Selección de Controles

Aquí seleccionamos los controles del Anexo A de la ISO 27001 o NIST para mitigar los riesgos anteriores.

Control 1: Copias de Seguridad de la Información (Mitiga R01)

- **Referencia:** ISO 27001 A.8.13
- **Implementación:** Se establece una política de backup 3-2-1. Se realizarán copias diarias incrementales y semanales completas. Una copia se almacenará en una ubicación inmutable (offline) para proteger contra ransomware.

Control 2: Uso de Criptografía (Mitiga R02)

- **Referencia:** ISO 27001 A.8.24
- **Implementación:** Se forzará el cifrado de disco completo en todos los dispositivos portátiles del hospital a través de políticas de grupo .

Control 3: Autenticación Segura (Mitiga R03)

- **Referencia:** ISO 27001 A.5.17
- **Implementación:** Implementación obligatoria de Autenticación Multifactor (MFA) para todo acceso remoto (VPN) y para administradores de sistemas. Política de contraseñas de al menos 12 caracteres.

Control 4: Seguridad de las Operaciones (Mitiga R04)

- **Referencia:** ISO 27001 A.8.15
- **Implementación:** Implementación de un Firewall de Aplicación Web (WAF) y contratación de servicio anti-DDoS con el proveedor de internet.

Control 5: Política de Escritorio Limpio (Mitiga R05)

- **Referencia:** ISO 27001 A.7.7
- **Implementación:** Normativa que obliga a guardar documentos sensibles bajo llave y bloquear la sesión del ordenador al ausentarse.