TEMA 047. SEGURIDAD DE SISTEMAS (1). ANÁLISIS Y GESTIÓN DE RIESGOS. HERRAMIENTAS.

Actualizado a 28/04/2023

1. SEGURIDAD DE SISTEMAS DE INFORMACIÓN

En el Anexo IV del **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)**, se define la **seguridad de los sistemas de información** como la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

Es decir, es la capacidad de los sistemas de información para resistir acciones que comprometan las diferentes dimensiones de la seguridad de los datos y servicios. Siendo estas dimensiones:

- **Disponibilidad**: Disposición de los servicios a ser usados cuando sea necesario.
- **Integridad**: Mantenimiento de las características de completitud y corrección de los datos.
- **Confidencialidad**: Que la información llegue solamente a las personas autorizadas.
- **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad**: En todo momento se podrá determinar quién hizo qué y en qué momento.

Los **Sistemas de Gestión de la Seguridad de la Información (SGSI)** juegan un papel clave para gestionar la seguridad de los sistemas de información de manera continua, a partir del tratamiento y la gestión efectiva de los riesgos.

Las organizaciones de todo tipo y tamaño trabajan con distintas clases de información que son sensibles a amenazas de ataque, error, daños naturales, etc., así como a vulnerabilidades propias de su uso.

Proteger los distintos activos de información mediante **Sistemas de Gestión de la Seguridad de la Información (SGSI)** es esencial para que una organización pueda conseguir sus objetivos.

2. ANÁLISIS Y GESTIÓN DE RIESGOS

La **gestión de riesgos** es el proceso destinado a modificar el riesgo. Las tareas de **gestión de los riesgos** no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

La **gestión del riesgo** supone buscar el equilibrio entre los riesgos a asumir y el coste que suponen sus medidas de control. En función de dicho análisis y del riesgo asumido, se tomarán las decisiones como la implantación o no de controles para mitigarlos, los planes de continuidad del negocio, el tratamiento o no de ciertos datos, etc.

Existen diversas **formas de gestionar un riesgo**: evitando las circunstancias que lo provocan, reduciendo las posibilidades de que ocurra o incluso aceptando que pueda ocurrir y previendo recursos para actuar en caso de que sea necesario. Supone buscar el equilibrio entre los riesgos a asumir y el coste que suponen sus medidas de control.

Dentro de la gestión del riesgo, se consideran de forma general las siguientes tareas:

- Análisis de riesgos
- Tratamiento de los riesgos

2.1. DEFINICIONES

- **Activos:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Los activos esenciales de una organización son la **información** que se maneja y los **servicios** que se prestan.
- **Amenazas**: Eventos que pueden originar un incidente produciendo daños materiales o inmateriales. También, causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Se consideran los siguientes tipos de amenaza:
    - Desastres naturales.
    - De origen industrial.
    - Errores y fallos no intencionados.
    - Ataques intencionados.
- **Desastre:** Interrupción que ocasionan que los recursos críticos de información queden inoperantes por un periodo de tiempo. Los desastres requieren esfuerzos de recuperación para restaurar el estado operativo, su origen puede ser:
    - Desastres naturales.
    - Origen humano.
    - Indisponibilidad de servicios externos.
- **Impacto:** Medida del daño sobre el activo derivado de la materialización de una amenaza.
- **Incidente:** Cualquier evento que no es parte de la operación normal de un servicio y el cual causa, o puede causar, una interrupción o reducción en la calidad de éste. Algunos incidentes típicos son: servicio no disponible; corrupción de software; fallo hardware; detección de un virus; caída de un sistema; uso no autorizado de la cuenta de un usuario; uso no autorizado de Privilegios de acceso al sistema; desfase de una o más páginas web; ejecución de código malicioso que destruye datos; una inundación o un incendio en el CPD; la interrupción en el suministro de energía eléctrica; un calentamiento excesivo que provoque que falle un sistema; un desastre natural.
- **Mecanismos de seguridad:** Son las acciones llevadas a cabo encaminadas a reducir el riesgo sobre alguna vulnerabilidad.
- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Probabilidad de que se materialice una vulnerabilidad.
- **Salvaguardas**: Aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Defensas desplegadas para que las amenazas no causen tanto daño (mitigación).
- **Vulnerabilidades**: Posibilidad de materialización de una amenaza sobre un activo. Toda debilidad que puede ser aprovechada por una amenaza.

Los **sistemas (activos)** pueden tener **vulnerabilidades** que se pueden explotar porque estamos expuestos a **amenazas**. La probabilidad de que esto se lleve a cabo y tenga efecto es el **riesgo**. El **impacto** es el daño que produce en nuestra organización. Para prevenirlos y **minimizar el riesgo** tenemos que implantar **mecanismos de seguridad y salvaguardas** (contramedidas). El proceso para gestionar todo esto es lo que se conoce como **gestión del riesgo.**

2.2. ANÁLISIS DE RIESGOS

El **análisis de riesgos** es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. Es decir, permite determinar qué se tiene y estimar lo que podría pasar. El análisis de riesgos proporciona un modelo del sistema en términos de **activos, amenazas, vulnerabilidades y salvaguardas**.

Existen diversas metodologías para realizar los análisis de riesgos. Tomando como referencia **Magerit** (por ser una metodología creada para la Administración Públicas) el análisis de riesgos dispone de las siguientes fases:

1. **Caracterización de los activos**, que comprende:
    a. La Identificación de los activos, pudiendo ser esenciales (información que se maneja o servicio que presta) o relevantes (software, hardware, soportes de información, equipamiento auxiliar, redes de comunicación, instalaciones o personas)
    b. Identificación de las dependencias entre dichos activos
    c. Valoración del activo
2. **Caracterización de las amenazas**, que comprende:
    a. La identificación de las amenazas, que pueden ser de origen natural, del entorno, defectos, causadas de forma accidental, etc.
    b. La valoración de las amenazas, en función de la degradación que sufriría el activo y de la probabilidad de ocurrencia de la amenaza
3. **Determinación del impacto,** siendo este el daño producido en el activo como consecuencia de la materialización de una amenaza sobre dicho activo
4. **Determinación del riesgo potencial en función de la probabilidad y del impacto.**
5. **Caracterización de las salvaguardas:**
    a. identificación de salvaguardas: controles o medidas existentes que reducen la probabilidad o limitan el daño sobre el activo.
    b. Valoración de salvaguardas
6. **Estimación del estado de riesgo**: La estimación del estado de riesgo es la estimación del impacto residual y del riesgo residual existentes que permanecen sobre el activo una vez implantadas las salvaguardas.

Los activos vienen a formar **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'.

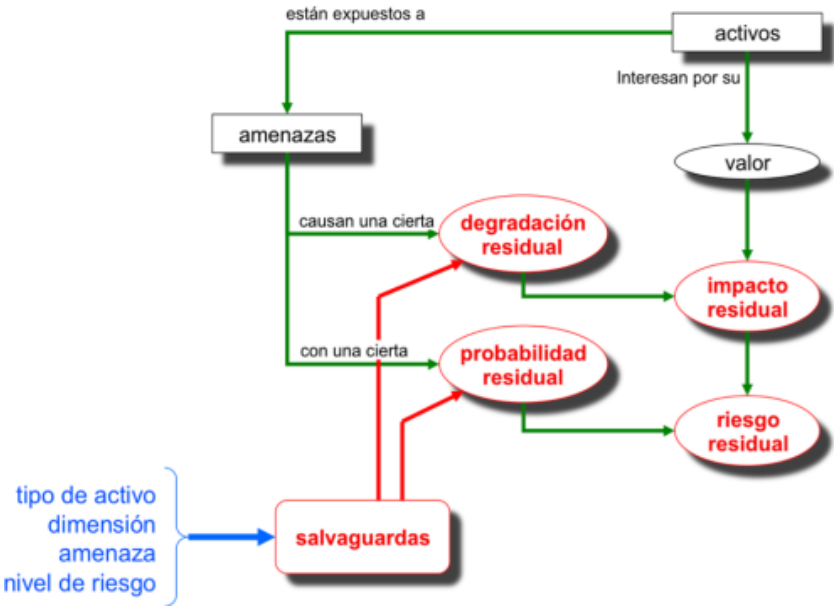

Ilustración de Magerit3.0 sobre los elementos del riesgo residual

2.3. TRATAMIENTO DE RIESGOS

El **tratamiento de riesgos** es el conjunto de actividades dentro de la gestión de riesgos destinadas a modificar el estado de los riesgos que se ha determinado en la etapa de análisis. Permite organizar las defensas o medidas de seguridad hasta alcanzar el nivel residual de riesgo que se desea asumir.

Una vez identificado y valorado el riesgo residual actual, se procede a su tratamiento, encontrando siguientes estrategias de tratamiento de riesgos:

- **Evitar**: Eliminando la causa se elimina el riesgo.
- **Mitigar**: Reducir la probabilidad o impacto de riesgo estableciendo los controles oportunos.
- **Compartir/transferir**: Se comparte o transfiere el riesgo a través de la cobertura de un seguro, acuerdo contractual u otros métodos.
- **Aceptar**: Reconocimiento formal de la existencia del riesgo y de las posibles consecuencias.

A la hora de hablar de riesgos es necesario hablar de costes, ya que una vez conocidas las amenazas y las vulnerabilidades y estimado el posible nivel de riesgo, es necesario establecer controles (también denominados contramedidas o salvaguardas) que permitan reducirlo a un nivel aceptable para la organización.

El coste de las contramedidas o salvaguardas a aplicar no puede ser mayor que el posible coste de la materialización de las amenazas a las que están expuestos los activos que proteger, ya que en este caso la relación coste-beneficio sería negativa para la organización.

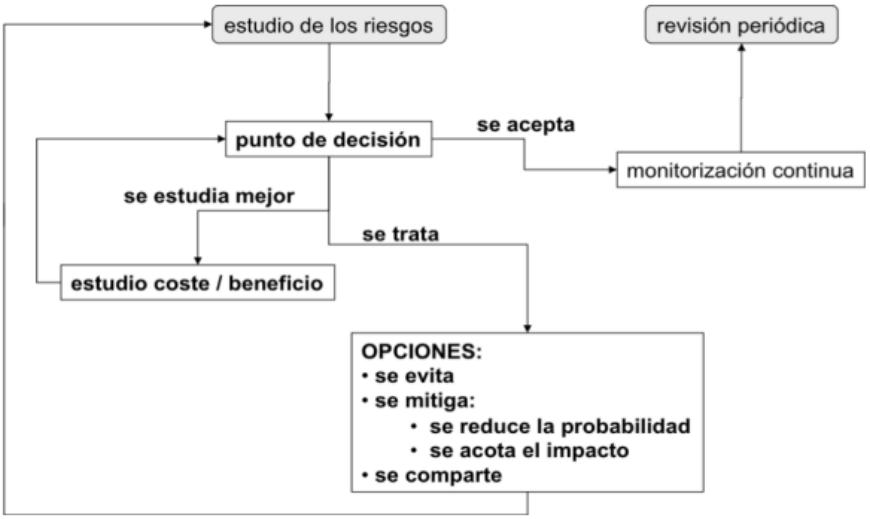

Ilustración de Magerit 3.0 de decisiones de tratamiento de los riesgos

En caso de que la estrategia de gestión sea evitar o mitigar, se deberán establecer unos controles que nos faciliten esta tarea. Los controles podrán ser:

- **PREVENTIVOS**
  - Impedir problemas antes de que ocurran.
  - Visualizar entradas y operaciones.
  - Procurar predecir potenciales problemas antes de que ocurran.
  - Evitar errores, omisiones y actos maliciosos.
- **DETECTIVOS**
  - Detectan cuándo se ha producido un error, omisión o acto indebido e informan de ello.
- **CORRECTIVOS**
  - Minimizan el impacto de una amenaza
  - Remedian problemas identificados mediante un control detectivo.
  - Identifican la causa de un problema.
  - Corrigen errores surgidos como consecuencia de un problema.
  - Modifican los sistemas de proceso para evitar futuras repeticiones del mismo problema.

2.4. ANÁLISIS DE RIESGOS EN EL ENS

Sobre el Análisis de riesgos, en el Esquema Nacional de Seguridad RD 311/2010, dentro del Capítulo II Principios Básicos:

> *"Artículo 7. Gestión de la seguridad basada en los riesgos.*
>
> *1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.*
>
> *2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad."*

Adicionalmente, el Anexo II sobre las Medidas de Seguridad, se contempla dentro del marco operacional de Planificación el "Análisis de riesgos" [op.pl.1]:

Categoría BÁSICA (Requisito): *Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:*

a) Identifique los activos más valiosos del sistema.
b) Identifique las amenazas más probables.
c) Identifique las salvaguardas que protegen de dichas amenazas.
d) Identifique los principales riesgos residuales.

Categoría MEDIA (Refuerzo R1): *Se deberá realizar un análisis de riesgos semi formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:*

a) Valore cualitativamente los activos más valiosos del sistema.
b) Cuantifique las amenazas más probables.
c) Valore las salvaguardas que protegen de dichas amenazas.
d) Valore el riesgo residual.

Categoría ALTA (Refuerzo R1): *Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:*

a) Valore cualitativamente los activos más valiosos del sistema.
b) Cuantifique las amenazas posibles.
c) Valore y priorice las salvaguardas adecuadas.
d) Valore y asuma formalmente el riesgo residual.

3. MARCOS DE REFERENCIA RELACIONADOS CON ANÁLISIS Y GESTIÓN DE RIESGOS

Entre los marcos de referencia relacionados con el análisis y gestión de riesgos más relevantes se encuentran:

- ISOs
- COBIT
- COSO
- Magerit v3

ISOs

- **ISO/IEC 27000:2018** Familia de normas/estándares en seguridad de la información. Las normas más importantes de la serie son:
  - ISO/IEC 27000:2018 contiene una descripción general y vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.
  - ISO/IEC 27001:2018: Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información.
  - ISO/IEC 27005:2018: Describe las fases recomendadas para analizar los riesgos (establecer contexto, evaluación, tratamiento, aceptación, comunicación y monitorización y revisión de los riesgos)

- **ISO 31000:2018 (En España UNE-ISO 31000:2018):** Estándar internacional para el sistema de gestión de riesgos dentro de las organizaciones, incluyendo tanto el análisis y tratamiento del riesgo como la comunicación, responsabilidades, evaluación, mantenimiento y seguimiento del sistema.

COBIT

Guía de mejores prácticas dirigida al control y supervisión de tecnología de la información (Ver tema 107). Hay varios objetos de gobierno/gestión del core COBIT dedicados a la gestión del riesgo (EDM03/APO12).

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

COSO es un marco de referencia que proporciona directrices y orientaciones generales relacionadas con la gestión del riesgo, control interno y disuasión del fraude. Su versión actual es la COSO ERM 2017.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

Magerit es la metodología de análisis y gestión de riesgos promovida por el CSAE (Comisión Sectorial de Administración Electrónica). Su versión actual es **MAGERIT v.3**.

Según Magerit, el análisis de riesgos es una actividad obligatoria para poder llevar a cabo los procesos de evaluación, certificación, auditoría y acreditación:

- **Evaluación:** Permite medir el grado de confianza que merece o inspira un sistema de información.
- **Certificación:** Consiste en asegurar responsablemente y por escrito un comportamiento. La evaluación puede llevar a una certificación o registro de la seguridad de la información. Existen certificaciones de:
  - Productos: es impersonal, se trata de comprobar que contiene determinadas características técnicas.
  - Sistemas: tiene que ver con el componente humano de las organizaciones buscando el análisis de cómo se explotan los sistemas.
- **Auditorías:** Dentro de las auditorías internas o externas es posible distinguir entre:
  - Auditorías requeridas por ley para operar en cierto sector (cumplimiento)
  - Auditorías requeridas por la Dirección de la Organización.
  - Auditorías requeridas por entidades colaboradoras que ven su nivel de riesgo ligado al de nuestra organización.
- **Acreditación:** Proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios.

Los informes más importantes, resultado de un análisis de riesgos con Magerit son:

- **Modelo de valor:** Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

- **Mapa de riesgos:** Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.
- **Declaración de aplicabilidad:** Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.
- **Evaluación de salvaguardas:** Informe que detalla las salvaguardas existentes calificándolas según su eficacia para reducir el riesgo que afrontan.
- **Informe de insuficiencias o vulnerabilidades:** Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.
- **Estado de riesgo:** Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

4. TÉCNICAS Y HERRAMIENTAS PARA LA GESTIÓN DE RIESGOS

Técnicas para la gestión de riesgos (MAGERIT)

Algunas de las técnicas propuestas dentro de Magerit v3 para la gestión de riesgos son:

- **Técnicas específicas para el análisis de riesgos:**
    - Tablas para la estimación del impacto y el riesgo: Tablas en las que se representa cualitativamente tanto el impacto como la probabilidad de ocurrencia de una amenaza, de manera que se puede estimar el riesgo asociado a la misma, en una escala con valores que van desde riesgo despreciable a riesgo crítico.
    - Análisis algorítmico: Modelos para la valoración cuantitativa o cualitativa del riesgo que corren los activos.
    - Árboles de ataque: Representación gráfica de las posibles formas que un atacante podría emplear para alcanzar su objetivo (por ejemplo, la vulneración de un servidor).

- **Técnicas generales:**
    - Técnicas gráficas: Histogramas, diagramas de Pareto, diagramas de radar, etc., para representar de manera visual indicadores o variables relevantes sobre el estado de la seguridad, que permiten facilitar la toma de decisiones o la priorización de las medidas a implantar.
    - Sesiones de trabajo: Con el fin de obtener información, comunicar resultados, reducir el tiempo de implantación de medidas de seguridad, fomentar la participación de los usuarios, etc., y que se pueden concretar como entrevistas, reuniones o presentaciones.
    - Valoración Delphi: Técnica cualitativa basada en cuestionarios que posibilita la identificación de problemas y el desarrollo de estrategias para la solución de los mismos, a partir de un rango de alternativas posibles que se obtienen contrastando las opiniones que los participantes del método tienen respecto al tema tratado.

Herramientas EAR (Entorno de Análisis de Riesgos)

De uso en la Administración pública, las herramientas EAR (Entorno de Análisis de Riesgos) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes:

- • PILAR: versión íntegra de la herramienta.
- • PILAR Basic: versión sencilla para Pymes y Administración Local.
- • µPILAR: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos.
- • RMAT (Risk Management Additional Tools) Personalización de herramientas.

Nota (relación con otros temas):

Conocer los riesgos que afectan a un activo, área, sistema u organización es fundamental para tener un buen entendimiento de los aspectos que pueden afectar a su funcionamiento. De hecho, el Análisis de Riesgos y su gestión es una parte fundamental de otros sistemas y procesos, como, por ejemplo:

- Como paso necesario en la implantación del Sistema de Gestión de Continuidad de Negocio (ISO 22301) (ver Tema 127)
- Como paso necesario en la implantación del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001).
- En la determinación de medidas de seguridad en la aplicación del Esquema Nacional de seguridad (apartado 2.4 y Tema 48).
- En la determinación de medidas de seguridad a aplicar en el tratamiento de datos de carácter personal, así como en la determinación de si el tratamiento supone un riesgo alto para los derechos y libertades de las personas físicas, según Reglamento UE 2016/679 (Reglamento General de Protección de Datos) (ver Tema 27).