

Definición del Alcance del SGSI

Organización: Hospital General Universitario "Sanitas Publica

Normativa Base: ISO/IEC 27001:2022 y Esquema Nacional de Seguridad (ENS).

1. Introducción

El Sistema de Gestión de Seguridad de la Información (SGSI) se establece para proteger la confidencialidad, integridad y disponibilidad de la información de los pacientes (PHI), personal y datos administrativos del Hospital.

2. Activos de Información (Inventario de Alto Nivel)

- **Críticos:** Base de datos de Historias Clínicas Electrónicas (HCE), Sistema de Imágenes Médicas (PACS), Servidores de Identidad (Active Directory).
- **Alto:** Datos de facturación, Nóminas del personal, Correo electrónico corporativo.
- **Medio:** Página web informativa, Wi-Fi de invitados.

3. Límites Físicos

El alcance incluye:

- **Sede Principal:** Edificio de Hospitalización y Consultas Externas.
- **Centro de Datos (CPD):** Ubicado en el sótano del edificio principal (Sala B-02).
- **Exclusiones:** Centros de atención primaria satélites (serán incluidos en la Fase 2).

4. Límites Virtuales

- Red LAN interna del hospital (VLAN Médica y VLAN Administrativa).
- Conexiones VPN para teletrabajo de personal administrativo.
- Nube híbrida (Azure) utilizada para backups cifrados.

5. Partes Interesadas (Stakeholders)

- **Internas:** Dirección Médica, Personal Sanitario, Departamento de TI, Pacientes.
- **Externas:** Ministerio de Sanidad, Proveedores de equipamiento médico, Agencia de Protección de Datos.