# Capítulo 2 Estado del arte

## 2.1 Evolución de los CPD

Un vistazo a la evolución de los CPD en las últimas décadas nos muestra que dicha evolución ha sido cíclica.

Según [Kas09], inicialmente el CPD los constituían los *mainframes*. Los *mainframes* eran computadoras de gran tamaño ubicadas en salas exclusivas que tenían la capacidad de ejecutar a la vez varios sistemas operativos, funcionando como varias máquinas virtuales. Poseían una gran potencia y velocidad, pero su principal problema era su elevado coste, tanto en desembolso inicial como en su puesta en marcha y mantenimiento, lo que desencadenó el avance hacia nuevas plataformas, más rápidas y baratas.

Fue durante los años 70 y 80 cuando los minicomputadores se convir*tier*on en una alternativa a los *mainframes*. Eran más pequeños, más baratos, y no requerían una ubicación tan específica como los *mainframes*.

La computación paralela apareció en los años 80. Los terminales empleados para interactuar con los sistemas *mainframe* fueron gradualmente reemplazados por redes de ordenadores personales conectados a servidores. Los sistemas de computación paralela permitían que muchos dispositivos trabajasen simultáneamente en la resolución de un problema.

La computación distribuida aparece en forma de ordenadores independientes conectados a través de una red de comunicaciones trabajan en un objetivo común. Una de las principales características de los entornos de computación distribuida es que todos los sistemas operativos están disponibles para los pequeños servidores de bajo coste. Las aplicaciones podían compartirse entre las estaciones de trabajo, que se convertían en servidores que servían a muchos usuarios.

A pesar de que este sistema proporcionó una gran libertad a la computación, fue también una de las causas de la creciente complejidad que ha llevado a las principales tendencias de hoy en día hacia la consolidación y la simplificación. Se fomentaron la dispersión y los entornos caóticos, ya que cada propietario gestionaba su minicomputador como deseara y cada vendedor tenía su propio sistema operativo. Pronto, muchos vendedores ofrecían ordenadores con sistema operativo UNIX. Este fue el comienzo de la computación distribuida moderna.

Con el tiempo, Linux y Windows NT han crecido en popularidad en los CPDs, pero UNIX permanece como el más común y más desarrollado. UNIX es el único sistema operativo capaz de soportar adecuadamente múltiples aplicaciones en una única instancia del sistema operativo. También permite la gestión de la carga de trabajo. A pesar de que los sistemas

operativos UNIX no están todavía presentes en los *mainframes*, las características de gestión de carga de trabajo proporcionan un adecuado soporte para la consolidación.

El siguiente paso en la evolución de los CPDs fue el *Grid Computing*, que hacía uso de las comunicaciones sobre internet para trabajar en un determinado problema. Utilizaba todos los recursos de varios ordenadores para funcionar como un supercomputador. La cima del *grid computing* fue en los años 90. Su principal uso era una única aplicación que requería una gran cantidad de fuentes dedicadas.

A mediados de los años 90 aparecen los primeros *clusters*. Un *cluster* es un conjunto de ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como una única unidad, empleada para mejorar el rendimiento, la eficiencia y la disponibilidad, siendo además más económico que computadores individuales. Los componentes de hardware de un *cluster* son básicos, como los de cualquier PC, capaz de ejecutar un sistema operativo Unix, con adaptadores Ethernet estándar. No contienen ningún componente hardware personalizado y es fácilmente reproducible.

La libertad en el diseño de sistemas y aplicaciones fue beneficiosa en el sentido de que las aplicaciones se desarrollaban y salían al mercado con mucha rapidez. Mientras que esto supuso una gran ventaja competitiva en el entorno de negocio, conllevó un coste considerable. Se produjo un aumento del número de servidores en los CPDs, lo que provocó que la complejidad de gestionar estos servidores aumentara considerablemente, aumentando así mismo el coste de gestión global.

Es entonces cuando aparece la virtualización. Una máquina virtual es una implementación de una máquina en *software* que ejecuta programas como si fuera una máquina física. Los sistemas con máquinas virtuales permiten compartir los recursos físicos de la máquina anfitriona (*host*) entre diferentes máquinas virtuales huéspedes (*guest*), cada una ejecutando su propio sistema operativo.

Tras esto, apareció el concepto de Nube (*Cloud*). La Nube representa la utilización de recursos a través de internet, de forma flexible, y pagando únicamente por el consumo efectuado. Esto nos lleva a los conceptos de Infraestructura como servicio (IaaS, *Infrastructure as a Service*), Plataforma como servicio (PaaS, *Platform as a Service*) y Software como servicio (SaaS, *Software as a Service*).

La Infraestructura como servicio consiste en la externalización del equipamiento empleado para soportar las operaciones, incluyendo los componentes de *hardware* de almacenamiento, servidores y red [Scc12]. Hace que el acceso a recursos como servidores, conexiones, almacenamiento o herramientas relacionadas con Internet, sea fácil y asequible, permitiendo a las empresas desarrollar un entorno de aplicaciones bajo demanda, en el que pagas por lo que usas.

La Plataforma como servicio facilita el acceso a sistemas operativos y servicios asociados sobre Internet sin necesidad de descargas o instalación [Scc12]. Hace que el despliegue y

escalabilidad de una aplicación sea trivial y sus costes razonables y predecibles – una plataforma en la que cada uno puede desplegar sus aplicaciones.

Las aplicaciones de SaaS es un modelo de distribución de software en el que las aplicaciones son almacenadas por un vendedor o proveedor de servicios y puestas a disposición de los consumidores a través de una red (típicamente Internet) [Scc12]. Son aplicaciones para el usuario final, no propietarias, bajo demanda y sin TI tras ellas.

Hoy en día la tendencia vuelve a ser la consolidación, con el fin minimizar la complejidad del CPD. Reduciendo el número de dispositivos a gestionar se minimizan también las formas de gestionarlo, y se simplificará la infraestructura del CPD. Una infraestructura más simple permite gestionar el CPD con mayor eficiencia, además de reducir el coste total de propiedad (TCO, *Total Cost of Ownership*).

## 2.2 Los CPDs en la actualidad

A medida que la información se ha convertido en un factor clave para los negocios y para la continuidad de los mismos, se requería una solución más robusta que implicase garantizar una fuente de alimentación secundaria (grupo electrógeno), sistemas de alimentación ininterrumpida (SAIs), refrigeración, detección y extinción de incendios, control de acceso, monitorización, etc. Por este motivo la necesidad de establecer y mantener un CPD eficiente surge cuando las organizaciones demandan continuidad, disponibilidad y escalabilidad para la estabilidad de sus negocios.

Cada día, las organizaciones de todo el mundo generan información de manera exponencial que necesita ser almacenada y mantenida en instalaciones que almacenen ingentes cantidades de datos. El CPD se convierte en un centro de operaciones crítico de cualquier negocio. El coste del tiempo de inactividad es tan elevado que la disponibilidad de las tecnologías IT es la mejor métrica para evaluar el CPD.

## 2.3 Problemas de los CPDs

En un estudio realizado por Emerson Network Power[1] en 2011 [Eme11a] basándose en las respuestas proporcionadas por 41 empresas de distintos sectores (financiero, telecomunicaciones, sanidad, gobierno,…) se estima que el coste medio por minuto de la caída de un CPD es 5.600$, basados en la pérdida o corrupción de datos, pérdida de productividad, daños en el equipamiento, repercusiones legales, repercusiones en la reputación de la compañía, y un largo etcétera.

[1] Emerson Network Power es una empresa líder global en soluciones de redes de comunicaciones, CPDs, servicios de salud e instalaciones industriales. Web: www.emerson.com.

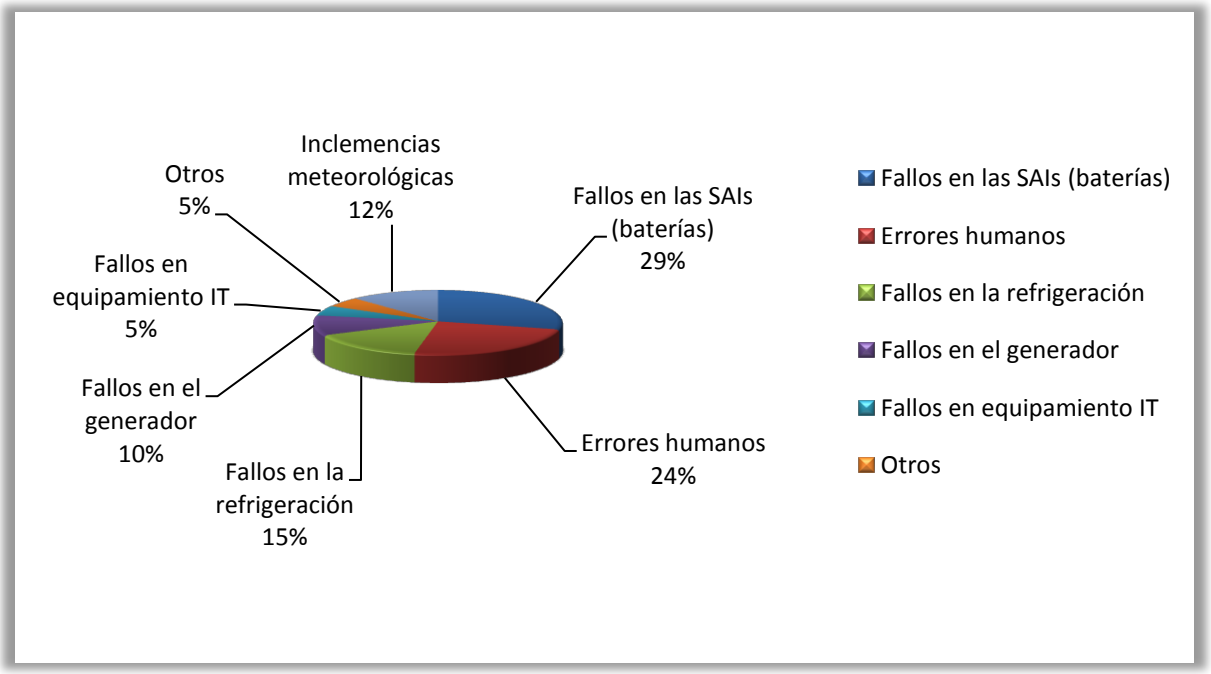



**Ilustración 1: Causas de paradas de servicio**

Como se muestra en la Ilustración 1 [Eme12], la mayoría de las causas de las paradas de servicio del CPD fueron fallos en las infraestructuras de alimentación y refrigeración. Sin embargo, otro gran porcentaje se corresponde a los errores humanos, por lo que es imprescindible promover los buenos hábitos en el CPD.

La disponibilidad se mide como un porcentaje de tiempo y normalmente se representa utilizando el número de "nueves". Cuantos más nueves de disponibilidad, más cercano al 100% de tiempo activo tiene el CPD. Otra forma de entender la disponibilidad es considerar el tiempo que el CPD está sin servicio por año (Tabla 1, de *Designing the Data Center (BICSI)*).

| Nivel de Disponibilidad | Porcentaje | Tiempo de caída por año |
|---|---|---|
| Seis Nueves | 99,9999 | 32 segundos |
| Cinco Nueves | 99,999 | 5 minutos, 15 segundos |
| Cuatro Nueves | 99,99 | 52 minutos, 36 segundos |
| Tres Nueves | 99,9 | 8 horas, 46 minutos |
| Dos Nueves | 99 | 3 días, 15 horas y 40 minutos |

**Tabla 1: Niveles de disponibilidad del servicio**

### *Niveles (Tiers)*

Cuanto mayor sea la disponibilidad que queramos alcanzar para nuestro CPD, mayor será el número de niveles de infraestructura que deberá tener.

A la cantidad de infraestructura requerida para soportar todos los servidores o equipos de red que estén funcionando en el CPD, se le denomina capacidad *N*.

Este término puede aplicarse a todos los tipos de infraestructura, pero comúnmente se emplea para la alimentación de respaldo (o *standby*), refrigeración, y red del CPD.

*N* es el nivel más bajo para el que se diseña y construye un CPD. Sólo tiene los componentes imprescindibles para que funcione. *N+1* es el siguiente nivel. La infraestructura *N+1* puede soportar el CPD a capacidad completa e incluye un componente adicional, de modo que puede continuar funcionando normalmente si falla un único componente. Otros niveles superiores son *N+2*, *N+3*, y siguientes incrementando el número de componentes redundantes. Un nivel más alto es *2N* e implica duplicar el número de componentes requeridos.

A pesar de que cada nivel añade protección, también añade complejidad. Paradójicamente, a medida que la complejidad aumenta, mayor es la probabilidad de que ocurra un error, bien durante la instalación, bien durante una emergencia, cuando el sistema de respaldo se necesita. Además el coste aumenta proporcionalmente a la redundancia.

El Uptime Institute[2] introduce el concepto de los *tiers*. El *tier* indica la fiabilidad de un CPD asociado a cuatro niveles de disponibilidad definidos. A mayor número de *tier* mayor disponibilidad. Existen cuatro *tiers* [Par2010]:

- *Tier* I – Básico: 99.671% de disponibilidad
    - Línea de distribución de potencia y refrigeración única. No existen componentes redundantes (*N*).
    - Puede tener suelo elevado, SAIs o generadores.
    - Tiempo de inactividad de 28.8 horas al año.
    - Requiere una parada completa al menos una vez al año para realizar tareas de mantenimiento.
- *Tier* II – Componentes redundantes: 99.741% de disponibilidad
    - Menos susceptible a interrupciones por actividades planeadas o no planeadas.
    - Línea de distribución de potencia y refrigeración única. Incluye componentes redundantes (*N+1*).
    - Incluye suelo elevado, SAIs y generador/es.
    - Tiempo de inactividad de 22 horas al año.

[2] Organización enfocada a mejorar el rendimiento y la eficiencia del CPD. Propietaria del sistema de Certificación de *Tier* para CPDs.

- El mantenimiento de algunas partes de la infraestructura requiere una interrupción del servicio.

- *Tier* III – Mantenimiento simultaneo: 99.982% de disponibilidad
  - Permite interrupciones planificadas por mantenimiento sin afectar al servicio, pero eventos imprevistos pueden provocar paradas no planeadas.
  - Múltiples líneas de distribución de potencia y refrigeración, pero solo una activa. Incluye componentes redundantes (*N+1*).
  - Tiempo de inactividad de 1.6 horas al año.
  - Incluye suelo elevado y suficiente capacidad para soportar toda la carga en una de las líneas de distribución mientras se realizan tareas de mantenimiento en la otra.

- *Tier* IV – A prueba de fallos: 99.995% de disponibilidad
  - Las interrupciones planificadas no afectan al servicio y el CPD puede resistir al menos una interrupción no planificada sin que tenga impacto en la carga crítica.
  - Múltiples líneas de distribución de potencia y refrigeración. Incluye múltiples componentes redundantes (*2(N+1)*).
  - Tiempo de inactividad de 0.4 horas al año.

### *Parámetros de fiabilidad*

Además de la disponibilidad, existen ciertos parámetros que miden la fiabilidad del sistema. De acuerdo con [CEM12], dichos parámetros son:

#### *MTBF, Tiempo medio entre fallos*

El MTBF (*Mean Time Between Failures*) representa el tiempo de funcionamiento correcto del SAI entre dos fallos consecutivos.

#### *MTTR, Tiempo medio de reparación*

El MTTR (*Mean Time To Repair*) representa el tiempo que estará el SAI fuera de servicio a causa de reparaciones.

#### *Disponibilidad*

La disponibilidad viene definida por la siguiente fórmula:

$$A = \left(1 - \frac{MTTR}{MTBF}\right) * 100$$

### 2.3.1 Eficiencia y huella de carbono

Las dos magnitudes más extendidas para medir la eficiencia energética del CPD son las siguientes:

- *Power Usage Effectiveness* (PUE). Fue creado por los miembros del *Green Grid*[3]. Consiste en dividir la potencia total suministrada al CPD entre la potencia que consume el equipamiento IT. La máxima eficiencia es 1.
- *Data Center Infrastructure Efficiency* (DCIE) es el recíproco del PUE y se expresa como un porcentaje, que mejora a medida que se acerca al 100%.

Asociada a la eficiencia energética está la huella de carbono. La huella de carbono es la cantidad de gases de efecto invernadero generada por el CPD. Al igual que en otros sectores, debido en parte al encarecimiento de la energía y también a la cada vez mayor conciencia ecológica, reportar la huella de carbono está siendo cada vez más habitual. En los CPD se consume mucha electricidad y se genera mucha energía térmica que se desperdicia. El uso de CPDs supone un consumo del 1% de la energía a nivel mundial y las TIC suponen ya el 2% de las emisiones globales de gases de efecto invernadero a la atmósfera [Gar07]. En los últimos años, el coste de los servidores ha seguido una tendencia descendente y prácticamente se ha visto superado por el coste de la electricidad que consumen, tal como muestra la Ilustración 2 (de IDC, 2006).

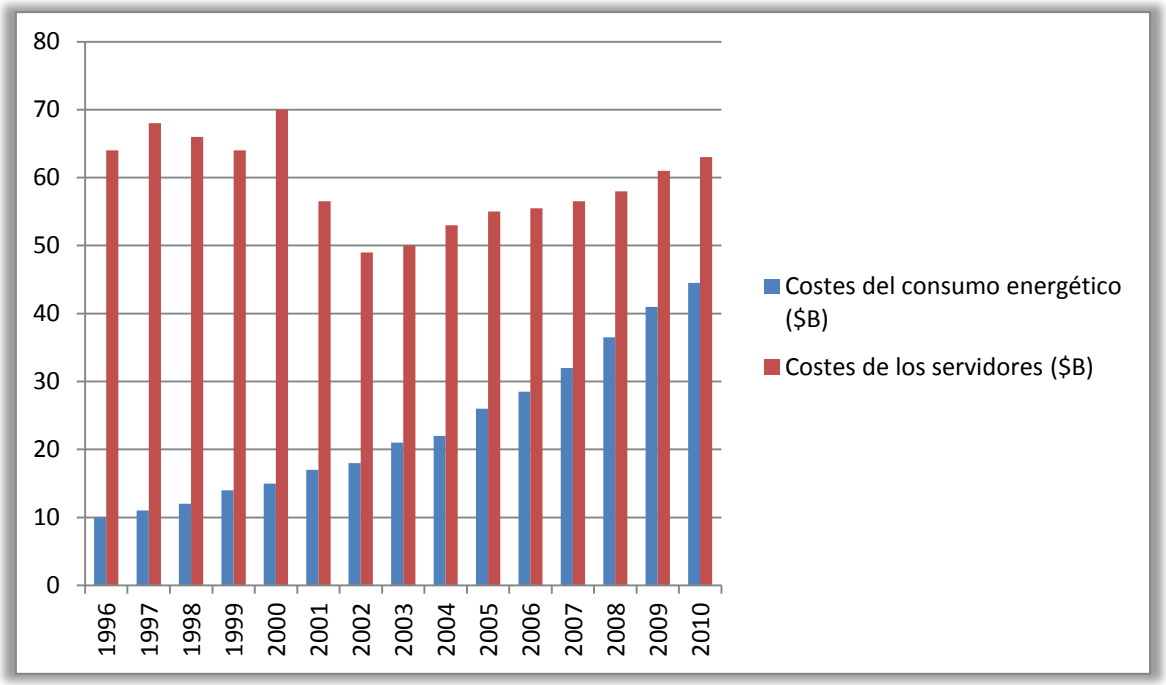



Ilustración 2: Evolución de los costes de servidores vs. Consumo energético

[3] *Green Grid:* Asociación de profesionales TI que busca aumentar la eficiencia de los CPDs.

En un CPD, a grandes rasgos, la mitad de la energía la consume el equipamiento TIC y la otra mitad los sistemas de soporte (alimentación y refrigeración), como se advierte en la Ilustración 3 [Eme12]:

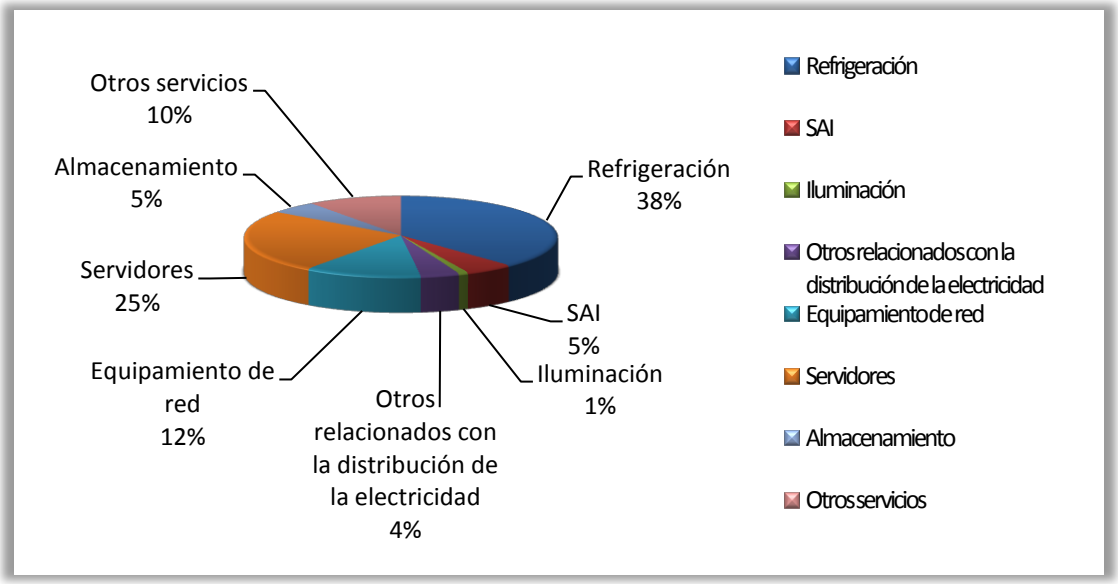



Ilustración 3: Distribución del consumo energético del CPD

Existe un efecto cascada al mejorar la eficiencia a nivel de componente de servidores, amplificándose en una menor demanda de los sistemas de apoyo. El ahorro de 1W de energía a nivel de componentes del servidor implica un ahorro total de 2,84W [Eme11b].

En cuanto a la refrigeración, todo equipo eléctrico produce calor, que debe extraerse para evitar que la temperatura del equipo aumente hasta un nivel inaceptable. La energía transmitida por el equipamiento TIC a través de las líneas de datos es insignificante. Por tanto, toda la energía que se consume de la red de suministro de alimentación de corriente alterna se convierte principalmente en calor, de modo que la energía térmica producida por los equipos de TI en vatios (W) iguala al consumo energético en vatios. La energía térmica total producida por un sistema es la suma de la energía térmica producida por cada uno de sus componentes. El sistema completo incluye los equipos de TIC, además de otros elementos como SAIs, unidades de aire acondicionado, iluminación y personas. Las unidades de aire acondicionado crean una cantidad importante de calor, que se extrae al exterior y no crea una carga térmica dentro del centro de datos, pero que afecta de forma negativa la eficiencia del sistema de aire acondicionado y normalmente se tiene en cuenta al dimensionar el mismo.

Las contribuciones de las SAIs y la distribución de alimentación a la energía térmica producida se amplifican por el hecho de que el sistema está funcionando normalmente sólo a un 30% de su capacidad [Ras12]. Si el sistema funcionara al 100% de su capacidad, la eficacia de los sistemas de alimentación se incrementaría y sus contribuciones a la energía térmica producida por el sistema disminuirían. El sobredimensionamiento del sistema conlleva una disminución de la eficacia, pero no siempre es evitable.

La demanda de infraestructuras y sistemas de información es cada vez más elevada y esto se traduce en una demanda energética cada vez mayor. El problema del ahorro energético es, por lo tanto, crucial para todas las empresas.

## 2.4 Coste Total de Propiedad (TCO) y Retorno de Inversión (ROI)

La infraestructura física del CPD es la base de las tecnologías de la información y de las redes de comunicaciones. Sus elementos suministran la potencia, refrigeración, espacio físico, seguridad, protección contra incendios y cableado, lo que permite el funcionamiento de las TIC. El valor de negocio de una organización está basado en tres objetivos: incrementar los ingresos, reducir costes y utilizar mejor los activos. Los tres están orientados a mejorar las ganancias [Tor11].

Inicialmente, el cálculo del valor de la infraestructura física del CPD estaba basado en el coste inicial y la disponibilidad, pero los continuos cambios en los entornos TIC han establecido dos criterios adicionales: flexibilidad y TCO. La flexibilidad es la capacidad del sistema para adaptarse a los cambios, lo que implica velocidad de despliegue, escalabilidad y habilidad para reconfigurarse. El coste inicial (*CAPex*) es solo una parte del TCO. Deben tenerse en cuenta también los costes de operación y mantenimiento (*OPex*) para hacerse una idea completa del negocio.

Predecir y calcular el TCO de la infraestructura física del CPD es necesario para realizar análisis de Retorno de Inversión (ROI, *Return of Investment*).

El desglose del coste de los componentes del CPD (Ilustración 4 [Eme12]) puede darnos una perspectiva sobre las oportunidades para controlar o reducir el TCO en varias áreas.

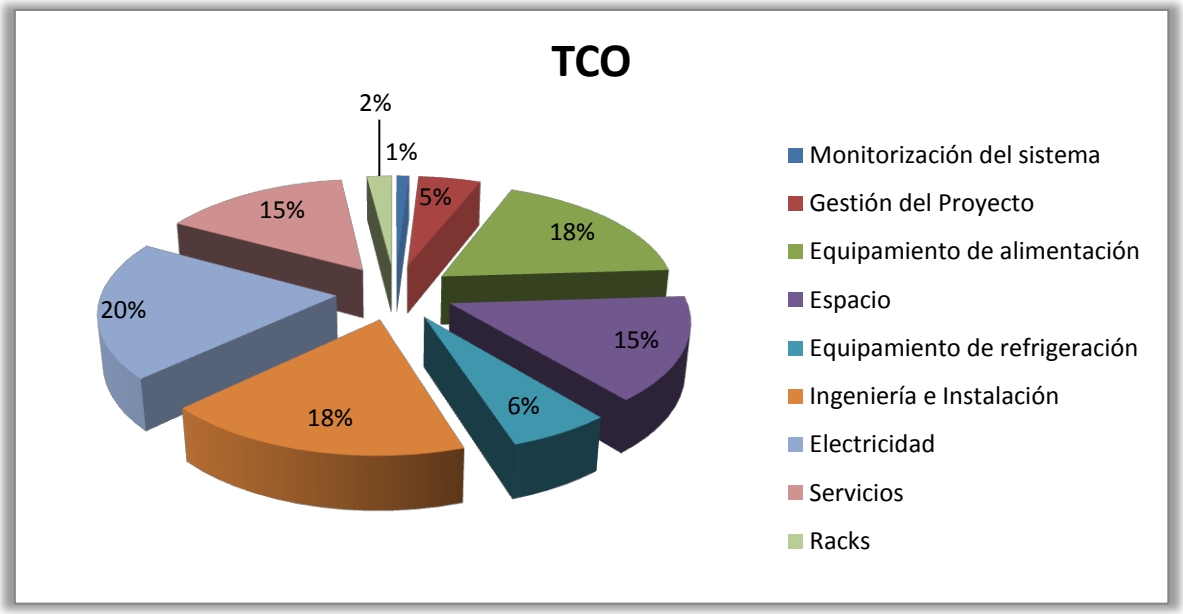



Ilustración 4: Coste Total de Propiedad

La mayoría de los ahorros se obtienen de redimensionar adecuadamente, por dos razones. La primera, el CPD que no se necesita nunca debería construirse. Segunda, la infraestructura que se necesita no debería desplegarse hasta que realmente se necesite, haciéndolo de un modo escalable para poder seguir creciendo de acuerdo a las necesidades futuras.

## 2.5 Estrategias de diseño

La primera decisión en el proyecto de un CPD es si alquilar un espacio para servidores a una compañía externa, o construirlo dentro de la suya. En el primer caso, los servidores están fuera de la empresa, en un CPD propiedad de otra compañía. Esta compañía proporciona y mantiene toda la infraestructura: alimentación, conectividad, refrigeración, sistemas de prevención/extinción de incendios, control de temperatura,… Los costes del alquiler de un CPD subcontratado vienen generalmente determinados por la superficie y los *racks* que los servidores ocupan, cuánta potencia consumen, y que cantidad de conectividad y soporte necesitan. En el segundo caso, el espacio y toda la infraestructura pertenecen a la propia empresa. La empresa establece el diseño, supervisa la construcción, lo gestiona y proporciona el soporte una vez que está en funcionamiento. Todo esto convierte a la empresa en responsable del CPD a la vez que le otorga completo control sobre él. La diferencia entre ambos radica en la propiedad, responsabilidad, acceso y costes.

Para crear un CPD resistente deben seguirse cinco estrategias de diseño [Alg05]:

1. **Robusto**: Sobretodo, un CPD debe ser resistente. La razón de la existencia de un CPD es salvaguardar el equipamiento más crítico de una compañía y sus aplicaciones. No importa qué catástrofes ocurran fuera, el CPD debe mantenerse operativo. La infraestructura debe estar preparada para no tener ningún punto único de vulnerabilidad.
2. **Modular**: El CPD debe diseñarse en segmentos intercambiables. Cabinas de servidores con idéntica infraestructura agrupadas en filas idénticas. La modularidad aporta al CPD simplicidad y escalabilidad.
3. **Flexible**: Cuanto mejor responda el CPD a los cambios, mayor valor tiene para los negocios. El nuevo equipamiento debe instalarse rápida y fácilmente, con el mínimo coste e interrupción de la operatividad. El CPD debe construirse empleando componentes fáciles de cambiar o mover.
4. **Estándar**: A pesar de que el CPD esté constituido de infraestructuras completamente diferentes unas de otras, debe diseñarse manteniendo una misma apariencia, señalización, código de colores, etiquetado,… Estandarizar el CPD facilita la resolución de problemas y asegura un control de calidad.
5. **Buenos hábitos**: Los usuarios del CPD siempre van a buscar la solución más rápida a los problemas y la de menor dificultad. Por este motivo, debe proporcionárseles accesibilidad y simplicidad para que ejerciten buenos hábitos.

# Parte I: Diseño de un CPD

De todo lo anterior podemos resumir que el CPD no son sólo los equipos de TI en los que reside la información de la organización. El CPD es también toda la infraestructura que garantizará el correcto funcionamiento de los equipos de TIC para que dicha información no se pierda.

A continuación veremos una breve descripción de cada una de las infraestructuras que detallaremos en los siguientes capítulos.

- Obra: Se refiere al área que ocupa el CPD y sus espacios asociados, como cuartos de electricidad y salas de almacenamiento y/o desembalaje. Suelos, techos, paredes.
- Energía: Suministro eléctrico, sistemas de alimentación ininterrumpida, grupo electrógeno, luminaria, toma de *tier*ra. Incluye paneles eléctricos, conductos y registros. La alimentación eléctrica es suministrada generalmente por un proveedor externo.
- Climatización: El sistema de climatización se compone de una unidad interior que absorbe el calor, una unidad exterior que lo libera, un compresor (aumenta la presión) y válvula de sobrepresión, y su principal misión radica en extraer el calor del CPD.
- Sistema de protección contra incendios (PCI): Incluye los sistemas de detección y los de extinción.
- *Racks*: Son los habitáculos donde se instalan los sistemas de información (servidores y comunicaciones).
- Cableado: Se trata del sistema de cableado estructurado del CPD. Cobre y fibra óptica son los medios típicos y terminan en varios tipos de conectores estandarizados.
- Seguridad: Controles de seguridad como lectores de tarjeta o cámaras de video vigilancia. Sistemas de monitorización.

Dichas infraestructuras son las que contribuirán a proporcionar la disponibilidad y seguridad requerida por los equipos de TIC que se encuentren en su interior.

# Capítulo 3 Instalaciones de Obra

Como ya se comentó en el capítulo anterior, la información se ha convertido en el primer patrimonio de las empresas. Por ese motivo, el CPD es una instalación de alto riesgo. La seguridad constituye, por consiguiente, uno de los principales problemas en todo CPD. El CPD deberá estar estructuralmente protegido contra fuego, agua e intrusiones.

## 3.1 Normativas

Existen normativas, tanto nacionales e internacionales, para definir el comportamiento de los elementos constructivos frente al fuego, agua, polvo e intrusiones:

- UNE-EN 13501-1[4] [Aen10a]: Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación. Parte 1: Clasificación a partir de datos obtenidos en ensayos de reacción al fuego.
- DB SI [CTE07]: Documento Básico de Seguridad en caso de Incendio que forma parte del CTE[5] y que tiene por objeto establecer reglas y procedimientos que permiten cumplir las exigencias básicas de seguridad en caso de incendio.
- UNE 20324 [UNE93]: Equivalente a la norma europea EN 60529[6]. Trata los grados de protección proporcionados por las envolventes en cuanto a la penetración de cuerpos sólidos y agua (Códigos IP).
- UNE-EN 50102 [UNE95]: Trata los grados de protección proporcionados por las envolventes contra impactos mecánicos nocivos (Códigos IK).
- DIN EN 1627[7] [DIN11]: Sistemas de protección antirrobo.

### 3.1.1 Resistencia al fuego de los elementos constructivos

Existen tres características principales del comportamiento de resistencia al fuego [VLV+10]:

[4]Normas UNE. Nomenclatura de Una Norma Española, normas creadas por AENOR (Asociación Española de Normalización y Certificación). Se trata de documentos de aplicación voluntaria que contienen especificaciones técnicas basadas en los resultados de la experiencia y del desarrollo tecnológico.

[5]CTE, Código Técnico de Edificación, es el marco normativo que establece las exigencias que deben cumplir los edificios en relación con los requisitos básicos de seguridad y habitabilidad establecidos en la Ley 38/1999 de 5 de noviembre, de Ordenación de Ordenación de la Edificación (LOE).

[6]Estándar Europeo, EN. Se trata de estándares que han sido adoptados por una de las tres organizaciones europeas de estandarización: CEN, CENELEC o ETSI.

[7]Deutsches Institut für Normung, (Instituto Alemán de Estandarización), DIN.

- *R*: Capacidad portante, es el tiempo durante el cual el elemento mantiene su resistencia mecánica.
- *E*: Integridad, es el tiempo durante el cual el elemento impide el paso de las llamas y la producción de gases calientes en la cara no expuesta al fuego.
- *I*: Aislamiento, es el tiempo durante el cual el elemento cumple su función de aislante térmico para que no se produzcan temperaturas excesivamente elevadas en la cara no expuesta al fuego.

Todos ellos seguidos de un número que representa el tiempo en minutos durante el cual se cumplen las exigencias. Por ejemplo, una pared con resistencia al fuego EI-120 es una pared cuya integridad y aislamiento perduran durante al menos 120 minutos.

Estos parámetros se combinan dependiendo de las características del elemento, siendo las más comunes R, EI y REI.

### 3.1.2 Reacción al fuego

Existen siete clases de reacción al fuego, que representan la inflamabilidad y contribución al fuego:

- A1: No combustible; sin contribuir al fuego en grado máximo.
- A2: No combustible; sin contribuir al fuego en grado menor.
- B: Combustible con contribución muy limitada al fuego.
- C: Combustible con contribución limitada al fuego.
- D: Combustible con contribución media al fuego.
- E: Combustible con contribución alta al fuego.
- F: Sin clasificar.

Además, otros dos parámetros complementan esta información:

*Opacidad de los humos producidos*

- s1: Baja opacidad.
- s2: Opacidad media.
- s3: Alta opacidad.

*Caída de gotas o partículas inflamadas*

- d0: No las produce.
- d1: Las produce en grado medio.
- d2: Las produce en grado alto.

*Según su aplicación*

- Sin subíndice para materiales de techos y paredes.
- Con subíndice FL para materiales de suelos.
- Con subíndice L para materiales de aislamientos de tuberías y conducciones en general.

Por ejemplo, un revestimiento clasificado como A1- s1, d0 es un revestimiento no combustible, que produce humos de baja opacidad, y que no produce gotas o partículas inflamadas. Un revestimiento de suelo $A1_{FL}$-s1 es un revestimiento para suelos no combustible y que produce humos de baja opacidad.

### 3.1.3 Códigos IP

Es un sistema de codificación para indicar los grados de protección proporcionados por la envolvente contra el acceso a las partes peligrosas, contra la penetración de cuerpos sólidos extraños, contra la penetración de agua y para suministrar una información adicional unida a la referida protección [Piq01].

El código IP está formado por dos números de una cifra cada uno, situados inmediatamente después de las letras IP, y que son independientes el uno del otro:

- Primera cifra característica, indica la protección de las personas contra el acceso a partes peligrosas (típicamente bajo tensión o piezas en movimiento que no sean ejes rotativos y análogos), limitando o impidiendo la penetración de una parte del cuerpo humano o de un objeto cogido por una persona y, garantizando simultáneamente la protección del equipo contra la penetración de cuerpos sólidos extraños (Tabla 2).

| Cifra | Grado de protección | |
|---|---|---|
| | Descripción abreviada | Indicación breve sobre los objetos que no deben penetrar en la envolvente |
| 0 | No protegida | Sin protección particular |
| 1 | Protegida contra cuerpos sólidos de más de 50 mm | Cuerpos sólidos con un diámetro superior a 50 mm |
| 2 | Protegida contra cuerpos sólidos de más de 12 mm | Cuerpos sólidos con un diámetro superior a 12 mm |
| 3 | Protegida contra cuerpos sólidos de más de 2,5 mm | Cuerpos sólidos con un diámetro superior a 2,5 mm |
| 4 | Protegida contra cuerpos sólidos de más de 1 mm | Cuerpos sólidos con un diámetro superior a 1 mm |
| 5 | Protegida contra la penetración de polvo | No se impide totalmente la entrada de polvo, pero sin que el polvo entre en la cantidad suficiente que llegue a perjudicar |

| | | |
|---|---|---|
| | | el funcionamiento satisfactorio del equipo |
| 6 | Totalmente estanco al polvo | Ninguna entrada de polvo |

Tabla 2: Códigos IP, primera cifra característica

- Segunda cifra característica, indica la protección del equipo en el interior de la envolvente contra los efectos perjudiciales debidos a la penetración de agua (Tabla 3).

| Cifra | Grado de protección | |
|---|---|---|
| | Descripción abreviada | Tipos de protección proporcionada por la envolvente |
| 0 | No protegida | Sin protección particular |
| 1 | Protegida contra la caída vertical de gotas de agua | La caída vertical de gotas de agua no deberá tener efectos perjudiciales |
| 2 | Protegida contra la caída de gotas de agua con una inclinación máxima de 15° | Las caídas verticales de gotas de agua no deberán tener efectos perjudiciales cuando la envolvente esté inclinada hasta 15° con respecto a la posición normal |
| 3 | Protegida contra la lluvia fina (pulverizada) | El agua pulverizada de lluvia que cae en una dirección que forma un ángulo de hasta 60° con la vertical, no deberá tener efectos perjudiciales |
| 4 | Protegida contra las proyecciones de agua | El agua proyectada en todas direcciones sobre la envolvente no deberá tener efectos perjudiciales |
| 5 | Protegida contra los chorros de agua | El agua proyectada con la ayuda de una boquilla, en todas direcciones, sobre la envolvente, no deberá tener efectos perjudiciales |
| 6 | Protegida contra fuertes chorros de agua o contra la mar gruesa | Bajo los efectos de fuertes chorros o con mar gruesa, el agua no deberá penetrar en la envolvente en cantidades perjudiciales |
| 7 | Protegida contra los efectos de la inmersión | Cuando se sumerge la envolvente en agua en unas condiciones de presión y con una duración determinada, no deberá ser posible la penetración de agua en el interior de la envolvente en cantidades perjudiciales |
| 8 | Protegida contra la inmersión prolongada | El equipo es adecuado para la inmersión prolongada en agua bajo las condiciones especificadas por el fabricante.<br><br>NOTA – Esto significa normalmente que el equipo es rigurosamente estanco. |

Tabla 3: Códigos IP, segunda cifra característica

- Adicionalmente, de forma opcional, y con objeto de proporcionar información suplementaria sobre el grado de protección de las personas contra el acceso a partes peligrosas, puede complementarse el código IP con una letra colocada inmediatamente después de las dos cifras características (Tabla 4). Estas letras proporcionan información sobre la accesibilidad de determinados objetos o partes del cuerpo a las partes peligrosas en el interior de la envolvente.

| Letra | La envolvente impide la accesibilidad a partes peligrosas con: |
|---|---|
| A | Una gran superficie del cuerpo humano tal como la mano (pero no impide una penetración deliberada). |
| B | Los dedos u objetos análogos que no excedan en una longitud de 80 mm. |
| C | Herramientas, alambres, etc., con diámetro o espesor superior a 2,5 mm. |
| D | Alambres o cintas con un espesor superior a 1 mm. |

Tabla 4: Códigos IP, letras adicionales

### 3.1.4 Códigos IK

Se trata de un sistema de codificación para indicar el grado de protección proporcionado por la envolvente contra los impactos mecánicos nocivos, salvaguardando así los materiales o equipos en su interior [Piq01] (Tabla 5).

| Grado IK | IK 00 | IK 01 | IK 02 | IK 03 | IK 04 | IK 05 | IK 06 | IK 07 | IK 08 | IK 09 | IK 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Energía (J) | - | 0,15 | 0,2 | 0,35 | 0,5 | 0,7 | 1 | 2 | 5 | 10 | 20 |
| Masa y altura de la pieza de golpeo | - | 0,2 Kg<br>70 mm | 0,2 Kg<br>100 mm | 0,2 Kg<br>175 mm | 0,2 Kg<br>250 mm | 0,2 Kg<br>350 mm | 0,5 Kg<br>200 mm | 0,5 Kg<br>400 mm | 1,7 Kg<br>295 mm | 5 Kg<br>200 mm | 5 Kg<br>400 mm |

Tabla 5: Grados IK

### 3.1.5 Resistencia antirrobo

La norma DIN V ENV 1672 define seis niveles de protección [Wik12a]:

- WK1: Los elementos tienen una protección básica contra intentos de entrar usando la fuerza física. Estos elementos solamente presentan poca protección contra palancas.
- WK2: Los elementos tienen protección contra la fuerza física y herramientas simples, como destornilladores, alicates y cuñas, durante al menos 3 minutos.
- WK3: Protección contra otras herramientas: un segundo destornillador y una palanca, durante al menos 5 minutos.
- WK4: Protección contra otro tipo de herramientas de corte y percusión como son el hacha, el escoplo, el martillo y el cincel, así como la taladradora de batería, durante al menos 10 minutos.
- WK-5: Protección contra herramientas eléctricas: taladradora, sierra eléctrica, durante al menos 15 minutos.
- WK-6: Lo mismo que WK-5 pero durante al menos 20 minutos.

## 3.2 Paredes

Los fuegos no suelen iniciarse en el interior del CPD. Los daños en un CPD generalmente resultan del fuego (o el humo y gases) que comienza en otras partes y se extiende a la sala del CPD. Debido al valor de la información almacenada y al impacto negativo para el negocio que supondría una pérdida de la misma, todos los materiales usados en la construcción de la sala de equipamiento IT deben ser incombustibles. El CPD debe convertirse en un recinto estanco. Sus paredes deben tener un grado mínimo de resistencia al fuego y deben proporcionar barrera frente al humo. También es importante el daño que puede producir el agua, por lo que todas las entradas del suelo, de la pared y del techo deben estar selladas.

Los métodos más comunes de proteger las paredes del CPD son mediante placas de yeso y mediante paneles.

### 3.2.1 Placas de yeso y trasdosados

Las placas de yeso son materiales para la construcción formados por un alma de yeso recubierta en ambos lados por capas de celulosa especial multi-hoja. Se presentan en tableros de diferentes medidas así como distintos espesores. Es un material no inflamable, que se puede cortar, atornillar, taladrar y que además tiene un excelente comportamiento frente al fuego, es buen aislante térmico y consigue grandes aislamientos acústicos, además de ser un regulador natural de la humedad [Pla12].

Los trasdosados son los revestimientos de la cara interior de un muro exterior o de cualquiera de las dos caras de un muro interior, que le aportan una mejora técnica o estética.

### 3.2.2 Paneles

Se trata de paneles modulares que forman en el interior de la sala del CPD un recinto protegido contra fuego, calor, humos, gases corrosivos, vapor, inundación, campos electromagnéticos de alta y baja frecuencia.

Las principales ventajas de este tipo de soluciones son:

- Modularidad
- Seguridad
- Ahorro de energía
- Adaptables
- Reutilizables
- Alta resistencia mecánica

## 3.3 Suelo técnico

Se le conoce también como falso suelo. Está compuesto de baldosas de medida estándar de 60x60 cm. apoyadas sobre pedestales de acero ajustables en altura, consiguiendo un falso suelo firme sobre la solera existente. Bajo el suelo técnico se crea una cámara (plenum) que consiste en un espacio libre para el alojamiento de cableado o para ser empleado en el circuito de refrigeración de la sala. Al ser los paneles idénticos se facilita el intercambio de los mismos, garantizando tanto la accesibilidad como la flexibilidad.

El suelo elevado está compuesto por las siguientes partes, tal y como muestra la Ilustración 5[8]:

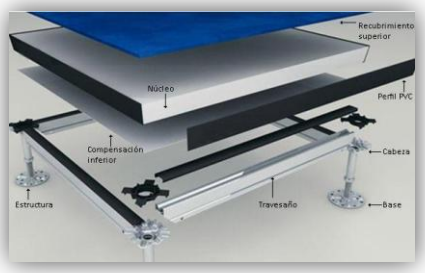



**Ilustración 5: Suelo elevado**

*Estructura*

La estructura está formada por dos partes, cabeza y base. Es regulable en altura. Sobre la cabeza se apoyan los travesaños, que sujetarán la baldosa. Existen diferentes tipos de estructuras, y sus parámetros más importantes son:

- Altura mínima
- Altura máxima
- Carga máxima axial sin deformación

Suelen ser de aluminio o acero.

*Baldosas*

Las baldosas son de un tamaño estándar de 60x60 cm. y 4 cm. de grosor.

Están constituidas por un núcleo central, recubierto superior e inferiormente por distintos materiales, y rematado por una protección perimetral de PVC de 2 mm de espesor [Esp12]. Los tableros pueden ser aglomerados de madera y otros materiales lignocelulósicos, de cemento o de anhidrita. Los recubrimientos pueden ser de PVC, Linóleum, tarimas, corchos, estratificados,...

[8] Ilustración extraída de Butech, *www.butech.es*.

Sus parámetros más importantes son:

- Lado
- Diagonal
- Espesor
- Peso
- Clasificación Reacción al Fuego según UNE 23727-90, dependiendo del recubrimiento superior

## 3.4 Techos suspendidos

Los techos, al igual que los suelos, deben contribuir a convertir el recinto del CPD en un lugar protegido contra fuego y humedad. Están formados por anclajes, perfilería y baldosas de 60x60 cm.

Las clases de reacción al fuego de revestimientos de paredes y techos son (ver apartado 3.1.2):

| Antigua clasificación | EN 13501-1 |
|---|---|
| M0 | A1 ó A2-s1,d0 |
| M1 | B-s3,d0 |
| M2 | C-s3,d0 |
| M3 | D-s3,d0 |

Tabla 6: Clasificación de reacción frente al fuego de paredes y techos

## 3.5 Pasamuros y pasacables

Para garantizar que el recinto del CPD está totalmente protegido contra amenazas externas, también es importante sellar los pasos de cables a través de las paredes, suelos o techos.

Los pasamuros ofrecen protección contra humedad, lluvia, polvo, arena, perturbaciones electromagnéticas (RFI/EMI) e incendios. No son solo para las paredes, también pueden emplearse en los *racks*. Al proporcionar un sellado estanco permiten un ahorro energético de hasta un 10%.

Otro tipo de soluciones son los pasacables para falso suelo. Se trata de unos marcos que se instalan en las baldosas del falso suelo en huecos cortados a medida, y llevan unos cepillos que impiden el paso de aire pero no de los cables. Entre sus principales ventajas destaca el aumento de la capacidad de refrigeración, contribuyendo a minimizar las pérdidas de aire refrigerado que se escapa desde el plenum hacia la sala por los orificios para cables.

# Capítulo 4 Instalaciones de Energía

La energía suministrada por los sistemas de distribución eléctrica, tanto públicos como privados, es una tensión senoidal de frecuencia y amplitud fijas, pero suele existir un cierto grado de fluctuación sobre estos valores nominales. Las fluctuaciones permitidas en el suministro de baja tensión están definidas en la norma EN 50160 [EN11]. Además de estas fluctuaciones, se pueden producir otras perturbaciones en el sistema que producen distorsiones de la onda senoidal de la tensión.

Todos los equipos necesitan una energía continua, libre de interrupciones y alteraciones. Un estudio realizado por Electric Power Research Institute muestra que las pérdidas del sector empresarial en EEUU alcanzan los 188 billones[9] de dólares al año, de los cuales hasta 24 billones de dólares pueden ser debidos a problemas de calidad de la señal y 164 billones de dólares a interrupciones en el suministro eléctrico [Sey11].

Por ello, muchas cargas[10] requieren un suministro que esté protegido contra dichas perturbaciones del sistema de distribución. El centro de datos o la sala de red deben estar preparados para interrupciones prolongadas del suministro eléctrico.

### *Señal eléctrica*

La electricidad que proporciona la red eléctrica es una corriente alterna (AC), representada como una señal suave, simétrica, y que varía 50 ciclos por segundo (Herzios).

Cuando la señal sufre algún cambio en su tamaño, forma, simetría, frecuencia o desarrolla muescas, impulsos, oscilaciones o caídas a cero, existe una alteración. Las principales alteraciones del suministro eléctrico son las que se enuncian a continuación [Sey11]:

- Transitorios: son las alteraciones más perjudiciales. Pueden ser:
    - Impulsivos: se trata de picos de tensión provocados por una mal puesta a *tier*ra, cargas inductivas, descargas electrostáticas,… (Ilustración 6, [Sch12]). Los resultados pueden ser la pérdida o corrupción de datos y el daño del equipamiento.

[9] Billones (USA) equivale a $10^9$.

[10] Mediante cargas se hace referencia a todos los equipos conectados al sistema de distribución eléctrico.

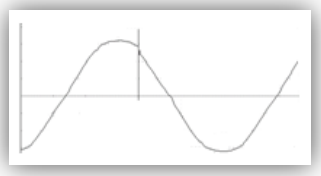


Ilustración 6: Transitorio impulsivo

- Oscilatorios: se trata de cambios en la onda estacionaria, provocando una subida y a continuación una disminución muy rápidas (Ilustración 7, [Sch12]). Ocurren al apagar una carga inductiva o capacitiva.

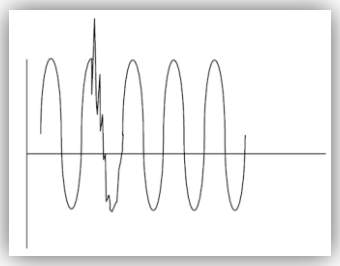


Ilustración 7: Transitorio oscilatorio

- Interrupciones: se definen como una pérdida total de voltaje o corriente eléctrica (Ilustración 8, [Sch12]). Dependiendo de la duración puede ser instantánea, momentánea, temporal o sostenida.

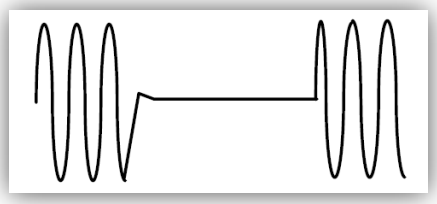


Ilustración 8: Interrupción

- Caída de tensión: es una reducción del voltaje a una determinada frecuencia (Ilustración 9, [Sch12]).

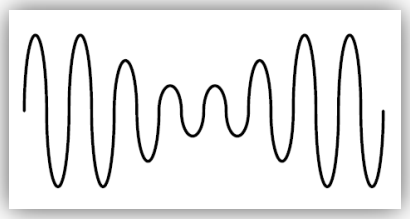


Ilustración 9: Caída de tensión

- Sobretensión: es un incremento del voltaje a una determinada frecuencia (Ilustración 10, [Sch12]).

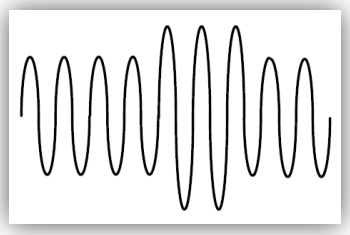


Ilustración 10: Sobretensión

- Distorsión de la forma de onda: algunas distorsiones son las que se muestran a continuación.
    - Offset de continua: una corriente continua atraviesa el sistema de alterna añadiendo corrientes no deseadas.
    - Armónicos: corrupción de la señal en frecuencias múltiplo de la frecuencia fundamental.
    - Interarmónicos: resultado de una tensión impuesta en la alimentación eléctrica.
    - Ruido: voltaje o corriente superpuestos a la forma de onda.
- Fluctuaciones: se trata de una variación sistemática de la forma de onda o de una serie de cambios aleatorios, de pequeñas dimensiones (Ilustración 11, [Sch12]).

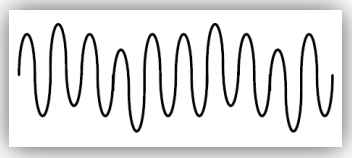


Ilustración 11: Fluctuaciones

- Variaciones de frecuencia: son extremadamente raras en sistemas eléctricos estables (Ilustración 12, [Sch12]).

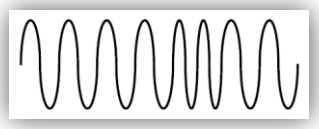


Ilustración 12: Variaciones de frecuencia

## 4.1 Sistemas de Alimentación Ininterrumpida

Un Sistema de Alimentación Ininterrumpida (SAI) es un dispositivo de suministro eléctrico que posee una batería a través de la cual proporciona energía a un equipo en el caso de interrupción eléctrica. En el caso de producirse un corte en el suministro eléctrico, la SAI se pone en marcha proporcionando energía a la carga durante unos minutos, hasta que arranque el sistema de alimentación de reserva o se restablezca el suministro de electricidad principal. Otra función de las SAIs es depurar la electricidad suministrada directamente por la compañía eléctrica (*corriente sucia*) y mejorar su calidad (*corriente limpia*).

Algunos de los principales parámetros de una SAI se muestran a continuación.

### *Potencia activa y potencia aparente*

La potencia aparente (S) de un SAI se especifica en voltamperios (VA) o kVA. No es la realmente útil (salvo cuando el Factor de Potencia es igual a 1). Se define como el producto del Voltaje por la Intensidad:

$$S = V * I$$

La potencia activa (P) de un SAI se especifica en W o KW y está definida como:

$$P = S * FP, \qquad donde\ FP\ es\ el\ Factor\ de\ Potencia$$

El valor nominal en VA es siempre igual o superior al valor nominal en W. La relación entre el valor nominal en vatios y el valor nominal en voltamperios se denomina factor de potencia. Los sistemas SAI tienen un valor nominal máximo en vatios y en voltamperios. Ninguno de estos valores nominales se puede sobrepasar [Ras06a].

### *Curva de eficiencia*

La forma básica de una curva de eficiencia es la que se muestra a continuación, en la Ilustración 13, [Sch12]:

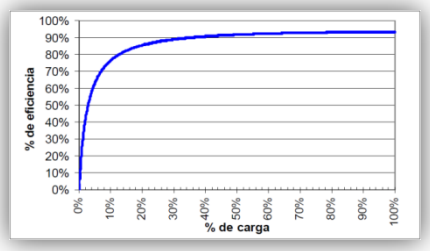



Ilustración 13: Curva de eficiencia

La curva de eficiencia muestra la relación entre la potencia de entrada y salida en función del nivel de carga.

*Pérdida sin carga*

Con una carga del 0%, toda la potencia de entrada es utilizada por la SAI; de ahí el nombre "sin carga". Además de la pérdida sin carga existen otro tipo de pérdidas que afectan a la eficiencia de la SAI:

- Pérdidas proporcionales: a medida que aumenta la carga, una mayor cantidad de energía debe ser empleada por diversos componentes de la SAI.
- Pérdidas de ley cuadrática: a medida que aumenta la carga, aumenta la corriente eléctrica que circula por sus componentes. La pérdida en potencia disipada en forma de calor es proporcional al cuadrado de la corriente.

*Otros parámetros*

Otros parámetros de la SAI son:

- Tiempo de autonomía, es el tiempo en que el SAI puede seguir alimentando la carga tras un corte del suministro eléctrico.
- Baterías, sirven para garantizar el tiempo de autonomía del SAI especificado para la potencia aparente de la carga y el factor de potencia para el que está diseñado. Normalmente pueden instalarse en el mismo armario que la SAI. Generalmente son de plomo o de una combinación de níquel y cadmio.

### 4.1.1 Tipos de SAIs

Además de la autonomía de la batería, el coste, el tamaño, el fabricante, el número de tomas o la capacidad de gestión, la tipología de un SAI afecta a su funcionamiento en distintos entornos, por lo que es un importante factor a tener en cuenta a la hora de elegir un SAI. A grandes rasgos, existen tres tipos de SAIs: *standby*, de línea interactiva y *on-line* de doble conversión. A continuación se resumen sus principales características [CEM12].

*SAI Standby*

En condiciones de suministro de energía normales, la fuente primaria es la entrada de corriente alterna (CA), que pasa a través de filtros y/o supresores de tensión (opcionales) hasta el interruptor de transferencia (circuito con línea continua). En caso de fallar la fuente primaria, el interruptor de transferencia conmuta la carga a la fuente de energía de respaldo de batería/ inversor (circuito con línea discontinua), poniéndose en funcionamiento el inversor y manteniéndose el suministro de energía mientras dure la energía almacenada en la batería o hasta que se restablezca el suministro principal. En la Ilustración 14, [Sch12], se presenta un esquema de este tipo de SAI.

Ventajas:

- Altos niveles de eficiencia.

- Tamaño pequeño.
- Bajo coste.

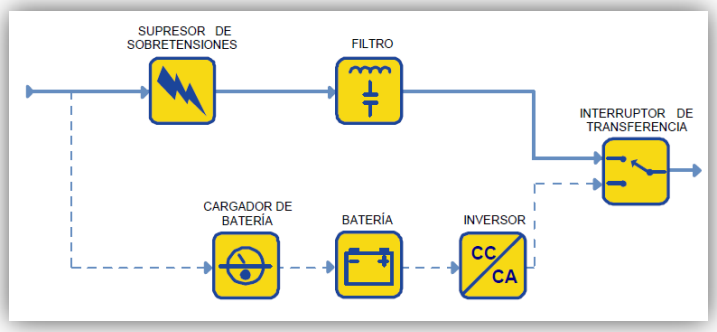



Ilustración 14: SAI Standby

*SAI de línea interactiva*

En este tipo de diseño, el inversor siempre está conectado a la salida del SAI. Mientras la alimentación CA de entrada es normal, se carga la batería.

Cuando falla la alimentación de entrada, el interruptor de transferencia se abre y el flujo de energía se produce desde la batería hasta la salida del SAI, tal y como se muestra en la Ilustración 15, [Sch12].

Ventajas:

- Altos niveles de eficiencia.
- Tamaño pequeño.
- Bajo coste.
- Alta confiabilidad.
- Capacidad de corregir condiciones de tensión de línea alta o baja.

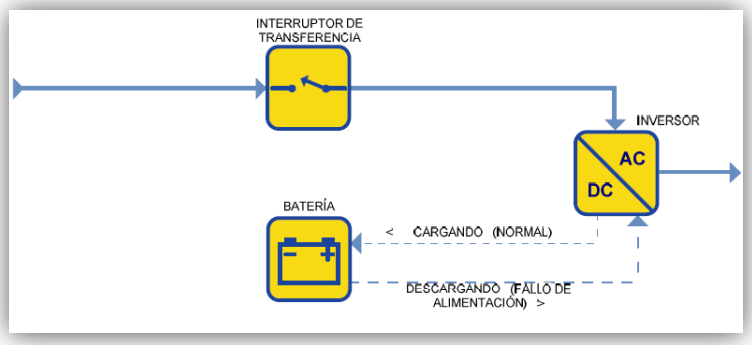



Ilustración 15: SAI de línea interactiva

*SAI en línea de doble conversión*

El diagrama de bloques (Ilustración 16, [Sch12]) es el mismo que para la SAI *standby*, excepto porque el circuito de energía primario es el del inversor en lugar de la red de CA.

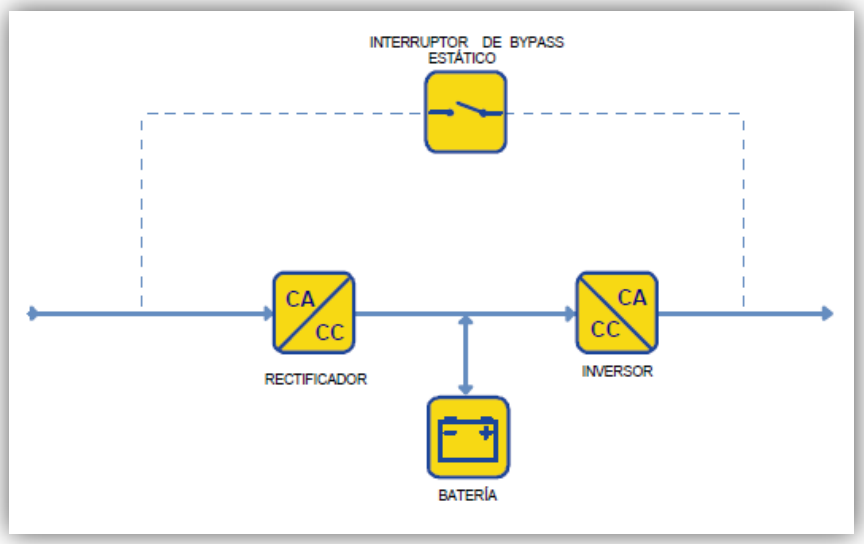



Ilustración 16: SAI en línea de doble conversión

La interrupción del suministro de CA de entrada no provoca la activación del interruptor de transferencia, ya que la alimentación de CA de entrada está cargando la batería de respaldo que suministra alimentación al inversor de salida. Por lo tanto, durante una interrupción en el suministro de entrada de CA, no se produce transferencia de carga. Sin embargo, el desgaste constante de los componentes de potencia reduce la fiabilidad respecto de otros diseños.

*Resumen*

La Tabla 7 muestra un resumen de las características de los diferentes tipos de SAIs[11]:

| | Rango de potencia para aplicación práctica (KVA) | Acondicionamiento de la tensión | Costo por VA | Eficiencia | Inversor con funcionamiento constante |
|---|---|---|---|---|---|
| **Standby** | 0 – 0,5 | Bajo | Bajo | Muy alta | No |
| **Línea Interactiva** | 0,5 – 5 | Según diseño | Medio | Muy Alta | Según diseño |
| **On-line de doble conversión** | 5 – 5000 | Alto | Alto | Baja – Media | Sí |

Tabla 7: Características de SAIs

[11] Información extraída de la página web de Schneider Electric, *www.schneider-electric.com*.

### 4.1.2 Configuraciones de sistemas SAIs

Existen cinco tipos de configuraciones de los sistemas SAIs, y su elección dependerá de las necesidades de disponibilidad, tolerancia a riesgos, tipos de carga del centro de datos, presupuesto e infraestructura existente.

*Disponibilidad vs. Coste*

Disponibilidad es tiempo que la potencia eléctrica se mantiene activa y en perfecto estado de funcionamiento para respaldar las cargas críticas. Cuanto más alto sea el lugar que ocupa la configuración en la escala de disponibilidad, más alto será también el coste [McC04]. En la Tabla 8 aparece un resumen de las distintas configuraciones de sistemas SAIs[12].

| Configuraciones | Escala de disponibilidad | Categoría del nivel | Escala de coste del centro de datos ($) |
|---|---|---|---|
| Capacidad (*N*) | 1 = La más baja | *Tier* I | 13.500$ - 18.000$ /*rack* |
| Redundante aislado | 2 | *Tier* II | 18.000$ - 24.000$ /*rack* |
| Redundante paralelo (*N+1*) | 3 | | |
| Redundante distribuido | 4 | *Tier* III | 24.000$ - 30.000$ /*rack* |
| Sistema *2N* (*2N*, *2N+1*) | 5 = La más alta | *Tier* IV | 36.000$ - 42.000$ /*rack* |

**Tabla 8: Disponibilidad de las configuraciones**

#### *4.1.2.1 Capacidad o sistema N*

Un sistema *N* es un sistema formado por un solo módulo SAI, o por un conjunto de módulos en paralelo cuya capacidad coincide con la carga crítica prevista. Dado que no existe ningún tipo de redundancia, es apropiado dotar al sistema de un bypass (llamado *bypass* de mantenimiento) que permita apagar todo el sistema SAI para realizar mantenimiento cuando la situación lo requiera o que permita el suministro de energía a la carga si se produjera algún fallo en el SAI que impidiese su funcionamiento, teniendo en cuenta que en ese caso la carga no dispondría de ningún tipo de protección frente a fallos en la red eléctrica. El diagrama de bloques se muestra a continuación, en la Ilustración 17, [Sch12]:

[12] Información extraída de la página web de Schneider Electric, *www.schneider-electric.com.*

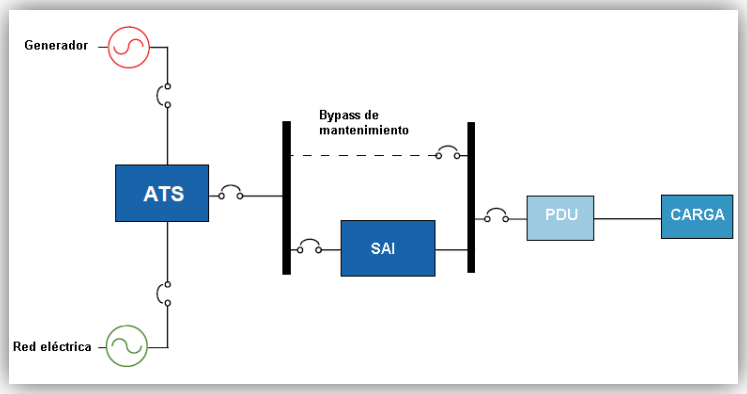



Ilustración 17: Capacidad o sistema N

### *4.1.2.2 Redundante aislado*

En esta configuración, cada módulo SAI incluye un bypass, que llamaremos bypass estático, que permitirá aportar redundancia a la configuración. El módulo SAI principal alimenta a toda la carga. El secundario va conectado al bypass estático del SAI principal y en condiciones normales de funcionamiento se encontrará totalmente descargado.

Si se produce una incidencia en el SAI primario, la carga se transfiere al bypass estático, de modo que el SAI secundario tomará la carga instantáneamente. Si se produjese alguna incidencia en el SAI secundario, éste transferiría la carga al bypass estático (suministro de red eléctrica sin protección). Esta configuración también permite que puedan realizarse tareas de mantenimiento o reparación en un SAI al transferir la carga al otro.

No debe olvidarse el bypass de mantenimiento, que continúa siendo importante en el caso de que fallasen ambos SAIs.

El diagrama de bloques de esta configuración se muestra a continuación, en la Ilustración 18, [Sch12]:

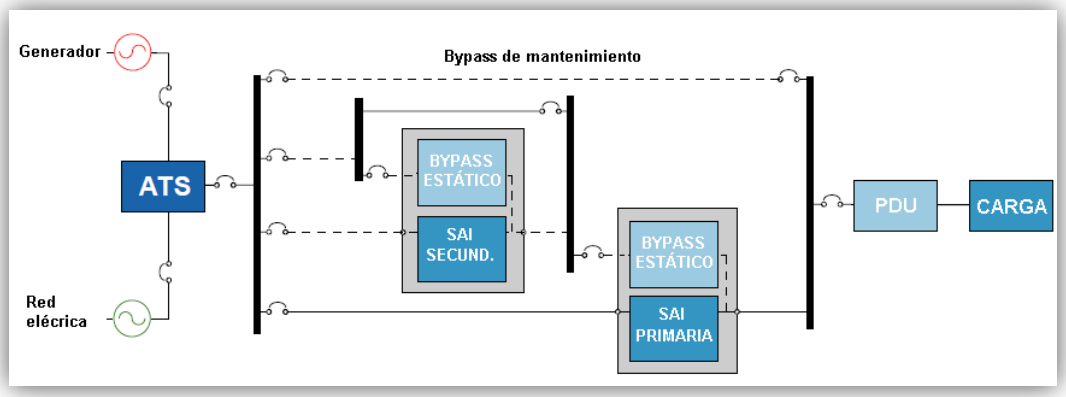



Ilustración 18: Redundante aislado

### *4.1.2.3 Redundante paralelo o sistema N+1*

Una configuración de diseño redundante paralelo consiste en varios módulos SAI iguales instalados en paralelo, de modo que la carga se reparte por igual entre todos los módulos pero con la peculiaridad de que si uno de los módulos falla, el resto pueden asumir su carga. El sistema será redundante *N+1* si la cantidad sobrante de potencia es al menos igual a la capacidad de un módulo del sistema; el sistema sería redundante *N+2* si la potencia sobrante fuera igual a dos módulos del sistema, y así sucesivamente.

Continúa siendo altamente recomendable un bypass de mantenimiento igual que en las configuraciones anteriores.

La Ilustración 19, [Sch12], muestra el diagrama de bloques de esta configuración:

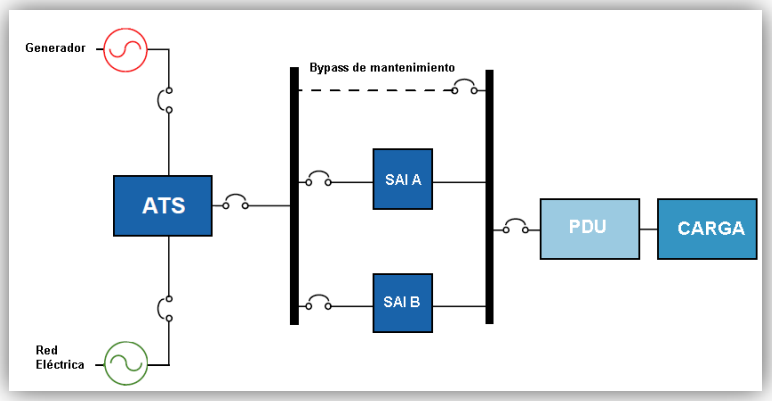



Ilustración 19: Redundante paralelo o sistema N+1

### *4.1.2.4 Redundante distribuido*

La base de este diseño utiliza tres o más módulos SAI con alimentadores de entrada y salida independientes, que se conectan a la carga crítica a través de diversas PDU (*Power Distribution Unit,* ver apartado 4.4) y STS (*Static Transfer Switch*[13]). Desde la entrada del servicio de la red eléctrica hasta el SAI, el diseño redundante distribuido y el diseño de sistema *2N* son muy similares. Ambos permiten el mantenimiento simultáneo y reducen los puntos individuales de fallo. La principal diferencia se encuentra en la cantidad de módulos SAI necesarios para lograr rutas de potencia redundantes hasta la carga crítica, así como la organización y distribución desde el SAI hasta la carga crítica. En la Ilustración 20, [Sch12], se observa uno de los esquemas de este tipo de configuración:

[13] *Static Transfer Switch* es un dispositivo que tiene dos entradas y una salida. Por lo general toma energía de dos SAIs diferentes, y provee a la carga energía acondicionada proveniente de una de ellas. Cuando falla uno de los circuitos de alimentación SAI primarios, el STS transfiere la carga al circuito de alimentación SAI secundario en unos 4 milisegundos, lo que mantiene la carga con energía protegida todo el tiempo.

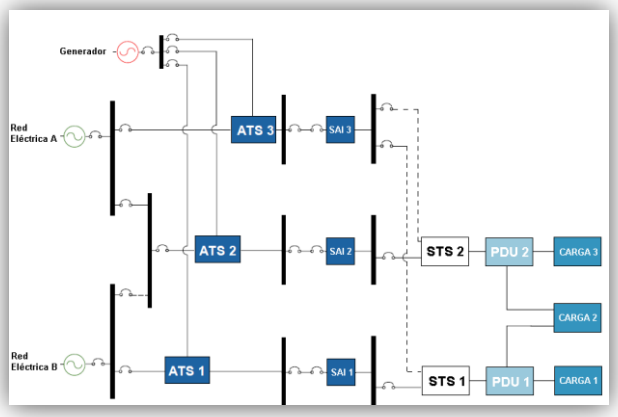



Ilustración 20: Redundante distribuido

En esta configuración, el módulo 3 generalmente está descargado y se conecta a la entrada secundaria en cada STS. Este módulo asumirá la carga en caso de que falle alguno de los módulos SAI primarios.

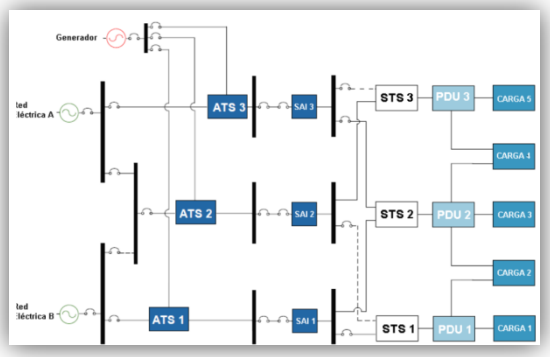



Ilustración 21: Redundante distribuido

El diseño mostrado en la Ilustración 21, [Sch12], es redundante distribuido con tres STS y con la carga distribuida por igual entre los tres módulos en condiciones de funcionamiento normal. El fallo de cualquiera de los módulos forzaría al STS a transferir la carga al módulo SAI que alimenta la fuente alternativa.

La debilidad principal de este diseño es el uso de interruptores estáticos de transferencia (STS). Estos dispositivos son muy complejos y presentan modos de fallo inesperados.

#### *4.1.2.5 Redundancia con sistema más sistema*

Con este diseño es posible crear sistemas SAI que tal vez nunca requieran la transferencia de la carga a la red eléctrica (Ilustración 22, [Sch12]). Estos sistemas pueden diseñarse para eliminar todos los puntos de fallo únicos posible, en detrimento del coste del sistema, que aumenta a la vez que lo hace su complejidad.

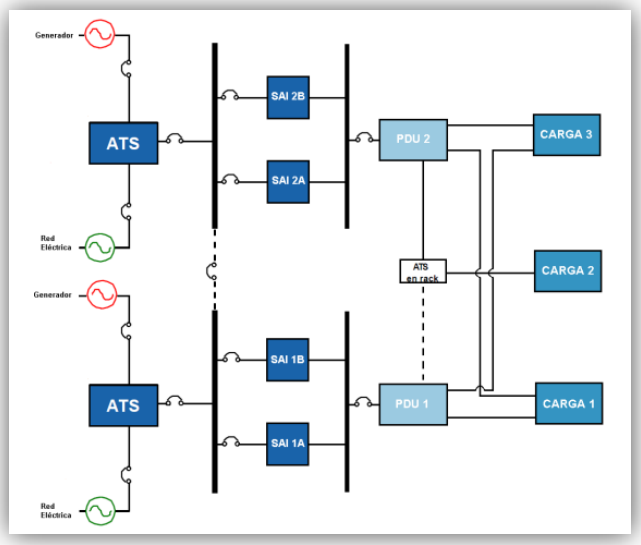



Ilustración 22: Sistema más Sistema

Las consideraciones para elegir la configuración apropiada son:

- Coste/ impacto del tiempo de inactividad.
- Tolerancia a los riesgos.
- Requisitos de disponibilidad: La Tabla 9[14] muestra la disponibilidad de cada una de las configuraciones de sistemas SAIs.

| Configuración SAI | Disponibilidad[15] |
|---|---|
| Capacidad (*N*) | 99,92% |
| Redundante Aislada | 99,93% |
| Paralela redundante (*N+1*) | 99,93% |
| Redundante distribuida | 99,9989% |
| Redundante distribuida | 99,9994% |
| *2 (N+1)* | 99,99997% |

Tabla 9: Disponibilidad

- Presupuesto.

[14] Información extraída de la página web de Schneider Electric, *www.schneider-electric.com.*

[15] Estudio realizado por APC Schneider Electric basándose en los supuestos expuestos en la Tabla A1 del Whitepaper 75: *Comparación de configuraciones de diseño de sistemas SAI.*

## 4.2 Generadores

En caso de un corte de suministro prolongado, el generador permite extender la autonomía de las baterías, que por supuesto proporcionan una continuidad en el suministro eléctrico mientras el generador arranca y 10 o más minutos en caso de que no arranque para que dé tiempo a iniciar todas las secuencias de cierre de aplicaciones.

Un generador está formado por dos subsistemas básicos [Wol04]:

- El generador, que está compuesto por el motor primario, el alternador y el regulador.
- El sistema de distribución, que está compuesto por el interruptor de transferencia automática (ATS) y los dispositivos de conmutación y distribución asociados.

*Generador*

El motor primario es un motor de combustión interna que convierte el combustible del que se alimenta en movimiento mecánico, a través de sus componentes móviles internos. El combustible utilizado puede ser gasóleo, gas natural, petróleo líquido y gasolina y su elección depende de diversas variables, entre ellas el almacenamiento, los costes y la accesibilidad. Es imprescindible un rápido arranque. Normalmente, el tiempo mínimo que necesita el generador para detectar el problema de alimentación, arrancar el motor primario, establecer una tensión y frecuencia de salida estables y conectarlas a las cargas, es de al menos 10-15 segundos. El elemento fundamental de los motores de arranque convencionales es claramente el sistema de batería.

El alternador convierte la energía mecánica procedente del motor primario en corriente alterna mientras que el regulador mantiene constantes las revoluciones del motor primario bajo una variedad de condiciones, ajustando el caudal de combustible que se suministra al motor primario. Este elemento es un componente clave para determinar la calidad de alimentación de salida de CA.

*Dispositivos de conmutación y distribución*

La distribución de la salida del generador a las cargas críticas es otro elemento fundamental del diseño del sistema. Los interruptores de transferencia automáticos (ATS) deben supervisar la fuente de alimentación e iniciar el arranque del motor y la transferencia de la carga al generador en cuanto ésta está disponible y es estable, así como la re-transferencia de la carga a la red eléctrica cuando se restablecen las condiciones normales. La Ilustración 23 [Sch12], nos permite ver el esquema de un sistema de alimentación de emergencia con generador.

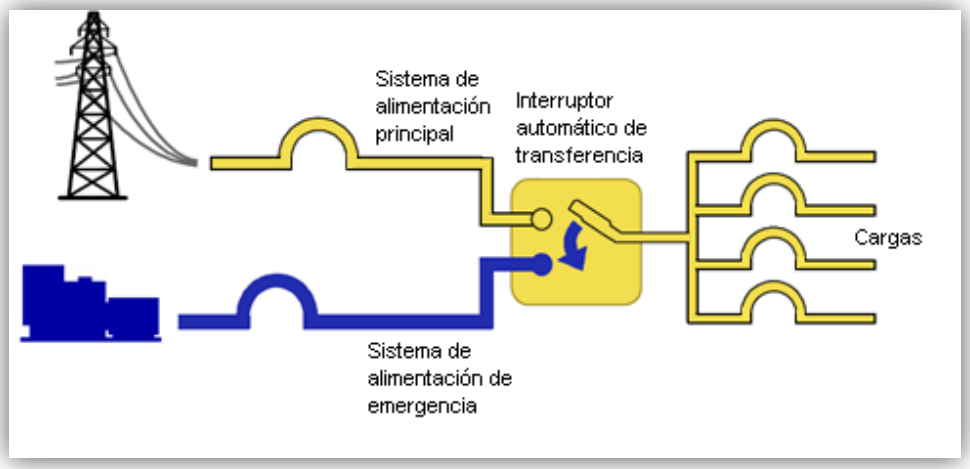



Ilustración 23: Sistema de alimentación de emergencia con generador

## 4.3 Alternativas para generación de energía en el CPD

Los sistemas de TIC pueden funcionar minutos o incluso unas horas gracias a baterías o un volante de inercia[16], pero es preciso contar con capacidad de generación energética local para lograr una disponibilidad de "cinco nueves". Los generadores de reserva a gasoil o a gas constituyen la solución convencional a este problema si se los combina con un SAIs [APC03].

Las pilas de combustible y las microturbinas pueden utilizarse en forma constante para alimentar la sala de gestión de redes o el centro de datos, con el fin de generar un excedente de energía eléctrica para otras cargas o para retroalimentar la red eléctrica, o como generación de reserva.

Las pilas de combustible son unos dispositivos que emplean el hidrógeno para obtener energía limpia, generando además en el proceso agua y calor (Ilustración 24[17]).

[16] El volante de inercia es un mecanismo que consiste en una rueda que gira gracias a un motor eléctrica. Cuando se produce un corte en el suministro eléctrico, la inercia del volante genera energía cinética que se convierte en energía eléctrica para que la carga no sufra cortes mientras arranca el generador o se restablece el suministro eléctrico.

[17] Ilustración extraída de la página web de Smart in the Grid, *http://www.smartinthegrid.com/*.

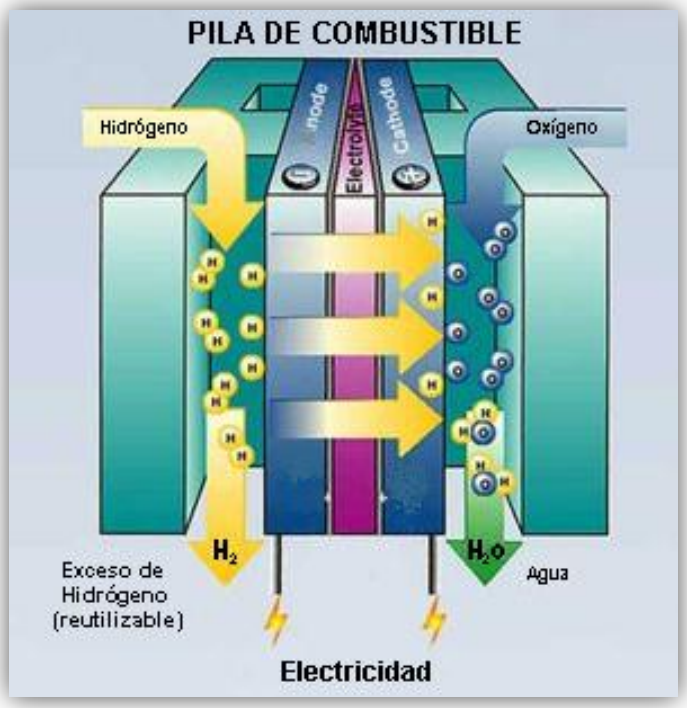



Ilustración 24: Pila de combustible

Con las microturbinas aparece el concepto de cogeneración, que se basa en el aprovechamiento del calor residual producido por la generación de energía eléctrica en energía térmica.

En el futuro inmediato, los grupos electrógenos que hacen uso de motores resultan todavía más económicos que las soluciones de pilas de combustible y microturbinas. Sin embargo, existe una gran variedad de situaciones o factores que podrían impulsar estas tecnologías, como la contaminación (el motor diesel es el sistema local de generación de energía que ocasiona el mayor problema de contaminación), la disponibilidad (las pilas de combustible y las microturbinas podrían mejorar la disponibilidad general del sistema, en comparación con los generadores de reserva), eliminación de SAIs (muchos análisis sobre pilas de combustible y microturbinas sugieren que esta tecnología podría eliminar otros dispositivos del sistema de energía, y así podría lograrse reducir los costos, incrementar la disponibilidad y aumentar la eficiencia). A pesar de todo, estas situaciones todavía poseen más inconvenientes que ventajas y los métodos para lograr las mejoras no están comprobados [APC03].

## 4.4 Regletas de distribución eléctrica, PDUs

Las unidades de distribución de la alimentación son regletas que proporcionan tensión eléctrica de manera fiable a los equipos de un *rack*.

Pueden ser:

- Básicas: proporcionan alimentación eléctrica a los equipos de un *rack*.
- Monitorizables: monitorizan el estado y la carga de cada toma. Pueden generar alarmas
- Gestionables: pueden actuar sobre cada toma.

## 4.5 Apagado de emergencia

El sistema de apagado de emergencia (*Emergency Power Off, EPO)*, es un mecanismo de seguridad que se emplea para apagar desde un único equipo a una sala de equipamiento eléctrico durante una emergencia, con el objetivo de proteger las instalaciones y el personal. Sin embargo, el EPO es una de las principales causas de apagado imprevisto del CPD. El diseño de un sistema EPO debe prevenir cualquier posibilidad de manipulación accidental, y debe minimizar su uso deliberado por razones ajenas a una emergencia o amenaza real.

La norma NFPA 75 [NFP75] expone que el EPO debe proporcionarse para desconectar la alimentación de todo el equipamiento electrónico. Esto incluye también desconectar las baterías de la carga. En el instante que se presiona el botón EPO se desconecta la alimentación de toda la instalación.

En la Ilustración 25 [Sch12], se observa un dispositivo EPO típico.

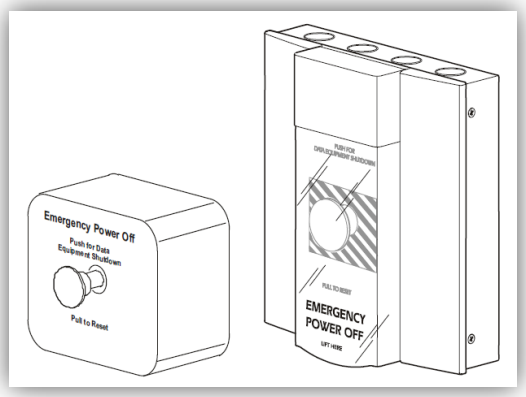



Ilustración 25: EPO

# Capítulo 5 Instalaciones de Clima

Cualquier consumo eléctrico en el CPD genera un calor que necesita ser eliminado de la sala. Este es uno de los aspectos más críticos en el diseño de un CPD. Una refrigeración inadecuada afecta negativamente al rendimiento del equipo y acorta su vida útil.

Los puntos calientes han aumentado de unos años a esta parte, ya que los fabricantes han disminuido el tamaño de los chasis permitiendo la instalación de más equipos en un mismo *rack*. Las altas velocidades a las que procesan la información estos equipos se traducen en un aumento del consumo eléctrico, que a su vez genera más calor. Mientras que la disminución del tamaño ha generado una reducción del espacio ocupado en el CPD, ya que pueden instalarse docenas de equipos en un espacio muy reducido, ha aumentado la concentración de calor en áreas de menor tamaño.

La figura siguiente (Ilustración 26[18]) muestra la evolución de la carga térmica de los diferentes sistemas electrónicos, del que se deduce que el incremento de la generación de calor en los CPDs va a continuar.

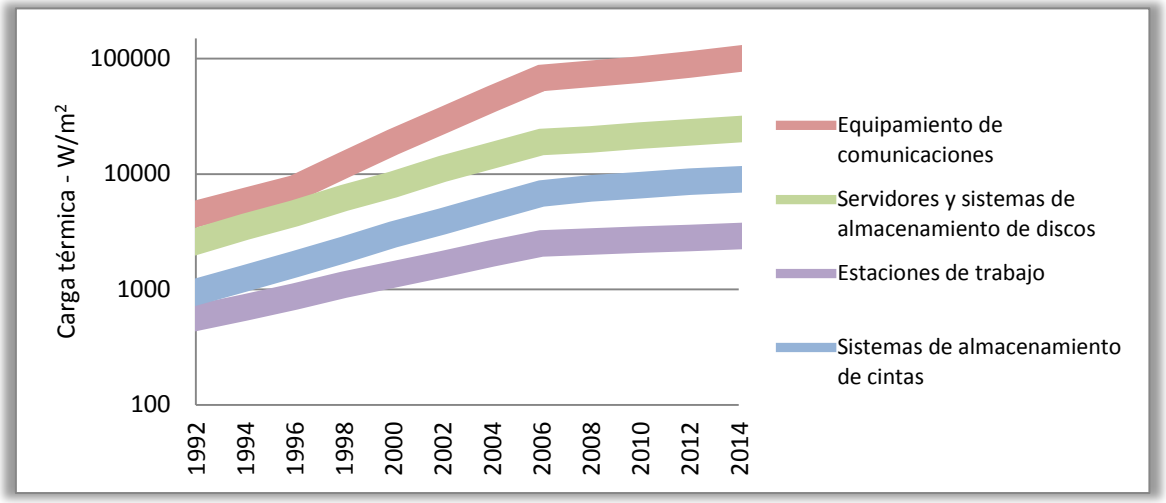



Ilustración 26: Evolución de la carga térmica del equipamiento TI

Para un diseño de refrigeración adecuado es fundamental el cálculo de las cargas térmicas, para el que deben tenerse en cuenta varios factores [Eme11c]:

- Incidencia del sol

[18] Ilustración extraída de *2005 ASHRAE TC 9.9.*

- Aire exterior – Renovaciones de aire de la sala. Además, debe existir una sobrepresión dentro de la sala para evitar la entrada de aire del exterior.

$$Sobrepresión = ¾ * Volumen\ de\ la\ sala$$

- Calor interior. Se puede considerar que está compuesto por calor sensible y calor latente.
    - Calor sensible: es el calor empleado en el cambio de temperatura, sin modificación del estado físico del cuerpo.
        - Equipamiento TI

$$\text{Potencia frigorífica (kW)} = \text{Potencia eléctrica consumida (kW)}$$

        - SAI – Su carga térmica depende de la carga de TI
        - Iluminación – Se estiman 20 W/m2.
        - Distribución de alimentación – 5% de la carga TI
        - Personas – Aproximadamente 100 W/ persona.
    - Calor latente, es el calor que, sin afectar a la temperatura, es necesario suministrar para producir un cambio de estado físico.

Sin embargo, el calor latente representa una parte muy pequeña del calor interior, por lo que suele considerarse sólo el calor sensible para los cálculos.

La refrigeración del sistema puede provocar la condensación de vapor de agua y en consecuencia la pérdida de humedad, por lo que será necesaria una humidificación suplementaria para mantener el nivel de humedad necesario. Sin embargo, la humidificación suplementaria crea una carga de calor adicional en la unidad de aire acondicionado disminuyendo la capacidad de refrigeración de la unidad y haciendo necesario un sobredimensionamiento [Ras03].

## 5.1 Normativa

La ASHRAE (*American Society of Heating Refrigeration and Air conditioning Engineers*) es una sociedad fundada en 1894 y se centra en la eficiencia energética, la calidad del aire interior, la refrigeración, y la sostenibilidad de la industria a través de la investigación, la redacción de normas, publicaciones y educación continua [Ash12].

El Comité Técnico 9.9 de la ASHRAE, mediante la edición de la Guías Térmicas para Entornos de Procesamiento de Datos, especifica los rangos de temperatura y humedad adecuados para el correcto funcionamiento del CPD, que se han ido ampliando a lo largo de los años para otorgar mayor flexibilidad a las operaciones dentro de los CPDs, con el objetivo de reducir el consumo energético. Las clases 1 y 2 son las que se refieren a entornos de servidores, productos de almacenamiento, ordenadores personales, etc.

| Clase | Temperatura de bulbo seco[19] (°C) | | Rango de humedad, sin condensación | |
|---|---|---|---|---|
| | Permitida | Recomendada | Permitida (% RH) | Recomendada |
| 1 | 15-32 | 18-27 | 20-80 | 5,5 °C DP[20] a 60% RH[21] y 15°C DP |
| 2 | 10-35 | 18-27 | 20-80 | 5,5 °C DP a 60% RH y 15°C DP |

Tabla 10: Rangos de temperatura y humedad

Los límites de temperatura recomendados van desde los 18°C hasta los 27°C. La humedad está limitada a menos del 60% con temperaturas del punto de condensación inferiores y superiores de 5,5°C y 15°C, respectivamente.

*Parámetros*

Los principales parámetros a considerar en la selección de un equipo de Aire Acondicionado son [Eme11c]:

- SHR (*Sensible Heat Ratio*) – Es el Factor de Calor Sensible (FCS). Se calcula como la relación entre la potencia total frigorífica de la máquina y la que realmente es útil para bajar la temperatura.

$$\text{SHR} = \frac{\text{Qs (Calor Sensible)}}{\text{Qt (Calor Total)}}$$

- EER (*Energy Efficiency Ratio*) – Es el coeficiente de eficacia frigorífica de la máquina y se calcula como la relación entre la potencia frigorífica entregada y la potencia eléctrica absorbida.

$$\text{EER} = \frac{\text{We (Potencia Entregada)}}{\text{Wa (Potencia Absorbida)}}$$

## 5.2 Ciclo de refrigeración

Los elementos de un ciclo de refrigeración son un condensador, una válvula de expansión (expansor), un evaporador, un compresor y líquido refrigerante. A través de este circuito se produce la transferencia de calor desde el CPD al exterior de la sala, tal y como se describe a continuación y se observa en la Ilustración 27.

[19] Temperatura de bulbo seco es aquella medida por un termómetro de mercurio o similar cuyo bulbo se encuentra seco [Wik12d].

[20] DP, *Dew point*, es el punto de rocío.

[21] RH, *Relative Humidity*, es la humedad relativa.

El líquido refrigerante absorbe el calor de la sala convirtiéndose en gas. El refrigerante en estado gaseoso a alta temperatura y presión debido a la reducción de volumen provocada por el compresor entra en el condensador, donde pasa a estado líquido a alta presión más o menos enfriado. De ahí, atraviesa el expansor, de donde se obtiene líquido refrigerado a baja presión listo para evaporar. En esta fase, gracias a un ventilador, se desprende calor.

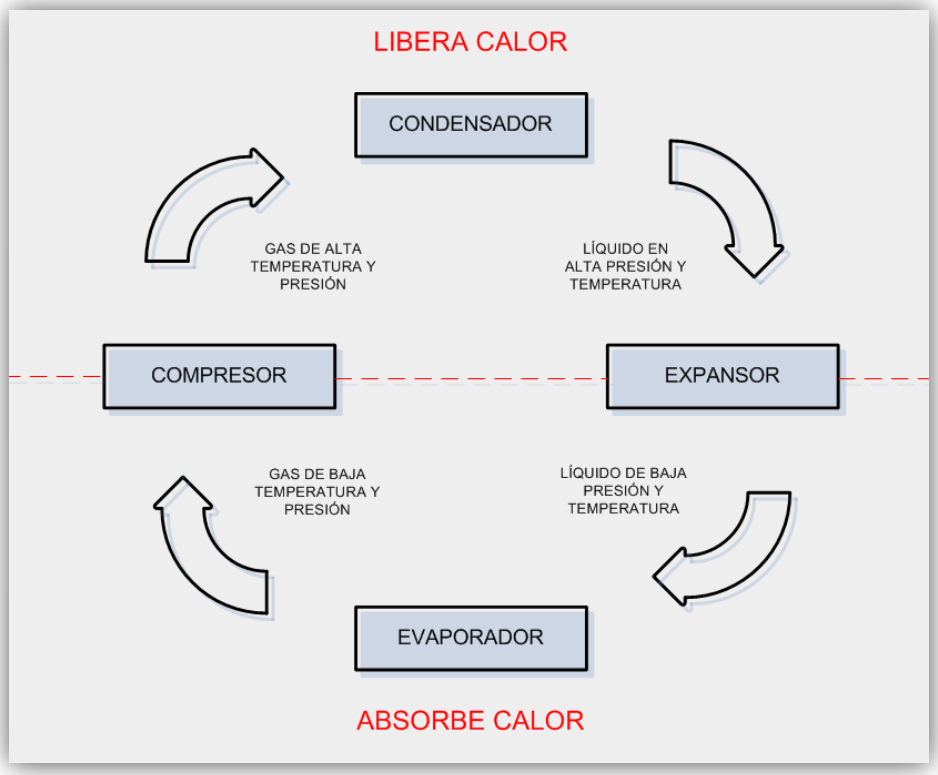



Ilustración 27: Ciclo de refrigeración

A continuación el líquido refrigerante a baja presión y temperatura pasa al evaporador, donde se convierte en gas a baja presión más o menos recalentado, tras absorber el calor de la sala. Finalmente pasa por el compresor, de donde sale gas a alta presión y temperatura listo para entrar al condensador y empezar un nuevo ciclo.

## 5.3 Tipos de refrigerantes

La refrigeración puede realizarse por gas o por agua.

Inicialmente, los gases refrigerantes más utilizados eran el R12 y el R22 (clorofluorocarbonos), pero fueron reemplazados por R407C, R410A (llamado comúnmente Puron) y R134A al comenzar la preocupación por la capa de ozono.

Algunas características de los nuevos refrigerantes gaseosos (extraídas de [Wik12b] y [Wik12c]) son:

- No dañan la capa de ozono
- Tienen bajo efecto invernadero
- No son tóxicos ni inflamables
- Son estables en condiciones normales de presión y temperatura
- Punto de congelación inferior a cualquier temperatura que existe en el sistema, para evitar congelamientos en el evaporador.
- Calor específico lo más alto posible para que una pequeña cantidad de líquido absorba una gran cantidad de calor.
- Temperatura de condensación, a la presión máxima de trabajo, lo menor posible.
- Temperatura de ebullición baja a presiones cercanas a la atmosférica (Tabla 11).

| Refrigerante | Punto de ebullición en °C a 1013 bar |
|---|---|
| R-12 | -29,8 |
| R-22 | -40,8 |
| R-407C | -43,44 |
| R410A | -48,5 |

Tabla 11: Puntos de ebullición de los refrigerantes

- Punto crítico[22] lo más elevado posible.

## 5.4 Tecnologías de refrigeración

### 5.4.1 Condensación por aire – Expansión Directa (DX)

El sistema está compuesto por dos unidades, una exterior y otra interior (Ilustración 28, [Eme12]). El refrigerante en estado líquido y baja temperatura fluye desde el condensador (exterior) hasta la evaporadora (interior), donde absorbe el calor de la sala pasando a estado gaseoso. El gas, a alta temperatura y presión tras abandonar el compresor, retorna hacia el

[22] Punto crítico: es la temperatura límite a la cual un gas no puede ser licuado por compresión. Por encima de esta temperatura es imposible condensar un gas aumentando la presión [Wik11a].

condensador, donde cederá el calor al ambiente tras circular por un serpentín aleteado que es atravesado por una corriente de aire, generalmente movida por un ventilador.

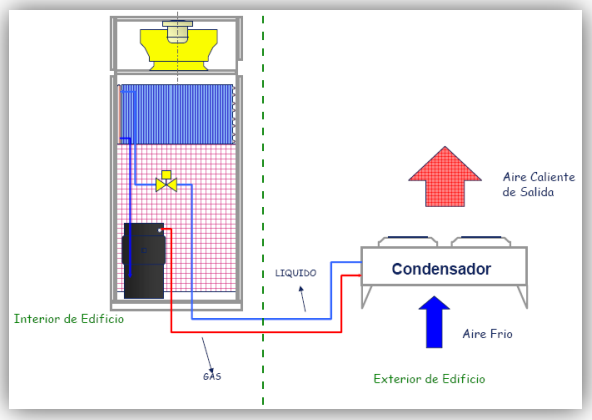



Ilustración 28: Condensación por aire

Entre las ventajas de esta solución se encuentran el bajo coste y la flexibilidad que aporta la solución, mientras que algunos de sus inconvenientes son la imposibilidad de conectar simultáneamente varias unidades interiores a una unidad exterior y un límite de distancia de 50 metros entre las unidades exterior e interior [Eme11c].

### 5.4.2 Condensación por agua/glicol – Expansión Directa (DX)

Se trata de un método en desuso. Hay dos circuitos, uno de refrigerante y otro de agua/glicol, que se unen en el intercambiador de calor (Ilustración 29 [Eme12]). En vez de condensador tiene un aero-refrigerador.

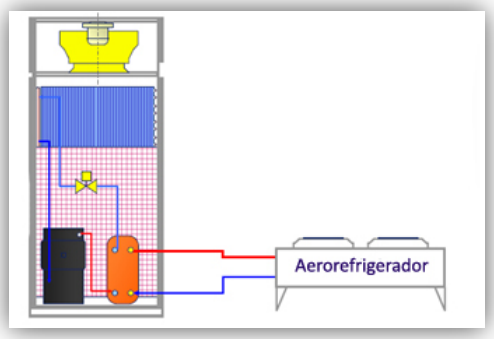



Ilustración 29: Condensadora por agua/glicol

No existe el límite de distancia de 50 metros entre unidades [Eme11c].

### 5.4.3 Condensación por torre de refrigeración

Este tipo de tecnología está formada por dos circuitos que se unen en el intercambiador de calor (Ilustración 30 [Eme12]). El intercambiador de calor es un dispositivo en el que se realiza

una transferencia de calor entre dos medios que están separados físicamente. Estos medios son el refrigerante y el agua. El circuito refrigerante se encuentra en la unidad interior. El circuito de agua circula desde el intercambiador de calor (interior) a la torre de refrigeración (unidad exterior), donde libera el calor al rociarse atravesando una corriente de aire movida por un ventilador.

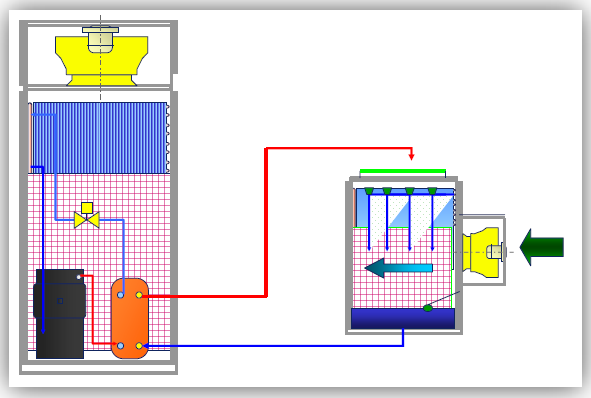


Ilustración 30: Condensación por torre de refrigeración

Algunas de sus ventajas son los elevados rendimientos que obtiene, o la elevada distancia que puede existir entre las unidades interior y exterior. Los principales inconvenientes son el peso de la torre y los tratamientos que deben hacerse para evitar la *legionella* [Eme11c].

### 5.4.4 *Chiller*

Un *chiller* es una unidad enfriadora de agua. La unidad interior no tiene ni evaporadora ni compresor. Está formada solo por un serpentín con un ventilador (CRAH). La evaporadora y la condensadora se encuentran en la unidad exterior (*chiller*). El esquema de este tipo de solución se muestra en la Ilustración 31 [Eme12]:

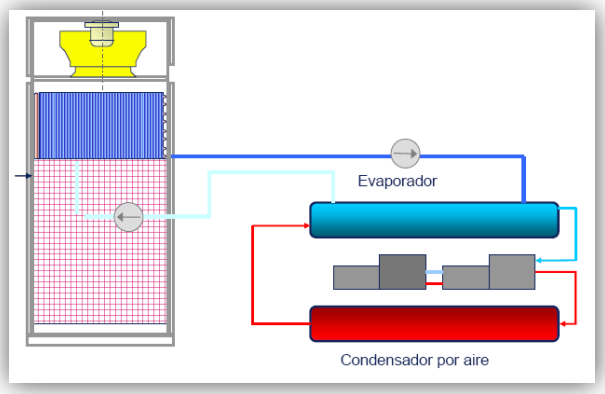



Ilustración 31: *Chiller*

Sus principales ventajas son el elevado rendimiento que se obtiene para instalaciones de gran tamaño, y la elevada distancia que puede existir entre las unidades interior y exterior. Su mayor inconveniente es el coste [Eme11c].

### 5.4.5 *Free Cooling*

El *free cooling* es una tecnología de refrigeración que aprovecha las bajas temperaturas exteriores para refrigerar el CPD, reduciendo el uso de los equipos de aire acondicionado y por lo tanto, el consumo y las emisiones de carbono, lo que la convierte en una tecnología "verde". Existen dos tipos de *free cooling*, directo e indirecto.

*Free Cooling Directo*

El aire exterior se emplea directamente en el proceso de refrigeración.

*Free Cooling Indirecto*

A diferencia del *free cooling* directo, transfiere el frío a través de un sistema que emplea una mezcla de agua y glicol. La carga térmica se traspasa al aire exterior a través del intercambiador de calor. En el caso óptimo (bajas temperaturas exteriores) el sistema puede refrigerar empleando únicamente el aire frío exterior. Las máquinas refrigerantes se pondrán en marcha únicamente cuando las temperaturas exteriores sean elevadas.

El *free cooling* indirecto, en los casos en que las temperaturas exteriores son bajas, es un método de refrigeración muy eficiente. El consumo de potencia necesario para refrigerar el CPD puede reducirse en un 70%.

## 5.5 Arquitecturas de refrigeración

Cada equipo de un CPD, en su proceso de refrigeración, toma el aire ambiente y expulsa el calor residual con el aire de escape, generando miles de trayectorias de circulación de aire caliente dentro de la sala convirtiéndose este aire caliente en un calor residual que se debe eliminar [Ras06b].

### 5.5.1 Refrigeración por salas

El principio básico de este modo de refrigeración es que los equipos de aire acondicionado, además de suministrar aire frío al CPD y absorber y expulsar el aire caliente, actúan como un mezclador, moviendo y mezclando constantemente el aire de la sala para que tenga una temperatura media homogénea, evitando de este modo que se produzcan puntos calientes. La experiencia demuestra que este método es eficaz si la densidad media de potencia del CPD es del orden de 1-2 kW por *rack*. Para evitar los problemas que surgen con densidades superiores, aparecen las arquitecturas de pasillo y *rack* [Ras06b].

### 5.5.2 Refrigeración por filas

En este modo de refrigeración, las unidades *CRAC* (*Computer Room Air Conditioning*) están asociadas a una fila por motivos de diseño. Pueden estar montadas entre los *racks*, en el techo o bajo el suelo. Las vías de circulación de aire son más cortas y están definidas con mayor claridad. Los flujos de aire son más predecibles, se puede aprovechar toda la capacidad de las unidades de CRAC y se puede alcanzar una mayor densidad de potencia [Ras06b].

Este tipo de arquitectura permite la configuración con sistemas de contención de pasillos calientes, eliminando cualquier posibilidad de que se mezcle el aire y mejorando la eficiencia de la solución.

### 5.5.3 Refrigeración por *racks*

Las unidades de CRAC están asociadas a un *rack* por motivos de diseño. Se montan directamente al lado o dentro de los *racks*. Las vías de circulación de aire son muy cortas y precisas. Se puede aprovechar toda la capacidad nominal de las unidades de CRAC y se puede alcanzar la máxima densidad de potencia [Ras06b].

En la Ilustración 32, [Sch12], muestra la capacidad utilizable de la máquina de aire acondicionado frente la densidad de potencia media por *rack* de cada uno de las arquitecturas de refrigeración.

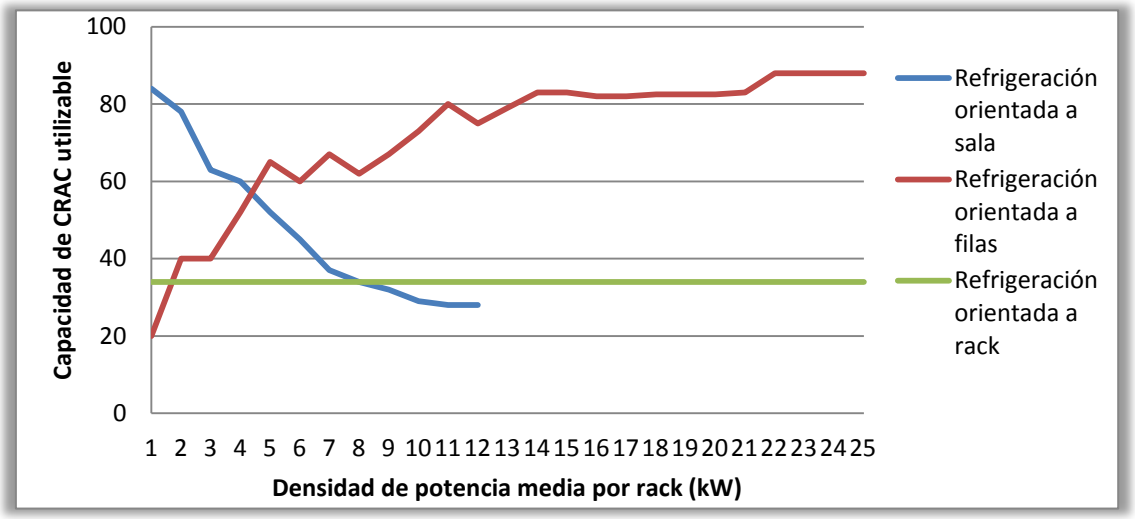



Ilustración 32: Comparación arquitecturas de refrigeración

## 5.6 Problemas de climatización

La mayor fuente de ineficiencia de los CPDs es la refrigeración, debido a una mala gestión de la distribución del aire. Esto se debe a que suelen mezclarse los flujos de aire frío y caliente,

originando lo que se conocen como flujos de bypass y flujos de recirculación (Ilustración 33[23]). La mezcla del aire de impulsión y el aire de retorno causa que la diferencia de temperaturas entre ellos sea menor, lo que motiva un aumento del consumo de la unidad enfriadora.

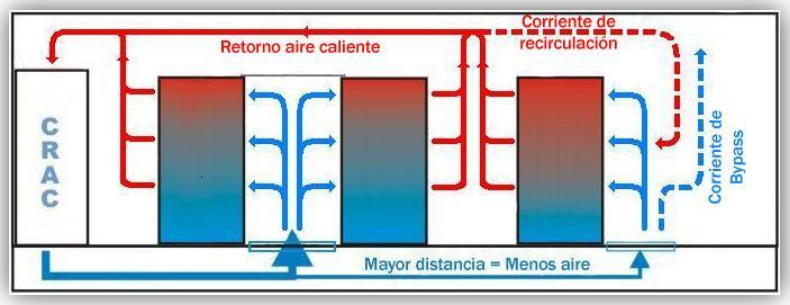



Ilustración 33: Flujo de aire

La solución a los problemas relacionados con el flujo de aire en el CPD son variados. En los sistemas de impulsión por falso suelo, la solución pasa por la selección de una altura de falso suelo que permita mantener una baja velocidad de aire, la apertura del falso suelo bajo los equipos electrónicos y la selección del tipo de rejilla a instalar y el número de las mismas. Un complemento a esta solución es el cerramiento de pasillo frío / caliente y la instalación de paneles ciegos en los *racks*.

[23] Ilustración extraída de documentación interna de Fujitsu Technology Solutions.

# Capítulo 6 Instalaciones de Protección contra incendios

Como se ha comentado con anterioridad, la mayoría de los fuegos empiezan fuera del CPD. Sin embargo, y pese a que estructuralmente el CPD debe estar preparado para resistir la amenaza de un fuego exterior, también debe existir un sistema de detección y extinción de incendios en el interior de la sala, por si se propagase desde el exterior al interior o por si se originase en el interior.

## 6.1 Normativas

Existe un amplio número de normas y estándares para los sistemas de detección y extinción de incendios, de las cuales las más destacables son las siguientes.

*NFPA 75, Protección de equipos de computación electrónicos / equipos procesadores de datos*

Esta norma trata los requisitos para la protección de los equipos y las áreas de equipos de tecnología de la información de los daños ocasionados por el fuego y sus efectos asociados – humo, corrosión, calor y agua [NFP75].

*NFPA 750, Estándar sobre sistemas de protección contra incendios con agua nebulizada*

Este estándar contiene los requisitos mínimos para el diseño, instalación, mantenimiento y pruebas de sistemas de protección contra incendios con agua nebulizada (ver apartado 6.3.2).

Este estándar no proporciona criterios definitivos sobre eficacia frente al fuego ni ofrece una guía específica sobre cómo diseñar un sistema para controlar, suprimir o extinguir un incendio. La fiabilidad se obtiene mediante la obtención e instalación de sistemas que han demostrado su eficacia en ensayos de incendio [NFP750].

*NFPA 2001, Estándar sobre Sistemas de extinción de incendios con agentes limpios*

Éste estándar contiene los requisitos mínimos para los sistemas de extinción de incendios por inundación total que utilizan agentes limpios (ver apartado 6.3.1).

El Protocolo de Montreal (16 de Septiembre de 1987) estableció una serie de restricciones sobre la producción de algunos agentes extintores, debido a los efectos dañinos que éstos tenían en el medio ambiente y la capa de ozono. Los agentes limpios aparecen como una alternativa *limpia* a estos gases [NFP2001].

## 6.2 Detección de incendios

El sistema de detección de incendios permite la localización de un incendio y activa la alarma correspondiente. La central de incendios puede estar controlada por personal adecuando o puede que esté programada para realizar determinadas acciones automáticamente.

Los componentes principales del sistema de detección de incendios son [Ntp40]:

- Detectores.
- Pulsadores manuales.
- Central de señalización.
- Líneas.
- Sistemas auxiliares: alarma general, teléfono, accionamiento de los sistemas de extinción, etcétera.

### 6.2.1 Tipos de detectores

Existen distintos tipos de detectores de incendios.

*Iónicos*

Los detectores iónicos detectan gases de combustión, que pueden ser visibles o invisibles. Consisten en dos cámaras, una de medida y otra estanca, ionizadas por un elemento radiactivo, y en las que se establece una corriente de iones se que ve modificada cuando los gases de combustión entran en las cámaras, interrumpiendo la corriente de iones y generando la señal de alarma [Ntp40].

*Ópticos*

Los detectores ópticos gestionan un sensor óptico de humos. Su función es tomar medidas de la luz que dispersan las partículas de humo (efecto Tyndall[24]), evaluar su densidad y su porcentaje de incremento en el tiempo, y después enviar a la central la información ya analizada. La central es quien compara los resultados obtenidos con los parámetros programados en cada caso y decide si es conveniente enviar la señal de alarma [Agu12].

*Termovelocimétricos*

Se trata de detectores de calor que gestionan dos parámetros de temperatura, uno diferencial que toma las medidas del incremento de temperatura en tiempo y otro que controla la temperatura ambiente que detecta en cada momento. Tanto el parámetro diferencial como el

[24] El efecto Tyndall es el efecto que provoca que las partículas coloidales de un gas sean visibles al dispersar la luz [Wik12e].

térmico son analizados y enviados a la central para que de la señal de alarma de acuerdo con la programación hecha en cada caso [Agu12].

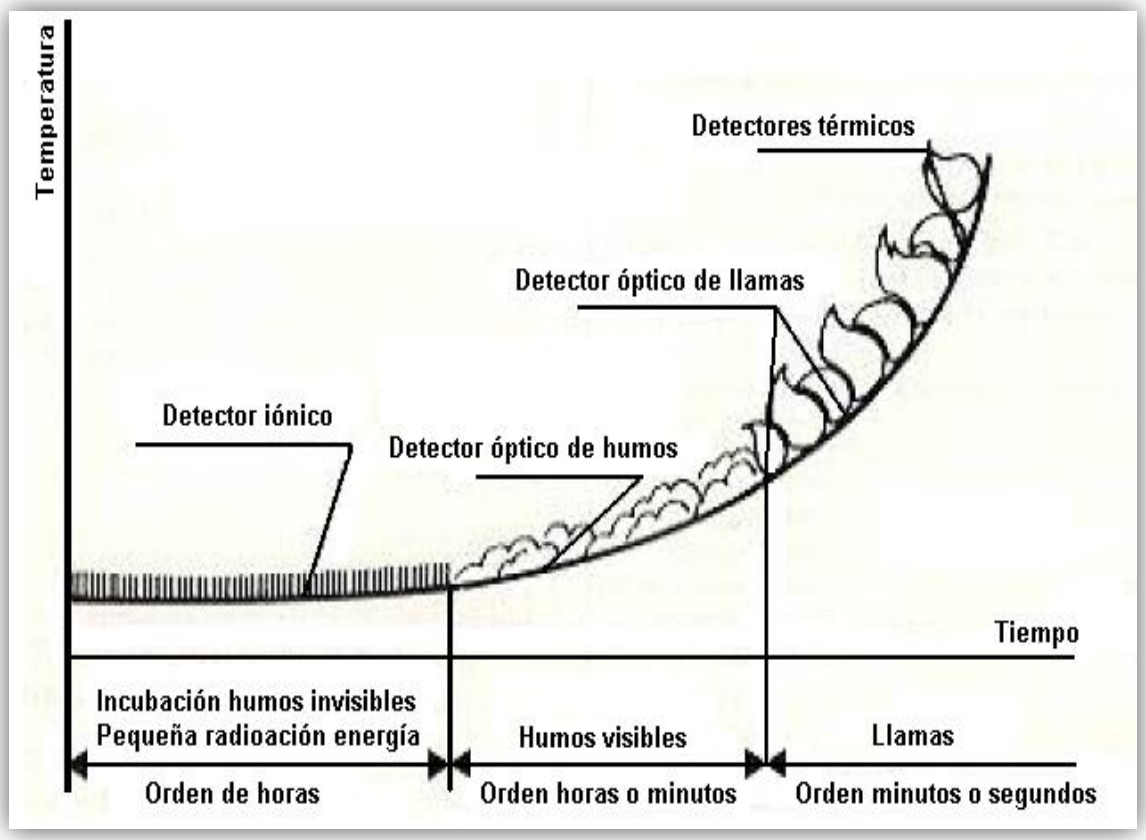



Ilustración 34: Fases de actuación de detectores

Como puede verse en la imagen superior (Ilustración 34[25]), cada tipo de detector se concentra en una franja de tiempo del inicio del incendio. El detector iónico es el que trabaja en la fase incipiente, cuando el humo aún no es visible al ojo humano. El detector óptico de humos se pone en funcionamiento cuando ya podemos ver el humo provocado por el incendio. Y finalmente el detector térmico actúa cuando ya existen llamas que generan calor.

### *Detección por aspiración*

La mayoría de los incendios poseen en su inicio una extensa fase de fuego latente.

Los sistemas de detección convencionales basan su funcionamiento en que el efecto que provoca el fuego (humo, gas, temperatura) alcance el detector. Pero es posible que existan obstáculos que impidan que el humo, u otro factor, alcance al detector. Para estos casos, es imprescindible una detección altamente sensible al humo que asegure una respuesta rápida y

[25] Ilustración extraída de la norma NTP 40.

así reduzca al mínimo las pérdidas por el fuego. Este tipo de detección es la detección por aspiración.

Se trata de sistemas que ofrecen aviso anticipado de un fuego potencial. Esto ofrece un tiempo adicional que permite intervenir evitando las consecuencias de la descarga de los agentes extintores.

El sistema de detección precoz por aspiración funciona succionando aire continuamente por una red de conductos a través de un aspirador de muy alta eficiencia. A continuación, una muestra de este aire se pasa a través de un filtro y llega a una cámara calibrada donde se expone a una fuente de luz láser. Cuando hay humo presente, la luz se dispersa dentro de la cámara de detección y el sistema receptor de alta sensibilidad lo identifica al instante [Xtr12].

### 6.2.2 Pulsadores manuales

Existen distintos tipos de pulsadores, que básicamente pueden agruparse en pulsadores de alarma de extinción, pulsadores de activación manual de extinción y pulsadores de bloqueo manual de extinción. Todos ellos con distintos mecanismos de protección para evitar manipulaciones fraudulentas o accidentales, tales como sistema de comprobación con llave de rearme o tapa de metacrilato.

### 6.2.3 Centrales

Las centrales son equipos que permiten controlar individualmente todos los equipos que componen las instalaciones de detección de incendios. Suelen tener uno o varios bucles a los que se conectan los detectores, pulsadores, módulos de maniobras, de control, y demás elementos que configuran la instalación [Agu12].

Tienen un control completo de funcionamiento de todos los equipos que componen la instalación, de forma programada o manual: rearmes, reposiciones, niveles, conexión y desconexión de puntos, activación y desactivación de evacuaciones, cierre de puertas y compuertas cortafuegos.

Incluyen indicadores luminosos y avisador acústico local, para presentación de estados generales de servicio, alarma, avería, desconexión, test, alimentación y estado de maniobras de evacuación y otros.

Disponen de puertos de comunicaciones para poder realizar la conexión con el puesto de control mediante protocolo TCP/IP.

## 6.3 Extinción de incendios

La extinción puede hacerse mediante gas o mediante agua. En el caso de CPDs, los métodos más empleados son el gas y el agua nebulizada.

*El tetraedro del fuego*

El tetraedro del fuego (Ilustración 35[26]) describe los componentes necesarios para generar un fuego.


Ilustración 35: Tetraedro del fuego

Ante la ausencia de cualquiera de los componentes (combustible, oxígeno, calor y reacción en cadena), el fuego se extingue. Por este motivo los agentes extintores atacan a uno o varios de los componentes.

### 6.3.1 Extinción por gas

La extinción por gas tiene una serie de ventajas frente a la extinción por agua:

- No dejan residuos.
- No conducen la electricidad.
- Evitan los daños producidos por el agua.
- Rápida actuación en el foco del incendio.
- La actividad se reinicia rápidamente tras la descarga.
- La inundación total permite que el agente extintor llegue incluso a las zonas menos accesibles.

[26] Ilustración extraída de Wikimedia Commons, *commons.wikimedia.org*.

Sin embargo, para que el sistema de extinción funcione correctamente, deben cumplirse unos requisitos de diseño e instalación adecuados. La estanqueidad del recinto o el sistema de refrigeración (las corrientes de aire, sus velocidades) pueden provocar en determinadas circunstancias que el sistema de extinción no se active porque falle la detección o que se active pero no lo extinga.

### *Tipos de gases*

Existen distintos tipos de gases que se emplean en la extinción de incendios en los CPDs:

- Halón
- Novec 1230
- $CO_2$
- Halocarburos, HFCs
- Inertes

#### *Halón*

El halón ha sido el gas más empleado en los últimos 30 años para la extinción de incendios en los CPDs. Se presentaba en estado líquido y su principal ventaja era la absorción de calor en el cambio de fase (de líquido a gas). Sobre el tetraedro del fuego, el halón actuaba de dos maneras: absorbiendo calor y rompiendo la reacción en cadena. Su margen de seguridad para el uso con personas era alto. Sin embargo, debido a su potencial de destrucción de la capa de ozono se procedió a la prohibición de fabricar e importar halón desde enero del 1994 y a la desactivación y retirada de los sistemas de halón como máximo el 31 de diciembre del 2003, en el protocolo de Montreal en 1987.

#### *Novec 1230*

Es un agente limpio que a temperatura ambiente es líquido y se transforma en gas durante la descarga, lo que lo convierte en un agente eficaz de inundación total. En el tetraedro del fuego, el Novec 1230 suprime incendios gracias a su efecto de enfriamiento.

Se trata de un agente que no deja residuos. Es de baja toxicidad, lo que hace que sea ideal para espacios ocupados donde el personal puede exponerse al agente una vez comenzada la descarga. No es corrosivo ni conductivo, y se evapora rápidamente. Posee un potencial de reducción de ozono de cero, una vida atmosférica corta (5 días) y un potencial de calentamiento global de 1 [3M07]. Su principal desventaja es que necesita mayor concentración que otros gases para lograr el mismo efecto extintor.

#### *Dióxido de carbono, $CO_2$*

El dióxido de carbono es, a presión atmosférica, un gas incoloro, inodoro, casi 1.5 veces más denso que el aire y que se almacena en forma líquida bajo presión [Afi12]. En el tetraedro del

fuego, el dióxido de carbono se centra en reducir la cantidad de oxígeno, hasta un punto en que no pueda existir combustión.

El principal problema del $CO_2$ es que la cantidad necesaria para extinguir un fuego puede resultar perjudicial para las personas, ya que tiene efecto asfixiante, por lo que es necesario adoptar las medidas de seguridad adecuadas para asegurar la pronta evacuación, así como para evitar la entrada a la zona de descarga y para facilitar el rescate de cualquier persona que hubiera quedado atrapada durante la descarga. Estas medidas comprenden alarmas previas a la descarga, señales de advertencia, entrenamiento para el personal, avisos audibles, etcétera.

*Halocarburos, HFCs*

Los HFCs son los agentes limpios más extendidos como sustitutos del Halón. Se almacenan en estado líquido y sobre el tetraedro del fuego actúan enfriando la llama. Se emplea en concentraciones relativamente bajas.

La ventaja respecto al $CO_2$ y los gases inertes es que con cantidades inferiores de gas es posible extinguir el incendio, a la vez que optimiza el espacio requerido para el sistema de almacenamiento del gas.

El mayor inconveniente de los HFCs es el efecto invernadero. Su índice de potencial de calentamiento global es de 3500. A pesar de esto, la incidencia de las emisiones de HFCs frente los gases de efecto invernadero es muy baja, por lo que de momento no se han impuesto limitaciones al uso de HFC en sistemas de supresión de incendios. Sin embargo, han comenzado a plantearse restricciones en algunos países por la generación de compuestos tóxicos por descomposición térmica durante el ataque al fuego.

Los más empleados son el HFC-227ea (FM-200) y el HFC-23 (FE-13).

*Gases Inertes*

Los gases inertes son otro tipo de agentes limpios, que resultan de combinaciones de nitrógeno y argón (puros o mezclados), y $CO_2$. Se almacenan como gases comprimidos a presión.

Requieren de concentraciones relativamente elevadas ya que apagan el fuego reduciendo la cantidad de oxígeno hasta niveles en los que no se sostiene la combustión. Este tipo de gases se emplean básicamente en riesgos tecnológicos, eléctricos y electrónicos, donde no es posible o es muy costosa la limpieza de los bienes protegidos.

Los productos que se comercializan por el momento son [Ing07]:

- El IG-541, Inergen, es una mezcla de nitrógeno (52%), argón (40%) y anhídrido carbónico (8%), fabricado por Wormald. La EPA permite su utilización en áreas ocupadas siempre que la concentración de oxígeno sea superior al 12% y la de $CO_2$ inferior al 5%.

- El IG-55, Argonite, es una mezcla al 50% de nitrógeno y argón, fabricado por Ginge-Kerr. Las condiciones de uso son las mismas descritas para el Inergen.
- El IG-01, Argón, está formado por gas argón al 100%. Esta marca es comercializada por la firma Preussag y sus parámetros de uso similares a los antes detallados.

Ninguno de los tres productos es tóxico y en caso de una descarga accidental no presentaría problemas para los ocupantes del área involucrada.

En la siguiente tabla (Tabla 12) podemos comparar las principales características del Inergen, FE-13 y FM-200.

| Nombre comercial | Inergen | FE-13 | FM-200 |
|---|---|---|---|
| Mecanismo de extinción | Disminución del oxigeno | Inhibe reacción en cadena | Inhibe reacción en cadena |
| Presión de vapor (77° F) | 2207 psi (Gas alta presión) | 686 psi (Gas alta presión) | 66.4 psi (Gas baja presión) |
| Potencial reducción de ozono | Ninguno | Ninguno | Ninguno |
| Potencial de calentamiento atmosférico | Ninguno | 100 años - GWP de 9.000 | 100 años - GWP de 3.300 |
| Tiempo de vida atmosférico | Cero-Derivado de la atmósfera | 235/280 años | 31/42 años |
| Concentración de diseño mínima | 35.0% | 14.4% | 7.0% |
| Tiempo de descarga | 60 segundos a concentración de diseño | en 10 segundos el 95% de la descarga | en 10 segundos el 95% de la descarga |

Tabla 12: Comparativa agentes extintores

### *Evaluación de riesgos*

La descarga de un sistema de extinción que utiliza un extintor del tipo halocarbonado (HFC), puede crear riesgos para el personal, derivados de la toxicidad intrínseca del mismo o de los productos de descomposición térmica en caso de incendio [Ing07].

La toxicidad de estos productos se mide por diversos parámetros:

- El NOAEL (*No Observed Adverse Effect Level*), que es la concentración más alta a la que ningún efecto psicológico o toxicológico adverso ha sido observado.
- El LOAEL (*Lowest Observed Adverse Effect Level*), que es la concentración más baja a la que ha sido observado algún efecto psicológico o toxicológico adverso.
- El LC (*Lethal concentration*), que es la concentración a la que sometida una población de ratas, resulta mortal para el 50% de las mismas en una exposición de 4 horas. Cuanto más alto es el valor de LC, menos tóxico es el producto.

A continuación, en la Tabla 13, se agrega una tabla donde se exponen los valores conocidos del LC, NOAEL y LOAEL para algunos agentes limpios.

| Agente | LC | NOAEL | LOAEL |
|---|---|---|---|
| FM-200 | > 80% | 9% | 10,5% |
| FE-13 | > 65% | 50% | >50% |
| INERGEN | No tóxico | 43% | 52% |
| ARGONITE | No tóxico | 43% | 52% |
| ARGON | No tóxico | 43% | 52% |

**Tabla 13: Toxicidad para gases**

El criterio que permite determinar si un agente extintor es utilizable en áreas normalmente ocupadas, es el análisis de su cardiotoxicidad, comparándola con su concentración de diseño. La concentración de diseño del gas debe ser siempre inferior al NOAEL para garantizar la seguridad del mismo.

En la tabla que se muestra a continuación, se exponen valores de *cup burner*[27], concentración de diseño y NOAEL para algunos agentes limpios:

| Agente | Conc. cup burner | Conc. diseño | NOAEL |
|---|---|---|---|
| FM-200 | 5,9% | 7,2% | 9% |
| FE-13 | 12% | 15% | 30% |
| INERGEN | 30% | 36% | 43% |

[27] El Test de *cup-burner* se emplea para determinar la concentración mínima de extinción (MEC, *Minimum Extinguishing Concentration*) de agentes supresores gaseosos contra líquidos inflamables como el n-heptano. La NFPA 2001 establece que la concentración de diseño siempre debe ser un 20% superior a la concentración de *cup burner*.

| | | | |
|---|---|---|---|
| ARGONITE | 30% | 36% | 43% |
| ARGON | 30% | 36% | 43% |

Tabla 14: Concentraciones gases

Además, para la eficacia de la protección, es importante no solo conseguir una buena concentración, sino que esta se mantenga durante un período mínimo de tiempo. El tiempo mínimo de permanencia de la concentración deberá ser superior a 10 minutos. La masa de agente extintor-aire después de la descarga, resulta más densa que el aire exterior al recinto, con lo que el agente extintor tenderá a vaciarse rápidamente por todas las aberturas que existan.

### 6.3.2 Extinción por agua nebulizada

El agua nebulizada es agua impulsada a alta presión a través de boquillas especiales [Mar12].

Está formada por microgotas descargadas a alta velocidad. La superficie de refrigeración es muy grande y la vaporización muy rápida. En la Tabla 15 se muestra una comparativa de los diferentes tipos de gotas en función del sistema de refrigeración.

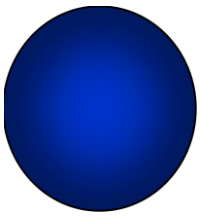
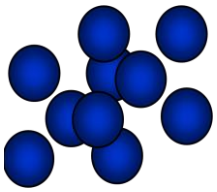
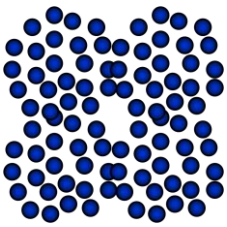
| | Nº de gotas | Tamaño gota (promedio) | Vaporización |
|---|---|---|---|
|  Rociador convencional | 1 | >1000 µm | 1 seg |
|  Niebla baja y media presión | 40 | 300 µm | 0,1 seg |
|  Agua nebulizada | 8000 | 50 µm | 0,003 seg |

Tabla 15: Agua nebulizada

En el tetraedro del fuego, el agua nebulizada suprime el incendio mediante enfriamiento, bloqueo de calor radiante e inertización del oxígeno. Son sistemas que emplean la humectación como principal mecanismo, y gracias a la nebulización conseguida, utilizan hasta

un 90% menos de agua que los sistemas de rociadores convencionales para la misma aplicación con un rendimiento equivalente o superior.

Frente a los sistemas de extinción convencionales y de agua pulverizada, el agua nebulizada presenta las siguientes ventajas:

- Consume entre un 60 - 90% menos de agua
- La descarga no produce daños a los equipos
- Al necesitar menos agua, ocupa menos espacio
- Extingue el incendio, mientras que los convencionales y el agua pulverizada son sistemas de control y supresión[28].

Frente a la extinción por gas presenta las siguientes ventajas:

- Mayor enfriamiento. Los gases no usan agua, así que existe posibilidad de re-ignición
- Los gases presentan daños por descarga indeseada (vidas humanas, coste recarga) y daños en descarga (productos descomposición térmica)
- No precisa estanqueidad en el recinto, mientras que los gases necesitan una estanqueidad próxima al 100%

*Beneficios*

- Alta eficacia: Eficacia demostrada en la lucha contra incendios de clase A y B[29].
- Sistema Inocuo: Es completamente inofensivo para las personas y el entorno.
- Limpieza: Emplea una menor cantidad de agua. Al tratarse de agua limpia en cantidades inferiores en comparación con otros sistemas, minimiza los daños causados por el agua y requiere un escaso trabajo de limpieza.
- No requiere estanqueidad.

El sistema está compuesto de depósito de agua, equipos modulares, equipos de bombeo, válvulas, tubería y boquillas nebulizadoras.

---

[28] Sistemas de extinción: Completa supresión del mismo hasta la desaparición total de posibilidad de re-ignición.

Sistemas de supresión: Intensa reducción del calor radiante y prevención de la re-ignición, durante el tiempo de descarga.

Sistemas de control**:** Limitación del crecimiento del fuego y prevención de daños estructurales.

[29] Existen cinco clases de fuegos: A (materiales que producen brasas), B (líquidos inflamables), C (gases inflamables), D (metales combustibles) y F (grasas) [UNE05].

*Lavado de humos*

La técnica del lavado de humos comprende la extracción del humo y gases corrosivos desde el falso suelo como parte del proceso de extinción del incendio. Utiliza un sistema de agua nebulizada del tipo alta presión, doble ruido (agua + nitrógeno), y una sola tubería.

# Capítulo 7 Instalaciones de *Racks* y cableado

## 7.1 Racks

Un *rack* es la estructura que alberga los equipos TIC. El *rack* es una estructura modular, como puede verse en la Ilustración 36[30], formado por las siguientes partes:

Ilustración 36: Elementos de un *rack*

- Estructura (armazón).
- Paneles laterales.
- Puertas.
- Paneles ciegos.
- PDUs (ver apartado 4.4).
- Techo.

[30] Ilustración extraída de la página web de Módulo, *www.modulo.pt*.

- Suelo.
- Cerradura.
- Pasahilos: se trata de un elemento organizador de cableado. Posee una serie de liras por las que se pasan los cables, tanto de fibra como de cobre. Pueden ser verticales u horizontales y suelen ser de 1U.
- Bandejas.
- Guías: elementos empleados para el montaje de bandejas, servidores, SAIs. Pueden ser fijas o extraíbles (telescópicas).

### 7.1.1 Normativa

Las medidas de los *racks* están estandarizadas por las normas que se describen a continuación:

- EN 60297-3-100:2009: Estructuras mecánicas para equipamiento electrónico. – Dimensiones de estructuras mecánicas de las series de 482,6 mm (19 pulgadas) – Parte 3-100. Especifica las dimensiones básicas de los paneles frontales, *subracks*, chasis, *racks* y cabinas de 482,6 mm.
- IEC 297: Dimensiones de estructuras mecánicas de las series de 482,6 mm
- EIA 310-D: *Racks*, paneles y equipamiento asociado.
- DIN 41494: Estructuras mecánicas para equipamiento electrónico; Estructuras mecánicas para equipamientos electrónico de las series de 482,6 mm; guía de aplicación.

## 7.2 Sistema de cableado

Desde el punto de vista de la infraestructura, una de las partes más importantes y complejas del diseño del CPD es el cableado estructurado. La red física establece cómo estos equipos se comunican unos con otros y con el mundo exterior.

Es de vital importancia que el sistema de cableado del CPD esté bien organizado para que sea fácil de entender y manejar. Si el sistema de cableado se diseña bien, aportará escalabilidad al CPD.

El uso de un CPD se ve afectado por los siguientes [Alg05] aspectos del cableado estructurado:

- Medios de cableado escogidos
- Número de conexiones
- Organización del cableado

### 7.2.1 Jerarquía de cableado

Existen dos jerarquías de cableado, conocidas como *Top of the Rack* (ToR) y *End of the Row* (EoR). Ambas parten de una hilera de *racks* donde se instalan la mayor parte de los dispositivos de red. Esta fila se llamará fila de red y desde ella debe partir el cableado que va a las filas de servidores.

Una opción sería que el cableado estructurado fuese directamente a cada *rack* (ToR), como se puede ver en la Ilustración 37 [Cis12]. Esto funciona muy bien en entornos pequeños, porque el cableado recorre distancias cortas y puede manejarse con facilidad. No ocurre lo mismo en entornos mayores. Sin embargo esta será la opción elegida en aquellos casos en que se focaliza el diseño en la topología lógica y se presta poca atención a la física. Sus diseños se basan en los caminos que los datos siguen de un punto a otro de la red, pero no se fijan en el cableado estructurado que debe instalarse para permitir esto.

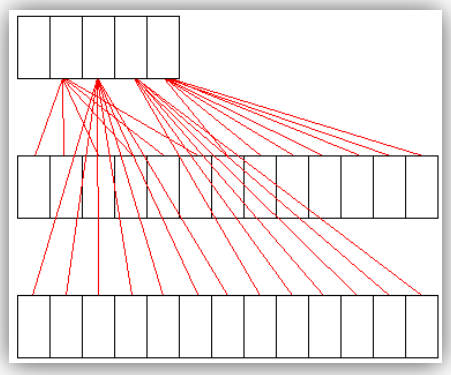


Ilustración 37: Top of the *rack*

En la Ilustración 38 [Cis12], se muestra otra opción, con un distribuidor de cableado de fila (conocida también como EoR), al que llegará el cableado, y desde allí se distribuirá a cada *rack* de la fila. Este modo sigue los principios del buen diseño de un CPD porque hace que el entorno de servidores sea más robusto, modular, flexible y estándar.

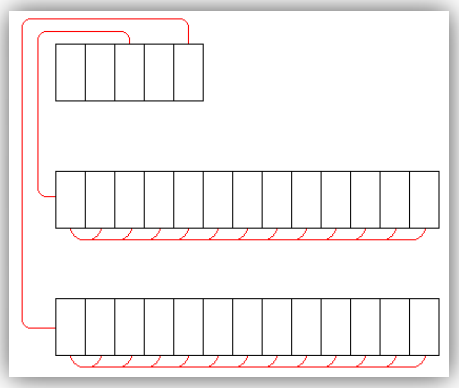


Ilustración 38: End of the row

El cableado, una vez en los *racks*, se distribuye a través de paneles de parcheo que pueden ser tanto de cobre como de fibra óptica. Se recomienda que se encamine el cableado estructurado por los laterales del *rack*. Es aquí donde se aprecia la importancia de limitar el tamaño de los haces de cables. Los instaladores de cableado pueden experimentar dificultades a la hora de encaminar el cableado estructurado en los *racks*, debido a que los haces son bastante rígidos y no moldeables, motivo por el cual el instalador deberá tener cuidado a la hora de manejarlo debido a los radios de curvatura de las fibras ópticas. Para facilitar esta tarea deben instalarse pasahilos y organizadores de cableado en los armarios, a través de los que se encaminarán los cables.

## 7.3 Arquitectura del CPD

### 7.3.1 Sistemas informáticos del CPD

Los principales componentes del CPD (en cuanto a sistemas informáticos se refiere) son los servidores, almacenamiento y elementos de comunicaciones [Ent12].

*Servidores*

Pueden ser en formato torre, *rack* y *blade*. El servidor tipo torre es el más básico, con un coste comparable al de un PC. Poseen todos los componentes tradicionales: disco duro, placa base y CPUs. Son bastante potentes ya que pueden tener más discos que las otras opciones, y se refrigeran fácilmente. Sin embargo, su principal problema es el espacio que ocupa, ya que no son enracables, lo que afecta a la escalabilidad de la solución. El servidor tipo *rack*, como su propio nombre indica, está diseñado para ser enracado, lo que supone un ahorro de espacio frente al formato anterior. Este formato dota de escalabilidad a la solución. Su principal problema radica en la dificultad que existe para refrigerarlos. Con la virtualización aparecen los servidores tipo *blade.* Se trata de un servidor modular diseñado para minimizar el uso de espacio físico. Un chasis *blade* contiene múltiples servidores *blade*, además de mecanismos de ventilación y alimentación. Es una solución altamente escalable. Sin embargo, requiere de mecanismos de refrigeración adicionales y mayor energía que los otros formatos, lo que incrementa su coste a largo plazo [Rok12]. En la Ilustración 39 pueden verse los tres tipos de servidores descritos:


Ilustración 39: Tipos de servidores

La virtualización de servidores proporciona mejor fiabilidad y alta disponibilidad en el caso de fallo en el *hardware*. Además, aumenta la utilización de los recursos *hardware* además de mejorar su administración al tener una única interfaz de gestión para todos los servidores virtuales.

*Almacenamiento*

Los requerimientos de almacenamiento varían dependiendo del tipo de servidor. Los servidores de aplicaciones requieren menos capacidad de almacenamiento que los servidores de bases de datos. Existen tres opciones de almacenamiento [Paw12]:

- *Direct Attached Storage* (DAS). Conexión directa de los servidores al almacenamiento. Cada servidor aloja los discos duros que utiliza.
- *Network Attached Storage* (NAS). Conexión del almacenamiento a la red Ethernet.
- *Storage Area Network* (SAN). Red de almacenamiento dedicada de alto rendimiento que transfiere datos entre servidores y dispositivos de almacenamiento [Dur04].

*Comunicaciones*

Los componentes de red (switches de nivel 2 y 3, routers WAN) proporcionan conectividad al CPD.

### 7.3.2 Diseño de red del CPD

El CPD aloja la potencia, almacenamiento y aplicaciones necesarias para soportar cualquier negocio. La infraestructura del CPD es el centro de la arquitectura TIC, desde donde se origina o pasan todos los datos. El diseño de la infraestructura de red del CPD es crítico, deben tenerse en cuenta para ello factores como el rendimiento, la resistencia, la escalabilidad o la flexibilidad.

El diseño de red del CPD está basado en una arquitectura por capas, tal y como se muestra en la Ilustración 40 [Cis07]:

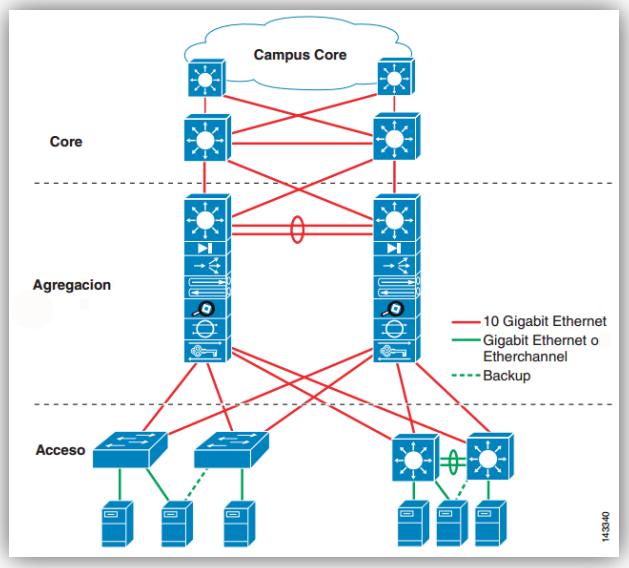



Ilustración 40: Arquitectura del CPD

Tal y como describe Cisco, las capas en las que se divide la red de un CPD son *Core*, Agregación y Acceso:

- *Core*. La capa de *Core* proporciona conmutación de paquetes a altas velocidades para todos los flujos de entrada y salida del CPD, además de conectividad balancear la carga entre el *Core* de Campus y las capas de agregación.
- Agregación. Proporciona funciones como la definición de dominios de nivel 2 (VLAN) y *spanning tree*. El tráfico entre los servidores atraviesa la capa de agregación y emplea servicios como el firewall o balanceo de carga para optimizar y dotar de seguridad las aplicaciones.
- Acceso. A la que se conectan físicamente los servidores para acceder a la red. El nivel de acceso se rige también por una topología de ToR y EoR, como la descrita anteriormente para el cableado.

Al igual que el resto de sistemas del CPD, también el sistema de comunicaciones está redundado en cada una de sus capas. Esto dota al sistema de robustez, escalabilidad y flexibilidad [Cis07].

En los CPDs actuales, gracias a la evolución de los equipos de acceso, es muy habitual encontrar diseños de dos niveles. Los switches de acceso a los que conexionan los servidores se conectan a los switches de agregación/*Core*, que proporcionan las funcionalidades de *switching* y *routing.* Entre las ventajas de la fusión de las capas de agregación y *Core* destacan la simplicidad de diseño, la reducción de costes y la menor latencia de red.

# Capítulo 8 Instalaciones de Seguridad

En este capítulo se exponen diferentes opciones de control de acceso al CPD y se recomiendan modos de operación para aquellos trabajadores que operan en ellos, basándonos en recomendaciones de Cisco [Alg05].

## 8.1 Restricciones físicas

Dado que el CPD contiene los servidores, aplicaciones y datos más críticos de la compañía, es importante asegurar físicamente el entorno. Se desea proteger al equipamiento de robos o vandalismo, de daños accidentales provocados por personal sin formación adecuada para trabajar en el CPD, y de extracción de información del CPD por parte de personal no autorizado.

La principal manera de proteger los equipos del CPD es controlar quién puede acceder a ellos mediante bloqueo de puertas, controles de acceso y *racks* con cerraduras. Las cámaras de video vigilancia pueden registrar quién entra o sale del CPD. Finalmente, establecer unas claras políticas de acceso asegurará que sólo el personal adecuado esté autorizado a entrar al CPD.

### 8.1.1 Puertas

Las puertas deben estar provistas de una cerradura. En un CPD pequeño en el que entran frecuentemente un determinado número de personas, puede concebirse proporcionar a cada empleado autorizado una llave o código para entrar, manteniendo un registro de las entradas al CPD y prohibiendo la distribución de copias de llaves. Este método se basa sin embargo en los empleados para asegurarse de que los mecanismos de entrada al CPD no se comparten con personas no deseadas.

La mayoría de las compañías optan por un sistema automatizado de seguridad, como lectores de tarjetas o sistemas biométricos. Cuando una persona se identifique en el lector mediante su tarjeta, huella dactilar, voz, rasgos faciales o iris, se desbloqueará la puerta siempre que la persona tenga el nivel adecuado de acreditación.

El sistema de seguridad mantendrá almacenadas unas listas de, permitiendo mayor control y flexibilidad que otorgando códigos de acceso a los empleados. Se puede autorizar a visitantes con tarjetas que expiren en un periodo determinado de tiempo, por ejemplo. Puede obtenerse información de los datos de acceso, por ejemplo, de las entradas y salidas en un determinado periodo de tiempo. Esto puede ser útil en caso de ocurrir algún evento indeseado, ayudando a conocer quién se encontraba allí en ese momento.

También deben introducirse mecanismos de seguridad que eviten que alguien se quede atrapado en la sala si ocurre un incendio o cualquier otro tipo de desastre.

### 8.1.2 Jaulas

Aunque la mayoría de los CPDs tienen paredes robustas, en ocasiones una organización puede preferir rodear una zona específica de servidores por una reja. Esto proporciona mayor seguridad física a los servidores y dispositivos de red que rodea. También puede emplearse para crear diferentes zonas de servidores, quizás porque la sala albergue servidores de diferentes clientes.

La mayor ventaja de una jaula es que es una manera muy sencilla de crear una barrera de acceso al entorno de servidores. Impide el acceso a personal no autorizado mientras que permite que la zona enjaulada reciba los efectos del resto de infraestructuras del CPD, como refrigeración y detección y extinción de incendios. Además es más barata y fácil de construir que una pared tradicional.

Sin embargo, debe tenerse cuidado porque una jaula permite a la gente ver y saber que algo de valor existe en su interior.

### 8.1.3 Cierre de *racks*

Otra opción para proporcionar una seguridad física extra a los servidores es el uso de *racks* con cerraduras. Las cabinas o *racks* para servidores, que suelen venir con puertas y paneles laterales, tienen la opción de estar equipados con cerraduras. Estas cerraduras son de diferentes tipos – llave, combinación o sistema lector de tarjetas. Sea cual sea, impide a una persona tener acceso directo a los servidores o equipos de red ubicados en el interior del *rack*.

### 8.1.4 Circuito de video vigilancia

Los lectores de tarjetas registran quién entra y sale del CPD, pero para una estrecha vigilancia de quién entra en el entorno de servidores se recomienda instalar un circuito cerrado de cámaras. Las cámaras pueden ubicarse fuera de las entradas al CPD y, para lograr mayor visibilidad, en puntos clave de la sala. Las cámaras son típicamente monitorizadas por personal de seguridad y pueden limitarse a reproducir las imágenes en directo o grabarlas para su archivo y su posterior visualización.

### 8.1.5 Control de acceso

Tan importante como los controles de seguridad físicos para proteger la sala lo son las reglas y normas que regulan la entrada. Ni siquiera el mejor sistema físico de seguridad puede proteger algo cuando alguien tiene la llave.

Deben establecerse políticas de acceso al CPD que definan quién está autorizado a entrar y bajo qué circunstancias. La mayoría de las políticas de acceso se crean en base a los trabajos que van a realizarse en el CPD. Otras políticas más sofisticadas distinguen entre dos tipos de accesos: a largo plazo y a corto plazo.

### 8.1.6 Buenas prácticas

La mejor protección para un CPD, después de infraestructura de respaldo y de controles de acceso que impidan el paso a personal no autorizado, es un conjunto de normas o estándares de operación que guíen a los usuarios del CPD acerca de cómo desarrollar su trabajo de manera segura en la sala y realizar un correcto uso de la infraestructura.

No se trata de una lista de normas. Primero, algunas normas de comportamiento se han obviado. Se asume que cualquier persona trabajando en el CPD va a mostrar un mínimo de sentido común y respeto a la infraestructura. Segundo, no importa cuántas normas se listen, siempre existirán circunstancias inusuales que no estarán contempladas.

Pese a las reglas, lo más importante es que la persona que entre al CPD sea consciente de de la criticidad de lo que está en la sala y se comporte adecuadamente.

#### *Gestión de cambios*

Un cambio es una alteración en cualquier elemento del CPD que puede afectar al cliente o puede dificultar la habilidad de la compañía para proveer sus servicios. Algunas compañías aplican la gestión de cambios a cualquier actividad que ocurra en el CPD o que pueda afectarlo mientras que otras lo obvian para actividades que no requieren interacción física con dispositivos o infraestructura del CPD y no tienen grandes probabilidades de causar una caída del servicio.

El trabajo de un CPD debe ser seguro y fiable. Se desea que la sala, y el equipamiento que se encuentra en ella, operen sin incidentes. Implementando una gestión de cambios pueden evitarse las sorpresas. Se trata de un método de planificación, coordinación y comunicación acerca de actividades que se desarrollan en torno a las instalaciones vitales de la compañía, aquellas que son imprescindibles para mantener la operación del negocio y el servicio a los clientes.

La idea es que cuando el CPD se encuentra funcionando adecuadamente, se desea limitar aquellos factores que pueden alterar su funcionamiento y controlar los que son necesarios. Cualquier acción que pueda cambiar las condiciones en estas salas debe ser previamente comunicada a las personas a las que puede influir. Esto permite planificar la situación que se aproxima y, en caso de ser necesario, solicitar una re-planificación de la actividad o incluso una cancelación de la misma.

Los cambios deben realizarse, siempre que sea posible, fuera del horario laboral. Esto tiene la ventaja de eliminar los problemas provocados en caso de una parada de servicio. El inconveniente de esto es que probablemente el precio de los trabajadores que vayan a intervenir en el cambio se incremente debido al horario. En caso de tener que realizarse en horario laboral, debe escogerse el momento en que menos impacto pueda tener para los trabajadores.

## 8.2 Monitorización

Cuando hablamos de proteger un CPD no solo nos referimos a realizar *backup* periódicos de los servidores, instalar *firewalls* y antivirus, y mantenerlos actualizados. Existen también amenazas más tangibles como son la generación de puntos calientes en los *racks*, la caída del sistema de climatización, los cambios de humedad o las fugas de agua.

El sistema de monitorización ambiental permite monitorizar en tiempo real las condiciones en los *racks*, salas de servidores y CPD. Las condiciones monitorizadas incluyen temperaturas extremas, humedad, caídas de tensión, fugas de agua, humo,… Con un sistema de monitorización adecuado se estará preparado para detectar a tiempo cualquier efecto adverso que estas condiciones pudieran tener en el CPD. Es posible también que el sistema de monitorización alerte de errores humanos o *hacking*. Pueden combinarse con las soluciones de video vigilancia.

Para notificar las alertas al administrador, la mayoría de los sistemas de monitorización disponen de la posibilidad de enviarlas vía correo electrónico, mensajes SMS o SNMP *traps*.

### *Temperatura*

En los CPDs actuales resulta muy complicado mantener un control de las temperaturas debido a la alta densidad de los *racks*. Como resultado, aparecen puntos calientes en zonas donde no debería. La instalación de sensores de temperatura con conectividad a la red Ethernet en el CPD permite controlar las temperaturas en estos puntos calientes. En caso de que dichas temperaturas sobrepasen un umbral determinado, el sistema genera una alerta que permite al administrador revisar el sistema de climatización o tomar las medidas preventivas necesarias para evitar daños mayores. Se recomienda la instalación de al menos un sensor por *rack*. En el caso de que la instalación sea con cerramiento de pasillo frío o caliente, se recomienda poner el sensor en el pasillo caliente.

### *Humedad*

Un sistema inteligente, cuando detecta un aumento de humedad en uno de sus sensores, comprobará el estado del resto de sensores antes de generar una alarma, monitorizando los niveles de humedad. En caso de que el nivel (alto o bajo) persista o que más de un sensor detecte la anomalía, generará la alerta correspondiente.

### *Fluidos*

Es recomendable instalar sensores de fugas en todos aquellos puntos del CPD por los que circula líquido. Estos puntos están generalmente relacionados con las instalaciones de climatización.

### *Integración con otros sensores*

Es imprescindible que los sensores anteriormente mencionados se integren adecuadamente con los detectores de humo/fuego instalados en el CPD para prevenir incendios, que a pesar de estar vinculados a su central de incendios, pueden integrarse en el sistema de monitorización para proporcionar a los administradores la oportunidad de tomar medidas antes de que se produzca la descarga del sistema de extinción. También pueden integrarse con las PDUs y las SAIs, monitorizando el estado de las baterías y condiciones de alarma.

### *Seguridad física*

Mediante sensores de contacto seco/sensores de movimiento, puede monitorizarse la apertura de puertas de la sala o de los *racks*, alertando a los administradores en caso de producirse un acceso no autorizado o un descuido.

A continuación, en la Ilustración 41[31], se muestra un típico esquema de solución de monitorización. Básicamente está compuesta por un dispositivo central (Hub) conectado a la red Ethernet, al que se conectarán los sistemas de video vigilancia y seguridad, y el resto de sensores inteligentes y de temperatura para su seguimiento. Cuando se detecte una alerta, la central enviará vía email, SMS o SNMP *trap* la información al administrador, que tomará las medidas que estime necesarias.

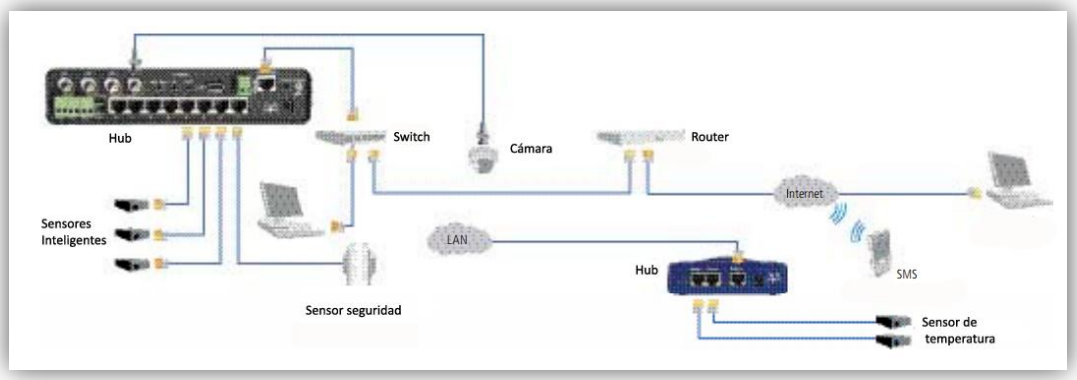



**Ilustración 41: Esquema de monitorización**

### *SNMP traps*

Los SNMP *traps* permiten que un agente notifique a la central de gestión los eventos más significativos y sin necesidad de que la central los solicite. No se trata, por tanto, de un sistema de petición y respuesta de mensajes, tal como muestra la Ilustración 42:

[31] Ilustración extraída de la página web de Blackbox, *www.blackbox.es*.

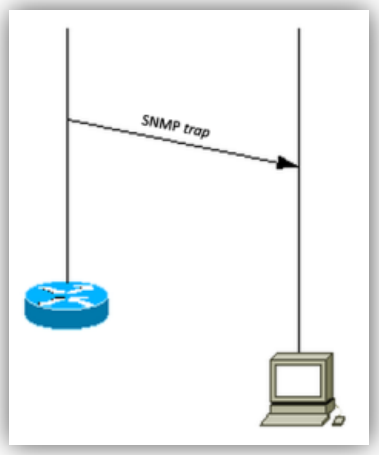



Ilustración 42: SNMP *trap*

SNMPv1 (*Simple Network Management Protocol*) y SNMPv2c junto con la MIB (*Management Information Base*) asociada, permiten la notificación directa mediante *traps*.

La idea es que dado que un gestor es responsable de un número muy alto de dispositivos, y cada dispositivo puede tener también un número elevado de agentes asociados, es impracticable para el gestor pedir información de cada agente. La solución es que cada agente del dispositivo gestionado envíe notificaciones al gestor sin que éste se las pida, mediante *traps* [Cis06].

La MIB es un fichero de texto ASCII que describe a los elementos de una red SNMP como una lista de objetos. Su función es traducir el contenido del *trap* en un mensaje comprensible para el operador, identificando los objetos a partir de su OID[32]. La MIB de un dispositivo es importante porque solo los objetos que aparezcan en la MIB pueden ser monitorizados [DPS12].

[32] OID, *Object Identifier*, es un identificador numérico que asigna SNMP a cada objeto de la MIB.

# Bibliografía de referencias


[3M07] Documento de 3M, *Novec 1230 Fluido de protección contra fuego para aplicaciones de gas y carburante*, 2007.

[Afi12] Información extraída de *Sistemas dióxido de carbono*, de Aficon, Agosto, 2012.

*http://www.aficon.com/catalogo.php?familia=46*

[Aen93] *Grados de protección proporcionados por las envolventes (Código IP)*, de Aenor, 1 de Agosto, 1993.

*http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0001122&tipo=N*

[Aen02] *Grados de protección proporcionados por las envolventes de materiales eléctricos contra los impactos mecánicos externos (código IK)*, de Aenor, 30 de Diciembre, 2002.

*http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0028258&tipo=N*

[Aen10a] *Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación. Parte 1: Clasificación a partir de datos obtenidos en ensayos de reacción al fuego*, de Aenor, 26 de Mayo, 2010.

*http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0045465&tipo=N*

[Agu12] Documento de Aguilera Electrónica, *Sistema algorítmico de detección y control de incendios*, 2012.

[Alg05] *Build the Best Data Center Facility for Your Business*, de Douglas Alger, June 16, 2005.

[APC03] Informe interno de American Power Conversion, *Tecnologías alternativas para generación de energía en centros de datos y salas de gestión de redes*, 2003.

[Ash12] Información extraída de la página web de la ASHRAE, 2012.

*http://www.ashrae.org/about-ashrae/*

[CEM12] *Guía Europea de los sistemas de alimentación ininterrumpida*, del CEMEP, 2012.

[Cis06] *Understanding Simple Network Management Protocol (SNMP) Traps*, de Cisco, 10 de Octubre, 2006.

*http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa5.shtml*

[Cis07] Documento de Cisco, *Cisco Data Center Infrastructure 2.5 Design Guide, Cisco Validated Design I,* 6 de Diciembre, 2007.

[Cis12] Ilustración extraída del documento *Designing the data center infrastructure (Cisco).*

[CTE07] *Documento Básico de Seguridad en Caso de Incendio,* del CTE, 19 de Octubre, 2007.

*http://www.codigotecnico.org/web/recursos/documentos/dbsi/*

[DEM11] Manual de DEMSA, *Manual de gases limpios*, Noviembre 2011.

[DIN11] *Pedestrian doorsets, windows, curtain walling, grilles and shutters. Burglar resistance. Requirements and classification*, de DIN, Septiembre, 2011.

*http://www.nabau.din.de/cmd?artid=116125567&bcrumblevel=1&contextid=nabau&subcommitteeid=54769889&level=tpl-art-detailansicht&committeeid=54738847&languageid=en*

[DPS12] *SNMP Tutorial: an introduction to SNMP*, de DPS Telecom.

*http://www.dpstele.com/layers/l2/snmp_tutorials.php*

[Dur04] Artículo de StorageSearch, *NAS, DAS or SAN? Choosing the rights Storage technology for your organization*, de Duran Alabi, Mayo de 2004.

*http://www.storagesearch.com/xtore-art1.html*

[Eme11a] White Paper de Emerson Network Power, *Understanding the Cost of Data Center Downtime*, 2011.

[Eme11b] Presentación de Emerson Network Power, *Liebert HPM Digital & Soluciones Alta Densidad Xtreme*, 2011.

[Eme11c] Presentación de Emerson Network Power, *Necesidades de refrigeración en un Datacenter*, 2011.

[Eme12] Ilustración extraída de la página web de Emerson Network Power, *www.emersonnetworkpower.com*.

[EN11] UNE-EN 50160:2011: Características de la tensión suministrada por las redes generales de distribución.

[Ent12] White Paper de Enterasys, *Data Center Networking – Connectivity and Topology Design Guide*, 2012.

[Esp12] Información extraída de la página web del fabricante Espacio.

*http://www.espacio.es/Welcome.html*

[Gar07] Nota de prensa sobre Gartner Symposium ITxpo 2007.

*http://www.gartner.com/it/page.jsp?id=503867*

[Ing07] Informe de Ingeniero Ambiental acerca de los gases de extinción¸ *Informe técnico – Selección de gases de extinción*, 2007.

*www.ingenieroambiental.com/?pagina=1649*

[Iru12] Artículo sobre Fibra Óptica OM4, *OM4 – La próxima generación*, de Tony Irujo.

*http://www.conectronica.com/Cables-de-/-para-Fibra-Optica/OM4-La-pr%C3%B3xima-generaci%C3%B3n-de-fibra-multimodo.html*

[Kas09] Artículo sobre la evolución de CPDs. *Data Center Evolution*, de Jim Kaskade. January 24, 2009.

*http://jameskaskade.com/?p=344*

[Kim02] Documento sobre las tecnologías de supresión de incendios, *Overview of recent progress in fire supression technology*, de Kim, A., 2002.

[LAN12] Documento sobre cableado de pleum y cableado riser, *Plenum (CMP) vs. Riser (CMR) cable types for Cat 5 and Cat 6*, de LANShack.

*http://www.lanshack.com/pdf/PlenumVsRiser.pdf*

[Mar12] Presentación de Marioff, *Sistema de Protección contra incendios mediante agua nebulizada*, 2012.

[McC04] White Paper de Schneider Electric, *Comparación de configuraciones de diseño de sistemas SAI*, de Kevin McCarthy, 2004.

[NFP75] Información extraída de la página web de NFPA acerca de la norma NFPA 75, *Norma para la protección de equipos de tecnología de la información*, 2009.

*http://www.nfpa.org/onlinepreview/online_preview_document_esp.asp?id=7509E#*

[NFP750] Información extraída de la página web de NFPA acerca de la norma NFPA 750, *Standard on water mist fire protection systems*, 2010.

*http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=750&cookie_test=1*

[NFP2001] Información extraída de la página web de NFPA acerca de la norma NFPA 2001, *Estándar sobre sistemas de extinción de incendios con agentes limpios*, 2008.

*http://www.nfpa.org/onlinepreview/online_preview_document_esp.asp?id=200108E#*

[NFP90A] Información extraída de la página web de NFPA acerca de la norma NFPA 90A, *Estándar para la instalación de sistemas de aire acondicionado y ventilación*, 2012.

*http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=90A*

[Ntp40] Notas Técnicas de Prevención del Ministerio de Empleo y Seguridad Social, *NTP 40: Detección de incendios*, de José Luis Villanueva Muñoz, 2010.

[Par10] Artículo sobre los *Tiers*, *Qué son los Tiers*, de Diego Parrilla. 11 de Octubre de 2010.

*http://www.nubeblog.com/2010/10/11/que-son-los-tiers-en-un-centro-de-datos-el-ansi-tia-942*

[Paw12] Presentación sobre almacenamiento, *Understanding storage basics – DAS-NAS-SAN,* de Ashwin Pawar, 2012.

*http://www.wiziq.com/tutorial/74910-Understanding-Storage-Basics-DAS-NAS-SAN*

[Piq01] *NTP 588: Grado de protección de las envolventes de los materiales eléctricos*, de Tomás Piqué Ardanuy, 2001.

*http://www.insht.es/InshtWeb/Contenidos/Documentacion/FichasTecnicas/NTP/Ficheros/501a600/ntp_588.pdf*

[Pla12] Información extraída de la página web del fabricante Pladur.

*www.pladur.com*

[Ras03] White Paper de Schneider Electric, *Cálculo de los requisitos totales de refrigeración para centros de datos*, de Neil Rasmussen, 2003.

[Ras06a] White Paper de Schneider Electric, *Vatios y Voltiamperios: confusión en potencia*, de Neil Rasmussen, 2006.

[Ras06b] White Paper de Schneider Electric, *Ventajas de las arquitecturas de refrigeración por filas y por racks para centros de datos*, de Neil Rasmussen, 2006.

[Ras12] White Paper de Schneider Electric, *Evitar costes de sobredimensionamiento en la estructura para Centros de Proceso de Datos (Datacenters)*, de Neil Rasmussen, 2012.

[Rok12] Artículo de HostWisely, *Tower vs. Rack vs. Blade servers – picking the right server review,* de Roko Nastic, 2012.

*http://hostwisely.com/blog/tower-vs-rack-vs-blade-servers-picking-the-right-server/*

[Scc12] Artículo de Search Cloud Computing, SPI model (SaaS, PaaS, IaaS), de Margaret Rouse, Febrero, 2012.

[Sch12] Ilustración extraída de la página web de Schneider Electric, *www.schneider-electric.com*.

[Sey11] White Paper de Schneider Electric, *The Seven Types of Power Problems*, de Joseph Seymour, 2011.

[Tor11] White Paper de Schneider Electric, *Data Center Physical Infrastructure: Optimizing Business Value*, de Wendy Torell, 2011.

[UNE01] Norma UNE-EN 60439-2:2001, *Conjuntos de aparamenta de baja tensión. Parte 2: Requisitos particulares para las canalizaciones prefabricadas*, 29 de Octubre, 2001.

*http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0025628&tipo=N*

[UNE05] Norma UNE-EN 2:1994/A1:2005*, Clases de fuego*, 30 de Noviembre, 2005.

*http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0034982&PDF=Si*

[UNE93] Norma UNE 20324:1993, *Grados de protección proporcionados por las envolventes (Código IP),* 01 de Agosto, 1993.

*http://www.en.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0001122&PDF=Si#.UNtSluQsB1g*

[UNE95] Norma UNE-EN 50102:1996, *Grados de protección proporcionados por las envolventes de materiales eléctricos contra los impactos mecánicos externos (código IK)*, 15 de Julio, 1996.

*http://www.en.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0011374&tipo=N&PDF=Si#.UNtTaOQsB1g*

[VLV+10] *Guía de construir con madera. Capítulo 3. Comportamiento frente al fuego. Documento de aplicación del CTE*, de Luis Vega Catalán, Mariana Llinares Cervera, Carlos Villagrá Fernández, Virginia Gallego Guinea y Beatriz González Rodrigo, 2010

*http://www.infomadera.net/uploads/descargas/archivo_17_Comportamiento%20al%20fuego%20CcM.pdf*

[Xtr12] Documento de Xtralis acerca de los sistemas VESDA, *Detección de humo por aspiración*, 2012.

[Wik11a] Artículo de Wikipedia sobre la temperatura crítica, 16 Agosto, 2011.

[Wik12a] Artículo de Wikipedia sobre la protección contra robo, 20 Julio, 2012.

*http://de.wikipedia.org/wiki/Einbruchschutz*

[Wik12b] Artículo de Wikipedia sobre los gases refrigerantes, 17 Julio, 2012.

*http://es.wikipedia.org/wiki/Refrigerante*

[Wik12c] Artículo de Wikipedia sobre el gas R22, 22 Junio, 2012.

*http://es.wikipedia.org/wiki/R22*

[Wik12d] Artículo de Wikipedia sobre la temperatura de bulbo seco, 18 Abril, 2012.

*http://es.wikipedia.org/wiki/Temperatura_de_bulbo_seco*

[Wik12e] Artículo de Wikipedia sobre el Efecto Tyndall, 25 Septiembre, 2012.

*http://es.wikipedia.org/wiki/Efecto_Tyndall*

[Wik12f] Artículo de Wikipedia sobre Fibre Channel, 2 Octubre, 2012.

*http://en.wikipedia.org/wiki/Fibre_Channel*

[Wik12g] Artículo de Wikipedia sobre MPLS, 15 Diciembre, 2012.

*http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching*

[Wik12h] Artículo de Wikipedia sobre VPN, 27 Diciembre, 2012.

*http://en.wikipedia.org/wiki/Vpn*

[Wik12i] Artículo de Wikipedia sobre VPLS, 28 Agosto, 2012.

*http://en.wikipedia.org/wiki/VPLS*

[Wik12j] Artículo de Wikipedia sobre Etherchannel, 20 Diciembre, 2012.

*http://en.wikipedia.org/wiki/Etherchannel*

[Wol04] White Paper de Schneider Electric, *Principios básicos sobre generadores para tecnologías de la información*, de Robert Wolfang, 2004.