TEMA 4: Seguridad física y del entorno

"Boot is root", dicen. Podríamos traducir como "arrancar es entrar". Con claves en la BIOS, no tanto, pero las claves en la BIOS dificultan el botado cuando hay un CPD entero esperando, o no se está físicamente presente (encendidos remotos o planificados). En todo caso, el acceso a los sistemas de almacenamiento proporciona la información.

Se les puede proteger de forma lógica:

- Encriptación de ficheros, de discos virtuales...
- incluso full disk encryption (FDE)
    - Particularmente interesante para portátiles
    - Obligatoria en agencias gubernamentales de EEUU [fde-whitehouse]
    - enero 2009: anuncio de encriptación hardware por las principales fabricantes de discos [fde]

Y también se pueden adoptar controles de seguridad física, no sólo para prevenir robos o pérdidas y garantizar la confidencialidad, también la disponibilidad (accidentes, fuegos...) y la integridad

1. ÁREAS SEGURAS

Definición de perímetros de seguridad:

Normalmente por niveles:

1) Público: alrededores del edificio, recepción...
2) Restringido: zonas de carga y descarga, despachos, zonas de maquinaria...
3) Seguro: CPD, archivos...

Definición de personas/roles que pueden acceder a los perímetros

La principal área segura es el Centro de Proceso de Datos (CPD)

- Requiere medidas especiales
- Existe normativa específica sobre su construcción [TIA-942]
- Hay medidas de disponibilidad (tiers) basadas en la redundancia
- ... siempre y cuando tengamos un CPD
- Nuestra infraestructura puede estar en la nube (Amazon, Google, Rackspace, DigitalOcean...)
- podemos tener un centro de datos gestionado [cdg-telef]

RACK en CPD

Centro Informático Científico de Andalucía (CICA)

Control de acceso

- Barreras físicas que impidan el acceso
    - En CPDs, cuidado con el suelo técnico y falso techo.

- Autentificación+autorización de visitantes y trabajadores
    - DNI para visitantes, por ejemplo (CICA)
    - Tarjetas magnéticas, claves, biometría, combinaciones de métodos (autentificación de dos factores) para trabajadores

- Acceso de trabajadores (y quizá visitantes a algunas zonas) requiere autorización por responsables
- Registro de entradas/salidas con hora
- Revisión y purgado periódicos de la lista de autorizaciones y del registro de entrada/salida
- Visitantes acompañados (en algunas zonas) e identificados (tarjeta visible)

Protección de las áreas seguras

- Sistemas críticos fuera de zonas públicas.
- Si es posible, evitar carteles e indicaciones.
- Sistemas de detección de intrusiones (volumétricos, sensores en ventanas...).
- Suministros y materiales peligrosos o inflamables deben almacenarse aparte.
- Sistemas de respaldo y copias de seguridad a distancia. Mejor, en otro edificio.

2. SEGURIDAD DEL HARDWARE

Evitar riesgos físicos:

a) *Fuego* (= llamas+calor+humo+agua). Eliminación mediante gas (halón, por ejemplo; peligroso)

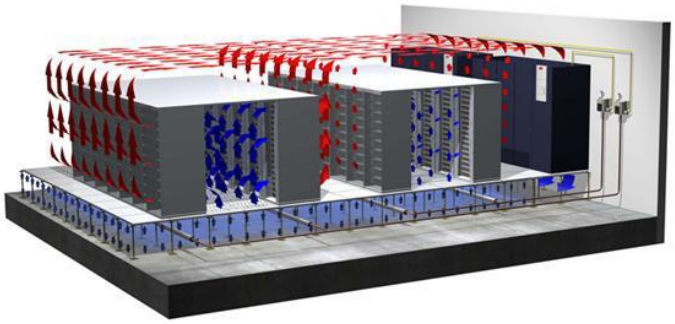
b) *Temperatura*. HVAC (heating, ventilation, air conditioning). Normalmente redundantes. Ventilación de racks y diseño adecuado de pasillos (p.ej.Cubo de agua).

c) *Humedad*. Poca: descargas estáticas. Mucha: condensación.

d) *Ruido eléctrico*. Producido por motores o líneas eléctricas mal aisladas.

e) *Polvo*. Ensucia partes móviles. Es ligeramente conductor. Buena ventilación y limpieza cuidadosa.

Cubo de agua:



Garantizar suministros:

- *HVAC (heating, ventilation, air conditioning)*: redundancia n+1
- *Agua / drenaje*
- *Electricidad*:
    - UPS (uninterruptible power supply) / SAI (sistema de alimentación ininterrumpida)
        - Estabilización (eliminación de ruidos, picos, caídas...)
        - Suministro de una determinada potencia (potencia aparente, medida en voltamperios, VA) durante un determinado tiempo. Suficiente para un apagado ordenado de los equipos.
        - Normalmente monitorizable: avisa de la condición de caída para iniciar el apagado de los equipos.
    - Generador de emergencia
        - Normalmente conectado al SAI.
        - Motor diesel+generador para garantizar un suministro contínuo

Evitar fugas de información:

- Cuidadosa colocación de pantallas con información sensible (evitar ventanas, pasillos, mostradores...)
- Cuidado con los terminales desatendidos:
    - Salvapantallas con clave
    - Desconexión automática de la sesión
- Impedir botado desde medios extraíbles
- Clave en BIOS
- Caja cerrada con llave

Cableado

- Etiquetado correcto para evitar errores
- Separación de cables de datos y cables de alimentación
- Enterrado u oculto
- Protección frente a intercepción
    - Canaletas metálicas de seguridad (posiblemente con detección de intrusiones)
    - Fibra óptica

Mantenimiento

- Deben monitorizarse los equipos para detectar fallos de forma proactiva (p.ej. SMART para los discos duros).
- Deben seguirse los programas y procedimientos de mantenimiento especificados por los fabricantes.

3. EQUIPOS MÓVILES

Incluyendo portátiles, PDAs, smartphones...

- El perímetro de seguridad ya no es tan controlable.
- El uso de equipos móviles debería requerir autorización.
- Los equipos deben estar siempre vigilados y deben transportarse de forma poco aparente.
- Candados tipo Kensington
- Los sistemas operativos y el software deben estar aún más protegidos y controlados por personal de la empresa
- Regulación del teletrabajo y del BYOD (bring your own device)

4. GESTIÓN DE MEDIOS

Almacenamiento de datos críticos

- Cajas fuertes
- Armarios ignífugos

Salida de soportes

- Envío de copias de seguridad a ubicaciones alternativas. Encriptadas y/o bajo llave.
- Registro de entrada/salida

Destrucción de soportes no necesarios

- Destrucción física (trituradoras de papel y CDs...)
- Borrado seguro: sobreescritura con varios patrones de bits. Desmagnetización (degaussing)

Bajas de equipos

- Destrucción previa de los datos contenidos en los mismos

Hay empresas especializadas, incluso.