Seguridad Pasiva: Equipos

Tema 3

Álvaro Rodríguez - IES Alonso de Madrigal (Ávila)
2º SMR

Seguridad Pasiva: Equipos

INTRODUCCIÓN

Las medidas de seguridad pueden ser pasivas o activas:

- Seguridad pasiva: destinada a solucionar o minimizar las consecuencias de un ataque o intrusión ya producida. Se centra en la arquitectura del sistema para reducir la superficie del ataque
- Seguridad activa: destinada a evitar posibles daños, detectando las amenazas y los ataques en tiempo real

Este tema va a tratar sobre la seguridad pasiva de los equipos, en especial de los Centros de Procesamiento de Datos (o CPD).

Veremos los siguientes aspectos de la seguridad:

1. **Ubicación del CPD**: protección, asilamiento, ventilación, suministro eléctrico, control de acceso...
2. **Centros de respaldo**
3. **SAI (o UPS)**

Seguridad Pasiva: Equipos

CENTRO DE PROCESAMIENTO DE DATOS (CPD)

Un centro de procesamiento de datos (o CPD) es la instalación que **centraliza las operaciones y la infraestructura** de TI de una organización, en la que se almacenan, procesan, tratan y difunden datos y aplicaciones.

Tienen una serie de características muy importantes para la seguridad:

- Al centralizar la infraestructura facilitan poner el foco principal de la seguridad en él, en lugar de en varias infraestructuras o sistemas diferentes
- La seguridad (tanto física como lógica) y confiabilidad son esenciales
- Consumen mucha energía y, al reunir tantos equipos en tan poco espacio, necesitan de unos buenos sistemas de ventilación y refrigeración
- Pueden tener diferentes funciones, pero principalmente: Almacenamiento, gestión, copia de seguridad y recuperación de datos; Aplicaciones de productividad, como correo electrónico; Transacciones de comercio electrónico; Big data, aprendizaje automático e inteligencia artificial

CPD: qué es un centro de procesamiento de datos y cómo funciona (xataka.com)

Seguridad Pasiva: Equipos

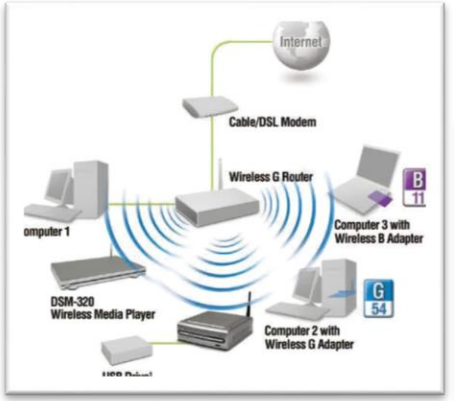
CENTRO DE PROCESAMIENTO DE DATOS (CPD)

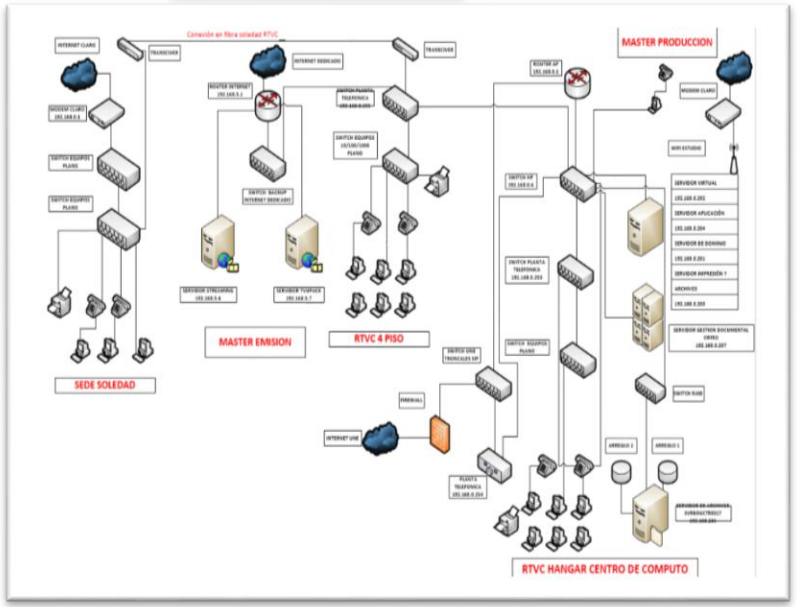
Cuando hablamos de un Sistema Informático podemos referirnos a cosas muy distintas: desde un ordenador personal a la gran infraestructura de todos los equipos informáticos de una empresa

(concepto de abstracción, importante en casi todas las áreas de informática)

Cuanto mayor y más complejo sea el sistema informático, más difícil es abordar la seguridad del sistema.

Por ello, ante infraestructuras informáticas grandes, aparece una manera de organizar los elementos más importantes del sistema, llamado Centro de Procesamiento de Datos.





Sistemas informáticos

Seguridad Pasiva: Equipos

UBICACIÓN DEL CPD

Las empresas colocan los **equipos de usuario cerca del usuario** (un ordenador sobre su mesa, un portátil que se lleva a casa); pero l**os servidores están todos juntos** en una misma sala. Esa sala tiene varios nombres: CPD (centro de proceso de datos), centro de cálculo, DataCenter, sala fría, «pecera», etc.

Centralizando se consigue:

- **Ahorrar** en costes de protección y mantenimiento. No necesitan duplicar la vigilancia, la refrigeración, etc.
- **Optimizar las comunicaciones** entre servidores. Al estar unos cerca de otros no necesitan utilizar cables largos o demasiados elementos intermedios que reducen el rendimiento.
- **Aprovechar mejor los recursos humano**s del departamento de informática. No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc.

Seguridad Pasiva: Equipos

UBICACIÓN DEL CPD

Todas las empresas deben tener documentado un plan de recuperación ante desastres que incluya:

- **Hardware**. Qué modelos de máquinas tenemos instalados (tanto servidores como equipamiento de red), qué modelos alternativos podemos utilizar y cómo se instalarán (conexiones, configuración).
- **Software**. Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc.).

- **Datos**. Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y cómo se hace el respaldo de datos (copias de seguridad).

Seguridad Pasiva: Equipos

ACTIVIDAD

- Investiga la reacción de la empresa Deloitte ante la pérdida de su CPD en el incendio del edificio Windsor de Madrid.

- Busca la clasificación de infraestructuras TIER 1 a 4 en las especificaciones del estándar ANSI\TIA-942.

Seguridad Pasiva: Equipos

PROTECCIÓN

Un CPD debe estar protegido al máximo en muchos aspectos:

- La **ubicación** debe plantearse según: probabilidad de accidentes naturales, proximidad a ríos, puertos, bases militares, industrias con procesos peligrosos...
- Elección de las **primeras plantas**: menos vulnerables a sabotajes, inundaciones, accidentes aereos, incendios...
- Edificio con **dos accesos:** Siempre habrá uno disponible y se permite el control de acceso con facilidad.
- Se recomienda **no informar de su ubicación** (por ejemplo: Noticia de 2012 --> El Data Center hoy en Google Maps)
- **Diseño adecuado del edificio: Pasillos** accesibles, anchos, con altura elevada y uso de falsos techos y suelos. Todo ello facilita la ventilación, la correcta distribución de cableado, etc.
- **Materiales** adecuados: cofre de hormigón, asilamiento de calor, de ruido y electromagnético, materiales ignífugos.
- **Equipos y sistemas** de detección de intrusos, de incendios, etc.

Seguridad Pasiva: Equipos

AISLAMIENTO

Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:

- **Temperatura.** Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.
- **Humedad**. No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.
- **Interferencias electromagnéticas.** El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.
- **Ruido.** Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico para no afectar a los trabajadores de las salas adyacentes.

Seguridad Pasiva: Equipos

ACTIVIDAD

1. Descarga y utiliza el programa Open Hardware Monitor
https://openhardwaremonitor.org/

2. ¿Qué valores mide este software?

3. Busca los valores "normales" en los que debería funcionar tu ordenador y compáralo con los datos que muestra

Seguridad Pasiva: Equipos

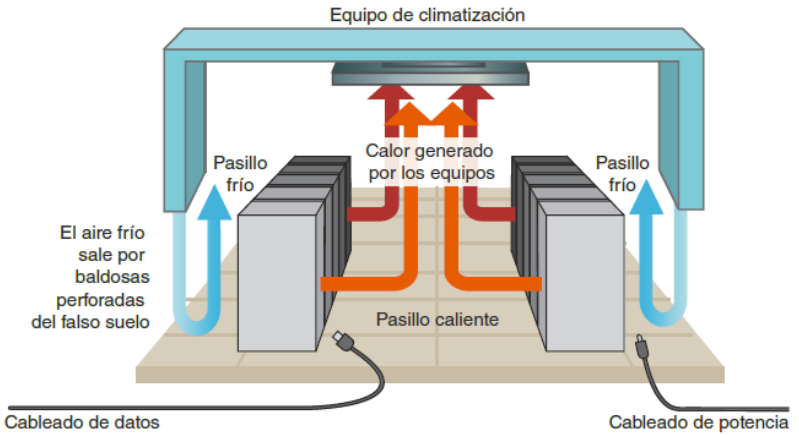
VENTILACIÓN

Los CPD **no suelen tener ventanas**: con ello se consigue mejorar el control de **acceso**, y mantener los valores de **temperatura** y **humedad** más constantes.
Se requiere **de ventilación artificial** para realizar todos estos controles.

La temperatura debe ser:

- Cercana a la ideal para el trabajo óptimo de las **máquinas**
- En un valor en el que los **trabajadores** puedan trabajar sin problemas

Para ello se configura una distribución de **pasillos calientes y fríos** como en la imagen



https://youtu.be/5MaDIHZYUQk?t=100

Seguridad Pasiva: Equipos

SUMINISTRO ELÉCTRICO Y COMUNICACIONES

Cualquier CPD necesita de ciertos servicios del exterior. Los principales son la alimentación eléctrica y las comunicaciones. Algunas **medidas** que se suelen tomar para asegurar estos dos recursos son:

- Tener que de servicio con varias empresas distintas, de manera que un fallo en una compañía suministradora no nos impida seguir trabajando
- **Separar el suministro** eléctrico del CPD del resto de la empresa
- Instalación **de generadores eléctricos** alimentados por combustible dedicados a los sistemas críticos
- Uso de varios **servicios diferentes de acceso** a comunicaciones: red de fibra, de ADSL u otra alternativa de conexión mediante red telefónica, red inalámbrica... de modo que si falla uno de los sistemas de suministro se siga teniendo otro disponible.

Seguridad Pasiva: Equipos

CONTROL DE ACCESO

Las máquinas del CPD son vitales para la empresa y solo necesitan ser utilizadas por un **reducido grupo** de especialistas. El acceso a esta sala de máquinas debe estar especialmente controlado.
Será vital tanto:

- Que nadie sin permiso pueda **acceder** al CPD y a las máquinas que se encuentran en ella
- Que nadie pueda **extraer** del CPD ninguna máquina o parte de ella.

Las **identificaciones** habituales (contraseñas, tarjetas de acceso) se complementan con medidas más seguras, como la **biometría**.
Se pueden utilizar además sistemas adicionales como: equipos de que de seguridad, red de que de presencia o **cámaras** de vídeo para detección de visitas inesperadas.

Seguridad Pasiva: Equipos

ACTIVIDADES

- Averigua qué sistemas de control de presencia y de acceso se utilizan en los equipos informáticos de los siguientes centros de trabajo: un banco, un ayuntamiento, un hospital, un supermercado

- Accede a la página web del Área de Sistemas de Información y Comunicaciones de la Universidad Politécnica de Valencia. (www.asic.upv.es). Indica las tareas que realiza y los servicios que ofrece. ¿Se le puede considerar un centro de proceso de datos? ¿Por qué?

- Imagina que el propietario de una pequeña tienda de golosinas acude a ti para que le asesores en cuanto a las medidas de seguridad a adoptar para evitar que los intrusos accedan al ordenador donde lleva la contabilidad, que está ubicado en la propia tienda. Indica qué sistemas de protección le recomendarías y por qué.

Seguridad Pasiva: Equipos

CENTRO DE RESPALDO

A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible.
Cuando se dispone de presupuesto suficiente, se debería instalar un segundo CPD, también llamado centro de respaldo (CR).

- En principio ofrecerá los mismos servicios que el centro principal, aunque si se requiere rebajar el presupuesto se puede limitar a unos servicios esenciales.
- Debe estar físicamente alejado del centro principal
- En condiciones normales, el CR está parado (stand-by), replicando los servicios del centro principal para que, en caso de necesidad, ningún usuario note el cambio. Se requiere una buena comunicación entre ambos CPD

Seguridad Pasiva: Equipos

ACTIVIDAD

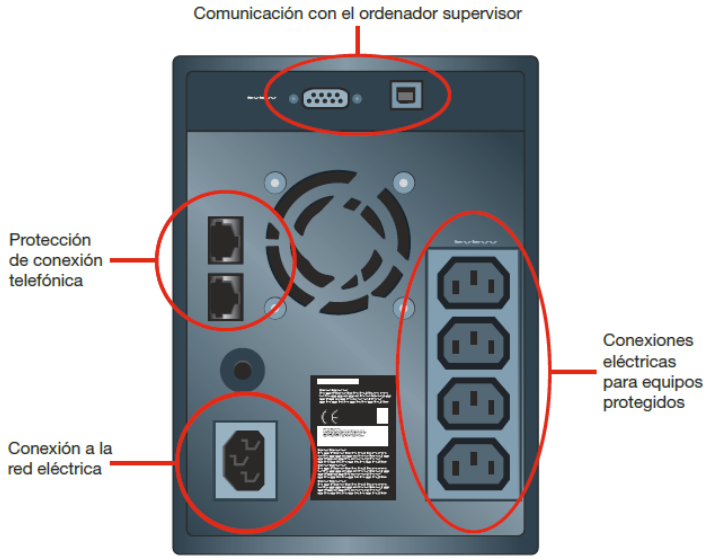
- La conmutación del CR al CP no siempre se debe a desastres en el CP. También puede ser una parada ordenada y planificada. ¿Se te ocurre algún ejemplo?
- En algunas empresas, el CR no está parado, sino que funciona al 100 %, en paralelo con el CP. Cuando uno falla, el otro asume toda la carga. Discute las ventajas y los inconvenientes de esta solución.

Seguridad Pasiva: Equipos

SAI/UPS

Anteriormente hemos dicho que como medida ante posibles fallos del suministro eléctrico podíamos contratar nuevos servicios o tener generadores eléctricos de respaldo. Existe otro recurso fundamental en cualquier centro de datos: Los **SAI (sistema de alimentación ininterrumpida),** en inglés UPS (Uninterruptible Power Supply).

En su versión más simple podemos decir que un SAI es un conjunto de baterías que alimentan una instalación eléctrica (en nuestro caso, equipos informáticos).
Sin embargo, existen diferentes tipos de SAI, que serán utilizados en función de las necesidades.



Seguridad Pasiva: Equipos

DISEÑO DE RED

En los CPD el diseño de la red cobra una importancia enorme, siendo necesario tomar en cuenta algunos aspectos que no son tan relevantes en redes locales pequeñas.
Algunos de esos aspectos son:

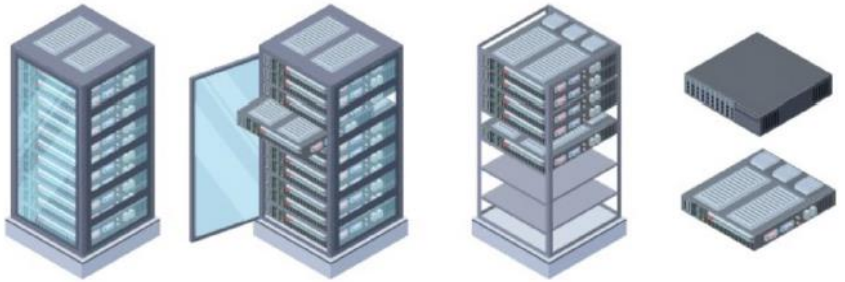
- Los armarios o racks
- La estructura del cableado
- La distribución de servidores
- El propio esquema de red: uso de switches y routers siguiendo topologías adecuadas.

Seguridad Pasiva: Equipos

DISTRIBUCIÓN DE SERVIDORES

A medida que la estructura de servidores se hace más grande se ve más necesario buscar una solución adecuada a la colocación y organización de los servidores. Podemos encontrar servidores:

- Tipo torre
- Orientados a estructuras modulares como los tipos Rack o Blade. Estos aportan una mayor:
  - Escalabilidad (puede aumentarse fácilmente el número de máquinas)
  - Optimización del espacio
  - Protección
  - Refrigeración
  - Facilidad en la distribución del cablea



Seguridad Pasiva: Equipos

ACTIVIDAD

Investiga sobre los distintos tipos de SAI que podemos encontrar, indicando para cada uno:

- Su nombre
- Qué ofrecen: Si aportan algo más que energía eléctrica ante fallos de suministro
- Cuándo entra en funcionamiento
- Diagrama de funcionamiento
- En qué casos es recomendable este tipo de SAI
- Algún ejemplo real de este tipo en una tienda, donde se vea el tipo de SAI, alguna foto y el precio.

Investiga sobre servidores

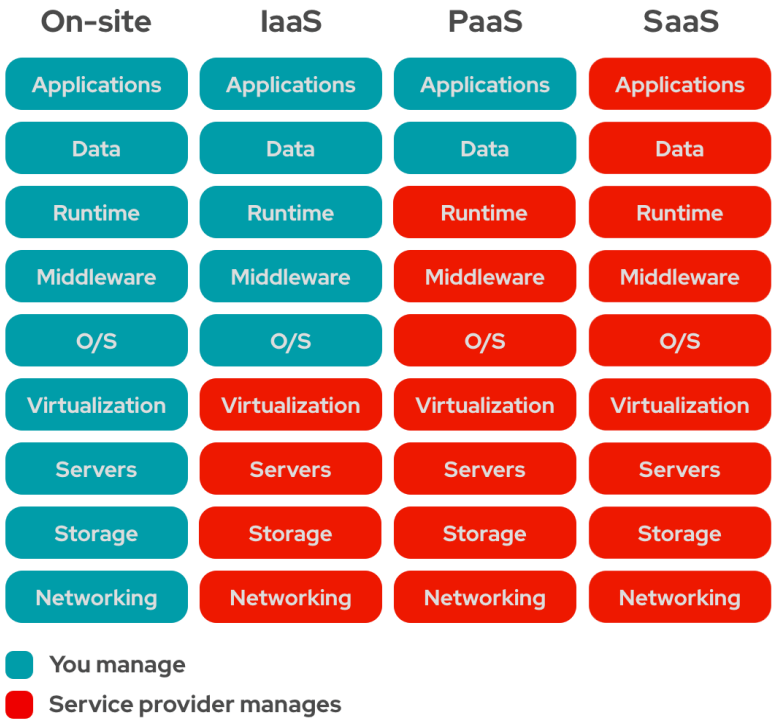
- Busca las diferencias entre servidores tipo Torre, Rack y Blade.
- Busca algún ejemplo real de servidores de cada tipo indicando el precio de cada uno de ellos.

Seguridad Pasiva: Equipos

LA ALTERNATIVA AL CPD: EL CPD EN LA NUBE

En ocasiones, bajo algunas circunstancias determinadas, muchas empresas optan por almacenar sus datos en la nube. Esto supone delegar la responsabilidad del mantenimiento y la disponibilidad de tus datos en un tercero.
Actualmente las empresas más importantes que dan este tipo de servicios son:

- Amazon, con sus Amazon Web Services (AWS)
- Microsoft, con Azure
- Google, con Google Cloud Servides



Seguridad Pasiva: Equipos

ACTIVIDAD

- Elige una de las tres grandes empresas de computación en la nube:
  - ØAmazon, Amazon Web Services (AWS)
  - ØMicrosoft, con Azure
  - ØGoogle, con Google Cloud Servides
- Investiga sobre qué soporte y garantías da con respecto a la seguridad de los datos. Recuerda tratar la seguridad de manera completa, siguiendo todos los ámbitos de las siglas CIDAN.

Seguridad Pasiva: Equipos

ACTIVIDAD

- Investiga sobre NextCloud o OwnCLoud.
  - ¿Qué es?
  - ¿Quién los utiliza?
  - ¿Cómo se implementa?

- Cómo se despliega cada uno de estos dos sistemas en Linux. Prueba a hacerlo en la máquina virtual de Parrot

Referencias

Seguridad informática. **José Fabián Roa Buendía**. **McGraw-Hill** España, 2013.

Seguridad informática (Edición 2020) **POSTIGO PALACIOS**, **ANTONIO**. Ediciones Paraninfo, S.A., May 19, 2020