	**4**	Alto
Datos tarifas	3	3	4	4	3	**4**	Alto

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Datos de usuarios del sistema de gestión	2	5	5	5	4	**5**	Muy Alto
Acceso remoto de Windows	2	3	2	4	3	**4**	Alto
Anydesk	2	3	2	2	3	**3**	Medio
Correo electrónico	3	5	3	3	3	**5**	Muy Alto
Almacenamiento de ficheros	2	3	3	3	3	**3**	Medio
Página web de la empresa	3	1	4	3	2	**4**	Alto
Servicio Web	3	3	4	3	3	**4**	Alto
Internet Information Services (IIS)	2	2	2	3	2	**3**	Medio
Sistema de Gestión	2	2	2	5	3	**5**	Muy Alto
Google Chrome	1	1	2	2	2	**2**	Bajo
SQL Server	3	1	4	5	3	**5**	Muy Alto
Office 365	2	1	2	3	2	**3**	Medio
Antivirus	2	2	2	3	3	**3**	Medio
Firewall	2	2	3	3	3	**3**	Medio

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Licencias Windows 7 Pro	1	2	2	2	2	**2**	Bajo
Licencias Windows 8	1	2	2	2	2	**2**	Bajo
Licencias Windows 10 Home	1	2	2	2	2	**2**	Bajo
Licencias Windows 10 Pro	1	2	2	3	2	**3**	Medio
Sistema de BackUp del servidor de aplicaciones	3	5	4	5	3	**5**	Muy Alto
Sistema de BackUp de la base de datos	3	5	4	5	3	**5**	Muy Alto
Servidor de base de datos	3	5	4	5	3	**5**	Muy Alto
Servidor de aplicaciones	3	3	3	5	3	**5**	Muy Alto
Ordenador del departamento de importaciones	2	3	3	5	2	**5**	Muy Alto
Ordenadores del departamento de contabilidad	3	4	4	3	3	**4**	Alto
Portátiles del departamento de Marketing	3	3	3	3	3	**3**	Medio
Portátiles del departamento de ventas	2	3	3	3	3	**3**	Medio

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Ordenadores de los escribientes	2	3	3	3	3	**3**	Medio
Portátil del CEO	2	4	4	3	3	**4**	Alto
Ordenadores de los puestos comerciales	2	3	3	4	3	**4**	Alto
Impresora Samsung	1	1	2	3	2	**3**	Medio
Impresora HP	1	1	2	3	2	**3**	Medio
Impresora HP	1	1	2	3	2	**3**	Medio
Switches	1	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Router Huawei	3	1	4	5	3	**5**	Muy Alto
Wifi	3	3	5	3	2	**5**	Muy Alto
LAN	3	3	2	5	1	**5**	Muy Alto
Memorias USB	1	2	3	1	2	**3**	Medio
Almacenamientos en RED	3	3	3	4	3	**4**	Alto
Material impreso	2	4	4	4	3	**4**	Alto

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Sistema de suministro eléctrico ininterrumpido (UPS)	NO APLICA	NO APLICA	NO APLICA	5	NO APLICA	**5**	Muy Alto
Aire acondicionado (CPD)	NO APLICA	NO APLICA	NO APLICA	2	NO APLICA	**2**	Bajo
Cableado	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Fibra óptica	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Red eléctrica	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Router de Movistar (ISP)	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Puestos comerciales de MercaMadrid	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Nave	NO APLICA	NO APLICA	NO APLICA	5	2	**5**	Muy Alto
CPD	NO APLICA	NO APLICA	NO APLICA	5	3	**5**	Muy Alto
Despacho CEO	NO APLICA	NO APLICA	NO APLICA	3	3	**3**	Medio
Sala Principal	NO APLICA	NO APLICA	NO APLICA	3	2	**3**	Medio
Despacho de Administración	NO APLICA	NO APLICA	NO APLICA	3	2	**3**	Medio
Sala 1	NO APLICA	NO APLICA	NO APLICA	3	2	**3**	Medio
Sala 2	NO APLICA	NO APLICA	NO APLICA	3	2	**3**	Medio

Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	**VALOR**	**Valor del activo**
Personal de Contabilidad	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Empleado de Marketing	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Personal de Ventas	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Escribientes	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Responsable de Cajas	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Empleado de Importaciones	NO APLICA	3	3	1	NO APLICA	**3**	Medio
Clientes de la página WEB	NO APLICA	2	3	1	NO APLICA	**3**	Medio
CEO	NO APLICA	4	3	4	NO APLICA	**4**	Alto
Proveedor del sistema de gestión	NO APLICA	3	4	5	NO APLICA	**5**	Muy Alto

Tabla 21: Valoración de los activos: Elaboración propia

8.6 Valoración del riesgo sin salvaguardas

La siguiente tabla identifica y calcula los diversos riesgos a los que está expuesto cada activo seleccionado, sin tener en cuenta las salvaguardas con las que cuenta actualmente la empresa, en función de la explicación del cálculo del riesgo.

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Datos de albaranes				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	3	15
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	3	15
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de facturación				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	3	15
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	3	15

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de pedidos				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	3	15
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de almacenes				
Errores en mantenimiento	Cambios de versión poco probados	4	4	16
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	3	12
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	3	16
Uso indebido de los sistemas de información	Falta de formación	4	2	8
ACTIVO: Datos de trazabilidad				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	3	15
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos contables				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	3	15
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de productos				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	3	12
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	2	8
Uso indebido de los sistemas de información	Falta de formación	4	2	8

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Datos de clientes				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	2	8
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	2	8
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	1	4
ACTIVO: Datos de proveedores				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	2	8
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	2	8
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	2	8
ACTIVO: Datos de usuarios del sistema de gestión				

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Errores en mantenimiento	Cambios de versión poco probados	5	1	5
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	2	10
Uso indebido de los sistemas de información	Usuarios poco formados	5	2	10
Revelación de información	Falta de formación y conciencia sobre seguridad	5	2	10
ACTIVO: Acceso remoto de Windows				
Acceso a la red o al sistema de información por personas no autorizadas	Contraseñas predeterminadas no modificadas	4	2	8
Acceso a la red o al sistema de información por personas no autorizadas	No existe políticas de contraseñas	4	2	8
Comprometer información confidencial	Clasificación inadecuada de la información	4	2	8
Comprometer información confidencial	Falta de política de acceso remoto	4	2	8
Suplantar la identidad de un usuario	Uso inadecuado de las credenciales de acceso	4	1	4
Fallo de los enlaces de comunicación	Inadecuada gestión de red	4	3	12
Mal funcionamiento del equipo	Uso de equipos con sistemas operativos obsoletos	4	2	8

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Correo electrónico				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	2	10
Revelación de información	Ausencia de políticas de correo electrónico	5	3	15
Revelación de información	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	3	15
Código malicioso	Inadecuada monitorización de los contenidos (enlaces, ficheros adjuntos) de los correos	5	4	20
Código malicioso	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	4	20
Uso indebido del correo electrónico	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	4	20
ACTIVO: Sistema de gestión				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	2	10
Revelación de información	Inadecuada segregación de roles de usuario	5	3	15
Uso indebido de sistemas de información	Falta de formación	5	4	20

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Malversación y fraude	Insuficiente supervisión de la información del sistema de gestión	5	2	10
Malversación y fraude	Inadecuada segregación de roles de usuario	5	2	10
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Interrupción de procesos de negocio	Inadecuada gestión de capacidad del sistema	5	3	15
Errores de software	Pruebas de software insuficientes	5	4	20
ACTIVO: SQL Server				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Acceso por personas no autorizadas.	Inadecuada gestión y protección de contraseñas	5	2	10
Comprometer información confidencial	Inadecuada gestión y protección de contraseñas	5	2	10
Destrucción de registros	Inadecuada segregación de roles de usuario	5	3	15
Revelación de información	Inadecuada segregación de roles de usuario	5	3	15
Errores en mantenimiento	Falta de actualizaciones	5	2	15
Interrupción de procesos de negocio	Falta de redundancia, copia única	5	2	10
ACTIVO: Servidor de base de datos				
Desastre por incendio	Falta de detectores de humo	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Desastre por inundación	Existencia de tuberías de agua en el techo donde se encuentra el equipo	5	1	5
Pérdida de electricidad	Falta de redundancia de servicio eléctrico	5	2	10
Mal funcionamiento del equipo	Inadecuada gestión de capacidad del sistema	5	2	10
Mal funcionamiento del equipo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Falta de redundancia, copia única.	5	3	15
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Router Huawei				
Interrupción de procesos de negocio	Falta de redundancia	5	1	5
Fallo en los enlaces de comunicación	Inadecuada seguridad del cableado	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Wifi				
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
ACTIVO: Almacenamiento en red				

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Interrupción de procesos de negocio	Inadecuada segregación de roles de usuario	4	3	12
Acceso a la red o al sistema de información por personas no autorizadas	Inadecuada segregación de roles de usuario	4	2	8
Comprometer información confidencial	Falta de formación y conciencia sobre seguridad	4	2	8
Código malicioso	Falta de herramientas de seguridad	4	3	12
ACTIVO: Red eléctrica				
Interrupción de procesos de negocio	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Pérdida de electricidad	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Fallo de los enlaces de comunicación	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
ACTIVO: Router de Movistar (ISP)				
Daño causado por un tercero	Inadecuada gestión del sistema	5	1	5
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Puestos comerciales de MercaMadrid				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Desastre generado por causas humanas	Falta de políticas de acceso	5	1	5
Desastre generado por causas humanas	Falta de formación	5	1	5
Acceso físico no autorizado	Protección física no apropiada	5	1	5
ACTIVO: CPD				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	1	5
Desastre generado por causas humanas	Falta de políticas de acceso	5	2	10
Desastre generado por causas humanas	Falta de formación	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10

Tabla 22: Estimación del riesgo sin salvaguardas: Elaboración propia

8.7 Valoración del riesgo con salvaguardas

En la siguiente tabla vemos reflejados de color verde aquellos riesgos que disminuyen al aplicar las salvaguardas que tiene la empresa.

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Datos de albaranes				

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	3	15
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de facturación				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	3	15
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de pedidos				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de almacenes				
Errores en mantenimiento	Cambios de versión poco probados	4	4	16
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	3	12
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Falta de formación	4	2	8
ACTIVO: Datos de trazabilidad				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos contables				
Errores en mantenimiento	Cambios de versión poco probados	5	4	20
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	3	15
Destrucción de registros	No existe política de contraseñas	5	2	10
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	2	10
ACTIVO: Datos de productos				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	3	12
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Falta de formación	4	2	8
ACTIVO: Datos de clientes				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	2	8

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	1	4
ACTIVO: Datos de proveedores				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	2	8
Destrucción de registros	No existe política de contraseñas	4	2	8
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	2	8
ACTIVO: Datos de usuarios del sistema de gestión				
Errores en mantenimiento	Cambios de versión poco probados	5	1	5
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Usuarios poco formados	5	2	10
Revelación de información	Falta de formación y conciencia sobre seguridad	5	2	10
ACTIVO: Acceso remoto de Windows				
Acceso a la red o al sistema de información por personas no autorizadas	Contraseñas predeterminadas no modificadas	4	2	8
Acceso a la red o al sistema de información por personas no autorizadas	No existe políticas de contraseñas	4	2	8
Comprometer información confidencial	Clasificación inadecuada de la información	4	2	8
Comprometer información confidencial	Falta de política de acceso remoto	4	2	8
Suplantar la identidad de un usuario	Uso inadecuado de las credenciales de acceso	4	1	4
Fallo de los enlaces de comunicación	Inadecuada gestión de red	4	3	12
Mal funcionamiento del equipo	Uso de equipos con sistemas operativos obsoletos	4	2	8
ACTIVO: Correo electrónico				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Revelación de información	Ausencia de políticas de correo electrónico	5	3	15
Revelación de información	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	3	15
Código malicioso	Inadecuada monitorización de los contenidos (enlaces, ficheros adjuntos) de los correos	5	1	5
Código malicioso	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	4	20
Uso indebido del correo electrónico	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	4	20
ACTIVO: Sistema de gestión				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	2	10
Revelación de información	Inadecuada segregación de roles de usuario	5	3	15
Uso indebido de sistemas de información	Falta de formación	5	4	20
Malversación y fraude	Insuficiente supervisión de la información del sistema de gestión	5	2	10
Malversación y fraude	Inadecuada segregación de roles de usuario	5	2	10
Errores en mantenimiento	Cambios de versión poco probados	5	4	20

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Interrupción de procesos de negocio	Inadecuada gestión de capacidad del sistema	5	3	15
Errores de software	Pruebas de software insuficientes	5	4	20
ACTIVO: SQL Server				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	2	10
Acceso por personas no autorizadas.	Inadecuada gestión y protección de contraseñas	5	2	10
Comprometer información confidencial	Inadecuada gestión y protección de contraseñas	5	2	10
Destrucción de registros	Inadecuada segregación de roles de usuario	5	3	15
Revelación de información	Inadecuada segregación de roles de usuario	5	3	15
Errores en mantenimiento	Falta de actualizaciones	5	2	15
Interrupción de procesos de negocio	Falta de redundancia, copia única	5	2	10
ACTIVO: Servidor de base de datos				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Existencia de tuberías de agua en el techo donde se encuentra el equipo	5	1	5
Pérdida de electricidad	Falta de redundancia de servicio eléctrico	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Mal funcionamiento del equipo	Inadecuada gestión de capacidad del sistema	5	2	10
Mal funcionamiento del equipo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Falta de redundancia, copia única.	5	3	15
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Router Huawei				
Interrupción de procesos de negocio	Falta de redundancia	5	1	5
Fallo en los enlaces de comunicación	Inadecuada seguridad del cableado	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Wifi				
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
ACTIVO: Almacenamiento en red				
Interrupción de procesos de negocio	Inadecuada segregación de roles de usuario	4	3	12
Acceso a la red o al sistema de información por personas no autorizadas	Inadecuada segregación de roles de usuario	4	2	8

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Comprometer información confidencial	Falta de formación y conciencia sobre seguridad	4	2	8
Código malicioso	Falta de herramientas de seguridad	4	3	12
ACTIVO: Red eléctrica				
Interrupción de procesos de negocio	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Pérdida de electricidad	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Fallo de los enlaces de comunicación	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
ACTIVO: Router de Movistar (ISP)				
Daño causado por un tercero	Inadecuada gestión del sistema	5	1	5
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Puestos comerciales de MercaMadrid				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	2	10
Desastre generado por causas humanas	Falta de políticas de acceso	5	1	5
Desastre generado por causas humanas	Falta de formación	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Acceso físico no autorizado	Protección física no apropiada	5	1	5
ACTIVO: CPD				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	1	5
Desastre generado por causas humanas	Falta de políticas de acceso	5	2	10
Desastre generado por causas humanas	Falta de formación	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10

Tabla 23: Estimación del riesgo con salvaguardas: Elaboración propia

8.8 Políticas de seguridad y procedimientos de seguridad de la información

8.8.1 Política de Seguridad de Acceso a los ordenadores y Servidores

Política: Es de carácter obligatorio que todos los ordenadores y servidores tengan configurada una contraseña por cada usuario que haga uso de estos. Las contraseñas deben cumplir con:

- Un estándar mínimo de contenido y este será que deben tener al menos 8 caracteres alfanuméricos alternando mayúsculas, minúsculas, números y caracteres especiales.
- Deben ser renovadas cada 180 días.

Responsable: El responsable de seguridad.

8.8.2 Política de concienciación y formación del personal

Todo el personal de la empresa que interactúe con los sistemas informáticos debe recibir formación sobre los riesgos y amenazas que representan el uso inadecuado de los ordenadores, además deben de conocer las responsabilidades a asumir en caso de que por un uso inadecuado pueda verse afectado la continuidad del negocio.

La presente política debe de ser entregada en el momento de la contratación del empleado.

Responsable: Por un lado el personal que desarrolla el rol de recursos humanos es el encargado de entregar la política a los empleados y asegurarse de la formación y concienciación de estos. Por otro lado, el responsable de seguridad deberá dictar las pautas y contenidos que serán transmitidos a los empleados.

8.8.3 Procedimiento de pruebas o actualización del software

Los pasos que seguir para realizar las pruebas y actualizaciones de software dentro de la empresa son los siguientes:

1. La empresa se debe asegurar de llevar a cabo las pruebas en un entorno controlado y con un número reducido de ordenadores para que en caso de que una actualización, mejora o prueba falle no se vea afectado el negocio.
2. Tras haber probado el correcto funcionamiento de la actualización, se debe extender de forma escalada a los demás equipos informáticos que lo requieran.
3. En caso de encontrar un problema con la nueva actualización debe existir un punto de restauración (copia de seguridad) del sistema anterior.

Responsable: El responsable de seguridad.

8.8.4 Políticas de segregación de funciones de documentos y aplicaciones compartidos en red

La empresa debe tener definidos los usuarios que pueden acceder, modificar o eliminar los archivos o documentos compartidos en la red según el siguiente procedimiento.

1. El usuario administrador debe ser el único que pueda eliminar documentos o directorios compartidos en la red de la empresa.
2. Se deben dictar los usuarios que puedan modificar los documentos o directorios compartidos en la red de la empresa.
3. Se deben dictar los usuarios que puedan acceder los documentos o directorios compartidos en la red de la empresa.

Responsable: El responsable de seguridad.

8.8.5 Políticas de segregación de funciones orientado al Sistema de Gestión de la empresa

Las funciones que puede llevar a cabo cada usuario del Sistema de Gestión de la empresa deben estar separadas y bien definidas siguiendo la siguiente tabla.

Nombre del activo	Usuarios con acceso
Datos de albaranes	Contabilidad, escribientes, responsable de cajas, prepación de pedidos y calidad.
Datos de facturación	Contabilidad, escribientes, responsable de cajas, prepación de pedidos y calidad.
Datos de pedidos	Contabilidad, escribientes, responsable de cajas, prepación de pedidos y calidad.
Datos de almacenes	Contabilidad, escribientes, responsable de cajas, prepación de pedidos y calidad.
Datos de trazabilidad	Contabilidad, escribientes, responsable de cajas, prepación de pedidos, calidad e importaciones.
Datos contables	Contabilidad.
Datos de productos	Todos los usuarios.
Datos de clientes	Todos los usuarios.
Datos de proveedores	Contabilidad, importaciones y calidad.
Datos tarifas	Contabilidad y ventas.
Datos de usuarios del sistema de gestión	Administrador.

Tabla 24: Segregación de funciones del Sistema de Gestión de la empresa: Elaboración propia

El usuario administrador tendrá acceso a todas las funcionalidades del sistema de gestión.

Responsable: El usuario Administrador del Sistema de Gestión de la empresa.

8.8.6 Políticas de monitorización de los sistemas informáticos

Se debe verificar como mínimo de forma trimestral que los equipos informáticos se encuentran operativos, actualizados y seguros. Además, se deben realizar las tareas que correspondan para que los equipos estén en un estado optimo.

Responsable: El responsable de seguridad.

8.8.7 Políticas de herramientas de seguridad

Todos los ordenadores deben contar con software de seguridad que garantice la protección contra virus, malware, troyanos o afines. Esas aplicaciones deben actualizarse de forma periódica y automatizada e igualmente deben estar programados los escaneos totales de los equipos por lo menos una vez a la semana.

Responsable: El responsable de seguridad.

8.8.8 Políticas para usuarios

Los usuarios deben seguir las siguientes políticas de seguridad de la información:

1. Evita pulsar en archivos de cuentas de correo desconocidas.
2. No descargues archivos de una página no oficial.
3. Debes de tener cuidado con su e-mail.
4. Pon contraseñas que sean difíciles de adivinar.
5. No compartas tus claves con ninguna persona.
6. No debes difundir la información confidencial (datos de proveedores, clientes, ventas, etc.) de la empresa.
7. Debes cerrar sesión al terminar de utilizar cualquier dispositivo o aplicación de la empresa.
8. Debes retirar todos los días cualquier información comercial sensible de tu escritorio.
9. Solo debes de guardar información de la empresa en las carpetas compartidas para dicho fin.

8.9 Cálculo del riesgo utilizando las políticas y procedimientos

Las filas de color verde representan aquellos riesgos que se han visto mitigados con la aplicación de las políticas y procedimientos definidos en el punto anterior.

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Datos de albaranes				
Errores en mantenimiento	Cambios de versión poco probados	5	2	10
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	1	5
ACTIVO: Datos de facturación				
Errores en mantenimiento	Cambios de versión poco probados	5	2	10
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Malversación y fraude	Inadecuada segregación de funciones de usuario	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Uso indebido de los sistemas de información	Falta de formación	5	1	5
ACTIVO: Datos de pedidos				
Errores en mantenimiento	Cambios de versión poco probados	5	2	10
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	1	5
ACTIVO: Datos de almacenes				
Errores en mantenimiento	Cambios de versión poco probados	4	2	8
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	1	4
Destrucción de registros	No existe política de contraseñas	4	1	4
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Falta de formación	4	1	4
ACTIVO: Datos de trazabilidad				
Errores en mantenimiento	Cambios de versión poco probados	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	1	5
ACTIVO: Datos contables				
Errores en mantenimiento	Cambios de versión poco probados	5	2	10
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Falta de formación	5	1	5
ACTIVO: Datos de productos				
Errores en mantenimiento	Cambios de versión poco probados	4	1	4
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	1	4
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Falta de formación	4	1	4

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Datos de clientes				
Errores en mantenimiento	Cambios de versión poco probados	4	1	4
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	1	4
Destrucción de registros	No existe política de contraseñas	4	1	4
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	1	4
ACTIVO: Datos de proveedores				
Errores en mantenimiento	Cambios de versión poco probados	4	1	4
Destrucción de registros	Inadecuada segregación de funciones de usuario	4	1	4
Destrucción de registros	No existe política de contraseñas	4	1	4
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	4	1	4
Uso indebido de los sistemas de información	Usuarios poco formados	4	2	8
Revelación de información	Falta de formación y conciencia sobre seguridad	4	1	4
ACTIVO: Datos de usuarios del sistema de gestión				

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Errores en mantenimiento	Cambios de versión poco probados	5	1	5
Destrucción de registros	Inadecuada segregación de funciones de usuario	5	1	5
Destrucción de registros	No existe política de contraseñas	5	1	5
Interrupción de procesos de negocio	Respaldo inapropiado o irregular	5	1	5
Uso indebido de los sistemas de información	Usuarios poco formados	5	1	5
Revelación de información	Falta de formación y conciencia sobre seguridad	5	1	5
ACTIVO: Acceso remoto de Windows				
Acceso a la red o al sistema de información por personas no autorizadas	Contraseñas predeterminadas no modificadas	4	1	4
Acceso a la red o al sistema de información por personas no autorizadas	No existe políticas de contraseñas	4	1	4
Comprometer información confidencial	Clasificación inadecuada de la información	4	2	8
Comprometer información confidencial	Falta de política de acceso remoto	4	2	8
Suplantar la identidad de un usuario	Uso inadecuado de las credenciales de acceso	4	1	4
Fallo de los enlaces de comunicación	Inadecuada gestión de red	4	3	12
Mal funcionamiento del equipo	Uso de equipos con sistemas operativos obsoletos	4	2	8

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
ACTIVO: Correo electrónico				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	1	5
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	1	5
Revelación de información	Ausencia de políticas de correo electrónico	5	3	15
Revelación de información	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	1	5
Código malicioso	Inadecuada monitorización de los contenidos (enlaces, ficheros adjuntos) de los correos	5	2	10
Código malicioso	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	2	10
Uso indebido del correo electrónico	Falta de formación, conciencia y faltas de instrucciones sobre seguridad	5	2	10
ACTIVO: Sistema de gestión				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	1	5
Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	5	1	5
Revelación de información	Inadecuada segregación de roles de usuario	5	3	15
Uso indebido de sistemas de información	Falta de formación	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Malversación y fraude	Insuficiente supervisión de la información del sistema de gestión	5	2	10
Malversación y fraude	Inadecuada segregación de roles de usuario	5	1	5
Errores en mantenimiento	Cambios de versión poco probados	5	1	10
Interrupción de procesos de negocio	Inadecuada gestión de capacidad del sistema	5	3	15
Errores de software	Pruebas de software insuficientes	5	4	20
ACTIVO: SQL Server				
Divulgación de contraseñas	Contraseñas predeterminadas no modificadas	5	1	5
Acceso por personas no autorizadas.	Inadecuada gestión y protección de contraseñas	5	1	5
Comprometer información confidencial	Inadecuada gestión y protección de contraseñas	5	1	5
Destrucción de registros	Inadecuada segregación de roles de usuario	5	1	5
Revelación de información	Inadecuada segregación de roles de usuario	5	1	5
Errores en mantenimiento	Falta de actualizaciones	5	2	15
Interrupción de procesos de negocio	Falta de redundancia, copia única	5	2	10
ACTIVO: Servidor de base de datos				
Desastre por incendio	Falta de detectores de humo	5	1	5

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Desastre por inundación	Existencia de tuberías de agua en el techo donde se encuentra el equipo	5	1	5
Pérdida de electricidad	Falta de redundancia de servicio eléctrico	5	2	10
Mal funcionamiento del equipo	Inadecuada gestión de capacidad del sistema	5	2	10
Mal funcionamiento del equipo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Mantenimiento inadecuado	5	2	10
Pérdida de servicios de apoyo	Falta de redundancia, copia única.	5	3	15
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Router Huawei				
Interrupción de procesos de negocio	Falta de redundancia	5	1	5
Fallo en los enlaces de comunicación	Inadecuada seguridad del cableado	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Wifi				
Interrupción de procesos de negocio	Falta de redundancia	5	2	10
ACTIVO: Almacenamiento en red				

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Interrupción de procesos de negocio	Inadecuada segregación de roles de usuario	4	1	4
Acceso a la red o al sistema de información por personas no autorizadas	Inadecuada segregación de roles de usuario	4	1	4
Comprometer información confidencial	Falta de formación y conciencia sobre seguridad	4	1	4
Código malicioso	Falta de herramientas de seguridad	4	3	16
ACTIVO: Red eléctrica				
Interrupción de procesos de negocio	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Pérdida de electricidad	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
Fallo de los enlaces de comunicación	Falta de redundancia o sistemas de alimentación ininterrumpida	5	1	5
ACTIVO: Router de Movistar (ISP)				
Daño causado por un tercero	Inadecuada gestión del sistema	5	1	5
Acceso físico no autorizado	Protección física no apropiada	5	2	10
ACTIVO: Puestos comerciales de MercaMadrid				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	2	10

Amenaza	Vulnerabilidad	Valor del activo	Valor probabilístico	Riesgo
Desastre generado por causas humanas	Falta de políticas de acceso	5	1	5
Desastre generado por causas humanas	Falta de formación	5	1	5
Acceso físico no autorizado	Protección física no apropiada	5	1	5
ACTIVO: CPD				
Desastre por incendio	Falta de detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento de los detectores de humo	5	1	5
Desastre por inundación	Falta de mantenimiento	5	1	5
Desastre generado por causas humanas	Falta de políticas de acceso	5	2	10
Desastre generado por causas humanas	Falta de formación	5	2	10
Acceso físico no autorizado	Protección física no apropiada	5	2	10

Tabla 25: Cálculo del riesgo utilizando las políticas y procedimientos: Elaboración propia

8.10 Glosario

El glosario necesario para entender el presente trabajo se encuentra en Magerit V3 e ISO/IEC 27000.

[Página dejada intencionalmente en blanco]