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**: como de fácil es para un agente descubrir la vulnerabilidad
- **Facilidad de explotación**: Como de fácil es para un grupo de agentes explotar la vulnerabilidad
- **Conocimiento**: Como de conocida es la vulnerabilidad entre el grupo de agentes.
- **Facilidad de intrusión**: Cual es la posibilidad de detectar el exploit.

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

Puntuaciones de Impacto del OWASP

Factores técnicos

- **Pérdida de confidencialidad**: Cuantos datos puieden ser difundidos y como de sensibles son.
- **Pérdida de integridad**: Cuantos datos pueden ser corrompidos o dañados
- **Perdida de disponibilidad**: Cuanto serivio puede ser perdido y como de vital es.

Factores de impacto de negocio

- **Daño financiero**: Cuanto daño financiero puede resultar de un exploit
- **Daño reputacional**: Cuando taño repuitacional puede provocar un exploit y como puede dañar al negocio.
- **No Cumplimiento**: Cuanta exposición puede provocar el no cumplimiento.
- **Violación de la privacidad**: Cuantos datos identificables pueden ser difundidos.

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

MAGERIT (Metodología de Análisis y GEstión de Riesgos para Information Technologies)

Indica un conjunto de pasos que se deben realizar al analizar el riesgo. Tiene los siguientes objetivos:

Objetivos

Objetivos directos

- Hacer que los responsables de los sistemas de la información sean conscientes de la existencia de riegos y la necesidad de mitigarlos a tiempo.
- Ofrecer un método sistemático para el análisis de dichos riresgos.
- Ayudar a describir y planear las medidas apropiadas para matener el riesgo bajo control.

Objetivos Indirectos

- Preparar la organización para el proceso de evaluación, auditoría, certificación y acreditación.

Dimensiones de la seguridad

- Confidencialidad, integridad y disponibilidad
- Autenticidad.
- Responsabilidad.

Método de Análisis de Riesgos

1. Determinar los **activos** relevantes de la organización, su valor y el coste causado por su daño o pérdida.
2. Determinar las **amenazas** a las que están expuestos dichos activos
3. Determinar que **salvaguardas** están disponibles y como de efectivas son contra el riesgo
4. Estimar el **impacto** de la aparición de una amenaza
5. Estimar el **riesgo**

ISO27005