Incidentes de Ciberseguridad – UD2.2

Auditorías de incidentes de Ciberseguridad

IES Chan do Monte – Curso 2025/26

Docente: Simal Paz, Daniel

2.3. Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física

---

📑 Índice del apartado 2.3

2.3. Introducción: por qué importa la seguridad física

La ciberseguridad no es solo contraseñas y firewalls: también depende de la **protección física** de edificios, salas, equipos, documentos y del propio personal.

Si la seguridad física falla:

- alguien puede entrar al CPD y conectar un dispositivo malicioso,
- se pueden **robar equipos** con información sensible,
- un incendio, inundación o corte de energía puede dejar inservibles sistemas y copias de seguridad.

Por eso la seguridad física forma parte de los **sistemas de gestión de seguridad de la información (SGSI)** definidos en la familia de normas **ISO/IEC 27000**, especialmente **ISO/IEC 27001**. (ISO)

Para contexto general de la familia 27000:

- Página oficial ISO/IEC 27000 family:
  - https://www.iso.org/iso-iec-27000-family (ISO)

2.3.1 Tipos de riesgos físicos

Principales riesgos físicos que pueden afectar a una organización:

Acceso no autorizado

Acceso de personas **no autorizadas** a:

- CPD o salas de servidores,
- armarios de comunicaciones,
- archivos con documentación sensible.

Puede ser personal externo (intrusos, visitas, proveedores) o incluso personal interno sin permisos para esa zona.

Robo

Robo de:

- portátiles, móviles, tablets,
- discos externos, pendrives,
- mini servidores u otros dispositivos.

Si no hay cifrado, el atacante puede acceder a correos, documentos, datos personales, etc.

🔹 Caída de suministro

Afecta principalmente a:

- **electricidad** (apagones, picos de tensión),
- **comunicaciones** (corte de fibra, fallo de router).

Puede provocar paradas de servicio o daños físicos en equipos.

🔹 Clima y desastres naturales

Ejemplos:

- inundaciones, tormentas, filtraciones de agua,
- incendios, humo, explosiones,
- olas de calor (sobrecalentamiento),
- bajas temperaturas,
- tormentas eléctricas, terremotos…

🔹 Gestión deficiente de eliminación de recursos

Se produce cuando:

- se tiran o venden equipos con el disco duro intacto,
- no se realiza un borrado seguro de soportes (USB, discos, cintas),
- se sacan documentos en papel sin destrucción previa.

🔹 Falta de mantenimiento

Sin mantenimiento periódico:

- aumentan las averías,
- sube la temperatura en racks y CPD,
- se dispara la probabilidad de pérdida de datos y caídas de servicio.

2.3.2 Medidas de seguridad física

Para reducir estos riesgos se aplican medidas de seguridad física en varios bloques:

1. Control de acceso.
2. Disuasión y alerta.
3. Protección de activos físicos.
4. Protección frente a desastres y accidentes.
5. Protección de suministros.
6. Protección del personal.

---

a) Medidas de control de acceso

Controlan **quién entra, por dónde y a qué zonas**.

Ejemplos:

- **Elementos de apertura:** llaves, tarjetas, códigos, mandos.
- **Biometría:** huella, iris, cara, voz (para zonas críticas).
- **Personal de seguridad** en accesos.
- **Elementos físicos:** vallas, muros, bolardos, puertas reforzadas, torniquetes.

📌 Objetivo: que solo entren personas autorizadas y quede **registro de accesos**.

---

b) Medidas de disuasión y alerta

Buscan disuadir y detectar intentos de intrusión:

- **Videovigilancia (CCTV):** cámaras en entradas, pasillos, salas importantes.
- **Alarmas:** sensores de movimiento, apertura de puertas/ventanas, rotura de cristal… conectadas a una central o a vigilancia.

---

c) Medidas de protección de activos físicos

Protegen equipos, soportes y documentación:

- Servidores en **racks con llave** dentro de un CPD restringido.
- Sistemas de **localización** de portátiles y móviles.
- Documentos en papel en **archivadores con llave** o cajas fuertes.
- Destrucción segura de papel (destructoras, servicios especializados).
- Borrado seguro o destrucción de discos y soportes.
- Mantenimiento periódico de hardware y sistemas de climatización.

---

d) Medidas contra desastres naturales y accidentes

Reducen el impacto de incendios, inundaciones, calor, etc.:

- Elegir bien la ubicación del CPD (no en sótano inundable).
- Sistemas de detección y extinción de incendios específicos para CPD.
- Sensores de agua y temperatura.
- Protecciones contra sobretensiones y tormentas eléctricas.

En el contexto español, el **CCN-CERT** publica guías CCN-STIC sobre cómo aplicar el **Esquema Nacional de Seguridad (ENS)** y verificar medidas de protección física y ambiental:

- Portal de guías CCN-STIC: https://www.ccn-cert.cni.es/es/guias.html (CCN-CERT)

---

e) Medidas de protección de los suministros

Protegen **electricidad y comunicaciones**:

- **Tomas de tierra** adecuadas.
- **Reguladores de tensión** y protectores de sobretensión.
- **SAI** (sistema de alimentación ininterrumpida) para que los servidores aguanten unos minutos y se puedan apagar correctamente.
- Canalizaciones y tubos para proteger cableado externo.
- Bandejas y canaletas para proteger cableado interno.

---

f) Medidas de protección del personal

Orientadas a la **seguridad y salud** de trabajadores y técnicos:

- Equipos de protección individual (EPI) cuando sea necesario.
- Diseño de salidas de emergencia y rutas de evacuación.
- Señalización y cumplimiento de la normativa de prevención de riesgos laborales.

2.3.3 ISO/IEC 27001 y 27002 aplicadas a la seguridad física

La familia **ISO/IEC 27000** define el marco general de los SGSI. Dentro de ella:

- **ISO/IEC 27001** define los **requisitos** de un SGSI. (ISO)
- **ISO/IEC 27002** proporciona un **catálogo de controles** y guías de implementación, incluyendo controles físicos y ambientales. (ISMS.online)

Enlaces oficiales:

- ISO/IEC 27001 (ficha de la norma):
  - https://www.iso.org/standard/27001 (ISO)
- ISO/IEC 27002 (vista en línea de la norma):
  - https://www.iso.org/obp/ui/en/ (buscando 27002 en el buscador interno). (ISO)

2.3.3.1 Anexo A.11 de la ISO 27001 – Seguridad física y del entorno

El **Anexo A** de ISO/IEC 27001 recoge un conjunto de controles. El **A.11** (en la versión 2013) y los controles físicos correspondientes en la versión 2022 se centran en: (ISMS.online)

- **Áreas seguras**: perímetro físico, entrada segura, oficinas, CPD.
- **Seguridad del equipamiento**: ubicación, protección, mantenimiento, eliminación.
- Protección frente a amenazas externas (clima, vandalismo).
- Política de escritorio y pantalla limpia, etc.

Aunque el texto completo de la norma es de pago, hay resúmenes y explicaciones oficiales y de organismos de certificación:

- Explicación de Annex A.11 (ejemplo divulgativo):
  - https://www.hicomply.com/hub/iso-27001-annex-a-11-physical-and-environmental-security (hicomply.com)

2.3.3.2 Apartado físico de la ISO 27002

La **ISO/IEC 27002:2022** reúne los controles de seguridad (incluyendo controles físicos) y los agrupa en capítulos temáticos; el capítulo de **controles físicos** (capítulo 7 en la versión 2022) detalla buenas prácticas para: (ISMS.online)

- entrada física,
- seguridad de oficinas e instalaciones,
- protección de equipos,
- seguridad del cableado,
- protección frente a amenazas físicas y ambientales.

Ejemplo de recurso divulgativo sobre controles físicos en 27002:

- https://ictinstitute.nl/iso270022022-explained-physical-controls/ (ICT Institute)

2.3.3.3 Otros marcos de referencia: NIST SP 800-53 (PE)

Como complemento internacional, el estándar **NIST SP 800-53 Rev.5** (Estados Unidos) define una familia de controles llamada **PE – Physical and Environmental Protection**, centrada en proteger ubicaciones físicas frente a amenazas humanas y ambientales. (csrc.nist.gov)

Enlace oficial NIST:

- NIST SP 800-53 Rev.5:
    - https://csrc.nist.gov/pubs/sp/800/53/r5/final

2.3.4 Resumen y relación con los incidentes de ciberseguridad

- La **seguridad física** es un pilar de la seguridad de la información: si falla, la ciberseguridad lógica se puede ver comprometida fácilmente. (ISO)
- Existen múltiples **riesgos físicos** (accesos no autorizados, robos, desastres, mala eliminación de equipos, falta de mantenimiento…) que deben identificarse y tratarse.
- Para mitigarlos se aplican **controles físicos** (accesos, videovigilancia, protección de equipos, SAI, climatización, etc.), que se recogen en marcos como **ISO/IEC 27001/27002**, **ENS + guías CCN-STIC** y **NIST SP 800-53**. (ISO)
- Estos controles tienen papel **preventivo** (reducen la probabilidad de incidente) y, junto con cámaras, sensores y registros de acceso, también ayudan a la **detección, investigación y auditoría** de incidentes físicos que pueden acabar en incidentes de ciberseguridad.