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

RESUMEN EXPRESS

Actualizado a 28/04/2023

1. SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Seguridad de los sistemas de información (Anexo IV **ENS)**: 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.

Dimensiones de la seguridad de los datos y servicios:

- **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.

2. ANÁLISIS Y GESTIÓN DE RIESGOS

Gestión de riesgos:

- Es el proceso destinado a modificar el riesgo.
- Encajan en la actividad continua de gestión de la seguridad.
- Supone buscar el equilibrio entre los riesgos a asumir y el coste que suponen sus medidas de control → Toma de decisiones para la implantación o no de controles para la mitigación de riesgos, planes de continuidad del negocio, tratamiento de datos, etc.

Tareas dentro de la gestión de riesgos:

- 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.

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**
    a. La Identificación de los activos
    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
    b. La valoración de las amenazas
3. **Determinación del impacto**
4. **Determinación del riesgo potencial en función de la probabilidad y del impacto.**
5. **Caracterización de las salvaguardas:**
    a. identificación de salvaguardas
    b. Valoración de las salvaguardas
6. **Estimación del estado de riesgo**

2.3. TRATAMIENTO DE RIESGOS

Tratamiento de riesgos: Conjunto de actividades 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.

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.

El **coste de las contramedidas o salvaguarda**s 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.

Controles para el tratamiento de riesgos:

- **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

La gestión de riesgos en el Esquema Nacional de Seguridad RD 311/2010 (ENS) está presente en:

- Capítulo II, sobre Principios Básicos: *Artículo 7. Gestión de la seguridad basada en los riesgos.*
- Anexo II sobre las Medidas de Seguridad, dónde se contemplan las acciones específicas a llevar a cabo según la categorización del sistema de información según el nivel 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:*
  - ***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.*
  - ***Categoría ALTA (Refuerzo R1):*** *Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente.*

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:
  - 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**.

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
    - Análisis algorítmico
    - Árboles de ataque
- **Técnicas generales:**
    - Técnicas gráficas
    - Sesiones de trabajo
    - Valoración Delphi

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.