3. Análisis de Gestión de Riesgos de Ciberseguridad

3.1. Introducción y objetivos

Un análisis de riesgos es un proceso sistemático que tiene como propósito estimar la magnitud y probabilidad de los riesgos a los que podría estar expuesta una organización y saber qué decisión tomar ante una posible eventualidad. Supone, por tanto, más que el hecho de calcular la posibilidad de que ocurran cosas negativas. De esta forma, se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado, seleccionando e implementando salvaguardas para poder conocer, prevenir, impedir, reducir o controlar los riesgos identificados, todo ello dentro de un marco de gestión de riesgos.

Cada vez más, se pone de relevancia la importancia de la realización de un análisis de riesgos como un proceso fundamental en cualquier organización, pues tiene en cuenta el valor y la sanción de los datos robados o filtrados en la organización y, por tanto, debe tener controlado el valor y los riesgos a los que esos activos están sometidos. Este valor se podrá utilizar para contrastar el coste de la protección de la información en análisis contra el coste de volverla a producir.

El desarrollo de un proceso de análisis de riesgos, con base en una metodología, debe dar a conocer qué se quiere proteger, dónde y cómo, asegurando que, con los costes en los que se incurre, se obtienen beneficios efectivos. Para esto, se deberán identificar los recursos (*hardware*, *software*, información personal, accesorios, etc.) con los que se cuenta y las amenazas a las que se está expuesto.

El análisis de riesgos es una de las dos partes relativas al tratamiento de los riesgos que hay que realizar en toda organización o sistema; la otra es la gestión de estos, que consiste en definir la estrategia por seguir para la mitigación de los riesgos resultados del análisis mediante la implantación de determinados controles de seguridad.

A blue and white screen with white text

Description automatically generated

Figura 1. Esquema del tratamiento de los riesgos. Fuente: elaboración propia.

El análisis y la gestión del riesgo se encuadran dentro de un sistema de seguridad de la información que define una serie de procesos de seguridad a partir de la implantación de la política de seguridad en la organización.

Realizar análisis de riesgos es un trabajo arduo y costoso. La construcción de mapas de activos y su valoración requiere la colaboración de diversos perfiles dentro de la organización, desde directivos hasta técnicos, y no solo hay que involucrar a un gran número de personas, sino que también hay que conseguir uniformidad de criterios entre todos porque, si es importante cuantificar los riesgos, también es importante ponerlos en perspectiva. Esto es así porque, a menudo, surgen muchos datos en este tipo de análisis. La mejor forma de gestionar la complejidad es centrarse en lo que más importa (máximo impacto, máximo riesgo) e ignorar lo que es secundario o incluso insignificante. Sin embargo, si los datos no están bien ordenados en términos relativos, no es posible interpretarlos.

El análisis de riesgos es muy recomendable e incluso obligatorio en cualquier organización que dependa de sistemas de información y comunicación para cumplir su misión, especialmente en cualquier entorno donde se lleve a cabo el tratamiento electrónico de bienes y servicios, ya sea en público o privado. El análisis de riesgos se utiliza para informar las decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro de reemplazo para garantizar la continuidad del negocio, incluidas las decisiones sobre la adquisición de garantías técnicas y la selección y capacitación de personal. En definitiva, no es una tarea pequeña que cualquiera realiza en su tiempo libre, sino que es una tarea mayor que requiere esfuerzo y coordinación. Por lo tanto, debe ser planificada y razonable.

El análisis de riesgos es una herramienta de gestión para la toma de decisiones. Las decisiones se pueden tomar antes de implementar un servicio o mientras se está ejecutando. Realmente es preciso hacer esto antes, para que las medidas tomadas se integren en el diseño del servicio, en la selección de componentes, en el desarrollo de aplicaciones y en el manual de usuario. Todo lo relacionado con la superación de riesgos imprevistos es costoso en términos de tiempo y dinero para los demás, puede dañar la imagen de la organización y, en última instancia, conducir a una pérdida de confianza en ella. Siempre se dice que más vale prevenir que corregir y aquí se aplica: no esperes a que un servicio falle, debes anticiparte y prepararte.

El análisis de riesgos es la base del proceso de valoración, certificación y acreditación que formaliza la confiabilidad que merece un sistema de información. Debido a que no existen dos sistemas de información exactamente iguales, la evaluación de cada sistema en particular requiere la adaptación a sus partes constituyentes. El análisis de riesgos proporciona una vista única de cómo se ve cada sistema, cuál es su valor, qué amenazas enfrenta y qué protecciones tiene.

El análisis y gestión de riesgos es, por tanto, un paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según la Figura 2:

A diagram of a company

Description automatically generated

Figura 2. Proceso de análisis y gestión de riesgos. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Los objetivos principales de este tema son los siguientes:

* Estudiar los principios y buenas prácticas que deben regir la fase de análisis de riesgos de un sistema y un marco para su gestión.
* Conocer las principales metodologías de análisis y gestión de riesgos.
* Explicar cómo planificar un proyecto de análisis y gestión de riesgos.
* Definir y explicar los aspectos fundamentales de la metodología de análisis y gestión de riesgos Magerit.
* Explicar cómo usar la herramienta de análisis y gestión del riesgo PILAR, patrocinado por dicho ministerio, el Centro Cristológico Nacional (CCN) y la Fábrica Nacional de la Moneda y Timbre (FNMT).

3.2. Principales metodologías y herramientas

Se pueden analizar muy diversos métodos de análisis de riesgos. Están orientados hacia el mismo objetivo, pero cada uno de ellos exhibe un conjunto específico de características (etapas, cálculos cuantitativos, cualitativos y mixtos, informes de cumplimiento respecto a estándares, ventajas e inconvenientes, etc.). Los principales métodos de análisis de riesgos identificados por INCIBE (INCIBE, s. f.) son Magerit, Octave, CRAMM, Mehari y NIST SP 800-30. Por su parte, CyBOK (Autoridad de Aviación Civil, 2020) analiza ISO/IEC 27005:2018, NIST SP 800-30/39, IRAM, FAIR, Octave y STRIDE.

Esta sección proporciona una descripción general de algunas de las principales metodologías. Además, se hace una comparación teórica con base en una variedad de artículos académicos reconocidos. Conocer las características, puntos fuertes y débiles permitirá la posterior selección del que mejor se adapte a las necesidades, nivel de conocimientos y cualificación de cada organización.

Magerit

Magerit es una metodología implementada por el Consejo Superior de Administración Electrónica (CSAE) con el objetivo de llevar a cabo el análisis y la gestión de los riesgos activos de una organización.

De acuerdo con lo descrito en el *Libro I* de la metodología, Magerit establece un marco que permite a los órganos de gobierno de las organizaciones tomar decisiones y gestionar los riesgos derivados del uso del sistema de información apoyándose en la terminología de la norma ISO 31000.

A diagram of a workflow

Description automatically generated

Figura 3. Marco de trabajo para la gestión de riesgos ISO 31000. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Los principales objetivos de esta metodología se pueden clasificar en directos e indirectos. El primero es sensibilizar a los reguladores sobre la prevalencia de los riesgos derivados del uso de la tecnología informática y la importancia de gestionarlos, estableciendo un enfoque de planificación eficaz de los sistemas y seleccionando los tratamientos adecuados para su control. Por otra parte, ayuda a las entidades que enfrentan procesos de auditoría, evaluación, acreditación o certificación.

Magerit v3 incluye dos libros y un manual técnico. El primer libro presenta la estructura del modelo, el segundo explica el enfoque para desarrollar el análisis y, por último, hay un manual de trabajo en el que se describen diversas técnicas, como el uso de árboles de ataque.

A diagram of a business process

Description automatically generated with medium confidence

Figura 4. Elementos de análisis del riesgo potencial y residual. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

De acuerdo con Pascua (2021), se identifican las siguientes ventajas asociadas a esta metodología:

«- Posibilita un alcance completo, tanto de la gestión de riesgos y el análisis.

- Facilita una gran cantidad de recursos para la identificación de las variables fundamentales, como por ejemplo tipos de activos o listado de amenazas.

- Se puede abordar el análisis de manera tanto cuantitativa como cualitativa.

- Tanto las guías como las herramientas son públicas, fácilmente accesibles en varios idiomas, y gratuitas. Para el uso de la herramienta es necesario solicitar la licencia vía correo electrónico.

- Está basada en las normas ISO (31000, 27001, 27002, 27005, 73, 7498-2,1843, etc.) y puede ser utilizada para dar cumplimiento con la certificación ISO/IEC 27001:2007».

Por el contrario, las principales desventajas, de acuerdo con el trabajo de Pascua (2021), son:

«- Dificultad a la hora de traducir una estimación cualitativa a una cuantía económica.

- No establece explícitamente la identificación de vulnerabilidades como uno de los pasos de la metodología.

- Dentro de todos los recursos de información disponibles no se enumeran políticas de seguridad de la información».

Octave

El método Operational Threat Asset and Vulnerability Assessment (Octave) fue creado originalmente por el Software Institute of Carnegie Mellon en colaboración con el Centro de Investigación de Tecnología Avanzada y Telemedicina (TATRC). Su propósito original era facilitar el cumplimiento por el Departamento de Defensa de los Estados Unidos con las disposiciones de la ley de responsabilidad y aprovisionamiento de seguros de salud (HIPAA) (Caralli et al., 2007).

Octave incluye tanto el proceso de análisis de riesgos como la planificación de las consecuencias de las acciones de tratamiento para reducir los riesgos considerados inaceptables (Alberts et al., 2003). Este método considera tanto aspectos operativos tecnológicos como de seguridad de la información, lo cual permite una toma de decisiones mejorada para proteger activos claves (Abril et al., 2013).

A diagram of a process

Description automatically generated

Figura 5. Fases de Octave. Fuente: Alberts et al., 2003.

Se dispone de tres variantes de Octave:

* Octave-S: dirigida para las denominadas pymes.
* Octave: centrado en grandes empresas que emplean a más de trescientos empleados y, en última instancia, sin importar el tamaño de la organización.
* Octave Allegro: tiene un enfoque orientado a los activos de información. Todos aplican los pasos descritos, con los ajustes pertinentes para satisfacer necesidades específicas.

De acuerdo con el trabajo de Pascua (2021), se identifican las siguientes ventajas asociadas a esta metodología:

«- Destaca la flexibilidad que ofrece, ya que puede ajustarse a entidades de diferentes tamaños e independientemente del entorno operativo, ya que está basada en los riesgos, la capacidad de recuperación y en el conocimiento y experiencia de cada estrato de la organización.

- Ofrece un alcance completo, ya que incluye la identificación y valoración de los riesgos, la planificación de acciones de mitigación y persigue el aseguramiento de la continuidad del negocio.

- Aproximación completa, cuyo modelo involucra, activos, interfaces, procesos, recursos, vulnerabilidades amenazas, medidas de seguridad, etc.

- Metodología auto dirigida, es decir, la organización gestiona y dirige la evaluación de sus riesgos, bien a través de un equipo multidisciplinar o a nivel individual (OCTAVE ALLEGRO).

- De carácter público, gratuita y, por tanto, puede ser utilizada en todas las organizaciones».

Por el contrario, entre las desventajas (Pascua, 2021) se encuentran:

«- No explica en forma clara la definición y determinación de los activos de información.

- Puede resultar tediosa, de difícil comprensión y aplicación.

- Implica un elevado nivel conocimientos tecnológicos y técnicos».

Mehari

El método de análisis armonizado de riesgo (*method for harmonized analysis of risk*, Mehari) fue creado por el Club de la Sécurité de l’Information Français (CLUSIF) en 1998. Es un marco para el análisis y gestión de riesgos de la información gratuito.

El propósito principal de esta metodología es proporcionar un método conforme a los requerimientos de la ISO/IEC 27005:2018. Para realizar el análisis de seguridad se tienen en cuenta las tres dimensiones básicas de seguridad: confidencialidad, integridad y disponibilidad.

A diagram of a security service

Description automatically generated

Figura 6. Fases Mehari. Fuente: PECB, 2015.

De acuerdo con el trabajo de Pascua (2021), se identifican las siguientes ventajas asociadas a esta metodología:

«- Método de evaluación y gestión de riesgos de la información gratuito y de código abierto desde 2007.

- Usa un modelo de análisis de riesgos cualitativo y cuantitativo, basado en los tres principios básicos de la seguridad.

- Alineado con los preceptos de la ISO/IEC 27005:2018».

Por el contrario, las desventajas principales (Pascua, 2021) tienen que ver con:

«- La estructura del proceso difiere enormemente respecto de otras metodologías, lo que puede hacer más difícil su aplicación.

- La recomendación de controles y la estimación del impacto están asociados a la parte de gestión, no de análisis de riesgos [Abril et al., 2013; Mogollón, 2015].

- La mayoría de documentación guía se encuentra en francés».

CRAMM

La Central Communication and Telecommunication Agency (CCTA) desarrolló la metodología CCTA Risk Analysis and Management Method (CRAMM). Tiene en cuenta tanto el análisis cuantitativo como cualitativo, de acuerdo con la norma ISO/IEC 27001, con el objetivo de asegurar la disponibilidad, confidencialidad e integridad de un sistema de información. En línea con otros métodos, el método incluye conceptos como activos, vulnerabilidades, amenazas, impacto, riesgo, salvaguardas o monitorización de las medidas adoptadas.

A diagram of a risk assessment

Description automatically generated

Figura 7. Fases de la metodología CRAMM. Fuente: Yevseiev, 2019.

De acuerdo con el trabajo de Pascua (2021), se identifican las siguientes ventajas asociadas a esta metodología:

«- Enfoque estructurado y completo para el análisis y la gestión de riesgos, alineado con las normas ISO.

- Permite una identificación adecuada de los activos y su nivel de exposición. Además, permite caracterizar el funcionamiento del sistema.

- Posibilidad de realizar revisiones completas y revisiones rápidas, permitiendo también revisiones de alto nivel.

- Actualización periódica de una amplia base de datos jerárquica de contramedidas, que abarca también áreas no técnicas, priorización relativa de las contramedidas, incluidos los criterios de eficacia y los costes de aplicación.

- Coherencia resultante de soluciones similares para perfiles de riesgo similares».

Por el contrario, las principales desventajas (Pascua, 2021) son:

«- Debe ser aplicado por personal cualificado y experimentado

- Las revisiones completas requieren mucho tiempo.

- Algunos resultados pueden perder valor por posibles demoras entre las fases de análisis y aplicación.

- Las herramientas CRAMM Expert y CRAMM Express son de pago».

NIST SP 800-30

NIST SP 800-30 es otra metodología desarrollada por el National Institute of Standards and Techonogy (NIST) para llevar a cabo un análisis y gestión del riesgo de los sistemas de información de una organización.

Las ventajas asociadas a esta metodología, de acuerdo con el trabajo de Pascua (2021), son:

«- La NIST SP 800-30 fue una de las primeras normas de evaluación de riesgos, y la mayoría de las demás normas están influidas por ella

- La identificación de los datos críticos y su sensibilidad es similar a la recopilación de información y al establecimiento del contexto en el marco de Octave

- Permite mapear las vulnerabilidades ya que señala las vulnerabilidades en cada uno de los límites definidos del sistema».

Por el contrario, las principales desventajas (Pascua, 2021) son:

«- No puede utilizarse para la evaluación de riesgos de la organización.

- No identifica los activos. Como tal, solo se centra en una infraestructura específica y sus límites a la vez.

- El objetivo es realizar un análisis de riesgo técnico de la infraestructura central de TI, se trata de una metodología muy prescriptiva».

Comparación de metodologías

En la Tabla 1 se evidencian las características y elementos propios de cada metodología, los cuales han sido expuestos de acuerdo con el trabajo de Pascua (2021).

Accede a la Tabla 1 a través de  [este enlace.](https://cms.unir.net/content/download/878181/3816366?version=3)

3.3. Planificación de un proyecto de análisis de riesgos

Se recomienda la visualización de la clase magistral *Proyectos de análisis y gestión de riesgos*, para saber cómo planificar un proyecto de este tipo.

La aplicación de la metodología Magerit es un proceso que se enmarca en un proyecto que consta de las siguientes etapas y actividades:

A screenshot of a computer screen

Description automatically generated

Figura 8. Fases de un proyecto de análisis de riesgos. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Un proyecto de análisis de riesgos de un sistema se inicia en el comité de dirección de la organización, que es el que promociona el o los distintos proyectos por llevar a cabo y los coordina a través de un comité de seguimiento mediante la designación de un director del equipo de proyecto:

A diagram of a project

Description automatically generated

Figura 9. Participantes en un proyecto de análisis de riesgos. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

El flujo de información entre los distintos comités de dirección y seguimiento y el equipo de proyecto se inicia con la presentación del análisis técnico del sistema por parte del director del proyecto al comité de seguimiento, que, a su vez, realiza la evaluación de negocio que se presenta al comité de dirección, que es el que toma las decisiones finales en cuanto a cómo gestionar el riesgo del sistema, lo que resulta en el plan de seguridad:

A diagram of a project

Description automatically generated

Figura 10. Flujo de información en un proyecto de análisis de riesgos. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

El promotor del comité de dirección determina la oportunidad del proyecto y elabora un informe preliminar previo a la formación del comité de seguimiento, que, junto con el director del proyecto, determina el alcance de este:

* Objetivos.
* Dominio y límites.
* Entorno y restricciones.
* Dimensiones y coste.

El director del proyecto y su equipo planifican toda su realización:

* Plan de entrevistas por realizar.
* Participantes por entrevistar.
* Calendario.

El lanzamiento del proyecto se lleva a cabo por el equipo de proyecto y el comité director:

* Preparación de cuestionarios.
* Elaboración de criterios de valoración.
* Determinación de los recursos necesarios.
* Preocupación por la sensibilización.

3.4. Análisis de riesgos

Se identifican todos los activos implicados en el sistema por parte del equipo de proyecto y grupos de interlocutores, se establecen las dependencias entre ellos y se valora en una escala de uno a diez si es un análisis cualitativo o, mediante su valor en euros, si es un análisis cuantitativo, de lo que resulta como salida un modelo de valor. Se utilizan técnicas como diagramas de flujo de datos y de procesos.

Se identifican y valoran las amenazas que el sistema puede sufrir por parte del equipo de proyecto y grupos de interlocutores, utilizando la experiencia acumulada en la organización, descubriendo y caracterizando al adversario, árboles de ataque, etc., lo que resulta en un informe de amenazas.

Se identifican y se valora la efectividad de las salvaguardas que se aplican al sistema para mitigar el riesgo, por parte del equipo de proyecto y grupos de interlocutores, lo que resulta en una declaración de aplicabilidad, informe de evaluación de las salvaguardas e informes de insuficiencias. Se estiman el impacto y el riesgo potenciales y residuales por parte del equipo de proyecto y se interpretan los resultados, lo que da como resultado el estado del riesgo.

El esquema de la Figura 11 explica las relaciones entre los artefactos anteriormente expuestos que utiliza la metodología Magerit:

A diagram of a work flow

Description automatically generated

Figura 11. Relaciones entre los artefactos en la metodología Magerit. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

3.5. Gestión de riesgos

En esta etapa, se abordan los impactos y riesgos identificados en el proceso de análisis, ya sea asumiéndolos o afrontándolos. Para hacer frente a los riesgos considerados inaceptables, se elaborará un plan de seguridad para remediar la situación actual.

Un plan de seguridad se incorpora a un conjunto de programas de seguridad. Algunos programas serán simples, mientras que otros alcanzarán un nivel de complejidad y costo suficiente para que su implementación sea un proyecto. Todos los programas (y, en su caso, proyectos) son planificados periódicamente por el denominado «plan de seguridad», que dicta y organiza acciones para llevar la situación de riesgo a un punto de riesgo aceptable para la dirección. Este proceso se desarrolla a través de las siguientes actividades y tareas:

* Toma de decisiones.
* Plan de seguridad.
* Ejecución del plan.

Toma de decisiones

En esta actividad se traducen las conclusiones técnicas del proceso anterior en decisiones de actuación.

Calificación de los riesgos

Se tiene como resultado de la fase 2 el estado del riesgo del sistema. ¿Qué se puede hacer con él?

* Evitarlo: si se puede, es la solución ideal.
* Reducirlo, mitigarlo: impacto limitado.
* Transferirlo: se lo pasa a otra organización. Ya no es «nuestro problema».
* Asumirlo, aceptarlo: pasa a contabilizarse como gasto operacional.

La aceptación del riesgo es una opción honrada pero peligrosa. El análisis de la fase 2 dice cuál es su nivel de peligrosidad y esta decisión solo puede ser tomada por el comité de dirección, nunca puede ser una decisión técnica. Todas las decisiones son propuestas por el comité de seguimiento, oída la opinión del director del proyecto, y todas son adoptadas por el comité de dirección. Un riesgo se puede interpretar de diversas formas:

* Es inaceptable, en el sentido de que requiere atención urgente.
* Es grave, en el sentido de que requiere atención.
* Es apreciable, en el sentido de que pueda ser objeto de estudio para su tratamiento.
* Es asumible/tolerable, en el sentido de que no se van a tomar acciones para atajarlo.

Las preguntas que hay que hacerse antes de tomar una decisión son: ¿hay datos suficientes para tomar decisiones? ¿De qué margen de incertidumbre adolecen los datos? Los elementos que valorar para responderlas, por su parte, son:

* Gravedad del impacto y del riesgo.
* Obligaciones por ley, reglamentos sectoriales o contratos.
* Intangibles:
  + Imagen pública de cara a la sociedad.
  + Política interna.
  + Relaciones con los proveedores.
  + Relaciones con los usuarios.
  + Relaciones con otras organizaciones.
  + Nuevas oportunidades.
  + Acceso a sellos o calificaciones reconocidas de seguridad.

A diagram of a decision

Description automatically generated

Figura 12. Estudio de los riesgos. Punto de decisión. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

La gestión del riesgo es un proceso recurrente que se puede organizar en microciclos o macrociclos en función de:

* Microciclos:
  + Hasta estado que se considera necesario.
  + Hasta satisfacer leyes, reglamentos, acuerdos, contratos, etc.
  + Hasta tener el certificado de acreditación correspondiente.
  + Mientras el coste compense el riesgo.
* Macrociclos:
  + De acuerdo con la política de certificación o acreditación.
  + Siguiendo incidentes propios y ajenos.
  + Siguiendo cambios en el alcance.

En la Figura 13, se observa un esquema que representa los ciclos que tienen lugar en la gestión de riesgos cuando se trata de la implantación de un sistema nuevo o tiene lugar un incidente o un cambio en el sistema.

A diagram of a problem

Description automatically generated

Figura 13. Ciclos en la gestión de riesgos. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Plan de seguridad

En esta actividad se traducen las decisiones de actuación en acciones concretas: proyectos de mejora de la seguridad planificados en el tiempo. Las tareas son:

* Programas de seguridad.
* Plan de ejecución.

Programas de seguridad

Básicamente, se llevan a cabo dos pasos:

* Se tomarán en consideración todos los escenarios de impacto y riesgo que se consideren críticos o graves como resultado de la tarea anterior.
* Se elaborará un conjunto de programas de seguridad que den respuesta a todos y cada uno de los escenarios anteriores, sabiendo que un mismo programa puede afrontar diferentes escenarios y que un escenario puede ser abordado por diferentes programas.

En última instancia, se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a niveles residuales asumidos por la dirección. Este tratamiento de las salvaguardas se materializa en una serie de tareas que llevar a cabo.

Un programa de seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción. Cada programa de seguridad debe detallar:

* Su objetivo genérico.
* Las salvaguardas concretas por implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia.
* La relación de escenarios de impacto o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo.
* La unidad responsable de su ejecución.
* Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
  + Costes de adquisición (de productos), de contratación (de servicios) o de desarrollo (de soluciones llave en mano), por los que puede ser necesario evaluar diferentes alternativas.
  + Costes de implantación inicial y mantenimiento en el tiempo.
  + Costes de formación, tanto de los operadores como de los usuarios, según convenga al caso.
  + Costes de explotación.
  + Impacto en la productividad de la organización.
* Una relación de subtareas que afrontar, teniendo en cuenta:
  + Cambios en la normativa y desarrollo de procedimientos.
  + Solución técnica: programas, equipos, comunicaciones e instalaciones.
  + Plan de despliegue.
  + Plan de formación.
* Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
* Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
* Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

3.6. Herramienta PILAR

Se recomienda la visualización de la clase magistral *Herramienta PILAR* para ver un análisis y gestión de riesgos con la herramienta PILAR de la metodología Magerit.

La herramienta PILAR maneja los mismos elementos o artefactos de seguridad asociados a la metodología Magerit:

* Activos que proteger.
* Amenazas sobre nuestros activos.
* Contramedidas o salvaguardas.
* Indicadores: impacto, riesgo.

Un esquema de análisis potencial de un sistema de información que relaciona estos elementos sería:

A diagram of a work flow

Description automatically generated

Figura 14. Análisis potencial. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Los pasos del proceso de análisis de riesgos por realizar con la herramienta PILAR conforme a la metodología Magerit son los representados en la Figura 15:

A white and blue list with blue text

Description automatically generated with medium confidence

Figura 15. Pasos por realizar con la herramienta PILAR. Fuente: elaboración propia.

Identificación de activos

La primera tarea que hay que realizar es la definición de los activos del sistema. Son los recursos del sistema de información y telecomunicaciones, o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Después de evaluar el riesgo real que corre el sistema de información, hay que tomar la decisión de aplicar las salvaguardas que correspondan para mitigar el riesgo producido por la frecuencia de las amenazas sobre los activos.

Pueden ser de los tipos siguientes:

* Esenciales:
  + Servicios.
  + Datos/información.
* De ingeniería y aprovisionamiento:
  + Aplicaciones *(software).*
  + Equipos informáticos *(hardware).*
  + Redes de comunicaciones.
  + Soportes de información.
  + Equipamiento auxiliar.
  + Instalaciones (locales, etc.).
  + Personal.

Establecimiento de dependencias entre activos

Una vez definidos los activos, hay que establecer las dependencias que entre ellos existen.

En la Figura 16, se muestra un ejemplo de dependencia entre activos, por ejemplo, el activo «servicios» depende del activo *«software»* y del activo «equipamiento»:

A diagram of a service

Description automatically generated

Figura 16. Dependencias entre activos. Fuente: adaptado de Centro Criptológico Nacional, 2021.

Las dependencias crean la necesidad de proteger los activos inferiores para que cumplan su misión última: acumulación de responsabilidad. Las dependencias hacen a los activos superiores víctimas pasivas de los defectos de los inferiores: repercusión de consecuencias.

Valoración de los activos

La siguiente actividad que hay que realizar es la valoración de los activos teniendo en cuenta el coste que supondría la ocurrencia de una amenaza. Se valoran los activos en una escala del uno al diez si el análisis es cualitativo, o mediante su valor en euros si el análisis es cuantitativo:

* Valor de reposición.
* Valor de reconstrucción.
* Horas perdidas de trabajo.
* Lucro cesante.
* Daños y perjuicios.

Hay que tener en cuenta en la valoración los siguientes aspectos:

* Seguridad de las personas.
* Información de carácter personal.
* Obligaciones derivadas de la ley, del marco regulatorio, de contratos, etc.
* Capacidad para la persecución de delitos.
* Intereses comerciales y económicos.
* Pérdidas financieras.
* Interrupción del servicio.
* Orden público.
* Política corporativa.
* Otros valores intangibles.

Se valoran las siguientes dimensiones:

* Disponibilidad. ¿Qué importancia tendría que el activo no estuviera disponible?
* Integridad. ¿Qué importancia tendría que el activo fuera modificado fuera de control?
* Confidencialidad. ¿Qué importancia tendría que el activo fuera conocido por personas no autorizadas?
* Autenticidad. ¿Qué importancia tendría que quien accede al activo no sea realmente quién se cree?
* Trazabilidad, imputabilidad*(accountability).*¿Qué importancia tendría que no quedara constancia del uso del activo?
* Datos personales. ¿Qué valor e importancia tienen los datos personales comprometidos?

Valor cualitativo (escala del uno al diez)

A table with different colored squares

Description automatically generated

Figura 17. Valor cualitativo de las salvaguardas. Fuente: elaboración propia.

Valor cuantitativo (euros)

A white paper with black text

Description automatically generated

Figura 18. Valor cuantitativo de las salvaguardas. Fuente: elaboración propia.

¿Qué activos se valoran?

Se puede valorar por dominios (por defecto en PILAR) o por activos, si se han establecido dependencias.

Por dominios, se hace una valoración rápida y aproximada, común para todos los activos en el dominio. Es más rápida que la valoración por dependencias. Usando este método, todos los activos en el dominio reciben los mismos valores.

El valor del sistema de información se establece por dominios. La valoración la imponen los activos esenciales (información y servicios) y se la traslada al dominio que los acoge y a los dominios a los que se asocian. La herramienta presenta unos criterios de valoración que ayudan a valorar cada dimensión de forma escalonada del uno a diez.

Si se está valorando el sistema por activos, se necesita establecer las dependencias entre los activos. Los que están más abajo en la cadena de dependencia heredan la valoración de los cuales dependen, así que, a lo mejor, no hay que valorar demasiados activos, normalmente son los datos y los servicios finales (esenciales).

Amenazas: identificación, clasificación y valoración

Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales. Pueden ser, según Magerit-PILAR:

* [N]: desastres naturales.
* [I]: de origen industrial.
* [E]: errores y fallos no intencionados.
* [A]: ataques deliberados.

Identificación

En la práctica, PILAR sugiere para cada tipo de activo las amenazas más probables según las bibliotecas de amenazas de las que disponga la licencia. Hay varias versiones de estas que se pueden cargar en función de características de los entornos cambiantes. No obstante, las amenazas se pueden asignar a los activos según el criterio del analista por su experiencia, por la naturaleza del activo y, por supuesto, basándose en los requisitos de seguridad y casos de abuso.

De la actividad de obtención de los casos de abuso se obtiene el modelo de ataque del sistema con los patrones de ataque que más probablemente puede sufrir. Hay que tener en cuenta que, a veces ―no siempre―, se hace un análisis de riesgos desde el principio del ciclo de vida de desarrollo del sistema y se pide realizar *a posteriori*. En este caso, no se dispone ni de casos de abuso ni de requisitos de seguridad; la herramienta ayuda mucho más al sugerir por defecto las amenazas más probables según el tipo de activo, sus dependencias de otros y su valoración.

A diagram of a personal injury

Description automatically generated

Figura 18. Clasificación de amenaza con base en el agente causante. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Impacto

El impacto es la consecuencia que sobre un activo tiene la materialización de una amenaza, lo que origina una posible pérdida de valor de este.

Valoración

* Cualitativa/subjetiva: irrelevante, grave, intolerable.
* Cuantitativa/económica: coste dinerario.

Impacto acumulado

Si el activo A depende del activo B, el valor de A se acumula en B en la proporción en que A depende de B:

impacto\_acumulado = valor\_acumulado\_B x degradación\_B

A diagram of a company

Description automatically generated

Figura 19. Impacto acumulado. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

Impacto repercutido

Si el activo A depende del activo B, el daño en B repercute en A en la proporción en que A depende de B:

impacto\_repercutido = valor\_A x dependencia x degradación\_B

Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización, lo que ocasionaría una pérdida probable.

Valoración

* Cualitativa/subjetiva: irrelevante, grave, intolerable.
* Cuantitativa/económica: coste dinerario.

Métodos

* Cualitativos: tabulares.

A table with different colored squares

Description automatically generated

Figura 20. Estimación del riesgo. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

* Cuantitativos: impacto x frecuencia.
  + Impacto = valor degradación.
  + Riesgo = impacto x frecuencia.

Riesgo acumulado

Si A depende de B en un g%, el valor de A se acumula en B en la proporción en que depende:

riesgo\_acumulado\_B = impacto\_acumulado\_B x frecuencia

Riesgo repercutido

Si A depende de B en un g%, las amenazas sobre B impactan sobre A en un g% con la frecuencia de materialización en B:

riesgo\_repercutido = impacto\_repercutido x frecuencia

Salvaguardas

Una vez obtenido el riesgo cualitativo o cuantitativo, a efectos prácticos de la herramienta PILAR, se tienen que seleccionar las salvaguardas necesarias y valorarlas para mitigar el riesgo.

¿Qué salvaguardas se requieren? Para saber más sobre este tema, accede al siguiente enlace: <https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf>

Hay que casar las salvaguardas con las amenazas identificadas. Se prepara una declaración de aplicabilidad (*statement of applicability*, SoA) y se evalúa el despliegue actual: existencia (o ausencia) y efectividad del despliegue.

Se proporciona una lista de riesgos ponderada asociada a activos, amenazas, dimensiones y rangos, ya que no todas las salvaguardas son igualmente efectivas. Se pueden proporcionar listas adicionales para activos específicos.

En la herramienta, se pueden seleccionar las categorías de salvaguardas que se pueden aplicar; hay una columna que indica la recomendación que sugiere la herramienta según el tipo de activo y las amenazas de que puede ser objeto.

Una vez analizadas las recomendaciones sobre qué salvaguardas son necesarias en los activos que tiene el sistema, hay que valorar las salvaguardas según la fase del proyecto en la que se está. Lo normal es que pase por varias fases determinadas por hitos de funcionalidades nuevas que se van implantando, por ejemplo. La valoración hay que hacerla para todas las salvaguardas en todas las fases. La cuantificación se hace con base en su eficacia medida en cómo la salvaguarda está implantada y es efectiva frente al riesgo al que se enfrenta o mediante opinión cualificada (de un experto).

La estimación de su eficacia se clasifica:

* NA: no aplica.
* 0 %: L0 inexistente.
* 10 %: L1 inicial / *ad hoc.*
* 50 %: L2 reproducible, pero intuitivo.
* 90 %: L3 proceso definido.
* 95 %: L4 gestionado y medible.
* 100 %: L5 optimizado.

Normativa y perfiles de seguridad

La siguiente actividad que hay que realizar en el análisis de riesgos con PILAR es valorar la adecuación a la normativa de seguridad y el cumplimiento con base en el perfil de seguridad que adopte la organización donde está inmerso el sistema. PILAR permite valorar el cumplimiento con respecto a ISO 27002:2013, ENS y GDPR:2016.

Impacto y riesgos residuales

PILAR calcula el impacto y riesgo residual que queda en el sistema después de aplicar y valorar las salvaguardas para mitigar el riesgo potencial:

* Impacto residual: impacto efectivo que queda tras contabilizar las salvaguardas.
* Riesgo residual: riesgo efectivo que queda tras contabilizar las salvaguardas.

En la Figura 21 se muestra lo explicado anteriormente. Como consecuencia de la aplicación de las salvaguardas se mitiga el riesgo, pero siempre van a quedar el impacto y riesgo residuales en el sistema.

A diagram of a work flow

Description automatically generated

Figura 21. Análisis residual. Fuente: adaptado de Ministerio de Hacienda y Administraciones Públicas, 2012.

El estado del riesgo que se presenta como resultado del análisis con la herramienta para cada activo, en cada dimensión, para cada amenaza es:

* Impacto potencial y residual en cada fase.
* Riesgo potencial y residual en cada fase.
* En términos de valor acumulado para decisiones técnicas.
* En términos de daño repercutido para decisiones de negocio.

Informes

Se pueden extraer de la herramienta informes:

* Del estado del impacto y riesgo con todas sus variantes de acumulado y repercutido.
* De amenazas, de cumplimiento de normativa de seguridad y procedimientos.
* Del grado en el que el sistema cumple un determinado perfil de seguridad.
* Como documento de especificación de requisitos del sistema SSRS.