

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 extremadamente 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
- Fair
- Nist SP800-30
 - Caracterización del sistema
 - Identificación de amenazadas
 - Análisis del control
 - Determinación de probabilidad de siceso
 - Análisis del impacto
- ISO 27005:
 - Identificación del riesgo:
 - Identificación de activos
 - Identificación de amenazas
 - Identificación de controles existentes
 - Identificación de vulnerabilidades
 - Identificación de consecuencias
 - Estimación del riesgo:
 - Estimación de consecuencias
 - Estimación de probabilidad de incidente
 - Estimación del nivel de riesgo
 - Evaluación del riesgo

Metodologías

Magerit

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

ISO27005

From:
<http://www.knoppia.net/> - Knoppia



Permanent link:
http://www.knoppia.net/doku.php?id=master_cs:gsi:tm1&rev=1757946367

Last update: **2025/09/15 14:26**