Control: 7.5 Protección de equipos

1. Propósito

El control 7.5 requiere la implementación de medidas de seguridad física para proteger los equipos (servidores, *hardware* de red y almacenamiento) de riesgos ambientales y físicos, incluyendo robo, acceso no autorizado, desastres naturales, fallos de energía y variaciones de temperatura.

Para "Alerta Mujer", la protección física de los equipos que alojan la Base de Datos (BD) y los servidores de aplicación es vital para la **Disponibilidad 24/7 (RNF1.1)** y la **Integridad (5.25)** de la información sensible.

2. Procedimiento de Protección de Equipos

El enfoque de este control dependerá del modelo de *hosting* seleccionado. Este procedimiento establece los requisitos mínimos para la **selección de un proveedor** y la **protección del *hardware***.

2.1. Requisitos para el Centro de Datos / Sala de Servidores

Si el proyecto utiliza un servicio de *co-location*, un servidor dedicado o un centro de datos propio, se deben cumplir los siguientes requisitos de protección física:

- **Protección del Perímetro Físico (7.1):** Las salas de servidores deben tener **acceso controlado** con métodos como tarjetas de acceso o biometría. Solo el personal autorizado (DevOps/DBA con acceso privilegiado, 8.2) y el personal del centro de datos pueden ingresar.
- **Control Ambiental:**
    - **Climatización:** Se deben mantener sistemas de aire acondicionado redundantes para asegurar que la temperatura y la humedad se mantengan dentro de los límites de operación del *hardware*.
    - **Detección de Incendios:** Se debe contar con sistemas automáticos de detección y supresión de incendios (ej. gas inerte, no agua) dentro de la sala de equipos.
- **Suministro Eléctrico:** Los equipos críticos (servidores de BD y *firewalls*) deben estar conectados a **Sistemas de Alimentación Ininterrumpida (UPS)** y/o generadores de energía con capacidad para mantener el servicio durante cortes de energía prolongados (Control 5.27).

2.2. Protección del *Hardware* Individual

- **Garantía y Mantenimiento:** Los acuerdos de servicio (*SLAs*) del *hardware* deben incluir **garantías** y **planes de mantenimiento preventivo** para asegurar la operatividad de los servidores y evitar fallos por desgaste.
- **Ubicación y Cableado:** Los equipos deben instalarse en **racks bloqueados** para prevenir el acceso visual o la manipulación. El cableado de red y de alimentación debe ser organizado y protegido contra daños físicos accidentales.
- **Protección contra Variaciones:** Se deben instalar **supresores de picos de voltaje** para proteger el *hardware* de daños causados por descargas eléctricas o variaciones en la red.

2.3. Gestión de la Seguridad en la Nube (AWS/Azure/GCP)

Si el proyecto utiliza la nube pública, este control se gestiona mediante la **responsabilidad compartida**:

- **Responsabilidad del Proveedor:** El proveedor de la nube es responsable de la protección física de los Centros de Datos (control 7.5). El equipo de "Alerta Mujer" debe **verificar los certificados de seguridad física** del proveedor (ej. ISO 27001, SOC 2 Type II) (Control 5.23).
- **Responsabilidad del Cliente:** El equipo de "Alerta Mujer" sigue siendo responsable de la **configuración lógica** de los equipos virtuales (ej. *hardening* de la VM, Control 8.9) y de asegurar que el *hardware* de red local (ej. dispositivos de los desarrolladores) esté protegido (Control 7.13).