Análisis de Riesgos

Existen normas para la gestión de la seguridad de la información como Esquema Nacional de Seguridad (ENS) ISO27001

Pero estas normas no establecen como se debe realizar el análisis de riesgo, para ello existen metodologías como Magerit o las ISO27005

Como medir el riesgos

Se tienen en cuenta la combinación de la probabilidad que ocurran y el impacto que puede provocar dicho riesgo. Cuanto mayores sean la probabilidad y el impacto, peor.

- El **impacto** se suele analizar calculando pérdidas económicas, reputacionales o pérdidas en el servicio. Se suelen usar escalas de 5 o 7 niveles yendo de extremadamenete bajo a extremadamente alto.
- Riesgo = Impacto (Consecuencias) * Probabilidad
- Formas
    - Cuantitativa: Cifra numérica
    - cualitativa
    - semicuantitativa: Permite establecer el valor de otros elementos.

Se suele hacer una tabla con la probabilidad y el impacto, marcando una zona roja, otra amarilla y una verde en función al riesgo siendo rojo el más alto y verde el más bajo.

El riesgo se puede analizar con las siguientes metodologías:

- **Octave**
    - Establecer un criterio de medición del riesgo
    - Desarrollar un perfil de información de los activos
- **Fair** (Factor Analysis of Information Risk)
- **Nist SP800-30**
    - Caracterización del sistema
    - Identificación de amenzadas
    - Análisis del control
    - Determinación de probabilidad de siceso
    - Analisis del impacto
    - Recomendaciones de control
    - Documentación resultante
- **ISO 27005**:
    - Identificación del riesgo:
        - Identificación de activos
        - Identificación de amenazas
        - Identificación de contorles existentes
        - Identifficación de vulnerabilidades
        - Identificación de consecuencias
    - Estimación del riesgo

        - Estimación de consecuencias
        - Estimación de posibilidad de incidente
        - Estimación del nivel de riesgo
    - Evaluación del riesgo

Puntuaciones de probabilidad del OWASP

Se tienen en cuenta los siguientes factores en caso de las personas:

- **Nivel de destreza** del agente que lanza una amenzasa: ¿Pueden ser el sistema explotado por un agente con poca destreza?
- **Motivo**: Recompensa alta o baja
- **Oportunidad**: Que oportunidades tiene un grupo de agentes de encontrar vulnerabilidades en el sistema.
- **Tamaño**: Como de grande es el grupo de agentes.

Se tienen en cuenta los siguientes factores en las vulnerabilideaes:

- Facilidad de descubrimiento
- Facilidad de explotación
- Facilidad de intrusión

Escala de impacto

- Nivel 1: Insignificante
- Nivel 2: Menor
- Nivel 3: Serio
- Nivel 4: Desastroso
- Nivel 5: Catastrófico

Existen 2 tipos de impactos:

- Impacto de negocio
    - Finaciero
    - Privacidad
    - Reputacional
- Impacto técnico
    - Confidencialidad
    - Integridad
    - Disponibilidad

Opciones del tratamiento del riesgo

- **Evitar el riesgo**: Tomar medidas que eliminen completamente el riesgo.
- **Reducir el riesgo**: Tomar medidas que mitiguen el riesgo.
    - Reducir la probabilidad de que ocurra
    - Reducir las consecuencias.

- **Trasferir el riesgo**
- **Aceptar el riesgo**: No tratarlo, tolerarlo. No confundir con no conocer el riesgo. Aunque no se trate, existen medidas de contingencia en caso de que ocurra.

Contramedidas

- A nivel operacional:
  - Controles físicos
  - Controles procedurales: Políticas empresariales
  - Controles técnicos: Equipamiento de red, firewalls...
- A nivel temporal:
  - Controles preventivos
  - Controles directivos
  - Controles detectores
  - Controles correcivos

Metodologías

Magerit

Indica un conjunto de pasos que se deben realizar al analizar el riesgo.

ISO27005