



## **TEMA 053**

**EQUIPOS DEPARTAMENTALES. SERVIDORES. MEDIDAS DE SEGURIDAD PARA EQUIPOS DEPARTAMENTALES Y SERVIDORES. CENTROS DE PROCESO DE DATOS: DISEÑO, IMPLANTACIÓN Y GESTIÓN.**

<b>Versión</b>	<b>30.2</b>
<b>Fecha de actualización</b>	<b>12/09/2024</b>



## ÍNDICE

ÍNDICE .....	2
1. EQUIPOS DEPARTAMENTALES. SERVIDORES .....	3
1.1 TIPOS .....	3
1.2 CARACTERÍSTICAS .....	3
2. MEDIDAS DE SEGURIDAD PARA EQUIPOS DEPARTAMENTALES Y SERVIDORES .....	4
3. CENTROS DE PROCESO DE DATOS: DISEÑO, IMPLANTACIÓN Y GESTIÓN .....	5
3.1 CLASIFICACIÓN .....	5
3.2 SUBSISTEMAS .....	6
3.3 ELEMENTOS .....	7
3.4 DISEÑO .....	7
3.5 MÉTRICAS DE EFICIENCIA EN LOS CPD .....	9



# 1. EQUIPOS DEPARTAMENTALES. SERVIDORES

---

## 1.1 TIPOS

---

Tipos de ordenadores, según su propósito:

- **Miniordenador:** ordenador de nivel medio, cálculos complejos y **multiusuario**. Actualmente en desuso frente al **downsizing**, se puede sustituir hoy en día por el término genérico servidor.
- **Microordenador:** Ordenador de sobremesa o portátil. El término utilizado hoy en día es ordenador personal o PC.
- **Estación de trabajo (workstation):** ordenador de gran rendimiento, habitualmente dedicado a una tarea específica (CAD, edición de vídeo, ...). Son habitualmente equipos de escritorio con hardware dedicado de mayor capacidad para el propósito a que se orientan como pueden ser tarjetas gráficas profesionales, además de disponer de mayor capacidad y rendimiento de cpu, memoria o disco.
- **Superordenador** u ordenador de altas prestaciones (**HPC**): Ordenador de gran capacidad y potencia, para cálculos complejos y tareas especiales.
- **Ordenador central (mainframe):** ordenador grande, potente y costoso, dedicado habitualmente al procesamiento de grandes cantidades de datos. Prioriza la capacidad de E/S frente a cpu.
- **Servidores:** Término genérico para referirse a un ordenador que provee servicios a través de una red.

En función de sus prestaciones, puede establecerse el siguiente orden: Microordenador < Estación de trabajo < Miniordenador < Ordenador central < Superordenador.

Según la taxonomía de Flynn, las arquitecturas de ordenadores se pueden clasificar en:

- **SISD** (Simple Instruction Simple Data) → no hay paralelismo ni en instrucciones ni en datos, corresponde a la arquitectura tradicional de cpu monoprocesador.
- **SIMD** (Simple Instruction Multiple Data) → una única instrucción opera múltiples datos. Ejemplos: arquitectura vectorial o matricial. También instrucciones multimedia de procesadores actuales, como SSE o MMX de Intel o 3dNow de AMD.
- **MISD** (Multiple Instruction Simple Data) → Múltiples instrucciones operan sobre un flujo de datos. No es una arquitectura habitual, generalmente se usa para tolerancia a fallos.
- **MIMD** (Multiple Instruction Multiple Data) → Múltiples procesadores autónomos ejecutando instrucciones sobre datos diferentes (como procesadores multicore/multinúcleo). Incluye sistemas multiprocesador o distribuidos, con esquemas de memoria compartida o distribuida.

## 1.2 CARACTERÍSTICAS

---

Un servidor (host o anfitrión) es un equipo informático especializado, habitualmente con altas capacidades de proceso, encargado de proveer diferentes servicios a las redes de datos o conjunto de ordenadores interconectados entre sí.

Los principales aspectos a tener en cuenta son:

- **Fiabilidad:** Dispone de múltiples elementos redundantes (fuentes de alimentación, tarjetas de red, discos, ...) para ofrecer la máxima disponibilidad en el tiempo, ante fallos del hardware o mantenimientos necesarios.
- **Facilidad de operación y mantenimiento:** Por ejemplo, herramientas de gestión remota y monitorización.
- **Eficiencia energética:** Una parte importante del coste de un CPD es el suministro energético, así



como la refrigeración del mismo. Los requisitos energéticos y de refrigeración de los servidores son fundamentales para una buena planificación y control del centro de datos en conjunto.

- **Capacidad de actualización o ampliación.**

Principales componentes:

- **Procesador:** los servidores actuales suelen admitir varios procesadores, cada uno con múltiples núcleos.
- **Memoria RAM:** Habitualmente en servidores se emplea memoria más fiable que en pc, con detección y corrección de errores ECC (*Error Code Correction*) como “Códigos de Hamming”.
- **Placa base:** Integran todos los dispositivos internos, incluyendo los buses de comunicaciones (USB, puertos serie/paralelo, red, etc.), buses de disco (SATA, SAS, ...) o de conexión de tarjetas de expansión (PCI, PCIe, ...).
- **Disco:** Generalmente disponen de sistemas RAID, de forma que el fallo de un disco no detiene el servicio.
- **Fuente de alimentación:** Son fuentes con un diseño robusto dado que deben estar encendidos periodos muy largos de tiempo. Generalmente están redundadas (2 o más fuentes).

Principales formatos:

- **Enracables:** servidores preparados para ser integrados en un rack o armario. Tienen dimensiones normalizadas (Unidades rack o simplemente “U”). Permiten una mayor consolidación y modularidad.
- **Torre:** No se colocan en un armario.
- **Blade:** Se integran en un chasis específico y proporcionan los mismos servicios que otros servidores en el mínimo espacio físico. Comparten algunos elementos (por ejemplo, las fuentes de alimentación) situados en el chasis, en lugar de disponer de ellos por cada servidor.
- **Sistemas convergentes:** se trata de sistemas que agrupan en un único equipo físico tanto la potencia de cálculo (el propio servidor), almacenamiento empresarial y comunicaciones. Al ser un único equipo estos elementos están ya integrados y su gestión y soporte se realiza desde un punto común.
- **Sistemas hiperconvergentes:** Al igual que los sistemas convergentes son equipos que agrupan cómputo, almacenamiento y comunicaciones. A diferencia de ellos utiliza tecnologías de virtualización del hardware para ofrecer una infraestructura definida por software (*SDDC – Software Defined Data Center*).

## 2. MEDIDAS DE SEGURIDAD PARA EQUIPOS DEPARTAMENTALES Y SERVIDORES

---

**A nivel físico:**

- Acceso físico al equipo (rack cerrado con llave, sala con acceso restringido).
- Redundancia de la fuente de alimentación.
- Redundancia de discos (RAID).
- Redundancia de comunicaciones (doble tarjeta de red, interfaz de gestión dedicada como puede ser la ILO de HP).
- Refrigeración (ventiladores redundados).



- Herramientas de monitorización a nivel físico (Nagios, Cacti, IBM Systems Director, Fujitsu ServerView, HP SIM).

#### A nivel lógico:

- Segmentación de la red: Separación de la red en zonas de seguridad, de forma que un fallo de seguridad en un servidor no comprometa toda la red. Disponer de VLAN distintas al menos para la red de servidores en la DMZ. En un caso extremo la **microsegmentación** (habitualmente realizada en entornos virtualizados) limita el acceso a red de cada servidor en función de su rol.
- Utilización de gestores de ancho de banda.
- Cortafuegos.
- Cortafuegos WAF (*Web Application Firewall*).
- Un sistema gestor de información de eventos de seguridad SIEM (*Security Information and Event Management*).
- Auditorías de Seguridad, escaneos periódicos de seguridad.
- Protección Anti-Spam & Anti-Virus.
- Bastionado (deshabilitar servicios inseguros o no utilizados, configuración segura de base, etc.)
- Política de actualizaciones de software de base.
- Backups, copias remotas, etc.
- Herramientas de seguridad como IDS/IPS y sondas. Por ejemplo, SAT-INET del CCN-CERT.
- Procedimientos reglados para la administración de servidores (instalación de software, conexión a red de nuevos servidores, acceso remoto, contraseñas, etc.).
- Política de mínimos privilegios.

Se recomienda ampliar la información sobre medidas de seguridad a través de la lectura del ENS (*Esquema Nacional de Seguridad*) - RD 311/2022 y de las Guías CCN-STIC, que se abordan con mayor profundidad en el Tema 48 del temario.

## 3. CENTROS DE PROCESO DE DATOS: DISEÑO, IMPLANTACIÓN Y GESTIÓN

Se pueden definir como aquellas ubicaciones donde se concentra el equipamiento para prestación de servicios TIC a una o varias organizaciones, disponiendo para ello de las infraestructuras para prestar estos servicios de manera gestionada, eficiente en coste, sostenible, predecible y con los requisitos de calidad, seguridad, eficiencia y robustez requeridos.

La norma que especifica los requisitos para la infraestructura de centros de datos es **ANSI/TIA-942-C** (*Telecommunications Infrastructure Standard for Data Centers*)

### 3.1 CLASIFICACIÓN

Puede establecerse una primera clasificación en cuanto al destinatario de los servicios proporcionados:

- CPD **corporativos o empresariales**, que proveen servicios a la propia organización, formando parte de su proceso de TI.



- CPD de **servicios gestionados**. Estos centros de datos son administrados por un tercero (o un proveedor de servicios administrados) en nombre de una empresa. La empresa alquila los equipos y la infraestructura en lugar de comprarlos.
- CPD de **colocación**. Son gestionados por una empresa que alquila el espacio y la infraestructura (refrigeración, seguridad, ancho de banda, etc.) a otras empresas para que estas alojen aquí sus componentes (servidores, enrutadores, cortafuegos, etc.).
- CPD en la **nube**. Los datos y aplicaciones se alojan en una infraestructura virtual en la nube, contratado como un servicio a través de un proveedor, como Amazon Web Services (AWS), Microsoft (Azure) o IBM Cloud u otro proveedor de nube pública.

Otra clasificación en cuanto al rol en la prestación de servicios:

- **CPD principal**, que provee servicios de forma habitual a la organización, encontrándose de forma general en operación continua (solo interrumpe su servicio por intervención planificada o en caso de desastre).
- **CPD de respaldo**, recuperación ante desastres o de contingencia, destinado a proporcionar un mecanismo alternativo para la prestación de los servicios en caso de que exista algún problema con el centro principal, por necesidades de interrupción del servicio debido a una intervención, o por desastre o avería grave. Los centros de respaldo pueden ser de diferentes tipos según las necesidades de tiempos de recuperación del desastre.
  - **Sala fría**: el centro de respaldo externo cuenta con toda la infraestructura requerida para replicar el centro de procesamiento de datos principal a partir de copias de seguridad. Es el método más barato, pero también requiere tiempo para trasladar los datos de una infraestructura a otra.
  - **Sala caliente**: son centros de respaldo que funcionan de forma análoga al CPD principal. Todos los datos que son introducidos en el CPD base se replican en la sala caliente, por lo que en caso de contingencia solo es necesario restaurar los datos en el último momento. Es un modelo más caro, pero mucho más rápido.
  - **Centro espejo**: es una versión avanzada de las salas calientes. En él, se replican los datos en tiempo real, por lo que es necesario utilizar redes de alta velocidad. Es el modelo más rápido y fiable, pero también el más caro.
  - **Mutual Backup**: se produce cuando dos empresas llegan a un acuerdo para hacer un respaldo de datos mutuo. Ambas deben reservar un espacio para los servidores de respaldo de la otra.

## 3.2 SUBSISTEMAS

---

De acuerdo con el estándar TIA-942, la infraestructura de soporte de un CPD estará compuesta por cuatro subsistemas:

- **Telecomunicaciones**: Cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y alimentación redundantes, patch panels y latiguillos, documentación.
- **Arquitectura**: Selección de ubicación, tipo de construcción, protección ignífuga y requerimientos NFPA 75 (Sistemas de protección contra el fuego para información), barreras de vapor, techos y pisos, áreas de oficina, salas de UPS y baterías, sala de generador, control de acceso, CCTV, NOC (Network Operations Center).
- **Sistema eléctrico**: Número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, puesta a tierra, EPO (Emergency Power Off- sistemas de corte de emergencia) baterías, monitorización, generadores, sistemas de transferencia.
- **Sistema mecánico**: Climatización, presión positiva, tuberías y drenajes, CRACs (Computer Room Air Conditioner) y condensadores, control de HVAC (High Ventilating Air Conditionning), detección de incendios y sprinklers, extinción por agente limpio (NFPA 2001), detección por aspiración (ASD), detección de líquidos.



### 3.3 ELEMENTOS

---

Según los estándares definidos por la norma TIA-942, generalmente en un centro de proceso de datos deberíamos encontrar los siguientes elementos, desde el punto de vista de organización de las comunicaciones:

- **Centro de operaciones:** oficina aledaña a las salas de servidores en donde se encuentran los operadores y técnicos de operación y soporte. Dispone habitualmente de sistemas de monitorización e inspección remota. Habitualmente se realiza también el control de acceso a las salas.
- **Sala de entrada:** Contiene los elementos de comunicaciones de los proveedores de acceso, así como almacenes o áreas de carga y descarga.
- **Sala principal:** Sala que contiene los servidores y otros equipos que forman parte del CPD. Habitualmente cuenta con un falso suelo para el mantenimiento más sencillo del cableado, y los equipos se distribuyen en armarios (rack) situados en hileras.
- **Armarios de comunicaciones:** La norma TIA-942 presenta un enfoque estructurado de los elementos de conectividad estableciendo una arquitectura en estrella, con una zona principal de distribución que agrupa el cableado del “backbone” de red, así como los conmutadores, enrutadores y centralitas del “core” de la LAN. Esta norma incluye el cable de categoría 6A como el nuevo mínimo.

### 3.4 DISEÑO

---

Los aspectos de diseño más relevantes a la hora del diseño de un centro de proceso de datos tienen mucho que ver con los requisitos de disponibilidad de los servicios que alberga.

La norma TIA-942 recoge la clasificación en “tiers”, que proporcionan un marco de evaluación de la disponibilidad de los servicios de TI que puede ofrecer un centro:

- **Tier 1 (CPD básico):** No hay redundancia en administración eléctrica y refrigeración. Puede tener o no suelo elevado y SAI (Sistema de Alimentación Ininterrumpido). El servicio puede interrumpirse por paradas programadas o no programadas. Tasa máxima de disponibilidad: 99,671 % (que equivaldría a ~28,82 horas al año de servicio interrumpido).
- **Tier 2 (CPD redundante):** Menos susceptible a paradas programadas o no. Tiene componentes redundantes. Tiene suelos elevados y SAI. Una única línea de distribución eléctrica y refrigeración. Tasa máxima de disponibilidad: 99,741 % (que equivaldría a ~22,69 horas al año de servicio interrumpido).
- **Tier 3 (CPD concurrentemente mantenible):** Permite planificar mantenimiento sin afectar al servicio, pero pueden existir paradas no planificadas. Tiene componentes redundantes, múltiples líneas de distribución eléctrica y de refrigeración, pero con una sola activa. Tasa máxima de disponibilidad: 99,982 % (que equivaldría a ~1,58 horas al año de servicio interrumpido).
- **Tier 4 (CPD tolerante a fallos):** Sin pérdida de servicio por paradas programadas, es capaz de soportar un evento no programado del tipo “peor escenario” sin pérdida de servicio. Múltiples líneas de distribución eléctrica y refrigeración, con múltiples componentes redundantes (ej.: 2 SAI redundados). Tasa máxima de disponibilidad: 99,995 % (que equivaldría a ~26,28 minutos al año de servicio interrumpido).

Son muchos los factores que influyen en el diseño de un centro de proceso de datos:

- Ubicación
- Distribución y uso del espacio de la sala
- Sistema eléctrico y de generación
- Sistemas de refrigeración
- Sistemas de detección y extinción de incendios



- Emplazamiento de los armarios o bastidores
- Cableado para la red de datos
- Monitorización y vigilancia

### 3.4.1 Sistema eléctrico y de generación

---

El “Uptime Institute” recomienda considerar el suministro de las compañías eléctricas como un suministro auxiliar de bajo coste, y la generación en el propio centro (mediante células de combustible, generadores u otros medios fiables), con el respaldo de unidades de suministro ininterrumpido (SAI).

- **Grupos electrógenos:** los generadores más habituales son los grupos electrógenos a gasolina o diésel.
- **Sistemas de alimentación ininterrumpida (SAI):** su potencia se mide en kVA.
- **Ruta de distribución y cuadros eléctricos:** es recomendable que existan dos rutas de suministro al equipamiento en paralelo.

### 3.4.2 Sistemas de refrigeración

---

Las condiciones de climatización se resumen en una temperatura entre 18°C y 27°C y una humedad relativa entre 30% y 50%.

Técnicas de climatización de aire:

- Sistemas de expansión directa (DX)
- Sistema de refrigeración por condensación en torre de refrigeración
- Sistemas de gestión de aire centralizado
- Entrega de aire a baja presión
- Técnicas de pasillo frío/caliente
- Refrigeración por aire exterior (“free-cooling”)
- Cerramiento de pasillos
- Cerramiento de bastidores

### 3.4.3 Sistemas de detección y extinción de incendios

---

Sistema de **detección** de incendios:

- Detectores de calor: termostáticos, termovelocimétricos y combinados.
- Detectores de humo: ópticos e iónicos.
- Detectores de gases.
- Detectores de llama.
- Detectores multisensor.

Sistema de **extinción** de incendios:

- Agua nebulizada.
- Mediante aspersión de gas inerte. Los gases más comunes son: Novec 1230, FE-13, FM-200 y CO<sub>2</sub>.





### 3.5 MÉTRICAS DE EFICIENCIA EN LOS CPD

- **Power Usage Effectiveness (PUE)**

El PUE hace referencia a la eficacia del uso de la energía y es la métrica más común a efectos de comparación y benchmarking. Se define como:

$$PUE = \text{Consumo total} / \text{Consumo del equipamiento TI}$$

Dado que, en la realidad, un PUE de 1 es un objetivo imposible, el objetivo estándar para la mayoría de Data Center es lograr un PUE inferior a 2. Además, el PUE objetivo para un Data Center de nueva construcción (dada la tecnología actual) debería ser inferior a 1,2; mientras que los Data Centers más energéticamente eficientes ya son capaces de alcanzar PUEs por debajo de 1,06.

- **Carbon Usage Effectiveness (CUE)**

El CUE hace referencia a la eficacia del uso del carbono, y mide las emisiones de carbono que emite un centro de datos a diario. Mientras que el PUE tiene un valor ideal de 1,0, el CUE tiene un valor ideal de 0,0.

- **Water Usage Effectiveness (WUE)** o efectividad del uso del agua.

