Actividad 15. Aplicación de MAGERIT

1. Explicar la Metodología Magerit, los pasos a seguir y las herramientas que se pueden utilizar

La **Metodología Magerit** es un conjunto de procedimientos y técnicas desarrollada para la gestión de riesgos en sistemas de información. El ***objetivo*** es identificar, analizar y gestionar los riesgos asociados a la seguridad de la información, asegurando la protección de activos y continuidad del negocio.

Su ***metodología*** consiste en:

1. ***Contexto y Marco de Trabajo***:
   - **1.1. Objetivo**: Establecer el contexto del análisis de riesgos, incluyendo alcance y límites.
   - **1.2. Actividades**: Definir los objetivos del análisis, el entorno de trabajo, los activos a proteger y amenazas potenciales.

2. ***Análisis de Riesgos***:
   - **2.1. Objetivo**: Identificar y evaluar los riesgos que puedan afectar a los activos de información.
   - **2.2. Actividades**:
     - *2.2.1. Identificación de Activos*: Enumerar y clasificar los activos de información (datos, hardware, software, personas, servicios, etc.).
     - *2.2.2. Identificación de Amenazas*: Reconocer las amenazas que puedan afectar a los activos (desastres naturales, errores humanos, ataques cibernéticos, etc.).

- *2.2.3.* *Identificación de Vulnerabilidades*: Determinar las debilidades que pueden ser explotadas por amenazas.
- *2.2.4.* *Valoración de Impacto*: Evaluar el impacto potencial de la explotación de cada vulnerabilidad.
- *2.2.5.* *Cálculo de Riesgo*: Estimar el riesgo combinando la probabilidad de ocurrencia de la amenaza con el impacto resultante.

3. ***Gestión de Riesgos***:
   - **3.1. Objetivo**: Desarrollar estrategias de mitigar, transferir, aceptar o evitar los riesgos identificados.
   - **3.2. Actividades**:
     - *3.2.1.* *Evaluación de controles*: Identificar y evaluar los controles existentes y su efectividad.
     - *3.2.2.* *Desarrollo de Planes de Acción*: Proponer y planificar la implementación de nuevos controles o mejora de los existentes.
     - *3.2.3.* *Priorización de Riesgos*: Clasificar los riesgos según su gravedad y urgencia de tratamiento.
     - *3.2.4.* *Implementación de Controles*: Ejecutar las acciones planificadas para mitigar los riesgos.

4. ***Monitoreo y Revisión***:
   - **4.1. Objetivo**: Asegurar la efectividad continua del proceso de gestión de riesgos.
   - **4.2. Actividades**:
     - *4.2.1.* *Revisión Periódica*: Evaluar regularmente el estado de los riesgos y la efectividad de los controles.
     - *4.2.2.* *Actualización del Análisis*: Revisar y actualizar el análisis de riesgos ante cambios en el entorno o aparición de nuevas amenazas.

5. ***Evaluación de Riesgos***:
   - **5.1. Objetivo**: Estimar el riesgo combinando la probabilidad de ocurrencia de la amenaza con el impacto resultante, y priorizar los riesgos en función de su severidad.
   - **5.2. Actividades**:
     - *5.2.1.* *Cálculo del Riesgo*: Utilizar modelos de evaluación para determinar el nivel de riesgo, combinando la probabilidad

de la ocurrencia de una amenaza con la magnitud del impacto sobre los activos.

5.2.2. *Valoración del Riesgo*: Asignar un valor cuantitativo o cualitativo a cada riesgo identificado, considerando la probabilidad de la ocurrencia y el impacto que tendría en los activos.

5.2.3. *Clasificación de Riesgos*: Ordenar los riesgos identificados según su nivel de gravedad, para focalizar los esfuerzos en los más críticos.

5.2.4. *Determinación de la Tolerancia al Riesgo*: Establecer el umbral del riesgo aceptable para la organización, identificando los riesgos que requieren medidas inmediatas y aquellos que pueden ser aceptados.

Sus ***herramientas*** utilizadas son las siguientes:

1. ***CRAMM (CCTA Risk Analysis Management Method)***:
    - Herramienta de análisis y gestión de riesgos que ayuda a identificar activos, evaluar amenazas y vulnerabilidades, y desarrollar planes de acción.

2. ***PILAR (PILoto para el Análisis de Riesgos)***:
    - Software diseñado para aplicar la Metodología Magerit, facilitando la identificación, análisis y gestión de riesgos.

3. ***OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)***:
    - Metodología y herramienta para la gestión de riesgos de seguridad que se centra en la evaluación de amenazas críticas operativas.

4. ***CORAS***:
    - Herramienta de análisis de riesgos basada en modelos gráficos, útil para la visualización y comunicación de riesgos.

5. ***ISO 27005 Toolkit***:
    - Conjunto de herramientas y plantillas alineadas con la norma ISO/IEC 27005, que proporciona directrices para la gestión de riesgos en la seguridad de la información.

magerit

METHODOLOGY FOR INFORMATION SYSTEMS
RISK ANALYSIS AND MANAGEMENT