# Mapa metodológico de riesgos

## Tabla de contenidos



# 1 Introducción

## 1.1 Objetivo

Definir un proceso estructurado de análisis de riesgos de seguridad de la información conforme a ISO/IEC 27001, para evaluar el entorno de la sede de Barcelona y facilitar una toma de decisiones informada sobre salvaguardas necesarias.

## 1.2 Alcance

Incluye todos los activos IT y de información usados en la sede de Barcelona: portátiles, infraestructura, redes, software, personal técnico y datos de clientes.

## 1.3 Normativas y marcos utilizados

- ISO/IEC 27001:2013
- ISO/IEC 27005:2018
- MAGERIT v3.0

# 2 Definición de activos

## 2.1 Metodología

Se elaboró un inventario segmentado por tipo de activo: hardware, software, red, datos, personal y servicios, siguiendo la plantilla MAGERIT.

## 2.2 Criterios de valoración CID

Cada activo se valoró según:

- **Confidencialidad**: exposición ante fuga o acceso no autorizado.
- **Integridad**: posibilidad de modificación no autorizada.
- **Disponibilidad**: impacto de la interrupción del servicio.

## 2.3 Criticidad

Obtenida de la combinación CID (escala 1–5) y clasificada como Bajo, Medio, Medio-Alto, Alto o Crítico.

# 3 Identificación de amenazas

Para el catálogo de las amenazas se emplearon:

- Catálogo MAGERIT.
- Escenarios propios del contexto (ej. movilidad de consultores).
- Informes de vulnerabilidad (CVE, CERT).
- Amenazas comunes OWASP/NIST.

## 3.1 Catálogo de amenazas

Durante el análisis se ha adoptado un enfoque estructurado basado en la metodología MAGERIT v3.0, complementado con buenas prácticas de ISO/IEC 27005. Las amenazas se han clasificado en función de su origen y naturaleza, abarcando:

**Amenazas Internas**

- Acciones accidentales del personal (errores humanos).
- Acceso indebido por empleados con privilegios.
- Uso de dispositivos no autorizados (USBs, BYOD).
- Fallos de configuración por negligencia.

**Amenazas Externas**

- Ataques desde Internet (malware, ransomware, DDoS)
- Suplantación de identidad (phishing, ingeniería social)
- Robo de equipos en ubicaciones no controladas
- Intrusiones a través de redes públicas o no cifradas

**Amenazas Intencionadas**

- Sabotaje lógico o físico.
- Espionaje industrial o fuga de información.
- Manipulación de datos.
- Uso fraudulento de credenciales o accesos.

**Amenazas Accidentales**

- Fallos de hardware o software.
- Errores involuntarios en el manejo de datos.
- Saturación de recursos informáticos.
- Pérdida o corrupción de archivos.

**Amenazas Ambientales o Naturales**

- Incendios, inundaciones o cortes eléctricos.
- Condiciones ambientales inadecuadas (humedad, temperatura).
- Ruido electromagnético que afecte dispositivos.
- Desastres naturales (terremotos, tormentas).

## 3.2 Fuentes y herramientas utilizadas

Para identificar amenazas relevantes al entorno de la sede de Barcelona, se utilizaron diversas fuentes técnicas, normativas y empíricas:

- **Catálogo de amenazas MAGERIT v3.0**
- **Base de datos CVE/NVD**: vulnerabilidades explotables por amenazas técnicas.
- **Informes CERT nacionales (INCIBE, CCN-CERT)** y europeos (ENISA).
- **Top 10 de OWASP** para amenazas en aplicaciones web.
- **Normativa ISO/IEC 27005** como marco conceptual.
- **Entrevistas con personal técnico y de soporte.**
- **Historial de incidentes internos** registrados en ejercicios anteriores.
- **Observación directa de prácticas operativas y configuración de equipos.**

# 4 Identificación de vulnerabilidades

Métodos aplicados:

- Análisis documental y entrevistas.
- Revisión de configuraciones de red y VPN.
- Evaluación de prácticas del personal.
- Detección de puntos débiles (contraseñas débiles, uso de USBs, etc.).

# 5 Valoración de impactos

Escala cualitativa:

- Bajo
- Medio
- Alto
- Muy Alto
- Crítico

Ejemplo:
Una fuga de información de clientes se evaluó con impacto Muy Alto por implicaciones legales y reputacionales.

# 6 Valoración de probabilidades

Escala definida:
- Baja
- Media
- Alta

Factores analizados:
- Frecuencia de uso del activo.
- Exposición a amenazas externas.
- Historial de incidentes.

# 7 Cálculo del riesgo

Fórmula empleada:

Riesgo = Impacto × Probabilidad

Ejemplo de evaluación real:
- Portátiles: Riesgo Alto (Pérdida + movilidad).
- VPN: Riesgo Alto (contraseñas débiles).
- Datos clientes: Muy Alto (fuga).
- Personal: Muy Alto (ingeniería social).

# 8 Evaluación y aceptación de riesgos

Criterios establecidos:
- De Bajo a Medio: aceptables con controles mínimos.
- De Alto a Muy Alto: requieren mitigación inmediata o reducción del impacto.

Participantes:
Responsables de IT, Compliance, Seguridad, Dirección regional y Comité de Seguridad.

# 9 Tratamiento de riesgos

Controles definidos por riesgo:
- Pérdida de portátiles: Cifrado, MDM, bloqueo remoto.
- Acceso no autorizado (VPN): MFA, contraseñas robustas.
- Fuga de datos: Cifrado de emails, repositorios seguros.
- Ingeniería social: Formación, simulacros, antiphishing.

# 10 Monitoreo y revisión

Frecuencia de revisión:
- Anual (mínimo).
- Tras cualquier incidente relevante.

KRI utilizados:
- Nº de incidentes de seguridad.
- Tiempo medio de detección/respuesta.
- Estado de cumplimiento de políticas.

# 11 Documentación y evidencia

Registros clave:

- Inventario actualizado.
- Matriz de riesgos.
- Informes de auditoría y seguimiento.
- Planes de tratamiento.

Auditoría:
Todo el ciclo de vida del riesgo está documentado para revisión por parte de auditores internos/externos.

# 12 Comunicación y formación

Difusión de riesgos:
- Informes ejecutivos a dirección.
- Reportes técnicos al equipo IT.

Formación activa:
- Talleres de concienciación anuales.
- Simulacros de ingeniería social.
- Reglas claras sobre el uso de dispositivos externos y datos sensibles.