UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

ESCUELA POLITÉCNICA SUPERIOR DE ELCHE

GRADO EN INGENIERÍA INFORMÁTICA EN TECNOLOGÍAS DE LA INFORMACIÓN

"ESTUDIO DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN Y RESOLUCIÓN DE UN CASO PRÁCTICO"

TRABAJO DE FIN DE GRADO

JULIO – 2025

AUTOR: Sergio Rodríguez Navarro
Director: Pablo José Piñol Peral

Índice de contenidos

Índice de tablas y figuras

1. INTRODUCCIÓN

1.1 Motivación

La creciente dependencia tecnológica en los diferentes sectores de la sociedad, ya sea en el ámbito empresarial, gubernamental y personal, ha traído un aumento exponencial de la actividad criminal. Este aumento obliga a las compañías, de cualquier tamaño o sector, a mejorar sus defensas y procedimientos para evitar así sufrir grandes daños debido a incidentes de seguridad.

Todo proyecto de mejora en seguridad debería comenzar mediante la realización de un análisis de riesgos, que permita detectar los puntos débiles de la compañía evaluada, existen varios tipos de análisis de riesgos: financieros, reputacionales… Sin embargo en este proyecto nos focalizamos en los relacionados con la ciberseguridad. En este campo un análisis de riesgos es una herramienta fundamental para identificar, evaluar y mitigar estos puntos débiles. Esto es debido a que permite a las organizaciones entender mejor las amenazas y vulnerabilidades a las que están expuestas, facilitando la toma de decisiones, la creación de un plan de contramedidas y la asignación de recursos de manera más eficiente para la mejora de seguridad de la compañía.

Un buen análisis de riesgos permite la creación de políticas y procedimientos de seguridad efectivos, además de la capacidad de obtener certificaciones sobre ciberseguridad, que no solo aporta el beneficio de cerciorarse sobre la calidad de las medidas defensivas implementadas sino que también aumentan el valor reputacional de la compañía que las obtenga.

La motivación para este trabajo surge de la necesidad de explorar y analizar en profundidad los métodos de gestión de riesgos, en este caso, tomando como referencia la metodología Magerit. Con el objetivo de comprender sus principios fundamentales y evaluar su efectividad en contextos prácticos. Este estudio se centra en realizar un repaso exhaustivo de Magerit, y en la aplicación práctica de esta metodología a través de un caso de estudio simulado.

La implementación del caso práctico permitirá la demostración sobre la aplicabilidad y eficacia de esta metodología en un entorno simulado, proporcionando ejemplos concretos de cómo puede ser utilizada para mejorar la ciberseguridad en las organizaciones, mediante la exposición de posibles medidas de seguridad junto con sus necesidades presupuestarias y de aplicación.

Este Trabajo de Fin de Grado está basado en mi experiencia profesional realizando este tipo de tareas y otras afines en el ámbito de la ciberseguridad. El conocimiento que tengo sobre esta problemática proviene directamente de mi trabajo en el sector, donde he tenido la oportunidad de enfrentar desafíos

similares, lo que ha enriquecido mi perspectiva y aportado un enfoque práctico a este estudio.

Además de contribuir al conocimiento teórico sobre Magerit, el objetivo de este trabajo es ofrecer un manual útil que los expertos del sector puedan utilizar para mejorar la gestión de riesgos de ciberseguridad o para apoyar el estudio del tema.

El objetivo final de este estudio teórico-práctico del análisis de riesgos es proporcionar un enfoque crítico y práctico que ayude a las organizaciones a abordar mejor los problemas de ciberseguridad, proteger sus activos digitales y mantener la continuidad del negocio.

1.2 Objetivos

El proyecto tiene dos objetivos principales. El primero es el análisis de la metodología de análisis y gestión de riesgos de los sistemas de información Magerit, así como la propuesta de herramientas útiles para la aplicación de dicha metodología.

El segundo objetivo es la realización de un análisis de riesgos en un escenario simulado pero realista y el diseño de las medidas de seguridad que sería recomendable implementar, así como una estimación del coste de dicha solución.

1.3 Análisis de Riesgos

Los análisis de riesgos son herramientas de gran utilidad**.** Empleadas por empresas de todo el mundo permiten realizar una evaluación sobre los activos y las medidas de seguridad integradas en los sistemas de la empresa evaluada. Estos análisis pueden ser tan detallados y profundos como el alcance lo requiera, pudiendo así, evaluar desde una infraestructura a toda una organización al completo.

En España existen varias normativas y Leyes que obligan a la realización de estos análisis y una posterior gestión de los riesgos resultantes:

- La Ley de Protección de Infraestructuras Críticas [3] creada a raíz de los atentados de 2008 en Madrid, define una serie de documentos y directrices de seguridad que ciertas empresas definidas como “operadores críticos” deben integrar. Estos operadores críticos son compañías privadas o públicas que pertenecen a un sector de extrema importancia para la población española, algunos ejemplos de estos sectores son: suministro eléctrico, área sanitaria, infraestructuras de alimentación…

  Esta Ley “fuerza” a la realización de un análisis de riesgos por cada una de las infraestructuras definidas como críticas mediante un listado de amenazas

facilitado por el organismo responsable de la gestión y cumplimiento de esta Ley: el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

- El “Esquema Nacional de Seguridad” (ENS)[4] define unas directrices en forma de controles divididos en tres niveles de seguridad. Surge con la intención de “forzar” a aquellas compañías proveedoras de instituciones públicas a tener unas medidas mínimas de seguridad. Cualquier compañía que así lo quiera puede certificarse en cualquiera de los tres niveles definidos.

Existen múltiples metodologías a la hora de realizar estos análisis, aunque es muy común que cada compañía tenga la suya propia. Estas metodologías siempre parten de la base de una metodología de reconocimiento internacional.

A continuación, se listan algunas de las metodologías más empleadas a nivel nacional e internacional.

- **ISO 31000 [5]:** Reconocida como una norma internacional, proporciona directrices generales que pueden ser aplicadas por cualquier organización, independientemente del sector en el que opere.
  Esta metodología se compone de seis capítulos. En esta sección se explican los tres más relevantes:
  - Principios: Los once principios rectores de ISO están diseñados para proporcionar una guía en la gestión de riesgos.
  - Marco de referencia: El objetivo del desarrollo del marco es aumentar la eficacia de la gestión de riesgos en toda la organización que lo implemente. .
  - Proceso: Consiste en establecer políticas y procedimientos que ayuden a las organizaciones a afrontar el cambio de manera que no solo lo prevengan y mitiguen, sino que también lo transformen en oportunidades.

- ***Information risk assessment methodology 2*** **(IRAM v2) [6]:** Aunque este enfoque es sencillo, también resulta suficientemente útil. Completar cada una de sus seis etapas principales permite realizar un análisis de riesgos exhaustivo que facilita a la organización identificar, gestionar, prevenir y mitigar los riesgos de manera eficaz.

  Las etapas son: definición del alcance, identificación de amenazas, evaluación de vulnerabilidades, análisis del impacto en el negocio, evaluación de riesgos y tratamiento de riesgos.

  Esta metodología fue desarrollada por un equipo técnico especializado

del Instituto Argentino de Normalización y Certificación (IRAM), conformado por expertos en seguridad de la información, gestión de riesgos y cumplimiento normativo.

- **Metodología Magerit**: metodología elaborada y promovida por el Consejo Superior de Administración Electrónica (CSAE) [2] como respuesta a la creciente dependencia de la sociedad en general sobre los sistemas informáticos. Magerit en diferencia con otras metodologías implementa el Proceso de gestión de riesgos dentro de un marco de trabajo y persigue los siguientes objetivos:
  - Concienciar sobre la existencia de los riesgos y la necesidad de aplacarlos.
  - Ofrecer un método para el análisis de los riesgos derivados del uso de los medios informáticos y de comunicación
  - Descubrimiento y gestión de los riesgos con el objetivo de mantenerlos bajo el control de la compañía que lo realice.

La siguiente tabla recoge un resumen de varias diferencias entre las metodologías expuestas anteriormente:

Criterio	Magerit	ISO 31000	IRAM2
Objetivo	Análisis de riesgos en sistemas de información (énfasis en ciberseguridad).	Gestión integral de riesgos empresariales (no limitado a TI).	Evaluación de riesgos de información (alineado con ISO 27001).
Estructura	Basado en activos, amenazas y salvaguardas.	Proceso genérico: identificación, evaluación, tratamiento y monitoreo.	Seis fases: alcance, impacto, amenazas, vulnerabilidades, evaluación y tratamiento.
Flexibilidad	Adaptable a normativas locales (ENS, LOPD).	Neutral a industrias y tamaños organizacionales.	Enfoque pragmático para PYMEs y sectores regulados.

Tabla 1: Comparativa entre Metodologías

1.4 Organización de la Memoria

La memoria se ha dividido en secciones que abordan de manera progresiva y lógica los distintos aspectos del tema de estudio. Desde la contextualización del problema y el marco teórico, pasando una explicación de la metodología empleada, revisión de los resultados obtenidos y las conclusiones finales. Buscando garantizar una compresión fluida y coherente del trabajo.

La documentación para el proyecto está organizada en seis apartados principales:

- **Introducción:** Este apartado presenta el contexto general de la ciberseguridad, la importancia de los análisis de riesgos, los objetivos planteados para el proyecto y la motivación detrás de la realización del mismo. Además, se expone una visión preliminar de la estructura del documento.

- **Metodología de Análisis de Riesgos:** Se detalla el conjunto de conceptos, teorías y fundamentos necesarios para comprender el procedimiento para la realización del análisis. En este caso, se profundiza en la metodología Magerit y en los principios de la gestión de riesgos aplicados a la ciberseguridad.

- **Realización práctica del análisis de riesgos:** Se desarrolla un escenario simulado con los datos necesarios para aplicar los principios teóricos estudiados. Se detallan las características del entorno, la identificación de activos, las amenazas identificadas, los pasos realizados durante el análisis.

- **Informe de resultados:** Este apartado analiza los resultados obtenidos tras la aplicación del caso práctico.

- **Propuesta de medidas:** En este apartado se presentan las soluciones y contramedidas diseñadas para abordar los riesgos identificados en el caso práctico. Se detallaran una serie de medidas de seguridad junto con varias soluciones de mercado que podrían implantarse, se incluirá un texto explicativo de cuales de estas son recomendadas según el cliente al que aplicarían. Además, se detallan las necesidades técnicas, organizativas y presupuestarias de cada propuesta, con el objetivo de ofrecer un plan de acción claro y aplicable.

- **Aplicaciones para la realización de análisis de riesgos:** Este apartado explora las herramientas y aplicaciones disponibles para llevar a cabo análisis de riesgos en el ámbito de la ciberseguridad. Se realiza una revisión de las características, ventajas y limitaciones de las principales soluciones tecnológicas utilizadas en el mercado, destacando aquellas que son más adecuadas para aplicar metodologías como Magerit.

2. Metodología de análisis de riesgos: Magerit

Esta metodología es de uso completamente libre y no requiere de ninguna autorización previa para su uso, como sí que ocurriría con metodologías de

desarrollo privado. Esta fue elaborada por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN).

Surge como respuesta a la gran dependencia existente (y creciente) tanto en la administración pública como en el sector privado respecto a las nuevas tecnologías para lograr desempeñar sus funciones.

Es inevitable el uso de las tecnologías anteriormente indicadas debido a que estas suponen una gran mejora tanto en eficiencia como eficacia para los servicios prestados, sin embargo, esto supone un aumento considerable de los riesgos y de la exposición a los ataques. El conocimiento del riesgo sobre un activo o servicio, permite a la compañía poseedora del mismo realizar una valoración entre los beneficios que aporta este mismo activo frente al coste que puede suponer un parcheo de seguridad o, en caso de no querer o poder parchearlo, el nivel de riesgo o peligro que supondría para la compañía.

De hecho, aunque este proyecto está fundamentalmente pensado para la aplicación práctica del análisis a nivel de ciberseguridad, estos análisis se pueden implementar con el objetivo de mejorar la seguridad física, revisando activos como el cableado externo o el perímetro de una infraestructura y amenazas como el robo de cableado o el allanamiento.

Magerit en sí mismo busca crear un marco de trabajo, que de manera metódica permite un análisis formal y estructurado que no deje oportunidades al azar ni a la improvisación, ni que dependa de la arbitrariedad del analista.

Los objetivos principales de esta metodología son:

- Directos:
    - Concienciar de la existencia de riesgos y la necesidad de aplacarlos o gestionarlos de la forma adecuada a los dirigentes de las organizaciones que realicen el análisis
    - Ofrecer un método sistemático para el análisis de los riesgos
    - Ayudar con la planificación del tratamiento a seguir para permitir mantener las amenazas encontradas bajo control
- Indirectos:
    - Servir de soporte para organizaciones que en un futuro quieran auditarse o certificarse de ciertas normativas. Por ejemplo el Esquema Nacional de Seguridad requiere de la realización de un análisis formal de riesgos, Magerit entraría en esta misma categoría.

2.1 Conceptos Básicos

La mayoría de los análisis de riesgos parten de un listado de pasos muy similares:

- **Identificación de los activos que se van a analizar**. Estos activos pueden ir desde los más relevantes de la compañía o grupos en concreto seleccionados por necesidades puntuales de esta.

- **Identificación de las amenazas relacionadas** con estos activos. Este listado puede ser más o menos extenso dependiendo de si se quiere analizar una parte en concreto de los riesgos que supone el uso de estos activos.

- **Evaluación de las medidas de seguridad ya implementadas**. Se realiza una comparación entre las amenazas detectadas y la seguridad existente para poder localizar el riesgo real que supone teniendo en cuenta la existencia (o no) de unas salvaguardas.

- **Cálculo del impacto** que supone el daño realizado sobre los activos por la acción de las amenazas.

- **Cálculo del riesgo** obtenido del impacto calculado anteriormente respecto a la probabilidad de que ocurran las amenazas previstas.

La guía oficial de la metodología Magerit [1] expone el siguiente gráfico para guiar de forma visual los pasos anteriormente explicados:

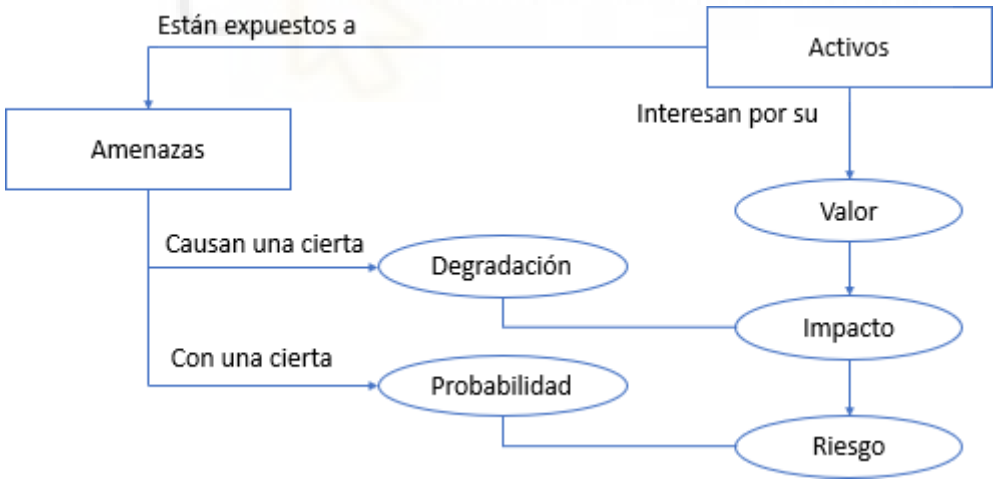

Figura 1: Elementos del análisis de riesgos potenciales
(Extraído de la guía metodológica de Magerit. Redactado por el Ministerio de Hacienda y Administraciones Públicas)

2.2 Activos

Los activos de una compañía son aquellos elementos que se emplean para el desarrollo de la función de dicha compañía, por ejemplo, los servidores de

donde se alojan las páginas web de una empresa.

Esencialmente a la hora de valorar los activos de información tenemos dos grandes características que les pueden dotar de mayor o menor importancia: el servicio que prestan o la información que manejan.

Por una parte, el servicio puede llegar a ser esencial en muchos casos ya que, por ejemplo, un banco en caso de perder los servidores que alojan las funciones de pagos online, quedarían incapaces de proporcionar a sus clientes una función clave para la compañía durante tanto tiempo como estén los servidores caídos. Por otra parte, la información también es vital,siendo esta tanto datos privados de la compañía como también información privada de clientes, cuentas bancarias, direcciones de residencia…

Además, estos grandes grupos agrupan otros tipos de activos que pueden ser también relevantes a la hora de su identificación ya sean activos de apoyo auxiliar, soportes de información, redes de comunicación… De nada sirve securizar únicamente los activos principales cuando un atacante podría causar daños similares mediante el daño realizado a activos auxiliares aprovechándose de las dependencias entre ellos.

2.2.1 Dependencias

En relación con lo que tratamos en el último párrafo, los activos pueden estar relacionados entre sí, ya sea a un nivel más físico como puede ser la red eléctrica que distribuye electricidad a los activos electrónicos o relaciones digitales como puede ser al que une una base de datos con una aplicación de gestión de identidades.

Desde el Centro Criptológico Nacional (CCN) se define al sistema de activos como: “árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o ‘superiores’ depende de los activos que se encuentran más abajo o ‘inferiores’”. Es debido a esto que un analista no debe únicamente centrarse en aquellos activos que en una primera instancia parezca que gozan de mayor importancia si no que también deberá tener en cuenta aquellos activos que contengan interdependencias con los de mayor valor o con aquellos que se encuentran “más arriba en el árbol”.

Relacionado con esta estructuración, se ha comprobado en la realización práctica de este tipo de análisis que, aunque es cierto que se pueden estructurar de forma esquemática el “árbol” de activos mencionado por el CCN, al final cada caso es particular y cada compañía goza de unas prioridades y recursos por lo que, en última instancia la teoría no deja de ser únicamente una base desde la que partir y que luego deberá amoldarse a cada situación concreta.

2.2.2 Dimensiones

Existen varias dimensiones en las que se pueden clasificar los activos .Estas serían las siguientes:

- **Confidencialidad**: mide el daño que podría suponer que personas sin la debida autorización pudiesen llegar a conocer información relacionada con el activo.

- **Integridad**: mide el daño que supone la corrupción o el deterioro de este, causando consecuencias como la pérdida del servicio o la exposición a amenazas de mayor importancia.

- **Disponibilidad**: mide el daño que causaría en una compañía la pérdida total o parcial del activo y las consecuencias que podría llegar a causar.

- **Autenticidad**: capacidad de detección o protección frente a casos de suplantación de la identidad, también mide a la capacidad de identificación de los usuarios de manera segura.

- **Trazabilidad**: mide el daño causado por la pérdida en la trazabilidad de responsabilidades y acciones ejecutadas en el activo seleccionado. En muchos casos resulta vital saber "quien" ha realizado "qué" acciones y bajo la responsabilidad de "quien". En este caso diferenciamos:

    - Trazabilidad del uso del servicio
    - Trazabilidad del acceso a los datos

Las tres primeras dimensiones (Confidencialidad, integridad y disponibilidad) se las considera dimensiones básicas y se tienen en cuenta en casi todas las metodologías de análisis de riesgos aceptadas internacionalmente. Magerit incluye el resto de estas con el objetivo de buscar un análisis más completo y fiable que otras metodologías.

2.2.3 Valoración cualitativa

La valoración cualitativa permite una rápida asignación de magnitudes a amenazas, activos y medidas de seguridad, el problema de estas valoraciones es que al no emplear asignaciones numéricas no permite realizar un análisis algorítmico y este se vuelve menos preciso.

2.2.4 Valoración cuantitativa

Al contrario de las valoraciones cualitativas, las cuantitativas consisten en una valoración realizada mediante el estudio de ciertos valores concretos en cuanto a activos, amenazas y medidas de seguridad. Estas valoraciones se pueden realizar a nivel monetario, temporal, de inversión…

Este tipo de valoración es más costosa de realizar y requiere de un esfuerzo mayor, sin embargo, permite obtener análisis más detallados y concretos en relación con lo que se busque con el mismo.

2.3 Amenazas

Dependiendo de la intencionalidad y el alcance del análisis de riesgo se emplea un listado de amenazas u otro, existen organismos y normativas que obligan a emplear su propio listado para poder certificarse en ellas, sin embargo, se puede realizar una identificación propia y crear un listado personalizado acorde con las necesidades de la compañía evaluada. Para la identificación de estas se suele buscar el origen que pueden tener las mismas:

- **Origen natural**: en estos casos, la entidad a analizar no es más que víctima de las circunstancias y no se le ataca de forma directa. Aun así, se deberá tener en cuenta a la hora de evaluar los daños que un temporal o un terremoto podría llegar a causar en una infraestructura o los activos que la componen.

- **Del entorno industrial**: se trata de fallos en maquinarias, desgastes o problemas de mantenimiento, de forma similar a las amenazas de origen natural estos no son ejercidos contra la compañía de forma deliberada, pero se deberán tener en cuenta ya que pueden llegar a ocasionar daños de gran magnitud para esta.

- **Vulnerabilidades de aplicaciones**: muchas de las herramientas con las que se trabaja diariamente contienen vulnerabilidades, algunas son descubiertas por la propia empresa creadora y se lanzan parches que permiten solventarlas, otras son descubiertas por grupos criminales y empleadas para la realización de ciberataques.

- **Causa humana accidental**: las personas con cierto nivel de acceso a información o ciertas áreas de trabajo pueden ser susceptibles del error humano o de una manipulación por parte de posibles atacantes, será necesario tener esto en cuenta para poder implementar las medidas necesarias en caso de requerirlo.

- **Causa humana deliberada**: se trata de amenazas causadas por atacantes externos e internos. Personas con los medios, ya sean por conocimiento técnico o acceso a la información, que debido a un interés monetario o personal pueden llegar a atacar y causar daños a la compañía analizada.

2.3.1 Valoración de las amenazas

Una vez determinadas las amenazas que se van a tener en cuenta se pasará a la valoración de estas, las amenazas se valorarán en dos categorías diferentes: el daño que podrían llegar a causar y la probabilidad de que ocurran.

La valoración del daño dependerá de si es causado de forma intencional o no, ya que los daños causados por el desgaste de una máquina o por un error humano se pueden acotar mucho más que los daños intencionales ya que en estos últimos el atacante puede causar grandes estragos en secciones muy concretas.

La degradación del valor por otro lado es más compleja de determinar, habitualmente se emplean tablas similares a esta, donde se emplean de forma cualitativa:

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 2: Degradación del valor

(Extraído de la guía metodológica de Magerit. Redactado por el Ministerio de Hacienda y Administraciones Públicas)

También existen expresiones numéricas y es habitual expresarlas empleando el año como referencia:

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 3: Frecuencia de la amenaza

(Extraído de la guía metodológica de Magerit. Redactado por el Ministerio de Hacienda y Administraciones Públicas)

2.4 Determinación del Impacto Potencial

Mediante el conocimiento de la vulnerabilidad de los activos y el daño causado por una amenaza en caso de materializarse, se puede obtener el impacto. Este impacto nos permitirá calcular el nivel de daño sucedido sobre el activo afectado.

Para una evaluación adecuada será necesario tener en cuenta las interdependencias de estos activos, mediante un grafo de dependencias se puede trasladar el impacto sufrido al resto de los activos dependientes.

Existen varios tipos de impactos calculables dependiendo de si son afectados por activos dependientes:

- **Impacto repercutido**: es aquel impacto calculado únicamente mediante las amenazas a las que está expuesto y el valor propio del activo en sí. Mediante este valor junto con el calculado de los activos dependientes se puede calcular el "impacto acumulado".
- **Impacto acumulado**: es aquel impacto que se calcula mediante las amenazas a las que está expuesto el activo, el valor del propio activo y el valor de los activos que dependen de él. De esta forma se puede calcular el daño resultante tanto por valor propio como por valor del daño indirecto causado. Un activo que es poco valioso por sí mismo, pero del que dependen gran cantidad de otros activos puede provocar un gran daño de ser amenazado.

2.5 Determinación del Riesgo Potencial

El riesgo es una medida calculada mediante el impacto (daño que causaría la materialización de una amenaza sobre un activo) y la probabilidad de éxito de esta amenaza. Por ejemplo, una amenaza poco probable pero muy destructiva como puede ser un coche bomba tendrá un riesgo similar que una amenaza muy probable y menos dañina, como un ataque DoS (Denial of Service).

A la hora de realizar estos cálculos se emplea un gráfico con zonas de calor, cada una de las zonas describen una situación diferente:

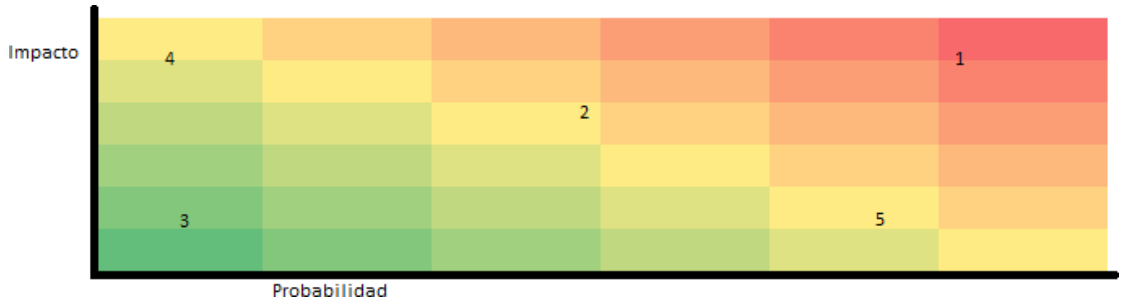

Figura 2: Gráfica de impacto sobre probabilidad

Como podemos observar hay 5 zonas diferenciadas, y según el tono de rojo que estas tomen serán de mayor o menor importancia para el análisis:

- La primera describe a aquellas amenazas con una alta probabilidad de materialización y alto impacto. Estas amenazas serán las que deberán solventar con mayor prioridad.
- La segunda y cuarta describe zonas más intermedias, donde debido a la baja probabilidad o el equilibrio entre impacto y probabilidad no les dan la importancia que tiene la zona número 1.
- La tercera zona describe amenazas poco probables y de un impacto relativamente bajo. Este tipo de amenazas suelen asumirse ya que el coste monetario y de recursos suele ser mayor a las pérdidas que podría llegar a causar.
- La quinta zona son aquellas amenazas con alta probabilidad y bajo impacto, estas pueden llegar a suponer un riesgo, ya que aunque no provocan grandes pérdidas, su continua aparición pueden, a la larga, ser peligrosas.

De igual manera que con el impacto, podemos diferenciar dos tipos de riesgos que cambian según el número e importancia de activos que dependen del activo analizado:

- **Riesgo acumulado**: mide las consecuencias que un incidente en un activo tiene, no solo en ese activo, sino también en otros que dependen de él. Este impacto aumenta cuanto mayor sea la criticidad del activo y la magnitud de las dependencias con otros activos. Refleja así el alcance total de las posibles afectaciones dentro de un sistema interconectado.

- **Riesgo repercutido**: es el resultado de combinar la probabilidad de una amenaza con su impacto repercutido, considerando las dependencias entre activos. Este impacto es mayor cuanto más crítico sea el activo afectado y más dependencias tenga con otros activos. Así, el riesgo repercutido refleja cómo un incidente en un activo puede propagarse y

afectar a otros, evaluando tanto los efectos directos como los indirectos en la organización.

2.6 Salvaguardas

Los cálculos indicados anteriormente son estimaciones brutas y suponen que los activos se encuentran en una situación de exposición total. En la práctica estos activos están dotados de ciertas protecciones tanto físicas como lógicas. Estas medidas de seguridad o salvaguardas deberán ser tomadas en cuenta a la hora de la realización de un análisis de riesgos.

Existen salvaguardas de muchos tipos, ya que, como comentábamos anteriormente, no solo existen protecciones físicas y lógicas sino también organizacionales. Estas medidas se centran en proteger a la organización mediante políticas y procedimientos, que puedan permitir a los empleados saber cómo actuar en cualquier situación.

Como es lógico pensar no todas las salvaguardas afectarán a los mismos activos ni servirán para aplacar las mismas amenazas. Es por ello que el evaluador deberá saber seleccionar aquellas medidas de seguridad que le sean útiles según la situación en la que se encuentre.

Para una selección adecuada, primero se deberá realizar una criba de las medidas ya existentes, para esto se recomienda tener en cuenta:

- Tipo de activos a proteger
- Dimensiones que requieren protección
- Amenazas de las que se requiere la protección
- Posibles medidas de seguridad que ya cubren estas amenazas

De esta criba el evaluador obtendrá una declaración de aplicabilidad donde se justifique qué medidas se han tomado para el análisis, cuáles no y el razonamiento que se ha seguido para llegar a las conclusiones.

Estas medidas seleccionadas afectarán al análisis en dos sentidos:

- Reduciendo la probabilidad de éxito de la amenaza: se trata de aquellas medidas que hacen de “escudo” para los activos que protegen, evitando que las amenazas puedan llegar a materializarse, por ejemplo, un muro alrededor de una infraestructura reducirá la probabilidad de que un intruso pueda acceder exitosamente a la misma.
- Limitando el daño causado por amenaza: se trata de aquellas medidas que permiten mitigar el daño causado por la materialización de una amenaza, por ejemplo, un guardia de seguridad puede llegar a atrapar a un intruso, y aunque es posible que este ya haya llegado a dañar alguna parte de la infraestructura, se ha evitado que pudiese continuar.

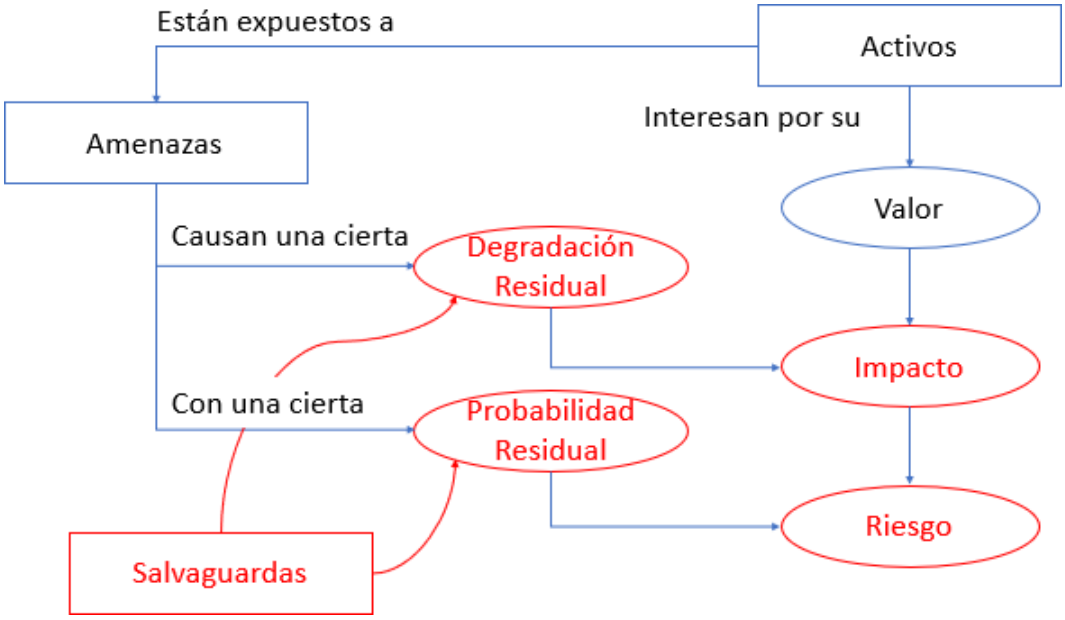

Figura 3: Esquema sobre el uso de las salvaguardas

(Extraído de la guía metodológica de Magerit. Redactado por el Ministerio de Hacienda y Administraciones Públicas)

Existen dos factores que permiten medir la efectividad de una salvaguarda. El técnico, que se refiere a el nivel de idoneidad de la medida para enfrentarse a una amenaza y el operativo, que trata de procedimientos y políticas de uso, formación de los operadores, mantenimiento…

Mediante estos dos factores, el evaluador deberá dotarse de un porcentaje de eficacia que afectará en el nivel de protección de la salvaguarda. Existirá un porcentaje de eficacia por cada salvaguarda y para cada amenaza en las que se pueda emplear.

2.7 Riesgo Inherente

El riesgo inherente es el resultado de aplicar la probabilidad de éxito de la amenaza y los impactos a los activos, obteniendo así la amenaza presente en los mismos sin tener en cuenta las medidas de seguridad que pudieran, o no, estar ya implementadas.

De la misma forma el riesgo residual se puede calcular para los activos dependientes tanto inferiores como superiores.

2.8 Riesgo Residual

Aplicando las medidas de seguridad a los cálculos obtenidos anteriormente, se puede obtener el riesgo residual, siendo este el riesgo real al que están expuestos los activos.

Una vez obtenido este cálculo ya habríamos acabado con la principal parte del análisis de riesgos. Con estos datos se puede obtener el nivel de riesgo real en la situación actual, tras esto, según lo que se busque con el análisis, se pueden aplicar nuevas medidas de seguridad o contratar seguros para poder paliar aquellas amenazas que supongan un alto riesgo para la compañía, aquí entraría el denominado como “apetito de riesgo”.

El apetito de riesgo de una compañía se define como la cantidad de amenazas de cierto valor de riesgo que está dispuesta una compañía a asumir. Por ejemplo, una compañía con alto apetito estará más dispuesta a asumir riesgos medios o incluso altos mientras que una con bajo apetito buscará salvaguardas que puedan reducir los riesgos lo máximo posible. Este apetito variará según el presupuesto y lo críticos que sean los activos evaluados durante el análisis.

2.9 Análisis de Metodología Magerit

En este apartado, se analizan las fortalezas y áreas de mejora de Magerit, se ofrecen recomendaciones para los analistas que deseen emplear la metodología.

Fortalezas de Magerit

- Magerit proporciona un enfoque exhaustivo que abarca todas las etapas del análisis de riesgos, desde la identificación de activos y amenazas hasta la evaluación de vulnerabilidades y la implementación de contramedidas, además de que su planteamiento respecto al uso de las cinco dimensiones de la seguridad dota al análisis de mayor profundidad que otras metodologías.
- La metodología es altamente adaptable a diferentes alcances. Su flexibilidad permite ajustar los procesos y herramientas a las necesidades específicas de cada entorno, asegurando su relevancia y efectividad.
- Permite la fácil integración con normas y marcos de referencia, como la ISO 27001, o el ENS, lo que la convierte en una opción versátil y atractiva para la gestión de riesgos.
- Se trata de una metodología muy flexible que permite ser empleada como base y abierta a posibles adaptaciones y modificaciones permitiendo una mejor usabilidad independientemente del contexto y las necesidades del análisis.

Áreas de Mejora

- La metodología puede resultar compleja y laboriosa, especialmente para organizaciones pequeñas, con bajo presupuestos o incluso para analistas con poca experiencia. La cantidad de documentación y los detallados procesos pueden ser abrumadores y requieren de tiempo de estudio y dedicación.
- Aunque se trata de un marco robusto, requiere actualizaciones periódicas para mantenerse al día con las nuevas amenazas y tecnologías emergentes. La falta de actualización podría limitar su efectividad en entornos dinámicos.
- Requiere de ajustes para poder aplicarse de forma práctica, ya que su complejidad en ciertos asuntos como las dependencias hace que sean necesarios grandes esfuerzos por parte del analista y del cliente para poder obtener todos los datos necesarios.

Recomendaciones para Analistas

- Una metodología tan cambiante y con actualizaciones tan constante requiere de mantenerse actualizados con las últimas versiones y mejores prácticas. Esto asegura la correcta aplicación de la misma.
- Adaptar Magerita a las necesidades específicas de la organización y del proyecto es crucial. Es necesario ser capaz de identificar las áreas más críticas y ajustar el alcance y la profundidad del análisis según los recursos disponibles y las peticiones del cliente.
- Para maximizar la efectividad de Magerit, se recomienda su integración con otros estándares y marcos de referencia de ciberseguridad. Esto permite obtener una visión más holística y coherente de la gestión de riesgos.

2.9.1 Aplicación teórica a la práctica

La metodología Magerit ofrece un marco de trabajo complejo que permite realizar análisis detallados y precisos. Sin embargo, esta metodología tal y como esta explicada en las guías ofrecidas por el CCN-CERT son generalistas, dan poco detalle y dejan atrás pasos comunes e importantes que muchas otras metodologías si tratas. Como opinión profesional la metodología Magerit debería tratarse mas como una base sobre la que realizar el análisis adaptándola a las necesidades y la realidad del cliente.

Teniendo como objetivo el realizar un ejercicio practico simulando una situación lo mas realista posible, se realizaran una serie de modificaciones y agregados a la metodología anteriormente revisada para adaptarla a la realidad, el contexto del proyecto, ademas de buscar un equilibrio entre la calidad del análisis y los esfuerzos que supondría la realización del mismo. En el siguiente listado veremos varias de estas adaptaciones:

- **Ajustes en la metodología**: parte propuesta por la metodología Magerit son las dependencias y los cálculos de los riesgos asociados a estas. Si bien es cierto que, realizado correctamente, permite una evaluación mas precisa y exhaustiva, en la practica muy pocas veces los clientes van a querer aplicarla, por esto y por la búsqueda de un ejercicio realista se ha optado en el ejercicio practico por una solución que perfectamente se podría aplicar en la realidad, esta consiste en el uso de las dependencias por activo para el aumento de la sensibilidad al riesgo de los mismos. A continuación veremos algunos de los motivos por los que no se suele usar la gestión de dependencias sugerida por Magerit de forma literal a lo que dice la metodología:

    - Realizar un análisis tan detallado sobre las dependencias y la aplicabilidad de las mismas sobre cada uno de los activos a evaluar requiere de un gran gasto de recursos y tiempo.
    - Si no se realiza el análisis de dependencias de forma correcta puede dar a aumentos irreales y exagerados de los riesgos resultantes.
    - Trabajar con las dependencias (aun habiendo obtenido los datos correctamente) supone un aumento del esfuerzo y el tiempo requerido para la realización del análisis y, en comparación con los resultados que se podrían obtener mediante ajustes como el realizado en el ejemplo practico, no compensa a nivel de aumento de precisión de la evaluación.

- **Probabilidad de éxito de la amenaza**: un dato que no contempla Magerit es la probabilidad de éxito de amenaza, aunque cuando se valoran las amenazas si que se analizan para obtener la frecuencia con la que estas amenazas se materializan, este dato no suele ser suficiente para identificar cuan posible es que, no solo se materialice una amenaza, si no que ademas tenga éxito sobre un activo. Para esto se realiza el calculo de probabilidad de éxito de amenaza, más adelante lo trataremos con más detalle.

- **Identificación de amenaza**: Magerit no aplica de forma explicita lo que se llamaría como la “identificación de amenaza”, esto consiste en la identificación de que amenazas aplicarían a que activos, fuera de la teoría no todas las amenazas afectan a todos los activos, por ejemplo, la amenaza “robo de cableado” nunca afectaría a un activo lógico, no tendría sentido. Mediante el ejercicio de identificación podemos hacer una diferenciación y crear un análisis mas preciso.

- **Cambios en la terminología**: es común que los analistas empleen las mismas terminologías para datos que se recogen de forma común independientemente de la metodología de análisis que se emplee. Por ejemplo en lugar de “Degradación” emplearemos el término “Impacto” o en lugar de “ Probabilidad de ocurrencia” se usará “Frecuencia” para evitar

confusiones con la “Probabilidad de éxito de amenaza” del punto anterior.

Para adaptar el ejercicio a la metodología que vamos a usar como base, haremos la identificación en base a las cinco dimensiones de la seguridad.

3. REALIZACIÓN DEL ANÁLISIS DE RIESGOS

3.1 Exposición del Caso Practico

Para realizar el análisis de riesgos vamos a crear una situación ficticia con una empresa tipo, en esta situación esta compañía será nuestro cliente y nos habrá encargado la realización de una análisis de riesgos usando como base la metodología Magerit. Se crearán unas necesidades o alcance, que simularán las expresadas por este cliente y en consecuencia se realizará una gestión y análisis del riesgo según estas especificaciones.

Las medidas de seguridad ya implementadas por este cliente se elegirán de forma que sean relevantes para el análisis y que sean lo suficientemente genéricas como para resultar en un caso factible en el mundo real.

La entidad contratista se llama “Data ESP”. Se trata de una compañía relacionada con el análisis de datos y la gestión de servidores privados. Este cliente ha expresado su preocupación en cuanto a la seguridad de una de sus infraestructuras a nivel lógico por lo que ha solicitado la realización de un análisis de riesgos relacionado con amenazas digitales y similares.

La compañía cuenta actualmente con una plantilla fija de 42 empleados internos y un equipo complementario de entre 10 y 15 colaboradores externos, entre los que se incluyen técnicos y administradores de red.

La empresa opera en un edificio tecnológico donde dispone de dos plantas completas. La primera está dedicada a funciones administrativas, comerciales y de soporte operativo, mientras que la segunda alberga el área técnica, que incluye acceso restringido al Centro de Procesamiento de Datos (CPD).

La compañía cuenta con unos 80 ordenadores entre estaciones de trabajo y portátiles cifrados, que permiten el trabajo híbrido o remoto de sus empleados. La facturación anual de la empresa ronda los 3,5 millones de euros, con una tasa de crecimiento anual promedio del 12% desde el año 2020.

No se cuenta con un presupuesto en ciberseguridad lo bastante elevado como para introducir tantas medidas de protección como sería óptimo, por lo que parte del trabajo consistirá en la investigación del mercado con el objetivo de encontrar una serie de medidas desglosadas con el coste aproximado para que el cliente pueda seleccionar aquellas que se adapten a sus necesidades presupuestarias.

A lo largo del documento se explicará de forma detallada la metodología y procedimiento realizado durante el análisis, como ya se ha explicado, se emplea como base la metodología Magerit, aunque cabe destacar que en condiciones normales cada compañía suele tener una metodología propia y privada, creada a partir de las ya existentes. Dado que en este caso la compañía es ficticia y que el análisis es genérico emplearemos de base directamente una internacional.

También tendremos un apartado donde se mostrará la realización de este análisis mediante la herramienta Excel (a nivel profesional es la más empleada para este tipo de análisis), y tras esto se redactará un informe ejecutivo similar al que se redactaría en una situación real para el cliente.

3.2 Datos Iniciales

La parte vital de todo proyecto es la comunicación y consonancia con los deseos y expectativas del cliente. A la hora de realizar un análisis de riesgos y posteriormente una gestión de los mismos se deben conocer con precisión los siguientes aspectos:

- **Alcance del proyecto:**

  Activos en análisis: aquellos activos que vamos a analizar, dependiendo de la situación se nos puede solicitar que analicemos determinados activos de una zona en concreto, todo el edificio o incluso de toda la compañía. En esta última situación se emplean aquellos activos más valiosos y expuestos a las amenazas seleccionadas por infraestructura, además de que, para reducir el tiempo de trabajo, se escogen las infraestructuras de mayor relevancia o criticidad.

  Amenazas contempladas: amenazas que se emplearán durante el análisis, en este caso el cliente solo quiere gestionar la seguridad lógica por lo que nos limitaremos a amenazas de este tipo.

- **Medidas de seguridad ya existentes**: medidas que la empresa tiene implementadas en sus sistemas, estas son determinantes para poder realizar el cálculo del riesgo real existente.

- **Vías de comunicación**: todo lo relacionado con la comunicación dentro del proyecto: reuniones de seguimiento semanales, contactos a los que poder consultar dudas o valores necesarios para los cálculos, visitas a las instalaciones en caso de resultar necesarias…

- **Necesidades adicionales**: aquellas necesidades específicas del cliente y que suponen un esfuerzo adicional fuera de lo que sería estrictamente el análisis de riesgos y la gestión del mismo, algunos ejemplos de estas podrían ser:
    - Informes corporativos.
    - Presentación de resultados.
    - Presupuestos.
    - Seguimiento para la implementación de las medidas acordadas.

3.2.1 Activos

En este apartado se listan aquellos activos pertenecientes a la empresa contratista. Se valorarán aquellos activos que puedan ser vulnerables a alguna de las amenazas seleccionadas. De esta forma, al igual que el cliente no está interesando en la seguridad física de la infraestructura, no se tendrán en cuenta activos como el perímetro físico o las instalaciones.

Al igual que en el resto de los apartados se seleccionarán activos que sean lo suficientemente rigurosos con la realidad y que vaya acorde con las necesidades del cliente/proyecto.

Categoría	Activo	Descripción
Activos de información	Datos	Información necesaria para el correcto desarrollo del servicio.
	Discos	Discos físicos donde se almacena la información.
Equipo humano	Empleados internos	Personal interno especializado que lleva a cabo las labores relacionadas con el servicio llevado a cabo en la compañía.
	Personal externo	Personal externo especializado que lleva a cabo las labores relacionadas con el servicio llevado a cabo en la compañía.
Instalación (Recinto)	Sala de equipos	Salas en las que se encuentra el hardware asociado a los servicios llevados a cabo, pudiendo incluir elementos de comunicaciones.
	Sala de servidores	Salas en las que se encuentra el hardware de almacenamiento de datos
	CPD	Sala donde se ubica el CPD del Centro de Control
	Sala de control de mantenimiento	Sala de empleada para el control del mantenimiento de los activos de la infraestructura
	CPUs	CPUs físicas necesarias para procesar las operaciones del servicio.
Sistemas	Alimentación eléctrica	Línea eléctrica externa a la instalación que suministra la energía

auxiliares	externa	necesaria para su funcionamiento.
	Servicios de telecomunicaciones	Servicios contratados con una empresa de comunicaciones para voz y/o datos.
Sistemas de control	Conexiones remotas por VPN	Equipos que se conectan de manera remota al CC (Centro de control) mediante VPN.
	Red de Enlace	Enlaces comunicativos entre la infraestructura y el exterior de la misma.
	Consolas administración	Herramientas de administración de servidores que facilitan la gestión de los operadores (configuración de puertos de acceso, gestión de accesos, etc.)

Tabla 4: Listado de activos

Este listado, habitualmente viene con una serie de datos que el cliente proporciona, o que tendremos que conseguir de áreas dentro de la compañía como puede ser la de arquitectura, "infrastructure protection", negocio…

Para este ejercicio, dado que es un caso hipotético, obtendremos los datos en base a lo estándar en el mercado y mi experiencia profesional. Estos datos estarán relacionados con el tipo de metodología que estemos empleando, al usar como base la metodología Magerit, deberemos obtener la categorización de estos activos según las cinco dimensiones de seguridad, además de las interdependencias de estos mismos.

Estos datos se introducirán en una tabla en Excel, ya que es la forma más habitual de ejecución del análisis gracias a su capacidad de automatización y su flexibilidad ante el cambio. El uso de esta herramienta permite dejar abierta la puerta a modificaciones en el futuro, como pueden ser la adición de activos, amenazas, o incluso modificación de las ya establecidas.

				Categorización							
ID	Activos identificados	Categoría	Descripción	Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Autenticidad	Vulnerabilidad	Dependencias	Valor
1ACT	Sala de equipos	Instalación (Recinto)	Salas en las que se e	Alto	Bajo	Mediobajo	Bajo	Bajo	2		2
2ACT	Sala de servidores	Instalación (Recinto)	Salas en las que se e	Alto	Alto	Alto	Bajo	Mediobajo	4		4
3ACT	Conexiones remotas por VPN	Sistemas de Control	Equipos que se cone	Alto	Bajo	Alto	MedioBajo	Alto	4		3
4ACT	Empleados internos	Equipo humano	Personal interno esp	Medio	Bajo	Bajo	Bajo	Medio	2	4 -> 3	3
5ACT	Personal externos	Equipo humano	Personal externo es	Medio	Bajo	Bajo	Bajo	Medio	2	5 -> 3 , 5->4	2
6ACT	Alimentación eléctrica extern	Sistemas auxiliares	Línea eléctrica exter	Medio	Bajo	Bajo	Bajo	Bajo	5		4
7ACT	Red de Enlace	Sistemas de Control	Enlace entre la infra	Mediobajo	Bajo	Alto	Bajo	Bajo	3	7->8	4
8ACT	Servicios de telecomunicacio	Sistemas auxiliares	Servicios contratadc	Mediobajo	Bajo	Alto	Bajo	Bajo	2		3
9ACT	CPD	Instalación (Recinto)	Sala donde se ubica	Alto	Alto	Alto	Alto	Medio	5	9->6, 9->10	5
10ACT	Sala de control de mantenimi	Instalación (Recinto)	Sala de empleada p	Alto	Bajo	Bajo	Bajo	Medio	5		3
11ACT	Consolas administración	Sistemas de Control	Herramientas de ad	Bajo	Bajo	Bajo	Medio	Alto	2	11 -> 9	3
12ACT	Datos sensibles	Activos de informaci	Información necesa	Alto	Alto	Bajo	Medio	Alto	5		5
13ACT	CPUs	Instalación (Recinto)	CPUs físicas necesar	Bajo	Medio	Bajo	Bajo	Bajo	4		1
14ACT	Discos	Activos de informaci	Discos físicos donde	Bajo	Medio	Bajo	Bajo	Bajo	4		3
15ACT	Bases de datos	Activos de informaci	Conjunto de tablas (	Bajo	Medio	Medio	Bajo	Alto	4	15 -> 13, 15 ->14	4
16ACT	Firewalls y dispositivos de se	Sistemas de seguridá	Sistemas implement	Bajo	Bajo	Medio	MedioBajo	Alto	3	16 -> 7	3
17ACT	Sistemas Operativos	Activos digitales	Activos que permite	Bajo	Bajo	Bajo	Bajo	Bajo	2		1
18ACT	Aplicaciones	Activos digitales	Programas utilizado	Bajo	Bajo	Bajo	Bajo	Bajo	1		1
19ACT	Usuarios y cuentas de acceso	Activos de informaci	Datos utilizados por	Bajo	Bajo	Bajo	Medio	Alto	2	19 -> 17	2
20ACT	Servicios en la nube	Activos digitales	Servicios, aplicacion	Bajo	Bajo	Mediobajo	Bajo	Medio	1	20 -> 3	2
21ACT	Activos de respuesta a incide	Sistemas de seguridá	Programas o aplicac	Bajo	Bajo	Medio	MedioBajo	Bajo	1	21 -> 7	4

Tabla 5: Categorización de activos

Como vemos en el cuadro anterior las categorizaciones se obtuvieron en valores cualitativos pero estos pueden ser variados a cuantitativos para facilitar el uso de fórmulas. De igual manera que la categorización va desde Bajo hasta Alto, podemos hacer una transposición numérica siendo Bajo y Alto lo mismo que uno y cinco respectivamente.

Normalmente el valor de los activos es facilitado por el cliente, en este caso usaremos un valor estándar para cada uno de ellos. Por otro lado la vulnerabilidad se obtiene mediante una medición de las diferentes categorizaciones de las dimensiones de seguridad y los activos de los que depende cada uno

3.2.2 Amenazas

A continuación, se listará una serie de amenazas de tipo lógico, estas amenazas se han seleccionado de un muestreo general, aunque en una situación práctica real se podrían seleccionar las amenazas a discreción del cliente o de las necesidades del proyecto, los análisis de riesgos acostumbran a ser totalmente flexibles en estos aspectos.

Categoría	Amenaza	Descripción
Acciones ilegítimas contra el patrimonio	Ataques al patrimonio	Ciberataque - Acciones ilegítimas contra el patrimonio
	Robo de activos de información – intruder	Robo de activos de información por intruder (en papel, haciendo fotos, en usbs…) - Acciones ilegítimas contra el patrimonio
Actividad subversiva y/o Hack	Hack de páginas web	Hackeo de páginas web modificando el contenido (defacement)
	Robo y publicación de información confidencial	Robo y publicación de información confidencial
Ataque cibernético	Escalada de privilegios	Acceso no autorizado a sistemas corporativos y escalada de privilegios
	Ataque de denegación de servicio (DoS) – servicios	Ataque de denegación de servicio (DoS) hacia servicios y equipos críticos
	Ataque de denegación de servicio (DoS) – aplicaciones	Ataques denegación de servicio contra aplicaciones clave
	Cracking de contraseñas	Cracking contraseñas privilegiadas de elementos clave
	Daños en equipos	Daños o destrucción de equipos, material o información
	Vulnerabilidades software o de red	Detección de vulnerabilidades en el software y tipología de red y explotación de estas
	Distribución de virus	Infección de virus informáticos entre los diferentes activos de la compañía
	Filtración de información	Filtración de información sensible de la organización

	Ingeniería social	Ataques de ingeniería social dirigidos a personal de la corporación
	Phising	Ataques de Phishing hacia empleados de la organización
	Descubrimiento de información	Descubrimiento y enumeración de equipos y servicios desde el exterior
	Malware	Introducción de código malicioso
	Suplantación de IP	Suplantación de identidades de usuario e IP
	Uso ilícito de la red corporativa	Utilización de los sistemas de la red corporativa con fines ilícitos o fuera de los objetivos de la organización
Espionaje	Espionaje	Ciberataque - Espionaje
	Robo de activos de información - outsider	Robo de activos de información por intruder (en papel, haciendo fotos, en usbs…)
	Robo de activos de información - insider	Robo/Hurto de activos de información por insider (en papel, haciendo fotos, en usbs…)
Sabotaje	Ciberataque	Dada la extensa lista de tipologías de ciberataques se añade esta amenaza a modo de ciberataque genérico
	Pérdida de comunicaciones	Pérdida total o parcial de comunicaciones
Terrorismo	Terrorismo	Ciberataque - Terrorismo

Tabla 6: Listado de amenazas

Para este listado de amenazas y de forma similar a los activos anteriormente mostrados deberemos obtener dos datos en concreto, el primero consistirá en las dimensiones en las que estas amenazas tienen impacto real. Si una amenaza afecta a una dimensión en la que el activo no tiene problemas esa amenaza no aplicará a ese activo en concreto. El otro dato consistirá en la frecuencia de este tipo de ataques, este dato se puede obtener con relativa facilidad mediante la búsqueda en internet y estadísticas de medios de ciberseguridad.

				Categorización					
Amenaza	Categoría	Descripción	Frequencia	Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Autenticidad	Impacto potencial
Escalada de privilegios	Ataque cibernético	Acceso no autorizado a sistemas corporativos y escalada de privilegios	4	X	X		X		5
Ataque de denegación de servicio (DoS) – servicios	Ataque cibernético	Ataque de denegación de servicio (DoS) hacia servicios y equipos críticos o contra aplicaciones clave	4			X			5
Ataque de denegación de servicio (DoS) – aplicaciones	Ataque cibernético	Ataques denegación de servicio contra aplicaciones clave	3			X			4
Ciberataque	Sabotaje	Ciberataque - Sabotaje	2	X				X	5
Cracking de contraseñas	Ataque cibernético	Cracking contraseñas privilegiadas de elementos clave	5	X				X	5
Daños en equipos – Ataque cibernético	Ataque cibernético	Daños o destrucción de equipos, material o información - Ataque cibernético	2	X	X	X	X	X	4
Explotación de vulnerabilidades sofware	Ataque cibernético	Detección de vulnerabilidades en el software y tipología de red y explotación de estas	4	X	X				4
Distribución de virus	Ataque cibernético	Distribución de virus	3	X					3
Filtración de información	Ataque cibernético	Filtración de información sensible de la organización	4	X	X	X	X	X	5
Ingeniería social	Ataque cibernético	Ataques de ingeniería social dirigidos a personal de la corporación	5	X				X	4
Phising	Ataque cibernético	Ataques de Phising hacia empleados de la organización	5	X	X				3
Ataques al patrimonio	Acciones ilegítimas con	Ciberataque - Acciones ilegitimas contra el patrimonio	3	X			X		3
Espionaje	Espionaje	Ciberataque - Espionaje	3	X	X	X	X	X	5
Terrorismo	Terrorismo	Ciberataque - Terrorismo	1	X					5
Descubrimiento de información	Ataque cibernético	Descubrimiento y enumeración de equipos y servicios desde el exterior	5	X	X				2
Malware	Ataque cibernético	Introducción de código malicioso	4	X				X	5
Suplantación de IP	Ataque cibernético	Suplantación de identidades de usuario e IP	3		X				4
Uso ilícito de la red corporativa	Ataque cibernético	Utilización de los sistemas de la red corporativa con fines ilícitos o fuera de los objetivos de la organizack	2	X	X		X	X	4
Hack de páginas web	Actividad subversiva y/	Hackeo de páginas web modificando el contenido (defacement)	2						3
Robo de activos - General	Espionaje	Robo de activos de información por intruder (en papel, haciendo fotos, en usbs...) - Espionaje	3	X	X	X			4
Robo y publicación de información confidencial	Actividad subversiva y/	Robo y publicación de información confidencial	4	X			X		5
Robo de activos de información - insider	Espionaje	Robo/Hurto de activos de información por insider (en papel, haciendo fotos, en usbs...)	3	X			X		5
Robo de activos de información	Acciones ilegítimas con	Robo de activos de información por intruder (en papel, haciendo fotos, en usbs...) - Acciones ilegitimas c	2	X					3
Perdida de comunicaciones	Sabotaje	Pérdida total o parcial de comunicaciones	3			X			4

Tabla 7: Categorización de amenazas

Aquellas dimensiones con una X en su celda corresponden a las dimensiones donde la amenaza tiene efecto.

A continuación se muestra una tabla con los valores vistos en la tabla anterior justo con la justificación de cada uno de ellos:

Amenaza	Frecuencia (1-5)	Justificación Frecuencia	Impacto (1-5)	Justificación Impacto
Escalada de privilegios	4	80% de brechas usan credenciales comprometidas (Infrodisa) [6]	5	Compromete sistemas críticos y datos sensibles
Ataque DoS a servicios/equipos críticos	4	58% de empresas reportan ≥1 ataque DoS anual (Cloudflare 2023) [7]	5	Paraliza operaciones: pérdidas >€100k/hora en sectores críticos.
Ataque DoS a aplicaciones clave	3	58% de empresas reportan ≥1 ataque DoS anual (Cloudflare 2023) [7]	4	Impacta experiencia de cliente
Ciberataque - Sabotaje	2	Raro pero en aumento	5	Destrucción irreversible de datos/infraestructura.
Cracking de contraseñas privilegiadas	5	Aumento de ataques de robo de información y advierte de que la compraventa de credenciales (CCN-CERT) [8]	5	Acceso a cuentas admin = control total del sistema.
Daños/destrucción de equipos (cibernético)	2	Típico en ataques dirigidos	4	Coste reposición + tiempo inactividad.
Explotación de vulnerabilidades SW/red	4	60% de brechas explotan vulnerabilidades conocidas (IBM X-Force) [9]	4	Puerta de entrada para múltiples amenazas
Distribución de virus	3	Menos relevante hoy	3	Controles modernos reducen impacto.
Filtración de información sensible	4	62% de las empresas latinoamericanas reconoce haber sufrido filtración de datos (EY) [10]	5	Multas GDPR (hasta 4% facturación) + daño reputacional.
Ingeniería social a personal	5	98% de incidentes la usan (Connectab2b) [11]	4	Facilita brechas profundas
Phishing a empleados	5	Ataques diarios a cualquier tipo de usuario	3	Impacto depende del rol comprometido.
Acciones ilegítimas contra patrimonio	3	Común en retail/logística	3	Robo físico de hardware/datos.
Ciberespionaje	3	Frecuente en sector defensa/tech	5	Pérdida de propiedad intelectual.
Ciberterrorismo	1	Muy raro en PYMEs	5	Impacto nacional en infraestructuras críticas.
Descubrimiento de información	5	Escaneos automáticos constantes	2	Primer paso para ataques, impacto directo bajo.
Introducción de código malicioso	4	62% en supply chain attacks (Sonatype 2024) [12]	5	Infección persistente
Suplantación de identidades/IP	3	Común en entornos cloud	4	Fraudes financieros o acceso a datos.
Uso ilícito de red corporativa	2	Asociado a insiders	4	Minado de criptomonedas/hosting ilegal.
Hack de páginas web	2	Menos frecuente desde 2020	3	Daño reputacional reversible.
Robo de información por intruder (espionaje)	3	Relevante en entornos con acceso físico no controlado	4	Filtración de secretos comerciales.
Robo/publicación información confidencial	4	Aumento en foros dark web	5	Multas regulatorias + pérdida de clientes.
Robo de información por insider	3	Mas habitual en grandes empresas	5	Difícil detección + alto acceso privilegiado.
Robo de información por intruder (patrimonio)	2	Mas habitual en grandes empresas	3	Valor de la información física robada.
Pérdida de comunicaciones	3	Frecuente en ataques a ISPs	4	Bloqueo operativo temporal.

Tabla 8: Justificación de valores de amenazas

3.3 Cálculo del Riesgo Inherente

Mediante los datos anteriormente obtenidos tendremos que realizar una serie de cálculos hasta llegar a obtener el riesgo inherente de cada uno de los activos. Comenzaremos calculando la probabilidad de éxito de la amenaza,

para ello emplearemos la siguiente fórmula:

$$P = F \times V$$

Siendo:

- **P (Probabilidad de éxito de la Amenaza) :** Es la posibilidad de que una amenaza se materialice con éxito. Se puede expresar en términos cualitativos (baja, media, alta) o cuantitativos (porcentaje, eventos por año)**.**

- **V (Vulnerabilidad):** Es cuan fácilmente atacable es un activo según su sensibilidad y exposición a las diferentes dimensiones.

- **F (Frecuencia):** Es la cantidad de veces que una amenaza se manifiesta en un periodo de tiempo (por ejemplo, al año).

Esta es la fórmula empleada para los cálculos realizados que pueden observarse en la tabla 12 del Anexo.

Para mantener la consistencia con el resto del análisis, en el propio cálculo emplearemos una transposición para escalar el resultado entre 1 y 5, de esta forma será más fácil aplicar los datos obtenidos con anterioridad y sacar conclusiones cualitativas para los informes ejecutivos.

Con las probabilidades calculadas ahora deberemos aplicarlas, sin embargo, debemos saber cuál sería la aplicación de las amenazas respecto a los activos ya que no todos los activos se ven amenazados por todas las amenazas seleccionadas. En la tabla 13 del Anexo se puede ver como se marcan las amenazas a las que aplicaría cada uno de los activos.

En caso de que la amenaza afecte a una dimensión donde el riesgo del activo en la misma sea bajo entonces esa amenaza no aplicará para ese mismo activo. Además deberemos calcular el daño que sufriría cada uno de estos activos en caso de que la amenaza se materializa sobre el mismo, para ello emplearemos la siguiente fórmula:

$$I = Val \times IP$$

Siendo:

- **I (Impacto)**
- **Val (valor del activo)**: también se le conoce como valor, pero la diferencia es únicamente terminológica
- **IP (impacto potencial de la amenaza)**: al igual que con la vulnerabilidad, también se le conoce como degradación, daño, nivel de amenaza…

Realizamos el cálculo del riesgo inherente mediante los datos calculados

anteriormente, pintaremos con distintas tonalidades los resultados obtenidos, a partir de riesgos medios ya son amenazas a tener en cuenta, aunque faltaría aplicar las medidas de seguridad ya implementadas en la compañía para poder obtener conclusiones. En la tabla 14 del Anexo además de realizar los cálculos se marcan mediante colores para poder tener una primera impresión de los resultados aunque más adelante obtendremos una serie de gráficas que nos permitirán tener una visión más generalizada.

3.4 Salvaguardas y Calculo del Riesgo Residual

El riesgo inherente nos permite ver qué activos están más afectados por las amenazas contempladas, en este caso la compañía tiene ciertas medidas de seguridad aplicadas, y estas deberán de tomarse en cuenta para realizar un análisis adecuado, empezaremos listando las medidas de seguridad (también llamadas salvaguardas) y definiendolas para así mas adelante poder determinar la efectividad de las mismas.

Salvaguarda	Descripción
Firewalls	Son dispositivos de seguridad que se utilizan para controlar y filtrar el tráfico de red, tanto entrante como saliente, basándose en un conjunto de reglas predefinidas. Su objetivo principal es proteger una red informática al bloquear o permitir el acceso a recursos según políticas de seguridad establecidas.
Identity and Access Management (IAM)	Es un conjunto de procesos, políticas y tecnologías utilizadas para gestionar y asegurar la identidad digital de usuarios, empleados y otras entidades dentro de una organización. El IAM abarca la administración de accesos, la autenticación, la autorización y la gestión de privilegios.
Cifrado de Datos	Es el proceso de convertir datos en un formato ilegible o cifrado, mediante algoritmos matemáticos y claves criptográficas, con el fin de proteger su confidencialidad y seguridad durante su almacenamiento o transmisión. Solo los usuarios autorizados con la clave de descifrado adecuada pueden acceder y leer los datos cifrados.
Sistema de Antivirus	Es un software diseñado para detectar, prevenir y eliminar programas maliciosos, como virus, gusanos, troyanos, spyware y otros tipos de malware, de los sistemas informáticos. Los sistemas de antivirus escanea archivos y actividades en busca de signos de actividad maliciosa, y toman medidas para neutralizar las amenazas identificadas.

Tabla 9: Listado de medidas de seguridad

Parte de labor del analista es la de juzgar en base a sus conocimientos, de la madurez de implementación y la configuración de las medidas de seguridad, el nivel de protección que pueden tener frente a las diferentes amenazas. En base a esto se ha realizado el siguiente cuadro con las categorizaciones de cada una de las salvaguardas según cada una de las amenazas previstas:

			Medidas de seguridad				Medidas de seguridad					
			Firewalls	Sistema de Antivirus	Sistema de Gestión de Identidades (IAM)	Cifrado de Datos	Firewalls	Sistema de Antivirus	Sistema de Gestión de Identidades (IAM)	Cifrado de Datos		
	Nombre	Tipología	Efectividad				Ponderación				Total Cuantitativo	Total Cualitativo
Amenaza	Escalada de privilegios	Ataque cibernético	0,2	0,2	0,3	0,3	0,2	0,1	0,9	0,5	0,48	Medio
	Ataque de denegación de servicio (DoS) – servicios	Ataque cibernético	0,3	0,1	0,3	0,2	0,7	0,1	0,1	0	0,25	Bajo
	Ataque de denegación de servicio (DoS) – aplicaciones	Ataque cibernético	0,3	0,1	0,3	0,2	0,6	0,1	0,1	0	0,22	Bajo
	Ciberataque	Sabotaje	0,3	0,3	0,3	0,3	0,6	0,5	0,4	0,3	0,54	Medio
	Cracking de contraseñas	Ataque cibernético	0,1	0,1	0,2	0,3	0,2	0	0,8	0,6	0,36	Bajo
	Daños en equipos – Ataque cibernético	Ataque cibernético	0,2	0,3	0,2	0,2	0,5	0,6	0,3	0,1	0,36	Bajo
	Explotación de vulnerabilidades sofware	Ataque cibernético	0,3	0,3	0,2	0,2	0,4	0,3	0,6	0,2	0,37	Bajo
	Distribución de virus	Ataque cibernético	0,2	0,3	0,2	0,2	0,3	0,9	0,3	0,1	0,41	Medio
	Filtración de información	Ataque cibernético	0,2	0,1	0,3	0,3	0,3	0,2	0,6	0,9	0,53	Medio
	Ingeniería social	Ataque cibernético	0,2	0,2	0,2	0,2	0,1	0,1	0,7	0,6	0,3	Bajo
	Phising	Ataque cibernético	0,1	0,2	0,3	0,2	0,3	0,4	0,8	0,4	0,43	Medio
	Ataques al patrimonio	Acciones ilegítimas contra el patrimonio	0	0	0	0	0,3	0,1	0,4	0,5	0	Muy Bajo
	Espionaje	Espionaje	0,3	0,3	0,3	0,3	0,2	0,1	0,6	0,8	0,51	Medio
	Terrorismo	Terrorismo	0	0	0	0	0,4	0,1	0,2	0,3	0	Muy Bajo
	Descubrimiento de información	Ataque cibernético	0,2	0,2	0,3	0,3	0,2	0,1	0,5	0,7	0,42	Medio
	Malware	Ataque cibernético	0,2	0,3	0,2	0,2	0,4	0,9	0,3	0,2	0,45	Medio
	Suplantación de IP	Ataque cibernético	0,3	0,1	0,3	0,3	0,6	0	0,4	0,1	0,33	Bajo
	Uso ilícito de la red corporativa	Ataque cibernético	0,3	0,2	0,2	0,2	0,7	0,2	0,6	0,3	0,43	Medio
	Hack de páginas web	Actividad subversiva y/o Hack	0,3	0,3	0,3	0,2	0,5	0,2	0,5	0,4	0,44	Medio
	Robo de activos de información	Espionaje	0,2	0,2	0,3	0,3	0,3	0,2	0,6	0,9	0,55	Medio
	Robo y publicación de información confidencial	Actividad subversiva y/o Hack	0,2	0,2	0,3	0,3	0,2	0,1	0,7	0,9	0,54	Medio
	Robo de activos de información - insider	Espionaje	0,2	0,2	0,3	0,3	0,2	0,1	0,9	0,8	0,57	Medio
	Robo de activos de información - intruder	Acciones ilegítimas contra el patrimonio	0,2	0,2	0,3	0,3	0,5	0,3	0,7	0,8	0,61	Alto
	Perdida de comunicaciones	Sabotaje	0	0	0	0	0,3	0	0,2	0,1	0	Muy Bajo

Tabla 10: Categorización de las medidas de seguridad

El total cualitativo obtenido es el valor que emplearemos para calcular el riesgo residual, es decir, el riesgo real que aplicaría para los activos. Los datos resultantes los veremos en el siguiente apartado, este simulará un informe real de resultados, es decir, tendrá el mismo formato que el informe que en este caso práctico entregaremos al cliente.

3.5 Informe de Resultados

3.5.1 Valoración de activos

Mediante la metodología magerit podemos realizar una valoración de cada activo según las cinco dimensiones de la seguridad. Estas valoraciones nos permiten medir el nivel de vulnerabilidad que tendrá un activo en total. Estas cinco dimensiones son:

- Confidencialidad [c]
- Integridad [I]
- Disponibilidad [D]
- Trazabilidad [T]
- Autenticidad [A]

Tras realizar este análisis con los activos que se han propuesto para la gestión de riesgos obtendremos una tabla con los siguientes resultados:

ACTIVOS	[c]	[I]	[D]	[T]	[A]
Sala de equipos	Alto	Bajo	Medio	Bajo	Bajo
Sala de servidores	Alto	Alto	Alto	Bajo	Medio
Conexiones remotas por VPN	Alto	Bajo	Alto	Medio	Alto
Empleados internos	Medio	Bajo	Bajo	Bajo	Medio
Personal externos	Medio	Bajo	Bajo	Bajo	Medio
Alimentación eléctrica externa	Medio	Bajo	Bajo	Bajo	Bajo
Red de Enlace	Medio	Bajo	Alto	Bajo	Bajo
Servicios de telecomunicaciones	Medio	Bajo	Alto	Bajo	Bajo
CPD	Alto	Alto	Alto	Alto	Medio
Sala de control de mantenimiento	Alto	Bajo	Bajo	Bajo	Medio
Consolas administración	Bajo	Bajo	Bajo	Medio	Alto
Datos sensibles	Alto	Alto	Bajo	Medio	Alto
CPUs	Bajo	Medio	Bajo	Bajo	Bajo
Discos	Bajo	Medio	Bajo	Bajo	Bajo
Bases de datos	Bajo	Medio	Medio	Bajo	Alto
Firewalls y dispositivos de seguric	Bajo	Bajo	Medio	Medio	Alto
Sistemas Operativos	Bajo	Bajo	Bajo	Bajo	Bajo
Aplicaciones	Bajo	Bajo	Bajo	Bajo	Bajo
Usuarios y cuentas de acceso	Bajo	Bajo	Bajo	Medio	Alto
Servicios en la nube	Bajo	Bajo	Medio	Bajo	Medio
Activos de respuesta a incidentes	Bajo	Bajo	Medio	Medio	Bajo

Tabla 11: Resultados sobre activos

3.5.2 Amenazas

Las amenazas planteadas para el análisis requieren, de igual manera que para los activos, de un análisis que permita juzgar tanto la aplicabilidad respecto al activo al que pueda afectar como la probabilidad de éxito de la propia amenaza y el impacto potencial que pueda llegar a tener.

El impacto se valora en consecuencia a, no solo el daño operacional, sino también a otros daños como pueden ser el reputacional, el de mercado, etc.

De esta forma se obtiene el siguiente análisis:

				Categorización				
Categoría	Amenaza	Frequencia	Impacto potencial	[c]	[I]	[D]	[T]	[A]
Acciones ilegítimas contra el patrimonio	Ataques al patrimonio	1	4		X	X	X	X
	Robo de activos de información - intruder	2	2	X	X	X		
Actividad subversiva y/o Hack	Hack de páginas web	4	2		X	X		
	Robo y publicación de información confidencial	3	1	X				
Ataque cibernético	Escalada de privilegios	5	5	X	X			X
	Ataque de denegación de servicio (DoS) – servicios	4	1			X		
	Ataque de denegación de servicio (DoS) – aplicaciones	4	1			X		
	Cracking de contraseñas	2	1	X				X
	Daños en equipos – Ataque cibernético	1	5		X			
	Explotación de vulnerabilidades sofware	3	5	X	X			
	Distribución de virus	2	3	X	X		X	X
	Filtración de información	2	4	X				
	Ingeniería social	5	5	X	X		X	X
	Phising	4	1	X				
	Descubrimiento de información	1	5	X				
	Malware	2	1	X	X		X	X
	Suplantación de IP	3	5		X			
	Uso ilícito de la red corporativa	3	3	X	X		X	X
Espionaje	Espionaje	1	2	X				
	Robo de activos de información	3	3	X	X	X		
	Robo de activos de información - insider	5	4	X	X	X		
Sabotaje	Ciberataque	3	1	X	X	X	X	X
	Pérdida de comunicaciones	4	2			X	X	X
Terrorismo	Terrorismo	1	3	X				

Tabla 12: Categorización y análisis de amenazas

3.5.3 Resultados del Análisis de Riesgos

Como hemos mencionado anteriormente, vamos a proceder a realizar los diferentes cálculos necesarios para realizar el análisis de riesgos. Para poder calcular la probabilidad de amenaza sobre un a activo se debe emplear la fórmula de la Probabilidad de éxito de amenaza que se ha definido anteriormente.

$$P = F \times V$$

Otro dato necesario para el cálculo del riesgo inherente es el cálculo del impacto sobre los activos en función de la vulnerabilidad de los activos y el impacto de las amenazas sobre ellos:

$$I = Val \times IP$$

Cada uno de estos factores se define de la siguiente manera:

- **I (Impacto)**: Es el daño esperado en caso de que la amenaza se materialice.

- **Val (Valor del activo)**: Representa qué tan expuesto está el activo a la amenaza (valor entre 0 y 1, donde 1 es totalmente vulnerable).

- **IP (Impacto potencial de la amenaza)**: Es la magnitud del daño que la amenaza puede causar si se materializa (puede expresarse en una escala cualitativa o cuantitativa).

Tras el cálculo de la probabilidad de éxito de la amenaza deberemos aplicarla a los diferentes activos para saber el riesgo potencial o "riesgo inherente". Mediante la siguiente formula obtendremos los nuevos datos:

$$\text{Riesgo Inherente} = \text{Probabilidad} \times \text{Impacto}$$

- **Riesgo Inherente:** Nivel de riesgo natural que existe en un sistema o proceso antes de aplicar cualquier medida de control o salvaguarda. Es el riesgo asociado a la exposición de un activo frente a una amenaza sin ninguna intervención para reducir su probabilidad de ocurrencia o el impacto de su materialización.
- **Probabilidad de éxito**: Representa la probabilidad de que una amenaza específica se materialice y afecte un activo. Se mide en una escala que puede ser cualitativa (por ejemplo, baja, media, alta) o cuantitativa (por ejemplo, un valor entre 0 y 1).
- **Impacto**: Representa la magnitud de las consecuencias que la materialización de la amenaza tendría sobre el activo. Al igual que la probabilidad, puede ser medido de manera cualitativa (bajo, medio, alto) o cuantitativa (un valor numérico representando la severidad del impacto).

Los cálculos se realizan sobre una tabla donde se cruzan los activos para

todas las amenazas que son de aplicación para los mismos. Cada uno de estos cruces nos indicaran el riesgo de el activo con la amenaza concreta que le corresponda. Una vez obtenida la tabla completa podemos sacar las siguientes gráficas para ilustrar el nivel de riesgo general para la compañía.

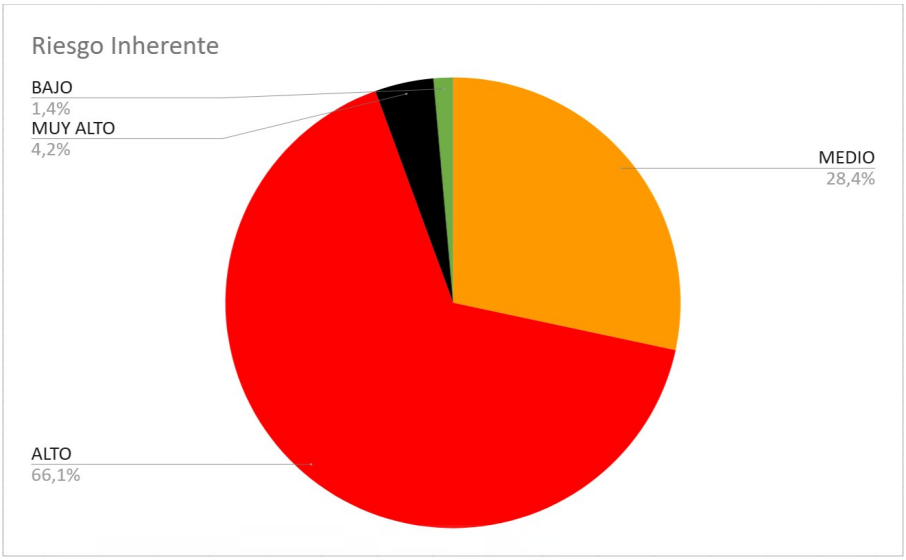

Figura 4: Gráfica sobre el riesgo inherente

El riesgo inherente, como ya se ha explicado, indica el nivel de riesgo que tienen los activos, sin tener en cuenta las medidas de seguridad ya implantadas, es decir, indica el riesgo en bruto a los que están expuestos los activos. Como podemos observar encontramos riesgos de gran preocupación como los 4,2% de riesgo MUY ALTO y el 66,1% de riesgo ALTO, por otra parte el riesgo BAJO es casi inexistente y el riesgo MEDIO es esta en unos margenes relativamente aceptables, dependiendo del apetito al riesgo del cliente.

A continuación aplicaremos estas medidas para averiguar cual es el riesgo real o “riesgo residual” con el que estamos trabajando. La fórmula empleada es la siguiente:

$$RR = (I \times P) \times (1 - E)$$

- **Riesgo Residual:** Es el riesgo que queda después de aplicar controles o salvaguardas de seguridad. Representa la amenaza que sigue existiendo a pesar de las medidas implementadas.
- **Riesgo Inherente (I×P):** El riesgo inherente es el nivel de riesgo al que está expuesto un activo antes de aplicar cualquier control o salvaguarda. Representa la vulnerabilidad natural del sistema

sin mitigaciones.

- **Eficacia de las salvaguardas aplicadas:** Es el grado en que las medidas de seguridad reducen el riesgo.

El resultado obtenido de este cálculo es el siguiente:

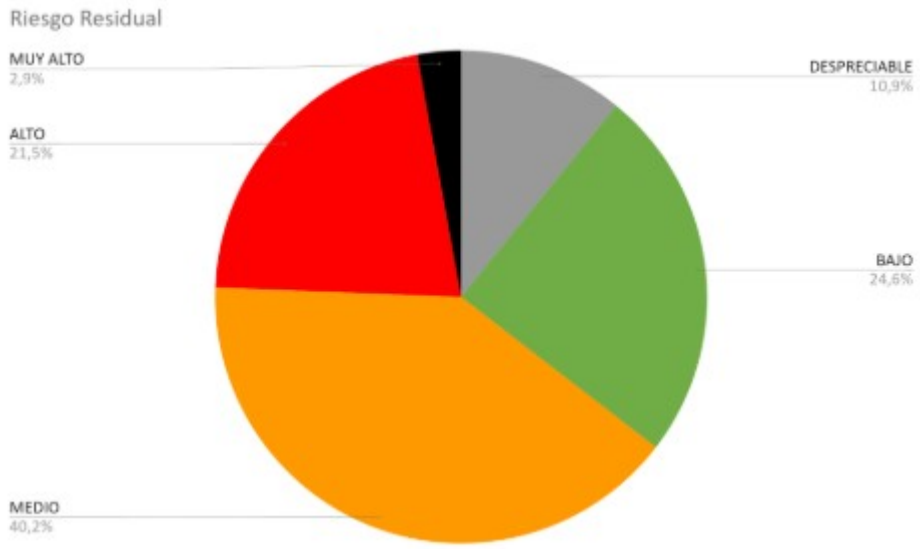

Figura 5: Gráfica sobre el riesgo residual

Como podemos observar las medidas de seguridad han permitido un gran descenso en los riesgos, reduciendo casi a la mitad (2.9%) el riesgo MUY ALTO y el riesgo ALTO pasa a ser prácticamente un tercio de los resultados anteriores (21,5%) aun así, y teniendo en cuenta el apetito al riesgo de la compañía deberemos solventar completamente los riesgos preocupantes (MUY ALTO y ALTO) por completo, además de reducir los riesgos medios, que aun no siendo tan perjudiciales como el resto, la gran cantidad que presentan pueden resultar peligrosos.

A continuación se recomendarán una serie de medidas de seguridad que podrían ayudar con el control de estos, dado que no tenemos un presupuesto fijo, se intentará abarcar un amplio abanico de opciones y se justificarán los gastos tanto económicos como de personal que la compañía deberá realizar en caso de querer aplicarlos.

3.5.4 Ampliación en caso del uso de dependencias de forma explícita

En apartados anteriores se ha mencionado que se ha optado por no modelar explícitamente las dependencias entre activos, a pesar de ser un componente clave de MAGERIT. Esta decisión se justifica por los siguientes motivos:

- **Sobrestimación de Riesgos**
  - En experiencias previas, se observó que incluir dependencias sin datos precisos lleva a resultados inflados.

- Para este ejercicio, se priorizó la claridad y la aplicabilidad práctica frente al rigor teórico.

- **Compensación Metodológica**

  - Se compensó la omisión de dependencias asignando valores de vulnerabilidad elevados a los activos más críticos (como servidores o firewalls), simulando indirectamente su dependencia de otros sistemas de soporte.

- **Búsqueda de realismo**

  - En la práctica profesional, las organizaciones medianas como *Data ESP* raramente disponen de recursos para:

    - Mapear exhaustivamente todas las interconexiones técnicas.

    - Mantener actualizada esta información en arquitecturas dinámicas.

  - La experiencia profesional muestra que as pymes tecnológicas priorizan análisis ágiles sobre exhaustividad.

A modo de ejemplo practico para contextualizar su utilización se presenta a continuación un escenario reducido y alternativo donde sí se considerarian las dependencias de forma explicita:

- **Activos y dependencias**

  - A1: Servidor de aplicaciones (Valor:5). Depende de A2.

  - A2: Firewall (Valor: 4). Depende de A3.

  - A3: Sistema de alimentación initerrumpida (SAI) (Valor:3).

  - Amenaza: Fallo del SAI (A3).

- **Calculo con Dependencias**

  - Impacto directo en A3:

    Empleando la formula del impacto:

    3 (valor del activo) x 4 (impacto potencial de la amenaza) = 12

  - Impacto repercutido en A2 (depende de A3):

    4 (valor del activo) x 4 (impacto potencial de la amenaza) = 16 → Total para A2: 16 + 12 = 28

- Impacto repercutido en A1 (depende de A2):

  5 (valor del activo) x 4 (impacto potencial de la amenaza) = 20 → Total para A1: 20 + 28 = 48

Como podemos observar en el ejemplo indicado, el impacto final calculado para A1 aumenta en gran medida respecto al valor que obtendríamos si se evaluase individualmente. Aunque este calculo puede ayudar a obtener una visión clara de los activos con mayor peligro por las dependencias que les afectan, también infla de forma irreal el riesgo de estos activos.

3.6 Propuesta de Medidas

En este apartado se citarán una serie de medidas de seguridad que podrían aplicarse para poder resolver los riesgos anteriormente calculados. Dividiremos estas medidas en dos grupos principales, las medidas de implementación, que requerirán de un esfuerzo extra por parte de la compañía para poder desarrollarlas e implementarlas y las medidas de contratación donde únicamente se necesitará un gasto económico.

3.6.1 Medidas de implementación

Las medidas de implementación son aquellas medidas que, además del gasto económico que conllevan, también necesitarán de tiempo y personal que las implementen y las pongan en funcionamiento. Aquí podemos distinguir las medidas lógicas y las organizativas.

Para todas las medidas que se van a nombrar a continuación se va a requerir de los siguientes esfuerzos por parte de la compañía:

- **Equipo de seguimiento**: el equipo de seguimiento consta de un grupo de personas que se encargaran de seguir todo el proceso de vida de la medida de seguridad. Realizarán planificaciones y se encargará de solventar aquellos problemas que puedan llegar a tener los desarrolladores. Una vez implementada la salvaguarda su función será la de realizar verificaciones periódicas para asegurar la madurez y buen funcionamiento de la misma.

- **Equipo de desarrollo**: este equipo estará formado principalmente por especialistas en el campo en el que se va a elaborar la medida de seguridad, por ejemplo en caso de una medida organizativa como puede ser una política de seguridad, los encargados de realizarla serán ejecutivos con experiencia en ciberseguridad, en caso de ser una medida lógica se encargará de su desarrollo perfiles técnicos con experiencia en el campo de aplicabilidad.

- **Equipo de implementación**: serán los encargados de trabajar sobre la medida implementada, este equipo no estará presente en todas las medidas, únicamente en aquellas que requieran de personal para llevarla a cabo, como puede ser un SOC (Security Operation Center) de seguridad.

Estos equipos necesitan tiempo, presupuestos y personal para poder realizar su trabajo. Dependiendo de la cantidad de cada una de las necesidades de las que se disponga el esfuerzo final de proyecto puede ser mayor o menor, siempre se puede compensar con alguna de las otras necesidades, por ejemplo si se tiene poco tiempo pero mucho personal para su desarrollo, el uso de este personal puede permitir llegar a estos ajustados tiempos.

Figura 6: Esquema del esfuerzo final

En este caso el desglose de medidas y presupuestos propuestos tienen unos rangos nivel económico de gran envergadura, esto es debido a diferentes factores que pueden determinar el coste total de implementación. Por ejemplo el alcance, la necesidad o no de contratar equipos externos para ejecutar el proyecto o la necesidad de desarrollar o contactar aplicaciones a terceros.

3.6.1.1 Medidas de tipo lógico

Las medidas de seguridad de tipo lógico son aquellas que se implementan mediante software y controles técnicos para proteger los sistemas de información, datos y redes de amenazas y accesos no autorizados.

- **Implementación de un Security Information and Event Management (SIEM)** : se refiere al proceso de despliegue y configuración de una solución tecnológica diseñada para recopilar, relacionar, analizar y gestionar eventos de seguridad en tiempo real en una red de sistemas informáticos. Estos eventos pueden incluir actividades como accesos de usuarios, intentos de intrusión, cambios en la configuración de sistemas, entre otros, que pueden ser indicativos de actividades maliciosas o incidentes de seguridad. Siguiendo el estándar definido por la ISO 27001 [13], esta medida sería extremadamente recomendable del cliente ya que define que se deben implementar soluciones que puedan monitorizar los eventos de seguridad con el objetivo de detectar actividades anómalas.
    - **Funciones**: recopilación de datos, correlación de eventos, generación de alertas, análisis forense…
    - **Presupuesto**:
        - Coste anual: 5.000€ - 50.000€ dependiendo de si se incluyen herramientas comerciales (Splunk, IBM QRadar, ArcSight, Wazuh SIEM, Elasticsearch, etc.), licencias por volumen de eventos (EPS), infraestructura y consultoría.
          .
    - **Recursos Humanos**:
        - 3 - 5 trabajadores para la implementación inicial (6-12 meses).
        - 2 - 3 trabajadores para el mantenimiento continuo y la monitorización.

  Debido a los datos facilitados por la compañía, la mejor recomendación seria emplear el software de Wazuh SIEM + Elasticsearch, su coste aproximado seria de 5.000€ al año ya que Wazuh es de uso gratuito y permite una fácil escalabilidad, es compatible con VPNs, logs de firewall y antivirus, se trata de una opción mas económica que otras marcas del mercado y en este caso podría cumplir perfectamente su función sin elevar en gran medida el coste.

- **Gestión de parches y actualizaciones**: muchas de las vulnerabilidades de las compañías vienen por parte de software obsoleto o que no ha sido actualizado en bastante tiempo. Los distribuidores de aplicaciones lanzan continuamente parches que permiten la correcciones de errores y vulnerabilidades en su software. Siguiendo el estándar de la ISO 27001 que explicita la necesidad de realizar actualizaciones de seguridad periódicas y prioritarias.
    - **Funciones**: Identificación de vulnerabilidades, evaluación de parches, planificación y programación, implementación de parches.
    - **Presupuesto**:

        - Implementación inicial: 20.000€ - 55.000€ incluyendo automatización parcial (Windows Server Update Services [WSUS], System Center Configuration Manager [SCCM], Ansible, etc.), formación y procedimientos iniciales..
        - Mantenimiento anual: 5.000€ - 20.000€ (puede ser mayor dependiendo de la complejidad del entorno).
    - **Recursos Humanos**:
        - 2 trabajadores para la implementación inicial (2-4 meses).
        - 1 - 2 trabajadores para el mantenimiento continuo y la monitorización

La mejor recomendación para la gestión de parches consistiría en una solución híbrida entre WSUS (gratuito para windows) y Ansible (código abierto). WSUS permite mantener una gestión de Windows centralizada, manteniendo los parches y actualizaciones al día evitando que se emplee software obsoleto. Por su parte Ansible gestionaría automáticamente las actualizaciones para los servidores Linux de forma similar a WSUS. Estas dos soluciones proporcionarían mensualmente reportes sobre los parches implementados, los procedimientos estas totalmente documentados y se pueden otorgar roles definidos por activo y criticidad. El coste aproximado de ambas aplicaciones estaría entre 10.000€ y 15.000€ entre implementación, formación del personal, licencias, etc.

- **Implementación de un sistema "Autenticación multifactor" (MFA)** : es una medida de seguridad esencial para proteger el acceso a los sistemas y datos sensibles de una organización. El MFA requiere que los usuarios proporcionen dos o más formas de autenticación antes de permitirles el acceso, lo que hace que sea considerablemente más difícil para los atacantes obtener acceso no autorizado incluso si obtienen credenciales de usuario válidas. Esta medida se recomienda en alineación del estándar principal de NIST SP 800-63B [14] donde se exige que existan por lo menos dos factores para acceder a sistemas críticos.
    - **Presupuesto**:
        - Implementación inicial: 1.500€ - 20.000€ si hablamos de soluciones como Azure MFA, Duo, Microsoft Authenticator, Google Auth, o tokens físicos en entornos pequeños-medios puede aumentar en mayores entornos.
        - Mantenimiento anual: 5.000€ - 20.000€ se han tomado cifras algo elevado suponiendo licencias per-user.
    - **Recursos Humanos**:
        - 2 trabajadores para la implementación inicial (4-8 meses).

        - 1 - 2 trabajadores para el mantenimiento continuo y la monitorización

En este caso se recomendaría el uso de múltiples aplicaciones. Por una parte se emplearía DUO Security como sistema base por la flexibilidad y escalabilidad que ofrece. Microsoft Authenticator (incluido en licencias Azure) en caso de que haya una integración fuerte con Microsoft. Para los administradores de red y aquellos con acceso a infraestructura critica se recomendaría YubiKeys y tokens físicos para los administradores e ingenieros de red. El coste de implementación seria de entre 10.000€ y 15.000€ con un añadido de 3€ por usuario al mes.

- **Configuración de un sistema de detección y prevención de intrusiones (IDS/IPS)** : herramienta de seguridad informática diseñada para monitorear y analizar el tráfico de red en busca de actividades sospechosas o maliciosas, con el fin de detectar y prevenir intrusiones en la red. Siguiendo el estandar de NIST SP 800-41 [15] sobre la protección perimetral con inspección profunda de paquetes.
    - **Funciones**: monitoreo del tráfico, detección de anomalías y de firmas, generación de alertas, bloqueo activo…
    - **Presupuesto**:
        - Implementación inicial: 35.000€ - 70.000€ según si se usa un IDS como Snort/Suricata o soluciones comerciales tipo Cisco Firepower, Palo Alto, Fortinet, etc..
        - Mantenimiento anual: 5.000€ - 45.000€ aunque normalmente se sitúa entre 10.000 € y 25.000 € en empresas medianas..
    - **Recursos Humanos**:
        - 2 - 4 trabajadores para la implementación inicial (2 - 3 meses).
        - 1 - 3 trabajadores para el mantenimiento continuo y la monitorización, dependiendo de si existe SOC interno, aunque en este ejemplo no se ha especificado.

Para esta medida de seguridad habrá una solución que dependerá del uso de VPNs, en este caso se recomienda FortiGate o Cisco con módulos IDS/IPS activos debido a que ofrecen una alta capacidad de inspección en tiempo real, soporte técnico especializado, y actualizaciones automáticas de firmas. Para los servidores clave y el trafico interno de la compañía se recomendaría Suricata + Wazuh ya que no solo son gratuitas si no que son muy potentes para el tráfico interno, detección de comportamiento anómalo y monitoreo continuo de

servidores, pero requieren más gestión manual. El coste estimado de estas implementaciones seria de entre 35.000€ y 55.000 € con un mantenimiento anual de 12.000€ y 20.000 €, si finalmente no fuese necesario emplear FortiGate o Cisco el coste bajaría entre 20.000€ y 35.000€

Las estimaciones calculadas en cuanto a presupuesto anual/puntual se han realizado calculado en total de los gastos en los gastos de hardware, licencias software, formación, servicios profesionales… entre otros. Los tiempos de aplicación y desarrollo se han calculado en base a los pasos necesarios para la implementación de las medidas. Estos valores dependen de la calidad y acuerdos a los que se puedan llegar con los diferentes actores y contratos involucrados, por ello se proporciona una horquilla de valores.

3.6.1.2 Medidas de tipo organizativo

Las medidas de seguridad de tipo organizativo se refieren a las prácticas, políticas y procedimientos establecidos dentro de una organización para proteger sus activos de información y garantizar la seguridad de la información en general. Estas medidas se centran en aspectos como la gestión de riesgos, la concienciación y capacitación del personal, la gestión de acceso y los procesos de seguridad.

- **Política de Seguridad**: política de seguridad es un conjunto de directrices, normas y procedimientos establecidos por una organización para proteger sus activos de información, sistemas y redes de amenazas y vulnerabilidades. Esta política define cómo se gestionan, protegen y distribuyen los recursos de información y establece las responsabilidades y acciones necesarias para garantizar la seguridad y la integridad de los datos.
    - **Funciones**: protección de los activos de información, control de accesos, seguridad de las comunicaciones, respuestas a incidentes…
    - **Presupuesto**
        - Implementación inicial: 40.000€ - 150.000€ teniendo en cuenta consultoría externa, alineamiento normativo (ISO 27001, Esquema Nacional de Seguridad [ENS], Segunda Directiva sobre Seguridad de las Redes y de la Información [NIS2]), sensibilización y formación.
        - Mantenimiento: 10.000€ - 30.000€ incluyendo actualizaciones periódicas, revisión anual y auditorías internas.
    - **Recursos humanos**:
        - 2 - 3 trabajadores para la implementación dependiendo del tamaño y alcance de la política (3 - 5 meses)
        - 1 – 2 trabajadores para mantenimiento (revisión y control

anual)

El presupuesto más acorde con las caracteristicas del cliente estaría entre 45.000€ y 85.000 € con un mantenimiento anual de entre 10.000€ y 15.000€, teniendo en cuenta gastos como consutoría externa, formación, implementación de procedimiento, etc.

- **Procedimientos de Gestión de Incidentes de Seguridad**: conjunto de pasos y acciones predefinidos que una organización debe seguir para identificar, analizar, y responder a eventos de seguridad o incidentes de seguridad. Estos procedimientos buscan minimizar el impacto de los incidentes, restaurar las operaciones normales lo antes posible y prevenir futuros incidentes.
    - **Funciones**: Identificación de incidentes de seguridad, análisis y clasificación de incidentes, contención y erradicación del incidente, recuperación y restauración de sistemas afectados…
    - **Presupuesto**:
        - Implementación inicial: 30.000€ - 100.000€ dependiendo de si se incluye definición de roles, playbooks, integración con SOC o SIEM, y formación/simulacros.
        - Mantenimiento: 5.000€ - 20.000€ dependiendo de la inclusión de revisiones y mejoras continuas
    - **Recursos humanos**:
        - 2 - 3 trabajadores para la implementación dependiendo del tamaño y alcance de los procedimientos (2 - 4 meses)
        - 1 – 2 trabajadores para mantenimiento (revisión + formación)

El presupuesto para una compañía con las características de Data ESP seria de entre 35.000€ y 90.000 € con un mantenimiento anual de 5.000€ y 15.000 €, entre consultoría externa, diseño de playbooks, integración técnica, simulación de incidentes, etc.

- **Gestión de Continuidad del Negocio y Recuperación ante Desastre**: proceso integral que asegura que una organización pueda continuar operando durante y después de una interrupción significativa, ya sea debido a desastres naturales, fallos tecnológicos o ataques cibernéticos. Este proceso incluye planes detallados para restaurar las funciones críticas del negocio y minimizar las pérdidas.
    - **Funciones**: Análisis de impacto en el negocio, desarrollo de planes de continuidad del negocio, implementación de estrategias de recuperación, pruebas y simulacros regulares…

- **Presupuesto**:
  - Implementación inicial: 50.000€ - 200.000€ varía en función de si se incluye si se incluye BIA (análisis de impacto), análisis de riesgos, planes de Business Continuity Plan [BCP] y Disaster Recovery Plan [DRP] y pruebas/simulacros.
  - Mantenimiento: 15.000€ - 50.000€ considerando posibles simulacros anuales y revisiones post-incidente.
- **Recursos humanos**:
  - 3 - 5 trabajadores para la implementación dependiendo del tamaño y alcance de los planes (5 - 8 meses)
  - 2 – 3 trabajadores para el mantenimiento (revisión y pruebas)

El presupuesto seria de entre 50.000€ y 165.000 € con un mantenimiento anual de 15.000€ y 50.000 €, entre consultoría externa, análisis de riesgos periódicos, redacciones de BCP y DRP, simulacros iniciales, herramientas de backup, pruebas anuales, etc.

- **Auditorías y Revisiones de Seguridad**: evaluaciones sistemáticas y periódicas de los controles de seguridad de una organización para asegurar que se cumplen con las políticas, normativas y estándares de seguridad establecidos. Estas auditorías ayudan a identificar vulnerabilidades, evaluar la efectividad de los controles y recomendar mejoras.
  - **Funciones**: evaluación de políticas y procedimientos de seguridad, identificación de vulnerabilidades y riesgos, revisión de controles de acceso y gestión de identidad, verificación de la seguridad de las redes y sistemas
  - **Presupuesto**:
    - Implementación inicial: 20.000€ - 80.000€ refiriendo auditorías iniciales completas (ISO 27001, ENS, análisis de GAP, etc.)
    - Mantenimiento: 5.000€ - 25.000€ si no se realizan certificaciones formales, en caso contrario podría ser mayor.
  - **Recursos humanos**:
    - 2 - 3 trabajadores para la implementación dependiendo del tamaño y alcance de las auditorías (2 - 3 meses).
    - 1 – 2 trabajadores para el mantenimiento (revisiones anuales y auditorias).

El presupuesto seria de entre 20.000€ y 80.000 € con un mantenimiento anual de 5.000€ y 25.000 €, entre auditoria inicial completa (externa),

consultoría para análisis GAP y remediación, auditorias anuales. Tambien se incluiría la posibilidad de la obtención de certificaciones como la ISO 27001 con un coste aproximado de 40.000€

3.6.2 Medidas de subcontratación o seguros

Se tratan de aquellas medidas que funcionan de forma similar a las medidas anteriormente expuestas, sin embargo, a coste de tener un mayor precio a nivel monetario la compañía se ahorra el tiempo de implementación y el gasto en tiempo de los trabajadores.

Ejemplos de estas medidas:

3.6.2.1 Contratación de seguros

Contratar seguros específicos para cubrir diversos riesgos, como seguros cibernéticos, de responsabilidad civil, de interrupción de negocios, entre otros. Estos seguros pueden proporcionar una red de seguridad financiera en caso de incidentes.

Esto permite a la compañía tener una cobertura financiera ante las pérdidas ocasionadas por los diferentes ataques, algunas de empresas que ofrecen estos servicios también permiten tener cierta protección ante demandas o responsabilidades legales y asistencia en la recuperación y la continuidad de negocio.

3.6.2.2 Formación y capacitación externa

Utilizar proveedores externos para la formación y capacitación del personal en áreas críticas como la ciberseguridad, la gestión de incidentes y la continuidad del negocio.

El acceso a programas de formación actualizados y especializados es fundamental para mantener al personal informado sobre las últimas amenazas y prácticas de seguridad. Esta formación aumenta la competencia y la concienciación del personal en materia de seguridad, lo que a su vez reduce la probabilidad de errores humanos y la mala gestión de incidentes. La inversión en capacitación externa fortalece la cultura de seguridad dentro de la empresa y mejora la respuesta ante posibles incidentes.

3.6.2.3 Servicios de monitoreo y respuesta a incidentes

Contratar un “Managed Security Services Provider” (MSSP). Este tipo de

servicios consisten en la asignación de un grupo de expertos que, mediante el uso de herramientas avanzadas y una alta capacitación, detectan y responden rápidamente a las amenazas detectadas.

La vigilancia continua y detección temprana de amenazas permiten una respuesta rápida y efectiva a incidentes, minimizando el impacto en las operaciones y activos de la empresa. Esto contribuye a una reducción del tiempo de inactividad, limitando los daños potenciales causados por incidentes de seguridad. Este tipo de servicios, permiten a la empresa mejorar significativamente su capacidad de respuesta y resiliencia ante posibles riesgos.

4. APLICACIONES PARA LA REALIZACIÓN DE ANÁLISIS DE RIESGOS

Existen varias aplicaciones orientadas exclusivamente a la realización de análisis de riesgos, muchas de estas presentan grandes ventajas y facilidades para los analistas, sin embargo, en el mundo de la consultoría no se suelen emplear.

Muchas veces este tipo de análisis se realizan de forma puntual o cada varios años y el tiempo que se tarda en aprender a utilizar estas herramientas, además de que muchas veces se suele partir de un trabajo realizado anteriormente, hace que no sea tan viable el uso de estas aplicaciones.

A continuación se expondrán algunas de las herramientas más utilizadas para realizar análisis del riesgo, junto con algunas de sus ventajas y desventajas:

4.1 PILAR

PILAR es una herramienta especializada en la gestión y análisis de riesgos en el ámbito de la seguridad de la información, está desarrollada exclusivamente para la metodología Magerit, está desarrollada y financiada parcialmente por el CCN. Se utiliza principalmente en sectores que requieren un alto nivel de seguridad y cumplimiento normativo.

Ventajas:

- Adherencia a estándares internacionales, lo que facilita el cumplimiento normativo.
- Proporciona informes detallados y personalizables.
- Actualizaciones regulares que incorporan nuevas normativas y mejores prácticas.

Desventajas:

- Puede ser costosa, especialmente para pequeñas y medianas empresas.
- Requiere capacitación especializada para aprovechar todas sus funcionalidades.
- Es tosca de utilizar.
- La integración con otros sistemas puede ser limitada.

4.2 RMSTUDIO

RMSTUDIO es una plataforma integral para la gestión de riesgos que abarca tanto la seguridad de la información como los riesgos empresariales generales. Es una solución flexible utilizada por diversas industrias para gestionar y mitigar riesgos.

Ventajas:

- Versatilidad a la hora de adaptarse a las necesidades de gestión de riesgos.
- Soporte para múltiples marcos normativos.
- Interfaz de usuario amigable y con grandes opciones de personalización.
- Gran capacidad de integración con otros sistemas y aplicaciones empresariales.

Desventajas:

- La amplitud de sus funcionalidades puede llegar a aumentar la complejidad de uso,
- Su precio puede ser elevado para empresas con reducido presupuesto.
- La personalización y configuración inicial pueden requerir una inversión significativa de tiempo y conocimiento de la herramienta.

4.3 INTEGRUM

Integrum es una plataforma de gestión que abarca la gestión tanto de los riesgos como de la calidad, salud y seguridad, y sostenibilidad de una compañía. Está diseñada para ofrecer una solución unificada para diversas necesidades de gestión empresarial.

Ventajas:

- Permite la gestión de varios aspectos empresariales en una sola aplicación.

- Gran capacidad de configuración y adaptabilidad a las necesidades específicas de cada organización.
- Buenas capacidades de integración con otros sistemas empresariales.
- Interfaz moderna y fácil de usar.

Desventajas:

- La complejidad de la plataforma puede requerir una considerable inversión de tiempo y estudio.
- Puede ser costosa para pequeñas y medianas empresas.
- La implementación y configuración inicial pueden ser complejas y llevar tiempo.

El uso de herramientas especializadas como PILAR es altamente recomendable para realizar análisis de riesgos siguiendo la metodología Magerit. PILAR está diseñada específicamente para este propósito, lo que permite una implementación precisa, eficiente y alineada con los estándares establecidos. Su capacidad para gestionar dependencias entre activos, calcular riesgos repercutidos y generar informes detallados la convierte en una opción ideal para organizaciones que buscan rigor y profesionalidad en la gestión de riesgos.

Sin embargo, el uso de Excel para llevar a cabo análisis de riesgos sigue siendo una alternativa válida en ciertos contextos. Aunque presenta limitaciones como probabilidad de errores manuales, falta de automatización y menor capacidad para gestionar sistemas complejos, Excel ofrece flexibilidad y adaptabilidad, No se justifica por qué Excel es la opción principal si hay herramientas especializadas, es familiar para la mayoría de clientes y analistas debido a su altísimo uso en consultorías. Es una opción especialmente útil en organizaciones pequeñas o en proyectos con recursos limitados, donde su facilidad de acceso y personalización pueden superar sus desventajas si se utiliza con un diseño cuidadoso y controles rigurosos.

5. CONCLUSIONES

Este proyecto ha permitido la realización de un estudio sobre los análisis de riesgos, más en concreto la metodología Magerit, tanto de forma teórica como práctica. A lo largo del trabajo, se ha demostrado cómo Magerit proporciona un marco estructurado y sistemático para la identificación, evaluación y gestión de riesgos, destacándose por su enfoque detallado y adaptabilidad a diferentes contextos organizacionales.

Esta metodología se ha mostrado efectiva y ventajosa en diferentes aspectos;

- Su estructura modular y detallada permite una evaluación exhaustiva de

los activos, facilitando la toma de decisiones informadas para la mitigación de riesgos.

- Es efectiva a la hora de identificar las amenazas y vulnerabilidades.
- Su escalabilidad permite aplicarse a gran cantidad de contextos y de alcances.
- Se trata de una metodología muy completa que permite realizar análisis de gran valor y utilidad.

El ejercicio práctico realizado ha permitido validar su funcionalidad y utilidad en posibles escenarios reales. Este estudio ha permitido observar como Magerit ayuda al analista a estructurar el proceso de gestión de riesgos, desde la identificación inicial hasta la implementación de medidas correctivas.

No obstante, se han identificado algunas áreas de posible mejora, como puede ser la necesidad de simplificar algunos de sus procesos para facilitar su implementación en organizaciones con recursos limitados o compañías de grandes dimensiones.

Mediante este trabajo se ha tenido la intención de contribuir al campo de la ciberseguridad al proporcionar un análisis detallado de la metodología Magerit y demostrar su aplicabilidad práctica. La documentación desarrollada puede servir como una guía o ayuda para aquellos profesionales del sector que necesiten de un apoyo para la realización de sus propios análisis o como forma de aumentar sus conocimientos en la parte más ejecutiva de la ciberseguridad.

En conclusión, la metodología Magerit se ha confirmado como una metodología valiosa y eficaz para el análisis de riesgos y la gestión de los mismos. Su aplicación práctica demuestra que, a pesar de la complejidad y áreas de mejora, Magerit ofrece un marco sólido para la gestión de los riesgos, la protección de los activos digitales y la continuidad operativa de las organizaciones. Este proyecto refuerza la importancia de una gestión de riesgos proactiva y organizada que permita enfrentar los crecientes desafíos en el ámbito de la ciberseguridad.

GLOSARIO DE TÉRMINOS

Centro Criptológico Nacional: Organismo español perteneciente al Centro Nacional de Inteligencia (CNI) dedicado a criptoanalizar y descifrar por procedimientos manuales, medios electrónicos y criptografía, así como realizar investigaciones criptográficas y formar al personal especializado en criptología.

Riesgo: La posibilidad de que un evento no deseado ocurra y tenga un impacto negativo en los activos de una organización, como la pérdida de datos, la interrupción del servicio o el daño a la reputación.

Riesgo residual: El nivel de riesgo que queda después de que se hayan aplicado medidas de mitigación o control. Es el riesgo que una organización está dispuesta a aceptar o retener.

Riesgo inherente: El nivel de riesgo antes de que se apliquen medidas de mitigación o control. Representa el riesgo tal como existe en su estado natural, sin intervención.

Apetito al riesgo: El nivel de riesgo que una organización está dispuesta a aceptar o asumir en la búsqueda de sus objetivos comerciales. Es una expresión de la disposición de una organización para tomar riesgos en función de sus metas y tolerancia al riesgo.

Activo: Cualquier recurso, información, sistema o infraestructura que tenga valor para una organización y que necesite ser protegido contra amenazas y riesgos. Un servidor, base de datos, incluso un trabajador, son algunos ejemplos de activos.

Vulnerabilidad: Una debilidad o fallo en un sistema o proceso que podría ser explotado por una amenaza para causar daño o pérdida. Las vulnerabilidades pueden ser de naturaleza técnica, humana o de procesos.

Medidas de seguridad lógicas: Las estrategias, políticas, procedimientos y tecnologías diseñadas para proteger los activos digitales y la información de una organización. Esto incluye firewalls, cifrado de datos, sistemas de detección de intrusiones, entre otros.

Medidas de seguridad física: Las medidas diseñadas para proteger los activos físicos de una organización, como los centros de datos, las instalaciones de oficinas y los equipos de hardware. Esto puede incluir controles de acceso, sistemas de cámaras de seguridad, cercas perimetrales, entre otros.

CPD (Centro de Procesamiento de Datos): También conocido como centro de datos, es un espacio físico donde se alojan y gestionan los sistemas informáticos y los componentes asociados, como servidores, almacenamiento de datos, redes y sistemas de seguridad.

DoS (Denial of Service): ciberataque que tiene como objetivo el de dañar las conexiones a un sistema informático, página web, servidor… ya sea mediante la saturación de la red o el bloqueo de la misma.

SOC (Security Operation Center): equipo especializado dentro de una empresa que se dedica a monitorear y mejorar la seguridad de la organización. Su principal objetivo es proteger los datos y sistemas de la empresa contratista.

Splunk: Plataforma comercial de análisis de datos y SIEM.
IBM QRadar: Solución SIEM comercial para detección y análisis de amenazas.

ArcSight: Plataforma SIEM de Micro Focus para análisis y correlación de eventos de seguridad.

Licencias por volumen de eventos (EPS): Modelo de licenciamiento basado en eventos por segundo que procesa un SIEM.

Wazuh SIEM: Solución open source para detección de intrusiones, análisis de logs y monitorización.

WSUS: Windows Server Update Services, herramienta para administrar actualizaciones Windows.

SCCM: System Center Configuration Manager; gestión y despliegue de software y actualizaciones.

Ansible: Herramienta open source de automatización para configuración y

despliegue.

Azure MFA: Servicio de autenticación multifactor de Microsoft Azure.

Duo: Plataforma de autenticación multifactor para verificación en dos pasos.

Google Authenticator: App móvil que genera códigos temporales para MFA.

Tokens físicos: Dispositivos hardware que generan códigos de un solo uso para autenticación segura.

Snort / Suricata: Herramientas open source IDS/IPS para detección y prevención de intrusiones en red.

Cisco Firepower: Solución comercial de Cisco para protección avanzada de red y firewall.

Palo Alto: Marca líder en firewalls de próxima generación y prevención de amenazas.

Fortinet / FortiGate: Empresa y línea de firewalls y productos de seguridad de red.

ISO: Organización Internacional de Normalización, define estándares como ISO 27001.

ENS: Esquema Nacional de Seguridad; marco normativo español para seguridad en sistemas públicos.

NIS2: Directiva europea para mejorar la ciberseguridad en sectores críticos.

Playbooks: Guías detalladas para responder a incidentes de seguridad.

BCP: Business Continuity Plan; plan para mantener operaciones durante incidentes.

DRP: Disaster Recovery Plan; plan para recuperación de sistemas tras desastres.

Análisis de GAP: Evaluación de diferencias entre situación actual y requisitos normativos o buenas prácticas.

ANEXO I

			FRECUENCIA																						
			Acciones ilegítimas contra el patrimonio		Actividad subversiva y/o Hack		Ataque cibernético														Espionaje			Sabotaje		Terrorismo
			Ataques al patrimonio	Robo de activos de información - intruder	Hack de páginas web	Robo y publicación de información confidencial	Escalada de privilegios	ue de denegación de servicio (DoS) – servicios	de denegación de servicio (DoS) – aplicaciones	Cracking de contraseñas	Daños en equipos – Ataque cibernético	Explotación de vulnerabilidades software	Distribución de virus	Filtración de información	Ingeniería social	Phishing	Descubrimiento de información	Malware	Suplantación de IP	Uso ilícito de la red corporativa	Espionaje	Robo de activos de información	Robo de activos de información - insider	Ciberataque	Pérdida de comunicaciones	Terrorismo
	Activos		3	3	3	4	4	3	3	3	2	5	4	4	2	3	3	3	3	3	4	3	3	4	3	2
Vulnerabilidad	Sala de equipos	2	2,5	2,8	2,9	3,4	3,7	3,4	3,2	3,1	2,5	3,8	3,9	3,9	3,0	3,0	3,0	3,0	3,0	3,0	3,5	3,2	3,1	3,6	3,3	2,6
	Sala de servidores	4	3,3	3,0	2,9	3,2	3,5	3,4	3,3	3,2	2,9	3,3	3,6	3,8	3,4	3,2	3,1	3,0	3,0	3,0	3,3	3,3	3,2	3,4	3,3	3,0
	Conexiones remotas por VPN	4	3,6	3,3	3,1	3,2	3,3	3,4	3,3	3,3	3,1	3,2	3,4	3,6	3,5	3,3	3,2	3,1	3,1	3,0	3,1	3,2	3,2	3,3	3,3	3,1
	Empleados internos	2	2,8	3,1	3,1	3,1	3,2	3,3	3,3	3,3	3,2	3,2	3,3	3,4	3,5	3,4	3,3	3,2	3,1	3,1	3,1	3,2	3,2	3,2	3,3	3,2
	Personal externos	2	2,4	2,7	2,9	3,0	3,1	3,2	3,3	3,3	3,2	3,2	3,2	3,3	3,4	3,4	3,3	3,3	3,2	3,2	3,1	3,1	3,2	3,2	3,2	3,2
	Alimentación eléctrica externa	5	3,7	3,2	3,1	3,0	3,1	3,1	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,4	3,4	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2
	Red de Enlace	3	3,4	3,3	3,2	3,1	3,1	3,1	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2
	Servicios de telecomunicaciones	2	2,7	3,0	3,1	3,1	3,1	3,1	3,1	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2
	CPD	5	3,8	3,4	3,2	3,2	3,1	3,1	3,1	3,1	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2
	Sala de control de mantenimiento	5	4,4	3,9	3,6	3,4	3,3	3,2	3,2	3,1	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,2
	Consolas administración	2	3,2	3,6	3,6	3,5	3,4	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2
	Datos sensibles	5	4,1	3,8	3,7	3,6	3,5	3,4	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,2	3,2
	CPUs	4	4,1	3,9	3,8	3,7	3,6	3,5	3,4	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3	3,2
	Discos	4	4,0	4,0	3,9	3,8	3,7	3,6	3,5	3,4	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3	3,3
	Bases de datos	4	4,0	4,0	4,0	3,9	3,8	3,7	3,6	3,5	3,4	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3	3,3
	Firewalls y dispositivos de seguridad	3	3,5	3,8	3,9	3,9	3,8	3,8	3,7	3,6	3,5	3,4	3,4	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3
	Sistemas Operativos	2	2,8	3,3	3,6	3,7	3,8	3,8	3,7	3,7	3,6	3,5	3,4	3,4	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3	3,3
	Aplicaciones	1	1,9	2,6	3,1	3,4	3,6	3,7	3,7	3,7	3,6	3,6	3,5	3,4	3,4	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,2	3,3	3,3	3,3
	Usuarios y cuentas de acceso	2	1,9	2,3	2,7	3,0	3,3	3,5	3,6	3,6	3,6	3,6	3,5	3,5	3,4	3,4	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,3	3,3
	Servicios en la nube	1	1,5	1,9	2,3	2,6	3,0	3,2	3,4	3,5	3,6	3,6	3,6	3,5	3,5	3,4	3,4	3,3	3,3	3,3	3,3	3,3	3,2	3,2	3,2	3,3
	Activos de respuesta a incidentes	1	1,2	1,5	1,9	2,3	2,6	2,9	3,2	3,3	3,5	3,5	3,5	3,5	3,5	3,5	3,4	3,4	3,3	3,3	3,3	3,3	3,3	3,3	3,3	3,3

Tabla 13: Calculo de la Probabilidad de Éxito de Amenaza

		Amenazas																							
		s ilegítimas contra el pat		idad subversiva y/o		Ataque cibernético													Espionaje			Sabotaje		Terrorismo
		Ataques al patrimonio	Robo de activos de información - intruder	Hack de páginas web	Robo y publicación de información confidencial	Escalada de privilegios	e de denegación de servicio (DoS) – servicios	e denegación de servicio (DoS) – aplicaciones	Cracking de contraseñas	Daños en equipos – Ataque cibernético	Explotación de vulnerabilidades sofware	Distribución de virus	Filtración de información	Ingeniería social	Phising	Descubrimiento de información	Malware	Suplantación de IP	Uso ilícito de la red corporativa	Espionaje	Robo de activos de información	Robo de activos de información - Insider	Ciberataque	Pérdida de comunicaciones	Terrorismo
	Activo																								
Vulnerabilidad	Sala de equipos	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Sala de servidores	X	X		X	X	X	X	X		X		X				X	X	X	X		X	X	X	
	Conexiones remotas por VPN	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Empleados internos	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Personal externos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Alimentación eléctrica externa		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Red de Enlace	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Servicios de telecomunicaciones	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	CPD	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Sala de control de mantenimiento	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Consolas administración	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Datos sensibles	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	CPUs	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Discos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Bases de datos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Firewalls y dispositivos de seguridad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Sistemas Operativos		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Aplicaciones		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Usuarios y cuentas de acceso	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Servicios en la nube	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Activos de respuesta a incidentes		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Tabla 14: Aplicabilidad de las amenazas

Activo	Amenaza	Impacto potencial	valor del activo	Impacto (num)	Impacto	Frecuencia de amenaza	Vulnerabilidad del activo	# Probabilidad de exito de Amenaza	Probabilidad de Amenaza	Magnitud del Riesgo Inherente	Clasificación del Riesgo Inherente
CPD	Escalada de privilegios	5	5	25	MUY ALTO	4,00	5,00	20,00	MUY ALTO	500,0	MUY ALTO
CPD	Ataque de denegación de servicio (DoS) – servicios	5	5	25	MUY ALTO	4,00	5,00	20,00	MUY ALTO	500,0	MUY ALTO
CPD	Cracking de contraseñas	5	5	25	MUY ALTO	5,00	5,00	25,00	MUY ALTO	625,0	MUY ALTO
CPD	Filtración de información	5	5	25	MUY ALTO	4,00	5,00	20,00	MUY ALTO	500,0	MUY ALTO
CPD	Ingeniería social	4	5	20	MUY ALTO	5,00	5,00	25,00	MUY ALTO	500,0	MUY ALTO
CPD	Malware	5	5	25	MUY ALTO	4,00	5,00	20,00	MUY ALTO	500,0	MUY ALTO
CPD	Robo y publicación de información confidencial	5	5	25	MUY ALTO	4,00	5,00	20,00	MUY ALTO	500,0	MUY ALTO
Sala de servidores	Ataque de denegación de servicio (DoS) – servicios	5	5	25	MUY ALTO	4,00	4,00	16,00	ALTO	400,0	MUY ALTO
Sala de servidores	Malware	5	5	25	MUY ALTO	4,00	4,00	16,00	ALTO	400,0	MUY ALTO
Conexiones remotas p	Cracking de contraseñas	5	4	20	MUY ALTO	5,00	3,00	15,00	ALTO	300,0	MUY ALTO
Sala de control de mar	Cracking de contraseñas	5	4	20	MUY ALTO	5,00	4,00	20,00	MUY ALTO	400,0	MUY ALTO
Activos de respuesta a	Cracking de contraseñas	5	3	15	MUY ALTO	5,00	4,00	20,00	MUY ALTO	300,0	MUY ALTO
Sala de servidores	Escalada de privilegios	5	5	25	MUY ALTO	4,00	4,00	16,00	ALTO	400,0	MUY ALTO
Sala de servidores	Ingeniería social	4	5	20	MUY ALTO	5,00	4,00	20,00	MUY ALTO	400,0	MUY ALTO
Personal externos	Cracking de contraseñas	5	3	15	MUY ALTO	5,00	5,00	25,00	MUY ALTO	375,0	MUY ALTO
Red de Enlace	Cracking de contraseñas	5	4	20	MUY ALTO	5,00	3,00	15,00	ALTO	300,0	MUY ALTO
CPD	Ataque de denegación de servicio (DoS) – aplicaciones	4	5	20	MUY ALTO	3,00	5,00	15,00	ALTO	300,0	MUY ALTO
CPD	Suplantación de IP	4	5	20	MUY ALTO	3,00	5,00	15,00	ALTO	300,0	MUY ALTO
CPD	Perdida de comunicaciones	4	5	20	MUY ALTO	3,00	5,00	15,00	ALTO	300,0	MUY ALTO
Sala de servidores	Cracking de contraseñas	5	5	25	MUY ALTO	5,00	4,00	20,00	MUY ALTO	500,0	MUY ALTO
CPD	Explotación de vulnerabilidades sofware	4	5	20	MUY ALTO	4,00	5,00	20,00	MUY ALTO	400,0	MUY ALTO
CPD	Phising	3	5	15	MUY ALTO	5,00	5,00	25,00	MUY ALTO	375,0	MUY ALTO
CPD	Espionaje	5	5	25	MUY ALTO	3,00	5,00	15,00	ALTO	375,0	MUY ALTO
CPD	Robo de activos de información - insider	5	5	25	MUY ALTO	3,00	5,00	15,00	ALTO	375,0	MUY ALTO
Empleados internos	Cracking de contraseñas	5	3	15	MUY ALTO	5,00	4,00	20,00	MUY ALTO	300,0	MUY ALTO
Personal externos	Ataque de denegación de servicio (DoS) – servicios	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Personal externos	Malware	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Sala de control de mar	Escalada de privilegios	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Sala de control de mar	Ataque de denegación de servicio (DoS) – servicios	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Sala de control de mar	Explotación de vulnerabilidades sofware	4	4	16	MUY ALTO	4,00	4,00	16,00	ALTO	256,0	ALTO
Sala de control de mar	Filtración de información	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Sala de control de mar	Ingeniería social	4	4	16	MUY ALTO	5,00	4,00	20,00	MUY ALTO	320,0	MUY ALTO
Sala de control de mar	Malware	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Sala de control de mar	Robo y publicación de información confidencial	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Discos	Escalada de privilegios	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Discos	Ataque de denegación de servicio (DoS) – servicios	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Discos	Cracking de contraseñas	5	4	20	MUY ALTO	5,00	4,00	20,00	MUY ALTO	400,0	MUY ALTO
Discos	Filtración de información	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Discos	Ingeniería social	4	4	16	MUY ALTO	5,00	4,00	20,00	MUY ALTO	320,0	MUY ALTO
Discos	Malware	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Discos	Robo y publicación de información confidencial	5	4	20	MUY ALTO	4,00	4,00	16,00	ALTO	320,0	MUY ALTO
Bases de datos	Ataque de denegación de servicio (DoS) – servicios	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Bases de datos	Malware	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Usuarios y cuentas de	Cracking de contraseñas	5	3	15	MUY ALTO	5,00	4,00	20,00	MUY ALTO	300,0	MUY ALTO
Sala de servidores	Robo de activos de información - insider	5	5	25	MUY ALTO	3,00	4,00	12,00	MEDIO	300,0	MUY ALTO
Personal externos	Escalada de privilegios	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Personal externos	Filtración de información	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Personal externos	Ingeniería social	4	3	12	MUY ALTO	5,00	5,00	25,00	MUY ALTO	300,0	MUY ALTO
Personal externos	Robo y publicación de información confidencial	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Alimentación eléctrica	Cracking de contraseñas	5	4	20	MUY ALTO	5,00	3,00	15,00	ALTO	300,0	MUY ALTO
Bases de datos	Escalada de privilegios	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Bases de datos	Cracking de contraseñas	5	3	15	MUY ALTO	5,00	5,00	25,00	MUY ALTO	375,0	MUY ALTO
Bases de datos	Filtración de información	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Bases de datos	Ingeniería social	4	3	12	MUY ALTO	5,00	5,00	25,00	MUY ALTO	300,0	MUY ALTO
Bases de datos	Robo y publicación de información confidencial	5	3	15	MUY ALTO	4,00	5,00	20,00	MUY ALTO	300,0	MUY ALTO
Discos	Explotación de vulnerabilidades sofware	4	4	16	MUY ALTO	4,00	4,00	16,00	ALTO	256,0	ALTO

Tabla 15: Cálculo del riesgo inherente

BIBLIOGRAFÍA

[1] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. - Jefatura del Estado «BOE» núm. 102, de 29 de abril de 2011- (https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf)
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad- Ministerio de asuntos tecnologicos y transformación digital - Miércoles 4 de mayo de 2022 - (https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html)

[2] MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.- Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012 - (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?comentarioContenido=0#:~:text=es%20una%20herramienta%20que%20implementa,en%20la%20administraci%C3%B3n%20p%C3%BAblica%20espa%C3%B1ola)

[3] ISO 31000:2018 Gestión del riesgo — Directrices - (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es)

[4] Information Risk Assessment Methodology 2 (IRAM2) -(https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-2-iram2/)

[5] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica - Madrid, octubre de 2012 - (https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html)

[6] Las brechas de seguridad se deben a contraseñas débil o comprometida - https://www.infordisa.com/es/brechas-de-seguridad-por-contrasenas-debiles-o-comprometidas/

[7] Ataques DDoS más conocidos | Los mayores ataques DDoS de la historia - https://www.cloudflare.com/es-es/learning/ddos/famous-ddos-attacks/

[8] El CCN-CERT alerta del aumento de ataques de robo de información y advierte de que la compraventa de credenciales es ya una de las principales vías empleadas para comprometer las redes corporativas - https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12839-el-ccn-cert-alerta-del-aumento-de-

ataques-de-robo-de-informacion-y-advierte-de-que-la-compraventa-de-credenciales-es-ya-una-de-las-principales-vias-empleadas-para-comprometer-las-redes-corporativas.html

[9] IBM X-Force Threat Index 2025: El robo de credenciales a gran escala se intensifica y los cibercriminales recurren a tácticas más sigilosas - https://es.newsroom.ibm.com/announcements?item=122866

[10] EY: 62% de las empresas latinoamericanas reconoce haber sufrido filtración de datos y 91% ha tenido incidentes de ciberseguridad - https://www.ey.com/es_pe/newsroom/2023/10/empresas-latinoamericanas-filtracion-datos-incidentes-cibersegur#:~:text=A%20nivel%20de%20costos%2C%20durante%202022%20un,millones%20y%20US$3%20millones%2C%20y%20un%2027

[11] El 98% de los ciberataques empiezan con ingeniería social - https://www.itnow.connectab2b.com/post/el-98-de-los-ciberataques-empiezan-con-ingenieria-social

[12] The hidden threat: Tackling malware in your software supply chain - https://www.sonatype.com/blog/the-hidden-threat-tackling-malware-in-your-software-supply-chain

[13] ISO 27001 - https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27001%20MINTUR.pdf

[14] NIST SP 800-63B - https://pages.nist.gov/800-63-3/sp800-63b.html

[15] NIST SP 800-41 - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf