

Medidas de seguridad pasiva

Objetivos

- Conocer los posibles riesgos físicos de los centros de proceso de datos (CPD).
- Profundizar en las diferentes infraestructuras de un CPD.
- Concretar el uso de sistemas de alimentación ininterrumpida (SAI).
- Describir los riesgos del espionaje a través de keyloggers.
- Clasificar los distintos métodos de almacenamiento redundante y distribuidos.
- Explotar métodos de almacenamiento redundantes.
- Ahondar en la gestión centralizada de eventos en sistemas Windows y Linux.
- Dominar la gestión de los centros de datos en la nube.

Contenidos

- 2.1. Protección física de equipos y servidores
- 2.2. Planificación del uso de sistemas de alimentación ininterrumpida
- 2.3. Seguridad ante intentos de espionaje
- 2.4. Seguridad en sistemas de almacenamiento
- 2.5. Seguridad en almacenamiento redundante y distribuido
- 2.6. Consideraciones en el uso de clústeres de servidores
- 2.7. Gestión de eventos en ciberseguridad
- 2.8. Gestión de los centros de datos en la nube

Introducción

La seguridad pasiva pretende minimizar los daños causados por cualquier agente que interactúe con un sistema informático. Estos pueden provenir desde usuarios sin mala intención hasta aquellos que pretenden aprovechar cualquier brecha para cometer un ataque. La mayoría suelen estar relacionados con el empleo incorrecto de los propios usuarios, aspectos aparentemente insignificantes como una incorrecta configuración de algún servicio, algún programa no chequeado o la asignación indebida de privilegios, y pueden acarrear una secuencia de riesgos inimaginables. Los accidentes también deben tenerse en cuenta, ya sean naturales o provocados por las personas. Ante todos estos riesgos, la primera metodología de protección hace referencia al uso del propio hardware y las políticas ante averías y funcionamientos incorrectos y mecanismos de respaldo, tanto de la arquitectura física como de la información almacenada en ella.

En esta unidad se aborda el diseño, planificación e implantación de los sistemas de procesamiento masivo de la información, los centros de cálculo, desde el diseño inicial hasta los cambios de una implantación ya realizada, teniendo en cuenta los espacios físicos, las necesidades actuales y futuras de la organización, las metodologías para el almacenamiento de datos y el despliegue en alta disponibilidad.

Se hará un estudio profundo sobre las cuestiones constructivas, eléctricas, ambientales y de detección de incendios. Se abordarán los sistemas de alimentación ininterrumpida, analizando los tipos, modos de funcionamiento y diferentes arquitecturas. Se analizarán los riesgos de los keyloggers y se profundizará en los sistemas de almacenamiento redundantes (RAID).

Por último, se estudiará la gestión de eventos de ciberseguridad y su importancia.

■ 2.1. Protección física de equipos y servidores

La planificación de la instalación física de una red de ordenadores es de suma importancia, ya no solo para proteger a los equipos que la conforman, sino también para prever futuros rediseños y que estos sean posibles atendiendo a los espacios físicos y sus estructuras. Entre los aspectos más importantes cabe destacar el análisis de los materiales de construcción, los equipos de detección y protección contra incendios, los sistemas de aire acondicionado, los aspectos técnicos de la instalación eléctrica, y los sistemas de control de acceso y formación del personal. Se deben emplear materiales no combustibles o tratados con pinturas, impregnaciones u otros elementos que retarden el fuego e instalar sistemas de detección de humo. Los sistemas de almacenamiento masivos deben estar protegidos y disponer de mecanismos de respaldo en lugares independientes.

El propio lugar debe ser construido y equipado de manera que no presente peligro para el equipo de empleados que trabajan en el mismo, con salidas de emergencia claramente marcadas. El control de acceso a la instalación debe estar centralizado en el mínimo número de entradas posible operadas por control remoto y, si es posible, monitorizadas

con el uso de cámaras en circuito cerrado. Todos estos aspectos son los que conforman la seguridad pasiva de un sistema de información.

Un **centro de procesos de datos** (CPD), proceso de datos o un data center es una sala de grandes dimensiones donde se concentra la mayoría de la tecnología informática de una organización. La mayoría de los dispositivos de red de seguridad, de conexiones entre redes, grandes servidores, sistemas de almacenamiento masivos, dispositivos de alimentación ininterrumpida, etc., se localizan en estas salas. El diseño de un CPD es un pilar importante para la propia organización para implantar efectivos sistemas informáticos. Debe contar con la previsión de su replanificación y rediseños futuros.

En la mayoría de las ocasiones, el centro de proceso de datos ya está construido y preparado, pero se hace necesario un continuo estudio de su viabilidad y futuras intenciones. Todas las consideraciones que se van a estudiar en este apartado son válidas tanto en situaciones en las que el **diseño, planificación e implantación** del CPD se comienza desde cero como en las que se hace necesario replantearse la evolución de estas etapas en cuanto lo hace la propia organización.

Instalación física	Suministro eléctrico	Climatización y control de incendios	Diseño de red	Sistemas de seguridad
<ul style="list-style-type: none"> ■ Obra ■ Ubicación ■ Paredes y suelos ■ Acústica ■ Iluminación 	<ul style="list-style-type: none"> ■ Distribución ■ Protección ■ Sistemas de alimentación ininterrumpida 	<ul style="list-style-type: none"> ■ Aires acondicionados ■ Sensores detectores ■ Sistemas de apagado ■ Gas y agua 	<ul style="list-style-type: none"> ■ Racks ■ Servidores tipo blade ■ Topologías core/acceso 	<ul style="list-style-type: none"> ■ Videovigilancia ■ Control de acceso

Figura 2.1. En el diseño, planificación e implantación de un centro de procesos de datos se debe tener presente dónde se va a implantar, el suministro eléctrico, cómo se distribuye, se protege y se mantiene, las condiciones ambientales óptimas para el personal y para el control de elementos que se calientan, los sistemas de detección de incendios e inundaciones, la ubicación y distribución de los grandes armarios y servidores blade y el cableado estructurado, y los sistemas de videovigilancia y control de acceso.

Las diferentes infraestructuras que componen un buen diseño y planificación de la implantación de un centro de procesos de datos son:

- **Obra:** área y sus espacios asociados, cuartos de electricidad, salas de almacenamiento, desembalaje, suelos, techos, paredes, etcétera.
- **Energía:** suministro eléctrico, sistemas de alimentación ininterrumpida, grupo eléctrico, iluminación, tomas a tierra, paneles eléctricos, conductos y registros.
- **Climatización:** elementos principales para extraer el calor del CPD, como la unidad interior que absorbe el calor, la exterior que lo libera, el compresor y la válvula de sobrepresión.
- **Sistema de protección contra incendios:** sistemas de detección y de extinción.
- **Racks:** elementos donde se ubican los servidores y dispositivos de comunicación.

- **Cableado:** cableado estructurado del CPD, tanto el horizontal como el vertical.
- **Seguridad:** sistemas de identificación, sistemas de videovigilancia y de monitorización.



Figura 2.2. El sistema de monitorización permite controlar parámetros críticos y fundamentales de un CPD. Permite conocer el estado de los equipos, planificar su ubicación y restitución, controlar valores relacionados con la temperatura, humedad y estado de los sensores, así como el estado de los sistemas de alimentación ininterrumpida, y programar tareas de mantenimiento.

■ ■ ■ 2.1.1. Ubicación del centro de proceso de datos

Como ya se ha dicho, los planes de seguridad física se basan en proteger el hardware, por lo que es importante tener en cuenta las limitaciones físicas y los futuros mecanismos de control. El lugar donde se localizará un servidor o un equipo es totalmente dependiente de las premisas anteriores. Es decir, atendiendo al lugar donde se encuentren estos equipos que hay que asegurar, los procedimientos de medidas para proteger los recursos y la información serán diferentes. Si la organización se encuentra en etapas de planificación debido a que no se dispone de la decisión final de su ubicación, se puede diseñar una protección física adecuada estudiando su posible lugar final.

Cuando se desea implantar una nueva sala de equipos informáticos, se debe estudiar la ubicación en función de la disponibilidad física y la facilidad para modificar estos aspectos con el fin de hacerla más segura. El primer elemento que se debe tener en cuenta es el espacio del que se dispone y sus accesos, ya que a lo largo de la explotación del sistema será necesario introducir y extraer equipamientos nuevos y antiguos. Por lo tanto, es muy importante hacer un análisis sobre estos accesos.

También es necesario estudiar los accesos para los operarios. El número de estos accesos condiciona los protocolos de seguridad, y se recomienda centralizarlos lo máximo posible, de tal forma que los caros equipamientos de control de personal queden centralizados tanto como se pueda. También es preciso estudiar las salidas de emergencias. En general, se recomienda una zona diáfana con buena localización que esté alejada de zonas de riesgos como sismicidad, inundaciones e incendios, y que esté en planta mejor que en altura, por cuestiones tales como luminosidad y evacuación. Otros factores inherentes son los servicios de energía eléctrica, antenas, líneas telefónicas, tranquilidad del entorno y niveles de vandalismo, sabotaje y terrorismo.



Figura 2.3. El diseño de un centro de procesos de datos debe contemplar los espacios para la entrada y salida de los equipos. Estos suelen ser de grandes dimensiones y de gran peso, por lo que se hace necesario habilitar accesos eficientes al personal de trabajo y a las propias máquinas.

Los equipos que dependen de otros que pueden ser ruidosos, por ejemplo, los sistemas de aire acondicionado, deben ser situados donde el ruido y la vibración puedan ser amortiguados en la medida de lo posible. De la misma manera, se debe elegir una localización con el menor nivel de interferencia electromagnética posible. Los motores son equipos que producen un nivel de interferencia electromagnética muy alto, por lo que se hace necesario evitar su cercanía a los equipos servidores. También deben evitarse las áreas con fuentes de interferencia de radiofrecuencia, tales como transmisores de radio y estaciones de televisión.

En cuanto a las grandes salas de computación o centro de proceso de datos, se intentarán evitar los espacios cercanos a las paredes exteriores del edificio, así como en planta baja o sótanos no provistos de sistemas contra inundaciones debidas a cañerías y otros elementos, como sumideros o depósitos de agua. También se deben rehusar las plantas más altas del edificio, así como aquellas cercanas a los garajes de vehículos de motor. Por tanto, la ubicación más conveniente es en las plantas intermedias del edificio. Sin embargo, se debe ser consciente de lo pesados que suelen ser los equipos que componen estos inmensos sistemas de información y si estas plantas idóneas pueden soportar dicho peso. Otra elección, atendiendo a esta cuestión, es el sótano del edificio, que soporta así mejor esas grandes cargas. Por ello, se hace necesario acondicionar dicho espacio desarrollando un buen plan de seguridad física del sistema.

■ ■ ■ 2.1.2. Condiciones de construcción para el centro de proceso de datos

Se debe estudiar el lugar del edificio más idóneo y seguro para ubicar el centro de proceso de datos, pero se deben tener en cuenta diferentes cuestiones determinantes para su éxito, como:

- Facilidades para la planificación del uso de energía eléctrica, **enchufes**, cableado usado (grosor), tomas a tierra, etcétera.
- Estudio de las **acometidas telefónicas** y comunicaciones, situación de las rosetas, de los puntos de acceso, de los dispositivos de conmutación y enrutamiento, cableado horizontal y vertical, armarios de los que se disponen, etc., ya que, atendiendo al número y ubicación de estos, la red de cableado puede cambiar y hacerse más o menos óptima.



Figura 2.4. Una de las fases más comprometidas, y que debe ser bien planificada, es la del diseño y planificación del uso de la energía eléctrica. Una incorrecta planificación provocaría que el resto de fases no se pudieran llevar a cabo de forma adecuada, según el plan de implantación.

- Análisis sobre la necesidad de la **climatización**, haciendo hincapié en los lugares donde se distribuirán tanto los conductos eléctricos como otros asociados a los dispositivos de aire acondicionado, potencias necesarias, aislamiento de los motores, extracción del aire caliente, etcétera.
- Adecuación de los servicios públicos y **salida de emergencia**. Hay que estudiar la distribución de los mismos, con buenos accesos y con la salida de emergencia más eficiente. Es imprescindible poseer un buen plan de riesgos laborales y de **autoprotección**.
- Estudio de la estructura, que debe ser lo suficientemente fuerte como para poder soportar el inmenso peso de los equipos que inmediatamente se prevé que se instalarán.

larán, y de los que en un futuro se pueden necesitar. Aquellos elementos, como los sistemas de alimentación ininterrumpida, que aportan un ingente peso al sistema, deben ubicarse en planta baja o será necesario reforzar las estructuras en caso de colocarlos en plantas medias.

- Previsión de los **elementos voluminosos** que será necesario introducir en las salas de grandes sistemas, ya que el acceso debe ser lo suficientemente diáfano y grande para permitir su entrada y salida. Estos objetos pueden ser grandes armarios o racks, sistemas de refrigeración, sistemas de extinción por gas, sistemas de alimentación ininterrumpida, etcétera.

A continuación, se detallan aspectos importantes que tener en cuenta en la etapa de diseño:

- **Vías de acceso:** es preciso preverlas y prestar especial atención a los pasillos, ventanas, pilares, puertas, etcétera.
- **Suelos:** para los suelos, la mejor opción es suelos flotantes, ya que permiten ubicar debajo cualquier tipo de conductos eléctricos, de aires acondicionados, cableado de datos, detección y extinción de gases, etc., pero lo suficientemente fuertes como para soportar toda la estructura. La pavimentación será antiestática, para evitar polvo. También es necesario estudiar la posibilidad de usar un falso techo para este objetivo. Se suele emplear especialmente para los sistemas de detección y extinción de incendios.
- **Espacios:** se estudiará el espacio que ocupan los equipos que se desean instalar, así como el necesario para la explotación y mantenimiento de los mismos. También es forzoso prever espacios necesarios para futuras ampliaciones o cambios.
- **Divisiones:** se diseñarán las divisiones del espacio a través de paramentos especiales que eviten el polvo y la propagación del fuego con el uso de pinturas destinadas para ello, y las canalizaciones que las atraviesan.

■ ■ ■ 2.1.3. Consideraciones ambientales, eléctricas y de detección de incendios

Se hace necesario un control sobre los intervalos de **temperatura** y **humedad** de las salas de equipos informáticos con el fin de reducir las posibilidades de fallos en los componentes y para proveer, en la medida de lo posible, el mayor confort a los operarios de las salas. Por ello, se recomienda una planificación adecuada sobre la temperatura y humedad relativa ambiente, ya que estas pueden causar fallos en los componentes hardware y, como consecuencia, períodos de inactividad del sistema.

El intervalo de temperatura óptimo para garantizar fiabilidad es de 21-23 °C, que garantiza niveles seguros de humedad relativa. El nivel de humedad relativa ambiente más adecuado es aquel que oscila entre 40-50 %. Huelga decir que la mayoría de los equipos pueden funcionar fuera de estos intervalos, sin embargo, se recomienda conseguir niveles cercanos a los óptimos, ya que ayuda a proteger de la corrosión por humedad alta, a controlar las descargas estáticas cuando la humedad relativa es demasiado baja, etcétera.



Figura 2.5. El sistema de refrigeración conlleva sistemas altamente pesados (air cooled water chillers) que deben colocarse en lugares que soporten su inmenso peso. Las cubiertas de los edificios son el lugar preferido para situar estos sistemas.

Actividad propuesta 2.1

Sistemas de refrigeración comerciales

Escribe una lista de los sistemas de refrigeración más usados para los centros de proceso de datos, buscando las especificaciones y precios de cada uno de ellos.

■ ■ ■ Aspectos eléctricos

La energía suministrada por los proveedores eléctricos suele tener fluctuaciones que pueden producir otras perturbaciones que, a su vez, pueden provocar daños a los componentes físicos de un CPD.

A todos los equipos les debe llegar un suministro de energía continuo, sin alteraciones ni interrupciones. Para ello, muchas cargas requieren suministro protegido contra estas perturbaciones. Los centros de proceso de datos deben estar preparados para dichas interrupciones prolongadas. Para ello, se instalan sistemas de alimentación ininterrumpida.

Nota técnica

Se hace referencia al concepto *cargas* como el conjunto de todos los equipos conectados a la red eléctrica.



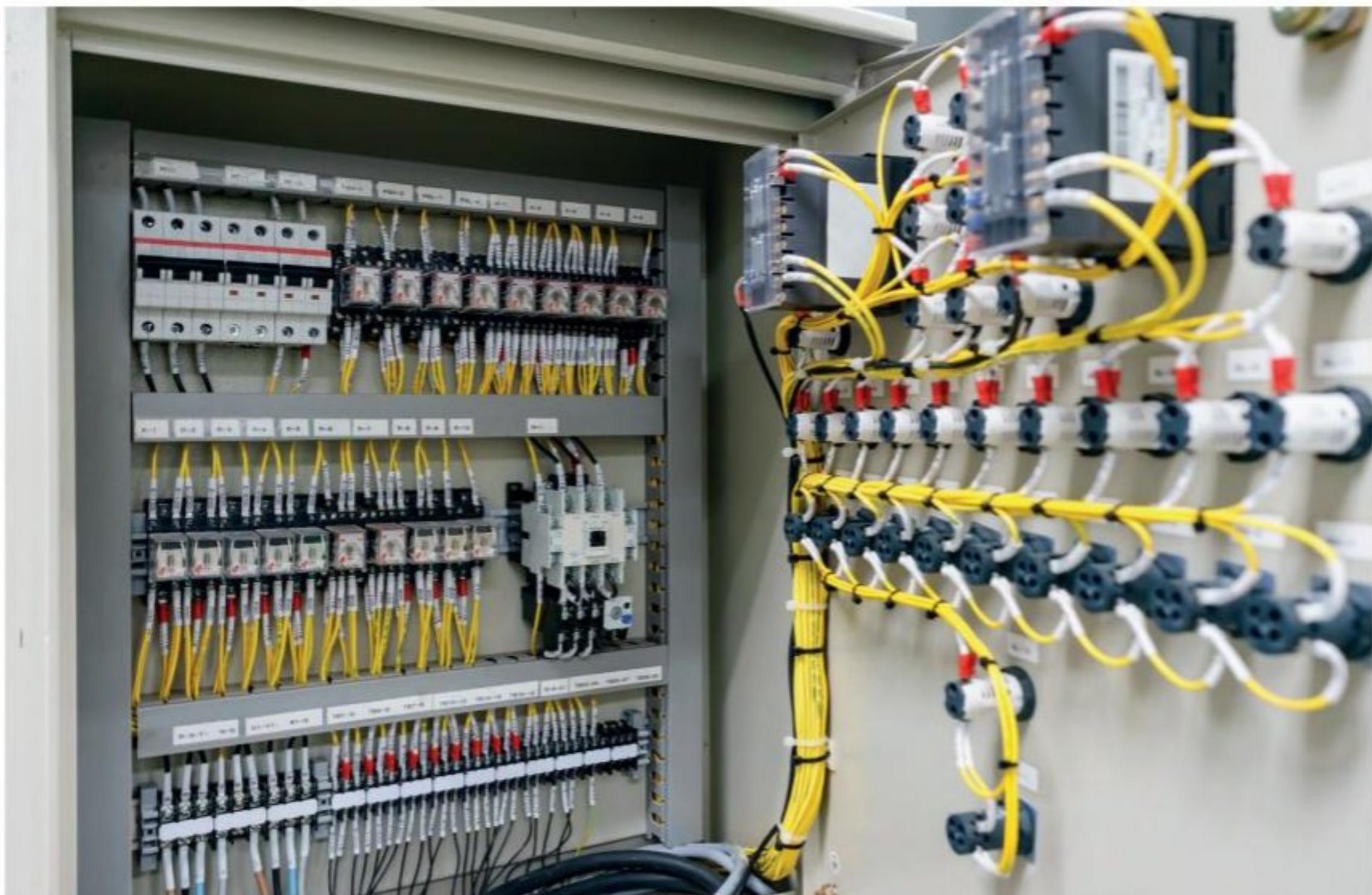


Figura 2.6. Los cuadros eléctricos deben estar dotados de unidades que organicen la distribución del cableado. Existen cuadros mixtos que permiten incluir, además de los canales de distribución eléctrica, los propios para datos en sistemas inmóticos y domóticos.

A continuación, se detallan las consideraciones que tener en relación a los aspectos eléctricos.

- **Apagado de emergencia:** desde un único equipo se apaga una sala de equipamiento eléctrico cuando ocurre una emergencia para proteger las instalaciones y al personal. Este debe estar en un lugar adecuado, identificado y conocido por todos los operarios que trabajan en la sala de grandes equipos informáticos.
- **Cableado:** si es posible desplegar el cableado internamente en paredes o techos, se usarán corrugados diferentes para los cables eléctricos y para el cableado de datos, para evitar interferencias electromagnéticas.
- **Conductos eléctricos:** los circuitos eléctricos deben estar aislados y ubicados en un lugar idóneo, preferiblemente, en el falso suelo. En caso de usar el falso techo, se deben tener en cuenta los conductos de agua para el sistema contra incendios.
- **Diferenciales:** se deben añadir a la instalación eléctrica elementos importantes, como diferenciales para evitar derivaciones, interruptores magnetotérmicos, etcétera.
- **Regletas de distribución eléctrica, PDU:** las unidades de distribución de la alimentación son regletas que proporcionan electricidad a los equipos de un rack. Debe hacerse una distribución correcta de estas regletas.
- **Toma de tierra:** es importante que el sistema eléctrico cuente con una buena toma de tierra. En caso de no disponer de ellas, o de disponer de algunas no válidas, es necesario construir pozos especiales para las tomas de tierra.

- **Transitorios:** los picos de intensidad de corriente pueden ser fatales. Se hace obligatorio protegerse contra ellos. Pueden derivarse de sistemas conectados a la misma instalación. Ejemplos son bombas eléctricas, ascensores, rayos, subestaciones eléctricas, grandes industrias cercanas, etc. Es conveniente incluir elementos de protección en los cuadros de distribución y a tierra.
- **Variaciones de voltaje:** caídas y sobretensiones por insuficiente regulación de la línea eléctrica. Para evitarlos, se usan estabilizadores de voltaje.

Actividad propuesta 2.2

Sistemas de regletas de distribución eléctrica

¿Cuáles son las características de las regletas de distribución eléctrica? ¿Qué especificaciones y precios tienen? ¿Dónde se ubican?

Detección de incendios

La acción de un fuego no suele comenzar en el interior del CPD, sino que más bien son el fuego, el humo y los gases los que producen el daño real. Todos los materiales usados en la construcción de la sala deben ser incombustibles. Las paredes deben ofrecer resistencia al fuego y funcionar como barrera frente al humo, protegiéndolo con placas de yeso y paneles.

El daño que provoca el agua es importante, así, todas las entradas del suelo, de la pared y del techo deben estar selladas.



Figura 2.7. La inmótica utilizada por los sistemas de control de incendios, inundaciones y sistemas de videovigilancia permite el control y supervisión de los sensores y cámaras, y su monitorización desde cualquier lugar del mundo, para la cual solo hay que disponer de conexión a internet.

Es necesario sellar los pasos de cables a través de las paredes, suelos o techos. Para ello, se pueden usar **pasamuros** que protegen contra perturbaciones electromagnéticas, incendios, humedad, lluvia, polvo, etcétera.

El sistema de detección de incendios permite localizarlo activando las **alarmas** correspondientes. El CPD puede contar con una central de incendios que actúe de forma programada automáticamente. Los elementos principales de los detectores de incendios son la central de señalización, los detectores, las líneas, los pulsadores manuales y los sistemas auxiliares, como alarma, teléfono, activación de los sistemas de extinción, etcétera.

La extinción puede hacerse mediante gas o mediante agua nebulizada. La extinción por gas tiene muchas ventajas: no conduce la electricidad, no deja residuos, actúa más rápidamente en el foco del incendio, provoca menos daños que el agua, presenta un menor tiempo de reinicio de la actividad, etcétera.

Sin embargo, es importante estudiar la **estanqueidad** del lugar y el sistema de **refrigeración**, ya que estos aspectos pueden provocar que el sistema de extinción no se active porque falle la propia detección, o que se active, pero no se extinga.

Actividad propuesta 2.3

Extintores en un CPD

¿Dónde se deben ubicar los extintores? ¿Tienen fecha de caducidad? Si es así, ¿qué se debe hacer cuando se alcanza esa fecha?

2.1.4. Diseño de red y recuperación ante desastres

En un CPD aparecen nuevos elementos con respecto a una pequeña red local. Los armarios o racks son de mayor tamaño, se usará cableado estructurado tanto horizontal como vertical, los servidores pueden ser apilables y empotrables, y el esquema de organización de los switches y routers debe seguir organigramas basados en topologías Núcleo/Acceso.

Los **racks** son estructuras modulares en las que se pueden instalar diferentes equipos tecnológicos, protegiéndolos y aportándoles refrigeración y seguridad. Además, ayudan a la distribución del cableado con el uso de paneles de parcheo y otros elementos de conexión.

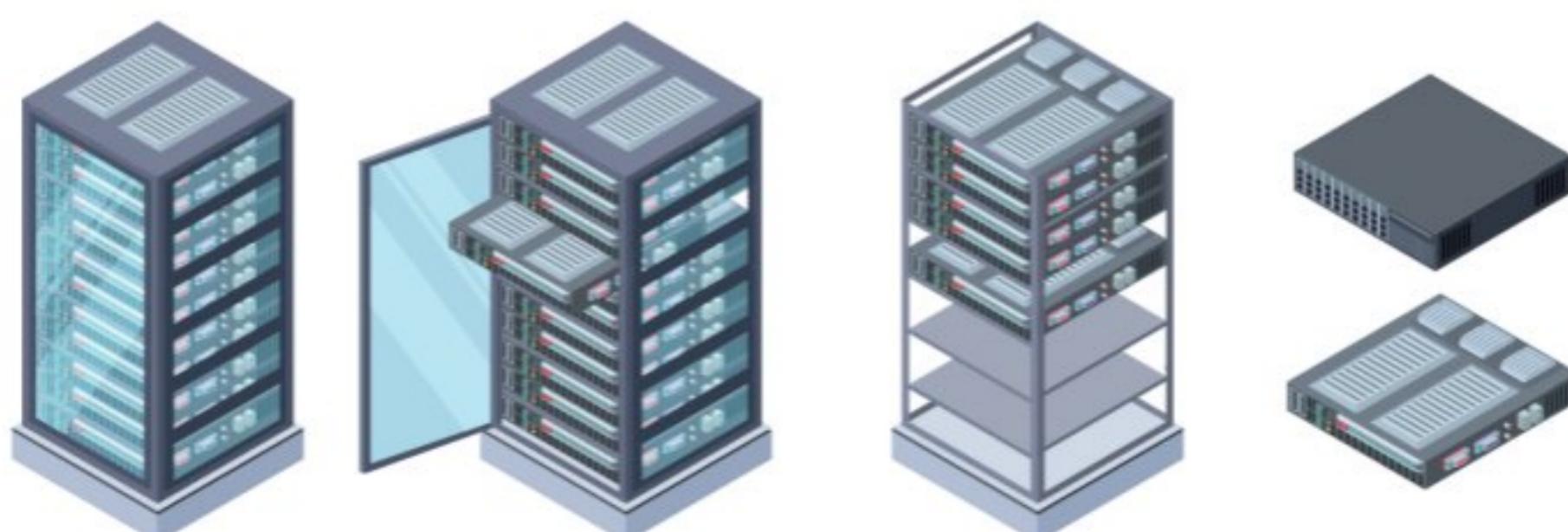


Figura 2.8. Los armarios rack protegen dispositivos de red y servidores rack. Algunos pueden proveer de sistemas de seguridad física.

La simple sustitución de un router por otro provocaría la posibilidad de una intrusión completa al sistema o la manipulación de los equipos de grabación de los sistemas de **videovigilancia**, lo que supondría la alteración de las pruebas de algún robo o acción malintencionada. Para proporcionar seguridad física a los servidores, dispositivos de red como routers y cortafuegos, y dispositivos de videovigilancia, los racks pueden estar compuestos por puertas y paneles que permiten la inclusión de cerraduras. Estas pueden ser llaves o mecanismos más avanzados, como lectores de tarjetas o sistemas biométricos.

El **sistema de cableado** permite la comunicación de los diferentes equipos y la comunicación externa. Este debe estar bien diseñado. Hay que elegir los medios de cableado que se adapten a las necesidades de transmisión del CPD, estudiar el número de conexiones, organizar el cableado de forma que aporte escalabilidad al CPD, etcétera.

Los servidores, además del típico servidor tipo torre, pueden ser rack o blade. El **servidor tipo rack** está diseñado para ser empotrado en armarios racks, ahorrando espacio y dotando de escalabilidad a la implantación. Su mayor problema es la refrigeración. Los **servidores tipo blade** son servidores modulares diseñados para minimizar el espacio usado. Estos se instalan en armarios metálicos denominados *blade* que son capaces de empotrar varios servidores en una misma columna, aportándoles, aunque son más costosos, un sistema adecuado de ventilación y alimentación.



Figura 2.9. Los armarios *blade* permiten instalar servidores apilados que minimizan el espacio físico ocupado.

Actividad propuesta 2.4

Los armarios rack y los servidores tipo rack y blade

Investiga sobre los tipos de rack que existen en el mercado, así como las especificaciones comerciales y sus precios. Haz lo mismo con los servidores tipo rack y tipo blade.

La red de datos de un CPD se puede dividir en dos niveles principalmente: nivel núcleo y nivel de acceso.

- **Nivel núcleo:** compuesto por dos subniveles, denominados Core y Agregación. Proporciona conmutación de paquetes a altas velocidades y balanceo de carga. Además, proporciona gestiones para las redes locales virtuales (VLAN y spanning tree).
- **Nivel de acceso:** a él se conectan físicamente los servidores para acceder a la red, usando topología tipo ToR.

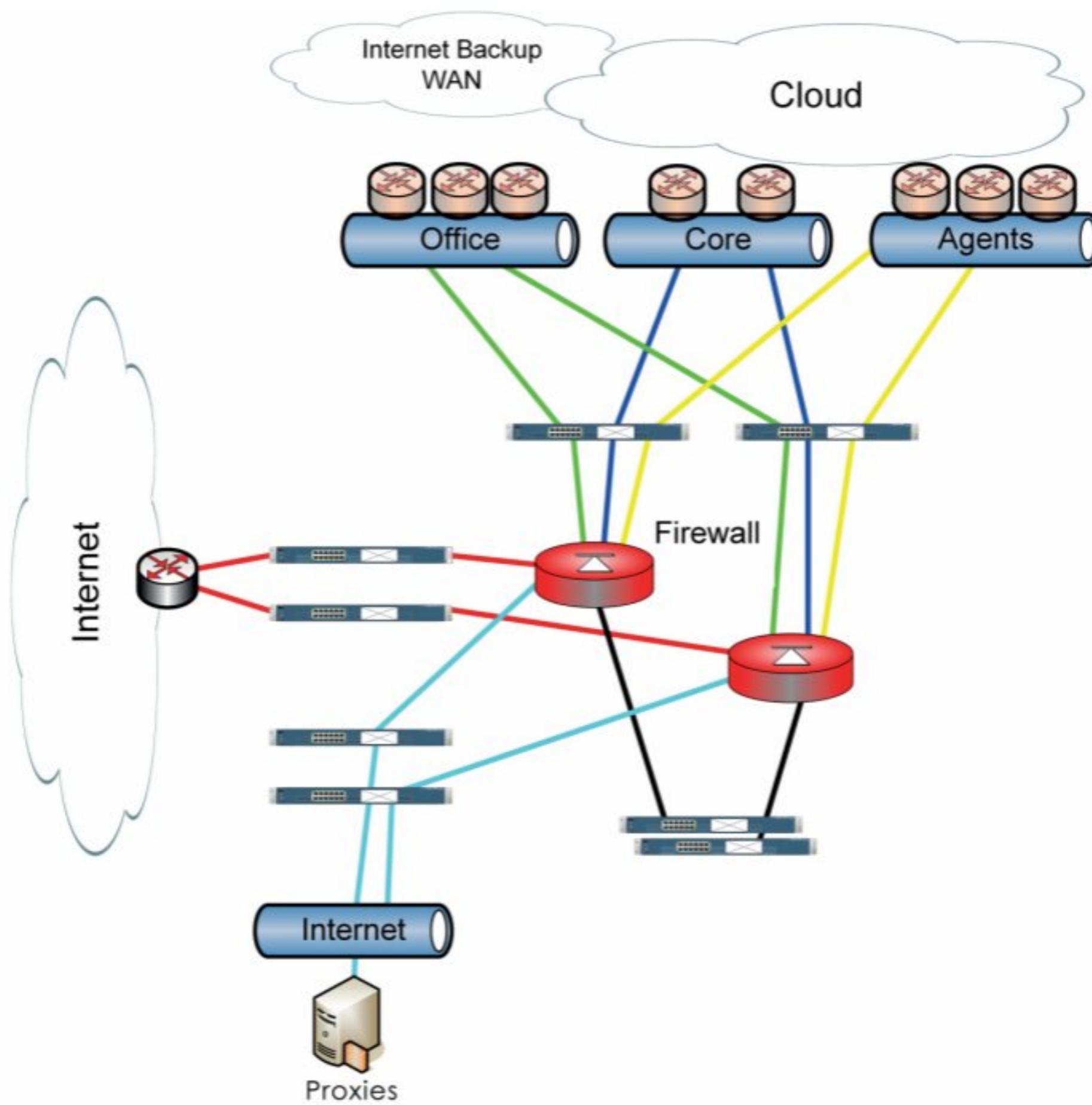


Figura 2.10. Ejemplo de una arquitectura con alta disponibilidad. El segmento Core corresponde al núcleo del sistema. Los segmentos office y agents son los elementos correspondientes al nivel de acceso. Las conexiones se duplican a través de múltiples routers y cortafuegos.

Nota técnica



Topologías tipo ToR (top of rack) son aquellas que usan un switch ToR, que permite las conexiones desde este a los servidores y que se coloca en la vía más alta del rack. Este tipo de arquitectura se despliega rápidamente.

Los commutadores que unen los servidores del nivel de acceso se conectan a los de nivel de núcleo, proporcionando funcionalidades de conmutación y encaminamiento.

Evidentemente, a pesar de tener establecido el mejor de los protocolos para evitar daños en el centro de proceso de datos, existirá la posibilidad de que este fracase y sea necesario ponerse en marcha en **caso de desastre**. Lo primero es tener un protocolo de recuperación de datos independiente y mecanismos de acceso a los mismos con un sistema auxiliar en caso de caída o avería de los equipos que componen la sala de máquinas. Se recomienda el uso de sistemas redundantes, de balanceo de carga y de alta disponibilidad.

El plan de contingencia comenzará con la recuperación de las bases de datos y ficheros esenciales, y el desvío de las comunicaciones a un centro alternativo, priorizando los procesos más importantes. Una solución a este tipo de situaciones son los **CPD de respaldo**, un segundo CPD que trabaja de forma auxiliar cuando otro CPD cae.

Actividad propuesta 2.5

Diseño de un centro de proceso de datos

Imagina un centro con varias salas con equipamiento informático y dispositivos de conexión y otros elementos de red necesarios (por ejemplo, varias aulas de un centro de formación).

Diseña y planifica la distribución de todos estos elementos de la red, estudiando la mejor ubicación de los diferentes equipos terminales, servidores, conmutadores, puntos de acceso, cableado estructurado, sistemas de almacenamiento masivo locales y remotos, aires acondicionados, salidas de emergencia, detección de incendios, sistemas de apagado de incendios por agua y por gas, distribución eléctrica, acometidas eléctricas y la sala para equipos pesados como grandes servidores, sistemas de alimentación ininterrumpida, sistemas de almacenamiento masivo, etcétera.

■ 2.2. Planificación del uso de sistemas de alimentación ininterrumpida

Un sistema de alimentación ininterrumpida (SAI) es un dispositivo de suministro eléctrico compuesto por baterías que proporciona energía a un equipo en caso de interrupción eléctrica. Otra función importante de los SAI es depurar la electricidad suministrada por la compañía eléctrica y mejorar su calidad.

Algunas características importantes de un SAI son el tiempo de autonomía y la especificación de la batería que lo compone. El tiempo de autonomía se refiere al tiempo en que el SAI puede seguir alimentando la carga tras un corte del suministro eléctrico. En cuanto a las baterías, se indica la potencia de la carga y el factor de potencia. Suelen instalarse en el mismo armario que los SAI.



Figura 2.11. Los sistemas SAI son muy pesados, ya que están compuestos por robustas baterías, por lo que su ubicación es determinante. Cuanto mayor es su tamaño, mayor autonomía ofrecen.

■ ■ ■ 2.2.1. Los sistemas de alimentación ininterrumpida

Se puede definir un *sistema de alimentación ininterrumpida* como un dispositivo que es capaz de asegurar y mantener la alimentación eléctrica de forma ininterrumpida y durante un tiempo delimitado cuando se produce una pérdida de alimentación. Están compuestos por elementos que almacenan energía que entran en funcionamiento cuando se produce una falta de suministro en la red eléctrica. Además de asegurar la alimentación eléctrica, la mayoría mejoran la calidad de la tensión y de la corriente eléctrica.

Los problemas y causas de las variaciones del suministro eléctrico pueden ser causados por diferentes factores, entre los que cabe destacar:

- Errores humanos, cortes e interrupciones de conexión, sabotajes y cortocircuitos.
- Inundaciones y tormentas, vientos fuertes y terremotos.
- Interferencia generada por elementos como ascensores, grúas, equipos de soldadura y máquinas con motores.

La alimentación eléctrica que llega a los edificios no siempre es perfecta. Por causas muy diversas, puede llegar a los equipos informáticos transformada o defectuosa. Estas imperfecciones de la alimentación eléctrica pueden provocar daños en el hardware, pérdida de datos, corrupción de ficheros y otros efectos no deseados en sistemas de información. Algunas de estas anomalías son las siguientes:

- **Corte de energía eléctrica:** también llamado apagón, supone una interrupción del suministro eléctrico.
- **Distorsión:** la onda eléctrica no es la que se quería transmitir. Generalmente, son los propios dispositivos de la red los que pueden ir transformando la señal, desvirtuando la original, como motores, dispositivos de línea telefónica e, incluso, algunos SAI.
- **Microcortes:** son bajadas de tensión durante un tránscurso corto de tiempo. Se deben al arranque de equipos de gran potencia.
- **Micropicos:** iguales que los microcortes, pero de duración muy corta. Pueden provocar pequeños defectos.
- **Ruido eléctrico:** se manifiesta en interferencias sobre la señal portadora. Se producen a causa de dispositivos como impresoras, máquinas de soldar, o fenómenos naturales como un rayo.
- **Sobretensiones:** subidas de tensión durante un transcurso corto de tiempo. La mayoría se deben a desconexiones de equipos de grandes potencias.
- **Sobretensiones prolongadas:** alto voltaje durante un tiempo prolongado. Como ejemplo, pueden servir las caídas de rayos en las líneas eléctricas.
- **Subtensiones prolongadas:** bajo voltaje sostenido en una línea eléctrica durante un tiempo prolongado. Suelen ser provocados por arranques de motores o de cargas muy inductivas.
- **Variación de la frecuencia:** la onda eléctrica tiene una frecuencia que generalmente es constante. A veces, esta frecuencia puede variar, lo que provoca daños electrónicos, malos funcionamientos, pérdidas de datos o caídas del sistema informático.

Los SAI están compuestos por diferentes partes. Cada una de ellas presenta funciones determinadas. Estos elementos son la batería, el bloque bypass estático, el bloque bypass manual, el bloque ondulador, el bloque rectificador, el filtro, el panel de control, el pulsador de emergencia y el software de control y comunicación. En la Figura 2.12, se detalla brevemente cada uno de ellos.

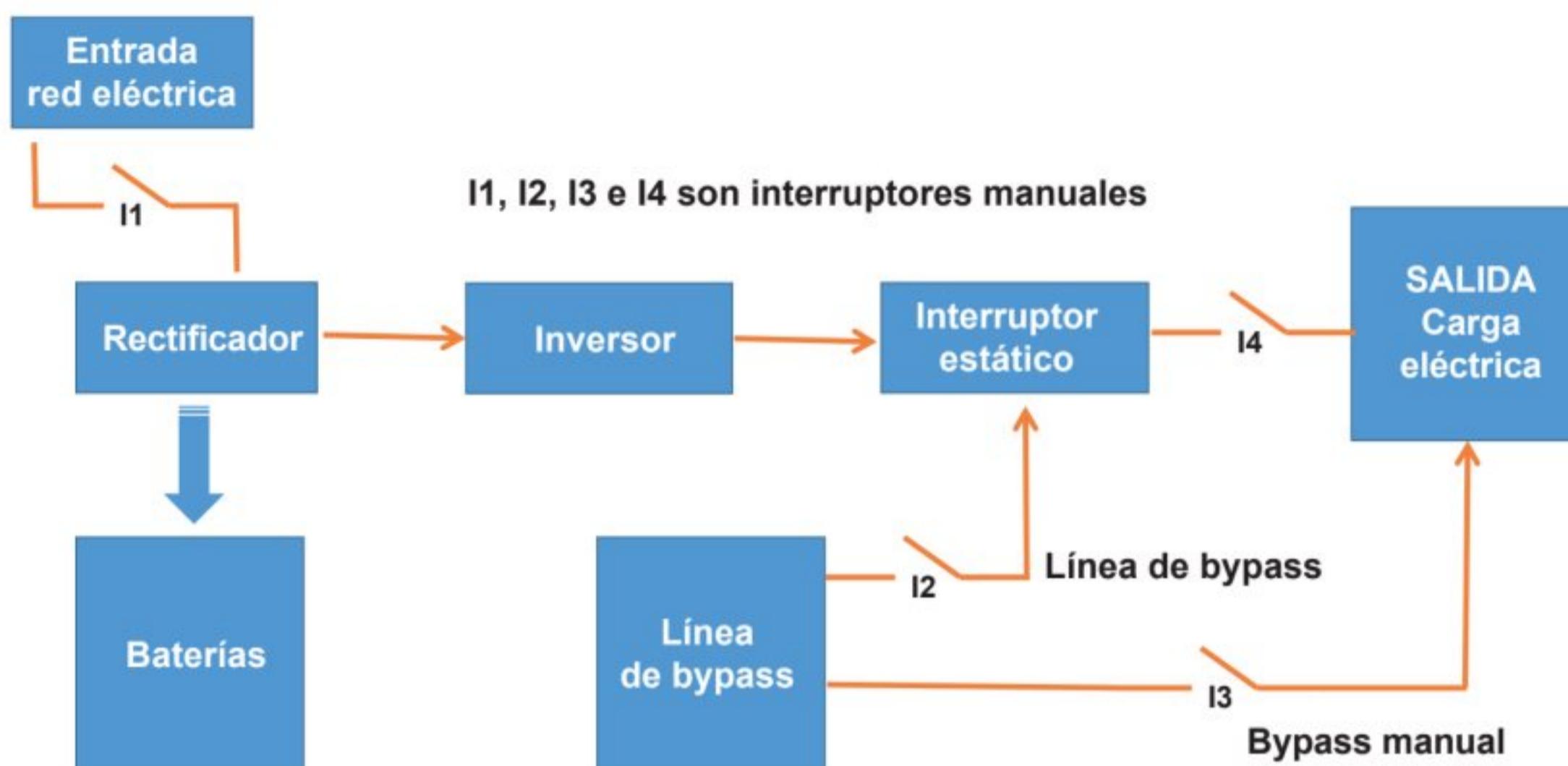


Figura 2.12. Las diferentes partes de un SAI son el rectificador, el inversor, el interruptor estático, la línea de bypass y las baterías.

- **Batería:** a través de condensadores, almacenan la energía eléctrica, y aportan dicha energía a la carga cuando existe algún problema en la línea de entrada de energía eléctrica al SAI. Cuanto mayor sea la batería, mayor será la potencia requerida y el tiempo de autonomía que ofrece el SAI.
- **Bloque bypass estático:** se usa para conmutar entre la energía eléctrica que ofrece el SAI y la que ofrece la red eléctrica.
- **Bloque bypass manual:** es un interruptor que permite el cerrado temporal de la conexión a los bornes del SAI, generalmente usado para tareas de mantenimiento.
- **Bloque ondulador:** realiza las conversiones entre corriente continua y alterna para los diferentes bloques del SAI.
- **Bloque rectificador:** mide y controla la corriente de entrada, la suaviza antes de ofrecer la corriente de salida, elimina armónicos de frecuencia y transforma la corriente alterna a corriente continua.
- **Filtro:** elimina perturbaciones provenientes de la red eléctrica, con el fin de proteger al equipo, evitando la propagación de dicha perturbación a la línea de salida hacia las máquinas.
- **Panel de control:** son paneles informativos sobre el estado del SAI.
- **Pulsador de emergencia:** es el pulsador externo de emergencia de salida que se conecta a los bornes del SAI y permite su desconexión total.
- **Software de control y comunicación:** diferentes programas que permiten la comunicación a través de un controlador común.

■ ■ 2.2.2. Tipos de sistemas de alimentación ininterrumpida

Los dispositivos de alimentación ininterrumpida se pueden clasificar según la corriente de carga y según el modo de funcionamiento:

1. En función de la corriente de carga: existen los sistemas de alimentación ininterrumpida de corriente continua y de corriente alterna.

- SAI de corriente continua: mantiene la tensión en la carga en corriente continua mediante un rectificador. Ante un fallo de red, se usa la batería conectada a la salida del rectificador.
- SAI de corriente alterna: mantiene la tensión en la carga en corriente alterna.

2. En función del modo de trabajo: se pueden encontrar sistemas de alimentación estáticos, mecánicos y mixtos.

- a) SAI estático: está compuesto por un rectificador, una batería y un inversor. La línea alimenta al rectificador, y este, a la batería. En caso de avería de la línea, no llega energía al rectificador, por lo que la batería se debe encargar de alimentar la carga a través del inversor.
- b) SAI mecánico o rotativo: existen dos tipos, unos con motores de combustión interna, y otros, con motores de corriente continua.
- c) SAI híbrido o mixto: mezcla elementos estáticos y elementos mecánicos. Existen principalmente dos tipos, los que disponen de un motor de corriente continua y un alternador, y los que disponen de un motor de corriente alterna y un alternador.

■ ■ 2.2.3. Modos de funcionamiento

Dependiendo del modo de funcionamiento, existen los siguientes tipos de sistemas de alimentación ininterrumpida: SAI en línea (*on-line*), SAI fuera de línea (*off-line*) y SAI interactivo o paralelo (*line-interactive*). A continuación, se detallan las características principales de cada uno:

1. SAI en línea: cuenta con cuatro elementos principalmente, que son un rectificador (conversor de corriente alterna a corriente continua), una batería, un inversor (conversor de corriente continua a alterna) y una carga.

La línea alimenta al rectificador, que surte, a su vez, a la batería y al inversor, que alimenta a la carga. En el instante que se produce algún defecto, el SAI se desconecta de la línea de alimentación, y entra a trabajar la batería a través del inversor.

2. SAI fuera de línea: está formado por seis elementos: un rectificador, una batería, un bypass estático, un inversor, un interruptor y una carga. El interruptor es un dispositivo estático o electromagnético que conmuta entre un modo de trabajo y otro. El rectificador también se conoce como *cargador*.

Si se produce algún fallo de alimentación, el interruptor comuta y la carga pasa a alimentarse por la batería a través del inversor, desconectándose el rectificador. En este tipo de SAI, al estar la carga conectada directamente a la red, cualquier defecto en la tensión de alimentación es transmitida directamente a la carga.

3. SAI interactivo: está compuesto por un interruptor de transferencia, un conversor reversible, una batería y una carga. La función del conversor es pasar la corriente alterna a continua, y viceversa.

Normalmente, el interruptor se encuentra cerrado y la carga se alimenta directamente de la red eléctrica. Si se produce un corte de suministro, el interruptor se abre, el conversor pasa a funcionar como un inversor y la batería comienza a alimentar la carga.

■ ■ ■ 2.2.4. Arquitectura entre SAI y comunicación entre ellos

Existen cuatro formas de configurar los sistemas SAI y sus cargas: distribuida, centralizada, modular y modular granular.

1. Distribuida: cada carga se conecta a su propio SAI, de tal forma que estos no se comparten, y se emplea cuando se pretende proteger un sistema no importante y la distribución de las cargas dificulta implementar esquemas más complejos y costosos.

2. Centralizada: se centraliza un SAI que se ocupa de controlar y vigilar varias cargas simultáneamente. Se usa para proteger un sistema completo de cargas con un único SAI.

3. Modular: existen varios SAI independientes llamados *módulos*. Aumentan la autonomía y la potencia, ya que permiten conectar y desconectar diferentes módulos según las necesidades de la carga.

4. Modular granular: se construyen los módulos de tal forma que uno averiado no influya en el comportamiento del resto.

Los equipos deben comunicarse con los sistemas SAI, y estos se pueden encontrar a cierta distancia. Para ello, se usan tarjetas de comunicación y de red que permiten la gestión, la comunicación y el mantenimiento entre los equipos y los SAI. Las formas más usadas para implementar la gestión y la comunicación entre SAI son la extensión de la protección local, la gestión de varios SAI, la integración con la red IP, la monitorización ambiental y la protección local.

■ **Extensión de la protección local:** cada ordenador tiene instalada una aplicación especial que permite recibir datos del SAI. En este tipo de arquitectura se hace necesario una red TCP/IP y el número de ordenadores conectados al servidor varía.

■ **Gestión de varios SAI:** se instala un servidor central con un conjunto de aplicaciones que monitoriza a los SAI tanto locales como remotos, independientemente del número de ellos. El servidor central se comunica con otros servidores locales, y estos, con los diferentes SAI.

- **Integración con la red IP:** el servidor se sustituye por una tarjeta de red y los ordenadores no necesitan ninguna aplicación especial con los datos recibidos del SAI, ya que la comunicación se establece por medio de la red IP. Al no existir ningún servidor intermediario, aumenta tanto la fiabilidad como la seguridad de alimentación.
- **Monitorización ambiental:** pueden existir sensores que controlen parámetros ambientales, como humedad, temperatura, humos. Estos valores son enviados a una interfaz de red que puede enviar señales de alarma al servidor controlado por el SAI.
- **Protección local:** se usa para sistemas de equipos individuales, ya sean servidores o puestos de trabajo, y los periféricos conectados a estos de forma directa. En el servidor se instalan aplicaciones para la gestión de los SAI y el coste de implementación es bajo.

Actividad propuesta 2.6

Accesorios y conectores para SAI

Busca información sobre los siguientes elementos que generalmente se adquieren para la gestión de sistemas de alimentación ininterrumpida. Haz una descripción breve de sus características y precios.

- Tarjeta de administración de redes de SAI con supervisión medioambiental.
- Accesorio de contacto seco de encendido/apagado.
- Instalación de SAI de tres fases de extensión escalable.
- SAI modulares tolerantes a fallos de 400-1600KW.
- Elementos RCB.

■ 2.3. Seguridad ante intentos de espionaje

Desde el punto de vista del hardware y desde la visión de los procesos que se arrancan en el inicio de una máquina, es necesario hacer una supervisión constante sobre su manipulación. La inclusión interna de un módulo hardware que espíe un equipo no es tarea difícil para un empleado interno al sistema, basta tener acceso a la máquina y conocer metodologías para conectar algún módulo en su placa base. Incluso se pueden realizar operaciones más básicas, como la conexión al puerto USB o al puerto de teclado PS/2 de un dispositivo que espíe las pulsaciones por teclado de los usuarios que se conectan a dicha máquina. Estos dispositivos, fáciles de conectar, se denominan *keyloggers*. El responsable de seguridad técnica debe revisar las diferentes conexiones físicas en búsqueda de algún dispositivo irregular conectado a los puertos internos y externos de las máquinas de la intranet.

Un keylogger es un dispositivo que permite registrar todas las pulsaciones del teclado sin que el usuario lo perciba. Su instalación es fácil, y supone un sistema de espionaje muy eficiente, debido a que, a medida que los usuarios teclean sus contraseñas, él registra los caracteres pulsados y los envía a los futuros atacantes.

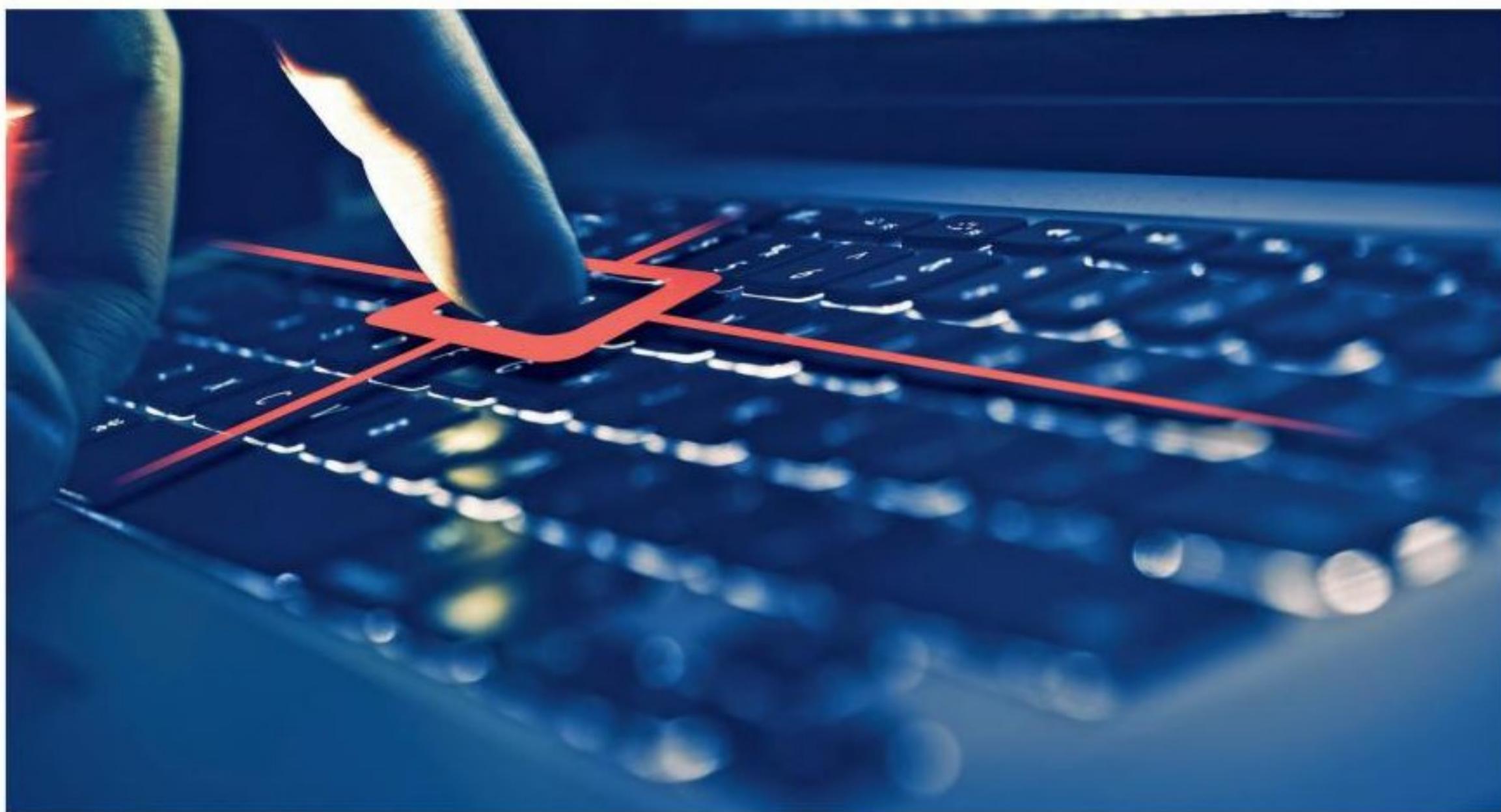


Figura 2.13. Los técnicos de seguridad de los centros de proceso de datos deben controlar los diferentes dispositivos que el personal que tiene acceso al CPD pueden conectar a los puertos externos de los servidores, e incluso al interior de los mismos, con el fin de evitar conexiones de dispositivos keylogger.

Los keyloggers pueden ser dispositivos hardware o programas que registran cada una de las pulsaciones del teclado. Estos dispositivos hardware se conectan como si fueran un teclado, de tipo USB o de tipo PS/2. También existen módulos keylogger que se conectan al circuito interno del teclado. Para instalar estos, se hace necesario acceder a la placa base de la máquina.

Los keyloggers se ejecutan en el inicio de la máquina que se quiere atacar, y envían por internet a una dirección de correo o a un servidor remoto la información capturada por teclado cifrada según técnicas que el atacante haya elegido.

La mayoría permiten configurar aspectos como los caracteres que interceptar, la ruta del archivo log, si se registran las pulsaciones Ctrl+C y Ctrl+V, los clics del ratón, e incluso definir los rangos temporales en los que se quiere hacer registro. Existen keyloggers que son capaces de registrar hasta las aplicaciones que el usuario está usando en todo momento, lo que supone un control de espionaje casi total.

Para no dejar rastro, permiten autodestruirse en una fecha determinada, con el fin de que el programa keylogger y sus registros desaparezcan del sistema de almacenamiento local de la máquina atacada. Evidentemente, su uso es ilegal sin el consentimiento del propietario de la máquina a la que se le quiere espiar.

Si en algún momento se sospecha que se está ejecutando un proceso keylogger en una máquina, la acción inmediata es desconectar el equipo de la red que ofrece servicio a internet y, cuanto antes, analizar los procesos que están en ejecución para detectar alguno que no debería estar activo.

La herramienta **HijackThis** (<http://sourceforge.net/projects/hjt>) permite detectar los programas que se ejecutan en el inicio del sistema.

Actividades propuestas

2.7. La aplicación HijackThis

Descarga la aplicación HijackThis en tu servidor. Hazlo en una máquina virtual y evalúa las diferentes herramientas de las que dispone. Haz un barrido con Scan y elimina los procesos que consideres perjudiciales para tu máquina con Fix checked. Configura qué elementos deseas tener en el inicio del equipo en Config-Misc Tools y cualquier otra función que consideres interesante.

2.8. Los comandos tasklist y taskkill

En equipos Windows, se pueden ejecutar dos comandos muy útiles para la supervisión de programas que están ejecutándose en segundo plano y la eliminación de memoria principal ocupada por estos programas. Estos comandos son tasklist y taskkill. Investiga cómo usar estos comandos, analiza los programas en ejecución y elimina aquel que consideres que no debería estar en segundo plano.

2.9. Control de procesos en segundo plano

Investiga sobre aplicaciones gratuitas, de código abierto o que permitan pruebas temporales, que muestren información sobre los procesos en ejecución en segundo plano y programas configurados en el inicio del sistema, y que permitan gestionarlos para la detección de programas maliciosos y su eliminación. Asegúrate siempre de que la aplicación que se intenta descargar está limpia de cualquier intento de malware, analizando minuciosamente el origen del sitio web al que accedes e instalándolo en una máquina virtual con Windows. Evalúa su utilidad y uso. Microsoft pone a tu disposición algunas herramientas que permiten espiar la actividad de los procesos en <http://technet.microsoft.com/en-us/sysinternals>. Entre ellas, la más interesante es Process Monitor. Usa una máquina virtual para instalar esta herramienta y evalúa su utilidad.

Recuerda



Un **proceso en segundo plano** es un bloque de instrucciones que no está usando todo el tiempo posible la unidad de procesamiento de la máquina, ya que no necesita que su ejecución sea inmediata. Estos procesos ejecutan código de vez en cuando con el fin de detectar la necesidad de ejecutar algún programa que necesita de ejecución inmediata.

■ 2.4. Seguridad en sistemas de almacenamiento

Se define la *seguridad de la información* como «la preservación de la confidencialidad, la integridad y la disponibilidad de los activos de la información». Por tanto, para confirmar la seguridad es necesario considerar estas tres dimensiones: el grado de confidencialidad, el grado de integridad y el grado de disponibilidad.

- **Grado de confidencialidad:** disposición de la información a terceros no autorizados.
- **Grado de integridad:** conservación de la exactitud y completitud de la información.
- **Grado de disponibilidad:** acceso y uso de la información por parte de terceros autorizados.

En otros contextos más complejos, se pueden tener en cuenta otras propiedades de la seguridad de la información, como son la responsabilidad y el no repudio.

- **Responsabilidad:** capacidad de justificar qué ha ocurrido, quién lo ha hecho y cuándo.
- **No repudio:** capacidad de poder certificar el origen de las operaciones, dónde se generaron, el destino a donde han llegado, etcétera.

En la Tabla 2.1, se detallan algunas de las situaciones que una correcta gestión de la seguridad de la información requeriría evitar durante el ciclo de vida de la información.

Tabla 2.1. Métodos de seguridad de la información

Pérdida o robo	Tanto los equipos como los soportes de almacenamiento masivos pueden ser extraviados o robados.
Difusión indebida	Por desconocimiento, error o con intención, el uso del correo electrónico y redes sociales puede incurrir en la difusión de información confidencial, incluidas contraseñas y credenciales.
Destrucción, manipulación o difusión no autorizadas	El acceso por entidades no autorizadas a la información puede dar lugar a alteraciones o destrucciones de la misma.
Daños de imagen	Manipulación de sitios web o tiendas online por entidades no autorizadas que puedan acceder al gestor de contenidos al poseer las credenciales de acceso. Soportes de almacenamiento que han dejado de usarse pueden contener información susceptible que interceptar, por lo que se recomienda borrarlos o destruirlos.
Divulgación de la información almacenada en sistemas compartidos o en la nube	Esta información también puede ser manipulada, destruida o divulgada si no se toman medidas seguras para el almacenamiento en sistemas locales.
Desastres naturales	Debido a desastres naturales no previsibles, la información puede ser destruida, y resultar imposible recuperarla. Se hace necesario establecer ciertos protocolos para las copias de seguridad y recuperación.
Deterioro de los soportes	Los soportes de almacenamiento masivo se deterioran con el tiempo. Además, las partes mecánicas pueden fallar y dejar inaccesible la información que contienen.
Vulnerabilidad del software que procesa la información	Este tipo de software es altamente susceptible a accesos no autorizados e infectados con software malicioso. Se hace obligatorio establecer planes para estudiar posibles vulnerabilidades, actualizándolos lo máximo posible.

Analizando lo anterior, es importante identificar tanto las aplicaciones que acceden al sistema de información como la propia información que se gestiona, sin importar el soporte y el formato. Se deberá registrar la ubicación de dichos soportes, el equipo responsable de su gestión y mantenimiento, y clasificarlos según unos criterios de seguridad adecuados, atendiendo al **cumplimiento legal**. Esta clasificación se convierte en algo esencial

para aplicar dichas medidas de seguridad, que se concretarán en distintas **políticas de seguridad**. Estas pueden ser:

- Cifrado de información crítica, tanto aquella que se almacena como la que se transfiere por sistemas de comunicación.
- Control de acceso a la información almacenada y a los servicios y programas para su gestión: permisos por roles, contraseñas robustas, etcétera.
- Control de uso de dispositivos externos de almacenamiento.
- Control de uso de almacenamiento y servicios en la nube.
- Destrucción segura de la información no útil.
- Copias de seguridad y planes de recuperación.
- Archivar de forma segura la información que se quiere conservar, y registrar la actividad como garantía del cumplimiento legal o normativo.

■ ■ ■ 2.4.1. Mecanismos para el almacenamiento de la información

Las organizaciones deben disponer de sistemas flexibles para el almacenamiento y mecanismos que protejan y resguarden la información. Estos sistemas deben ser capaces de adaptarse a rápidos cambios en el modelo del tratamiento de la información, de tal forma que se aprovechen las inversiones efectuadas. Por tanto, es importante que haya un equilibrio entre las soluciones de almacenamiento y los requerimientos del sistema de información. Estos sistemas se pueden clasificar, de forma general, en almacenamiento local, sistemas de copias de seguridad, dispositivos externos y servidores de almacenamiento en red. A continuación, se describe cada uno de ellos:

- **Almacenamiento local:** se refiere al sistema de almacenamiento masivo del que disponen los equipos de la red. La información se genera de forma local, se modifica y se transmite a otros equipos. Normalmente, estos sistemas son discos duros, pero también se puede considerar almacenamiento local el disponible en tabletas, dispositivos móviles o tarjetas de memoria.
- **Dispositivos externos:** los dispositivos externos se conectan directamente a los equipos y permiten almacenar información extra, evitando que ocupe espacio en el sistema de almacenamiento local. Estos pueden ser cintas magnéticas, discos duros externos, DVD o pendrives.
- **Servidores de almacenamiento en red:** los servidores de almacenamiento en red permiten disponer de un lugar común donde almacenar la información y poderla compartir.
- **Sistema de copias de seguridad:** se hace necesario establecer planes para automatizar los procesos de copias de seguridad de la información que la organización genera. Se suelen utilizar soportes externos.
- **Uso de almacenamiento en la nube:** otro medio de almacenamiento externo es el uso de servidores remotos destinados al almacenamiento de parte o toda la información de una organización. Además, se puede realizar la contratación de otros servicios añadidos como son backup, alojamiento de sitios webs o tiendas virtuales.

■ ■ ■ 2.4.2. Políticas de explotación de los sistemas de almacenamiento seguros

Se deben establecer políticas claras que determinen las metodologías adecuadas para la explotación de los sistemas destinados al almacenamiento masivo de la información de forma segura. Estas políticas se pueden resumir en que hay que indicar cuáles son las reglas generales, los criterios específicos y los procedimientos que se tienen que llevar a cabo por parte de los usuarios para garantizar seguridad y eficacia en estos sistemas de almacenamiento de la información.

En general, estas reglas deben:

- Garantizar el acceso a los recursos de usuarios y programas autorizados.
- Proveer de planes de recuperación tanto de la información como de la actividad en caso de fallos.
- Evitar la pérdida de información, el deterioro de la información almacenada y el uso de dispositivos no autorizados.
- Asegurar la eliminación de la información cuyo ciclo de vida ha acabado.

En la Tabla 2.2, se detallan las políticas generales para cada uno de los tipos de almacenamiento anteriormente indicados.

Tabla 2.2. Políticas para la gestión del almacenamiento de datos

Políticas de almacenamiento local	Normas para los equipos donde los usuarios deben cumplir con el tipo de información que se puede almacenar, su durabilidad y permanencia una vez transmitida a las máquinas no locales, ubicación y cifrado en el sistema de archivos, y normas sobre los archivos descargados.
Políticas de almacenamiento en la red	Normas para el uso de la información compartida en los servidores de almacenamiento y controles de acceso por parte de los usuarios. Aluden al tipo, momento y ubicación de la información almacenada, personas encargadas de su actualización y políticas sobre el almacenamiento individual en servidores compartidos (importancia de la eliminación de información no útil para la organización).
Políticas sobre el uso de dispositivos externos	Normas que se refieren al uso de la información almacenada en equipos externos (<i>bring your own device</i>) con el objeto de transportarla a otra ubicación o disponer de una copia personal: qué dispositivos y qué información están permitidos, gestión para las bajas de datos, etcétera.
Políticas de almacenamiento en la nube	Uso de servicios cloud donde se establecerán criterios de uso según normas y legislación vigentes que regulen qué información está permitido almacenar y las medidas para el borrado.

■ 2.5. Seguridad en almacenamiento redundante y distribuido

Uno de los sistemas de almacenamiento más usados es el que hace referencia a aquel que utiliza un conjunto de discos de almacenamiento masivos organizados con el fin de que el sistema operativo lo vea como un único elemento lógico de almacenamiento de datos. Los datos son almacenados de forma redundante y los discos, físicamente, son independientes. Estos sistemas se conocen con la sigla RAID (Redundant Array of Independent Disks). Permite combinar el almacenamiento en un grupo de dispositivos independientes en una única o varias unidades virtuales. Estos soportes de almacenamiento masivo pueden ser discos duros y dispositivos de estado sólido (solid-state drive, SSD) y ofrecen una mayor tolerancia a fallos, capacidad, rendimiento e integridad de los datos.

■ ■ 2.5.1. Tipos de RAID

Existen diferentes tipos de configuraciones, que se denominan **niveles**. Estas configuraciones aportarán ciertos beneficios respecto a integridad, capacidad, tolerancia a fallos y tasa de transferencia, y añadirán, también, algunos costes.

La elección de dicho nivel de configuración dependerá de las necesidades de almacenamiento que satisfacer y de los costes que se esté dispuesto a afrontar.

Los niveles de RAID más usados son el nivel 0 o RAID 0, el nivel 1 o RAID 1 y el nivel 5 o RAID5, donde la diferencia fundamental de su configuración radica en la configuración de réplica o distribución de la información almacenada en los discos.

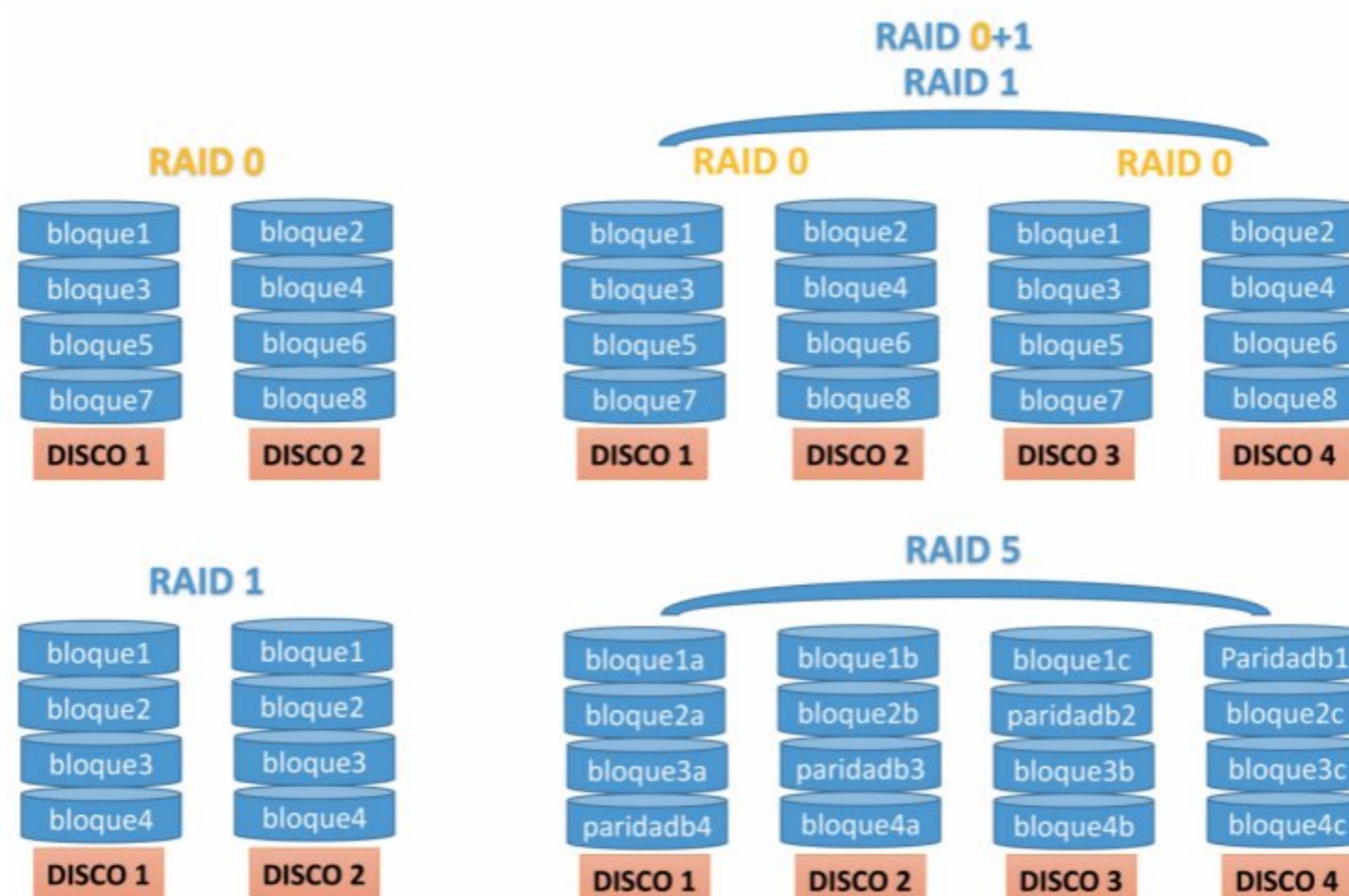


Figura 2.14. Los sistemas de matrices de discos redundantes usan diferentes discos con el fin de distribuir o replicar los datos contenidos en ellos. Los más conocidos son RAID nivel 0, RAID nivel 1, RAID nivel 0+1 y RAID nivel 5.

■ ■ 2.5.2. Nivel Disk Stripping o nivel RAID 0

En esta configuración, los datos están distribuidos equitativamente. Cuando un disco falla o se avería, la información no se pierde en su totalidad, solo la mitad, ya que se distribuye entre los diferentes discos. No existe redundancia, solo redistribución de la información en los diferentes soportes que conforman el sistema RAID. Como ventaja, ofrece mejora en la velocidad de acceso, ya que se puede escribir y leer datos a la vez, siempre que sea en discos diferentes. Se necesita un mínimo de dos discos. Esta configuración se recomienda cuando se utilizan aplicaciones de tratamiento de imágenes y vídeos.

Recuerda



Si no hay **redundancia de datos**, no hay **tolerancia a fallos**.

■ ■ 2.5.3. Nivel Disk Mirroring o nivel RAID 1

Los datos almacenados en los discos del RAID se copian de forma idéntica. En caso de que un disco falle, la información es alcanzable a través del otro disco. También se puede utilizar más de un disco, lo que incrementa la tolerancia a fallos y la integridad en los datos. Evidentemente, es una solución costosa.

El nivel **Striping+mirroring** (RAID 0+1) utiliza una combinación de ambas propuestas anteriormente planteadas, usando tanto redundancia de datos como distribución de los mismos. Para ello, se duplican los discos para conseguir dicha redundancia y se distribuye los datos para proporcionar velocidad y tolerancia a fallos. Se requiere como mínimo cuatro discos, donde solo dos de ellos se usan para el almacenamiento.

Actividad propuesta 2.10

Creación de un sistema raid nivel 1 en Windows

Configura un sistema RAID 1 en tu máquina Windows. Crea, usando la aplicación de gestión de máquinas virtuales (VMWare, VirtualBOx, XEN, o cualquier otra), diferentes discos, que luego usarás para acoplarlos al sistema RAID.

Recuerda que los volúmenes que tengas creados en tu sistema deben ser eliminados para que se pueda configurar un sistema RAID en Windows (Administración de discos).

■ ■ 2.5.4. Nivel stripping + distributed parity o nivel RAID 5

Se trata de un nivel en el que el acceso a los datos es independiente. Se emplea una técnica denominada *paridad distribuida*. Básicamente, se trata de calcular la información de paridad y almacenarla de forma alternativa en unidades llamadas *bloques*. Se combina fraccionamiento de la información y se usa la paridad como método para recuperar datos en caso de avería o fallo.

Este nivel es el más eficaz y es el más usado para los servidores, ya que ofrece una buena tasa de rendimiento frente al coste que supone su configuración. Se aconseja su uso en sistemas multiusuario. Se necesita un mínimo de tres discos, aunque se sugieren siete o más.

Actividad propuesta 2.11

Creación de un sistema raid nivel 5 en Windows

Configura un sistema RAID 5 en tu máquina Windows. Crea, usando la aplicación de gestión de máquinas virtuales (VMWare, VirtualBOx, XEN, o cualquier otra), diferentes discos, que luego usarás para acoplarlos al sistema RAID.

Recuerda que los volúmenes que tengas creados en tu sistema deben ser eliminados para que se pueda configurar un sistema RAID en Windows (Administración de discos).

■■■ 2.5.5. RAID basado en software

Los sistemas RAID basados en software hacen uso de la CPU para realizar operaciones implementadas al nivel del núcleo del sistema operativo, también llamado *kernel*.



Figura 2.15. El núcleo del sistema operativo mantiene información para la organización de los datos que se encuentran almacenados en diferentes discos, pero lo presenta con un solo dispositivo virtual a las aplicaciones. En Linux muchas distribuciones soportan RAID de forma nativa y añaden diferentes herramientas para crear, consultar y mantener los dispositivos RAID.

Se puede implementar a través de un sistema software puro o un sistema híbrido. En el primer caso, se trata de una aplicación que se ejecuta sin ningún hardware adicional. El sistema operativo podrá utilizar los discos en cuanto cargue los drivers del sistema RAID.

El coste de esta solución es reducido. Solo está condicionado por el número de discos de los que se dispongan. Como desventaja, presenta la desprotección del sistema al arrancar, ya que, si el disco duro falla antes de que el software RAID se active, el sistema no arrancará. También se debe tener en cuenta el rendimiento general del sistema cuando se dispone de sistemas RAID más complejos y con mayor número de discos. El reinicio del

sistema también supone un problema sobre la consistencia e integridad de los datos, ya que se pueden producir datos corruptos. Para solventar estos problemas, en configuraciones de BIOS, se pueden encontrar soluciones que permitan habilitar el sistema RAID en el momento del arranque del sistema.

Otro de los problemas es la vulnerabilidad. Los virus pueden atacar al sistema RAID, ya que se trata de un producto software.

Las soluciones RAID basadas en software son parte del sistema operativo, por lo que su coste es bajo. Además, funcionan al nivel de partición, por lo que puede aumentar su complejidad. En caso de cortes de energía, es posible perder ciertas escrituras pendientes, así que existe la posibilidad de perder información vital. El rendimiento dependerá de la capacidad de la unidad central de proceso y de la carga de trabajo en cada momento. Este tipo de soluciones se adapta para usuarios domésticos y pequeñas empresas.

■ ■ ■ 2.5.6. RAID basado en hardware

En este tipo de sistemas se hace uso de procesadores dedicados ubicados en los controladores de disco, que contienen un software embebido (firmware). Estos elementos hardware pueden ser controladoras RAID, dispositivos conectados a algún puerto, generalmente de tipo SCSI o Fiber Channel u otro tipo de dispositivo conectado a la red (por ejemplo, dispositivos storage area network, SAN).

Las tarjetas controladoras se conectan directamente a la placa base a través de alguna interfaz de conexión (por ejemplo, a través de algún slot PCI) y reciben la conexión a través de interfaces estándares (IDE, SATA, etc.). Para la configuración y mantenimiento de este tipo de sistemas RAID se dispone de alguna BIOS especial, y es importante asegurarse de que el sistema operativo soporta la totalidad de la configuración, tanto física como lógica.

Recuerda



El **firmware** es un programa generalmente almacenado en memorias ROM o PROM, que gestionan físicamente el funcionamiento de los dispositivos. La BIOS es un ejemplo de firmware.

Las soluciones RAID basadas en hardware no son parte del sistema operativo, por lo que su coste es mayor. En caso de cortes de energía, no se pierden las escrituras pendientes, ya que, al ser un dispositivo hardware, se pueden añadir dispositivos como unidades de backup de baterías que permiten almacenar la información en caso de dichos cortes. Este tipo de soluciones está más orientado al uso de clústeres o a sistemas con cargas de datos muy grande, como en bases de datos muy pesadas.

Actividad resuelta 2.1

Creación de un sistema raid nivel 1 en Linux

Configura un sistema de matriz de discos redundante RAID 1 en una máquina Ubuntu.

Solución

A través del programa de virtualización (VirtualBox, VMWare, etc), se crean dos nuevos discos duros, necesarios para simular un raid1. Con el comando `fdisk -l` se obtiene información sobre los diferentes discos que el sistema reconoce y que están debidamente montados.

Para el nuevo disco, denominado `/dev/sdb`, que es un disco SATA, se crea la tabla de particionamiento escribiendo el comando

```
fdisk /dev/sdb
```

Se seleccionará la partición primaria y el número de la partición será el uno. Con la opción `w` se modifica la tabla de particiones.

Para el segundo disco, llamado `/dev/sdc`, se copia la tabla de particiones recién creada para él. Para ello, se usa el comando `sfdisk` con el formato

```
sfdisk -d /dev/sdb | sfdisk /dev/sdc
```

y a continuación se formatean las particiones de ambos discos, usando el sistema de archivo ext4, aunque más tarde se deberá cambiar para montar el sistema raid. Para ello, se usa el comando `mkfs` escribiendo

```
mkfs -t ext4 /dev/sdb1
```

donde `sdb1` es la primera partición del disco `/dev/sdb`.

Se hace lo mismo para `/dev/sdc1`, escribiendo

```
mkfs -t ext4 -c /dev/sdc1
```

A continuación, se instala el paquete necesario para la gestión de sistemas raid en Linux denominado `mdadm` y otras herramientas útiles para dicha gestión

```
apt-get install mdadm initramfs-tools
```

Se activan los módulos `linear`, `multipath` y `raid1`, escribiendo

```
modprobe linear  
modprobe multipath  
modprobe raid1
```

Si se consulta el archivo `/etc/proc/mdstat`, se podrá comprobar que aún no existe ningún raid configurado.

A continuación, lo que se debe hacer es cambiar el tipo de partición que antes se usó, `ext4`, al tipo `Linux RAID Autodetect`, que permite la creación de sistemas raid1.

Para ello, se escribe `fdisk /dev/sdb` y el sistema pedirá que se indique qué orden se quiere realizar. Se pulsa `t`, y se indica que el nuevo sistema en código hexadecimal es `fd` (para `Linux raid autodetect`). A continuación, se pulsa `w` y la partición queda modificada.

Se hace lo mismo para el disco `/dev/sdc`, escribiendo

```
fdisk /dev/sdc
```

Si se vuelve a consultar el archivo `/proc/mdstat` se observará si está o no usando algún array de discos y de qué tipo es.

Aún no se dispone de un sistema array de disco. A continuación, se debe crear un nodo para el sistema raid, que se llamará `md0`. Para ello, se escribe

```
mknod /dev/md0 b 9 0
```

y ahora se crea el array para las unidades que van a intervenir en el raid que se acaba de apuntar con el comando

```
mdadm --create /dev/md0 --level=raid1 --raid-devices=2 /dev/sdb1  
/dev/sdc1
```

donde --create indica el nodo donde crear el raid, --level indica el nivel del sistema raid, --raid-devices indica el número de particiones que componen el sistema raid y, a continuación, se indica el nombre de cada una de ellas.

Consultando de nuevo el archivo /proc/mdstat se podrá comprobar que ya se encuentra montado el sistema raid nivel 1 con dos particiones. Con el comando `mdadm --detail /dev/md0` se podrá consultar información del raid. En status puede aparecer el estado clean, que indica que el raid está funcionando sin problemas, y el estado Active sync indica que ambas particiones están sincronizadas y activas.

Para añadir un nuevo disco al raid, se crea y se deja en espera. Para ello, se ejecuta el comando

```
mdadm --manage /dev/md0 --add /dev/sdf
```

Si se quisiera añadir al sistema raid, se ejecutaría el siguiente comando después de hacer una copia de seguridad para evitar perder la información en caso de que este proceso fallara:

```
mdadm --grow /dev/md0 --raid-disk=4 --backup-file=/backupdelraid
```

Consultando el archivo /proc/mdstat se puede observar que el sistema raid se está reconfigurando (*reshape*).

Actividad propuesta 2.12

Creación de un sistema raid nivel 5 en Linux

Siguiendo los mismos pasos que en la actividad anterior, genera un sistema RAID nivel 5 en una máquina Linux. Para ello, se crearán tres nuevos discos y se usarán para el nuevo RAID. A diferencia de la solución para un sistema RAID 1, se activará el módulo raid5 con modprobe raid5 y se usará el nivel 5 en el comando

```
mdadm --create /dev/md0 --level=raid5 --raid-devices=3 /dev/sdd1  
/dev/sde1 /dev/sdf1
```

2.6. Consideraciones en el uso de clústeres de servidores

Los **clústeres** son una colección de ordenadores interconectados a través de algún medio físico y lógico con el objetivo de trabajar en conjunto. Las tareas se distribuyen entre estas máquinas, que trabajan como si fuesen un solo equipo. Evidentemente, el medio físico que los une debe ser de alta velocidad, ya que este es un requisito imprescindible para permitir la comunicación de todos esos ordenadores.

Cada ordenador se va a llamar *nodo* del clúster. Los nodos pueden tener arquitectura hardware diferente, incluso pueden disponer de diferentes sistemas operativos. Un clúster

consta de, por lo menos, dos nodos, conectados entre sí a través de un canal de comunicación. Para su gestión se necesita un conjunto de aplicaciones de control.

El objetivo de la configuración de clústeres de servidores es conseguir una alta disponibilidad de los servicios que ofrece, un alto rendimiento al disponer de más procesadores y memoria principal, lo que minimiza sus tiempos ociosos, un balanceo de carga para distribuir y replicar los servicios ofrecidos, y una mayor **escalabilidad**.

Atendiendo a la homogeneidad de la arquitectura de los equipos de un clúster, hay dos tipos: homogéneos y heterogéneos.

- **Homogéneos:** los equipos que conforman el clúster tienen la misma arquitectura física y lógica, y los recursos de los que disponen son similares, no existiendo mucha diferencia entre nodo y nodo.
- **Heterogéneos:** los nodos del clúster pueden tener arquitectura distinta, diferentes sistemas operativos, recursos diversos y procesadores con distinta capacidad.

En cuanto a los servicios que se buscan en la configuración de un clúster, existen los clústeres de alta disponibilidad, alta confiabilidad y de alto rendimiento.

- **Alta disponibilidad (High Availability):** en este tipo de clúster, la información está repetida, de tal forma que se convierten en sistemas tolerantes a fallos y con capacidad de balancear la carga entre varios servidores. Además, su configuración permite balancear las conexiones entre varios nodos.
- **Alta confiabilidad (High Reliability):** los clústeres de alta confiabilidad suelen implementarse en entornos con necesidades especiales, y se necesita una arquitectura hardware más especializada.
- **Alto rendimiento (High Performance):** este tipo de sistemas se implanta en entornos con necesidades de cálculos muy altos: en el procesamiento de imágenes y vídeos, compilación de programas, compresión y cifrado de datos, etcétera.

■ 2.7. Gestión de eventos en ciberseguridad

Como ya se ha visto en la unidad anterior, la gestión de los eventos que ocurren en un sistema es bastante importante, no solo para las tareas asociadas a la administración estándar, sino también para dar respuestas a los procesos de auditoría de riesgos e impactos, en análisis de intrusión y análisis forense.

Por tanto, el diseño e implementación de una solución de gestión centralizada de eventos de aplicaciones, sistemas y dispositivos permiten desarrollar mecanismos para la explotación, el análisis y la monitorización de eventos de seguridad.

Conocer el procesamiento y el transporte de estos **esquemas log** y los métodos de implementación que usan diferentes tecnologías y relacionarlos con procesos de búsqueda, almacenamiento y análisis estadístico y monitorización en tiempo real son tareas de gran relevancia para cualquier responsable de la seguridad de los sistemas informáticos.

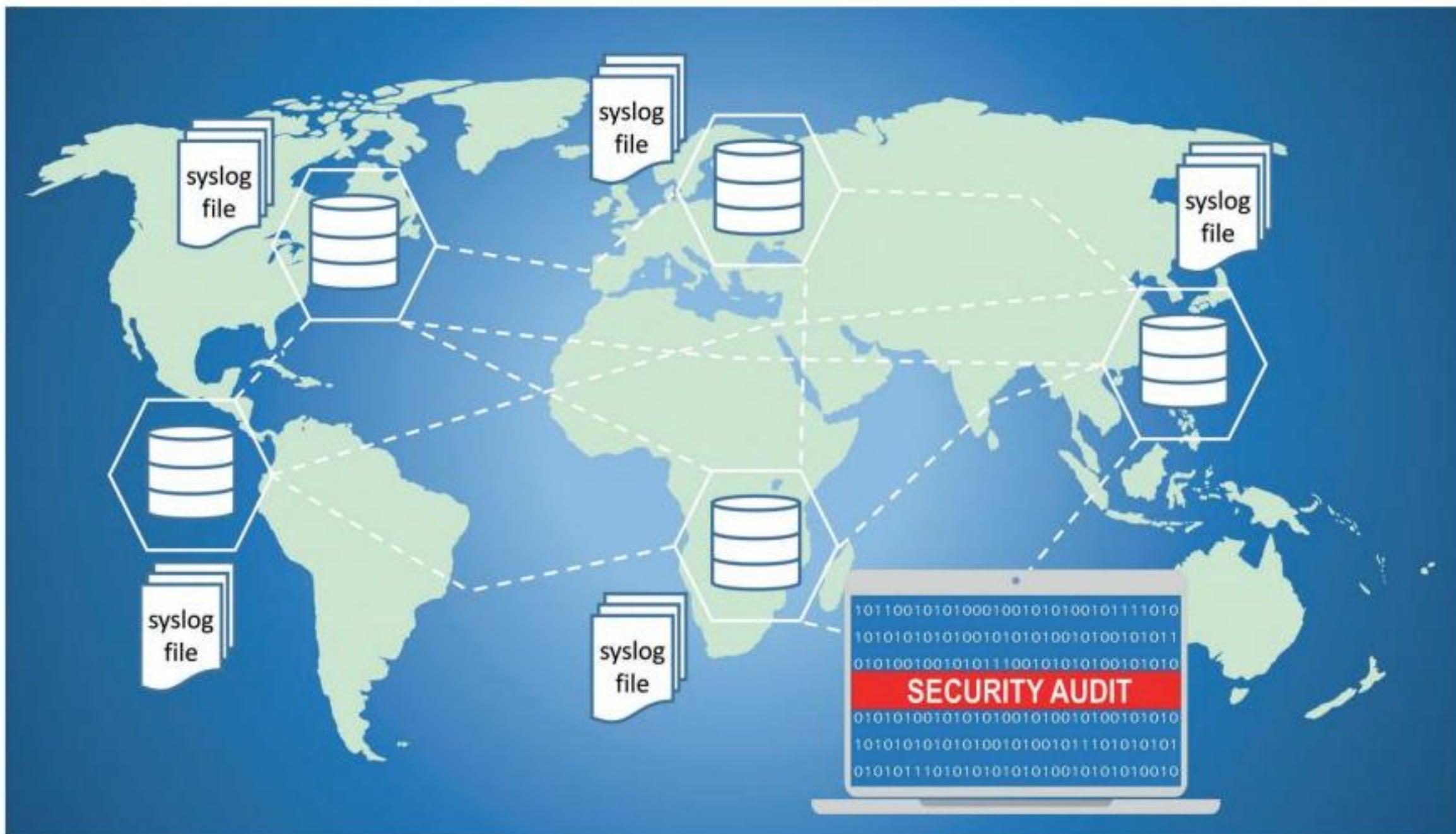


Figura 2.16. Los servidores de gestión de eventos o sistemas de gestión de información y eventos de seguridad (SIEM) centralizan las operaciones de supervisión de dispositivos perimetrales como switches, routers, cortafuegos, sistemas de detección de intrusos, gestión de servidores de bases de datos, servidores web y cualquier otro tipo de servicios.

2.7.1. Características de los logs

Esa **unidad de registro de evento** llamada *log* se genera al ocurrir un evento digno de registrar, según configuraciones sobre el sistema de registro local para cada servicio, proceso o aplicación en el sistema. Una vez que un evento se genera, la información de este se almacena con el fin de realizar más tarde procesos de exploración, análisis y monitorización. Según las políticas de archivado que se consideren oportunas y según el evento ocurrido, los registros log se rotarán, se almacenarán un tiempo considerable y se eliminarán.

Las operaciones básicas que se realizan en los diferentes tipos de logs se pueden resumir como sigue:

- **Acceso a datos y a sistemas:** registro de acceso a datos y a las aplicaciones.
- **Autenticación y autorización:** registro de decisiones de autenticación y autorización.
- **Errores y fallas:** registro de errores y fallas del sistema.
- **Gestión de amenazas:** registro de alertas de intrusión y acciones que violan la política de seguridad.
- **Gestión de cambios:** registro de cambios al sistema, componentes y cuentas de usuario.
- **Gestión de la disponibilidad y continuidad del negocio:** registro de mensajes del estado del sistema.

- **Gestión de rendimiento y capacidad:** registro de acciones que miden el rendimiento y capacidades del sistema.
- **Mensajes de depuración:** registro de mensajes usados para comprobar la funcionalidad de las aplicaciones y del sistema.

El almacenamiento de los logs registrados seguirá una política que defina el almacenamiento que usar, especificaciones de su rotación y archivado, y su eliminación. Los aspectos que se han de considerar en dicha política serán:

- Comprobar los requerimientos sobre el cumplimiento de estándares que se puedan aplicar (PCI DSS, NERC, etcétera).
- Revisar las especificaciones de dicha política, evaluando la utilidad de retención de los logs de seguridad.
- Evaluar la cantidad de subsistemas y logs que se generan con el fin de gestionar el espacio de almacenamiento que se necesita, revisando las tecnologías de almacenamiento de datos disponibles con el fin de mejorar dichos sistemas de gestión de eventos.

La información de los logs debe ser accesible por los usuarios autorizados, pero la gestión de esta ingesta masiva de registros debe ser analizada a través de programas especializados. Las técnicas más habituales usadas por estos programas son:

- **Correlación de logs:** para relacionar los diferentes logs. Herramienta ejemplo: SEC.
- **Filtro de logs:** para filtrar los registros según un criterio. Herramientas ejemplo: Grep, Awk, Sed, Kibana.
- **Minería de datos:** búsqueda de patrones y relaciones de los datos que se han recolectado.
- **Técnicas estadísticas:** uso de funciones estadísticas que estudien los datos log. Herramienta ejemplo: Kibana.

A continuación, se van a analizar los diferentes tipos de elementos que generan registros log:

- **Dispositivos de red y seguridad:** modificación de algún tipo de configuración, operaciones de conexión a un servicio: procesos de entrada y salida en la autenticación de usuarios, inicialización de algún proceso, cantidad en bytes de información transferida, etcétera.
- **Sistemas operativos:** autenticación, inicio, parada y reinicialización del sistema o de un servicio, finalización inesperada de algún servicio y mensajería de estado.
- **Aplicaciones:** actividades de usuarios normales o privilegiados, actividades críticas y reconfiguraciones.
- **Syslog:** el servicio syslogd escucha peticiones por el puerto UDP 514 y es configurable en /etc/syslog.conf.
- **SNMP:** uso del protocolo SNMP para la configuración y consulta de estados de los dispositivos.
- **Eventos Windows:** recolecta logs de eventos de aplicaciones, de seguridad y de sistema.

Existen muchas herramientas para la gestión de eventos. Las más populares son:

- **Awk:** para la búsqueda de patrones en archivos log de texto. Es de código abierto.
- **Grep:** para la búsqueda de patrones en archivos log de texto. Es de código abierto.
- **Loggly:** para la gestión de logs en la nube.
- **Microsoft Log Parser:** para filtrar fuentes de logs en sistemas Windows. Es gratuita.
- **OSSEC:** para la centralización, almacenamiento y retención de información log y reglas para analizarla. Es de código abierto.
- **OSSIM:** para evaluar vulnerabilidades, detección de amenazas y monitorización.
- **Rsyslog:** recoge logs de muchas fuentes y las centraliza en un servidor. Es de código abierto.
- **SED:** para extraer y analizar archivos log de texto. Es de código abierto.
- **Snare:** recolecta eventos Windows y los centraliza en un formato compatible con Syslog.
- **Syslog:** recoleta logs de muchas fuentes y los centraliza en un servidor. Es de código abierto.

La herramienta popularmente llamada **ELK**, que en realidad aglutina tres herramientas de análisis y gestión de registros, permite centralizar todas las notificaciones de servidores web, servidores de correo, servidores de bases de datos y diferentes dispositivos de red, y enviarlas a un alojamiento situado en la nube.

ELK está compuesto de ElasticSearch, encargado de buscar RESTful distribuido almacenando los mensajes registrados, Logstash, que recopila, procesa y reenvía los eventos y almacena los mensajes, y Kibana, que ofrece la búsqueda y análisis de código abierto basado en navegador.

El concepto Rest, Representational State Transfer, hace referencia a un modelo de arquitectura web que usa el protocolo HTTP para mejorar las comunicaciones entre el cliente y el servidor. RESTful son los programas basados en esta tecnología y no necesitan ser ejecutados en una red, por lo que lo pueden hacer desde un mismo ordenador.

Actividad propuesta 2.13

Despliegue de un servidor syslog y uso de herramienta ELK

Configura el servicio rsyslog en una máquina Linux. En las últimas versiones de Ubuntu el servicio ya viene instalado. Para comprobar el estado en el que se encuentra el servicio escribe systemctl status rsyslog. El fichero de configuración es /etc/rsyslog.conf o en Ubuntu /etc/rsyslog.d/default.conf. Asegura el puerto de rsyslog usando netstat -tnlp | grep rsyslog y configura los servicios que quiera ofrecer tu servidor rsyslog (también se puede hacer con su antecesor syslog que es más fácil de configurar).

Compara esta aplicación con ELK. Para ello, realiza en tu máquina Linux, con Apache instalado, el despliegue de las herramientas ElasticSearch, Logstash y Kibana. Explora la configuración para obtener un servidor de gestión de eventos. Descarga los productos y desplíégalos.

Los tipos más usuales de eventos que se registran son los siguientes:

- **Evento de acceso correcto auditado:** son sucesos relacionados con la seguridad que informan de procesos realizados correctamente.
- **Evento de acceso erróneo auditado:** al contrario que el anterior, refiere un fallo relacionado con un acceso de seguridad erróneo.
- **Evento de advertencia:** describe alguna situación que podría acarrear algún error importante más adelante.
- **Evento de error:** indica que el suceso ocurrido es de vital importancia.
- **Evento de información:** informa sobre el funcionamiento correcto de cualquier servicio, aplicación, programa del sistema, control, etcétera.

2.8. Gestión de los centros de datos en la nube

La **computación en la nube**, o servicios en la nube, o informática en la nube es una filosofía de trabajo que permite ofrecer cualquier servicio informático a través de la red internet. En la actualidad, las organizaciones más importantes en el desarrollo de herramientas orientadas a la computación en la nube son Amazon, con su plataforma Amazon Web Services (AWS), Microsoft, con su plataforma Azure, y Google, con su plataforma Google Cloud Services.



Figura 2.18. La base de la tecnología de centros de datos en la nube se basa en la contratación de no solo los servicios requeridos, sino también de la infraestructura tecnológica necesaria para proveer dichos servicios.

La base de la tecnología de centros de datos en la nube se basa en contratar servicios, pero no solo la parte software necesaria, sino también toda la tecnología física que se necesita para dar soporte a todos los servicios contratados.

Para la parte de Logstash, ten precaución con los siguientes pasos:

Comprueba que se dispone de Apache instalado en la máquina. El archivo de registro de Apache se encuentra en /var/log/apache2/Access.log.

A continuación, confecciona un fichero de configuración de Logstash. El nombre, aunque puede ser el que se quiera, va a ser apache.conf, y se va a ubicar en el directorio /etc/logstash/conf.d. Si se quiere ubicar en otro lugar, es necesario indicarlo en el fichero /var/log/apache2/Access.log, en la directiva path.

El contenido de este fichero Logstash puede ser el siguiente:

```
Input{ File {
    Path =>"/var/log/apache2/Access.log"
    Start_position =>beginning}}
Filter{Grok{
    Match =>{"message"}=>%{COMBINEDAPACHELOG}}
Date{
    Match=>["timestamp","dd/MM/yyyy:HH:mm:ss Z"]}
}
Output{Elasticsearch{host=>localhost}}
```

Después, despliega Kibuna y configura el producto para explotar la gestión de eventos.

■ ■ ■ 2.7.2. El visor de eventos en Windows (EventViewer)

Esta herramienta de Microsoft es un potente **visor de eventos** que permite configurar, administrar y supervisar mensajes producidos por la máquina local o en otra máquina a la que se pueda acceder remotamente. Los eventos ocurridos pueden ser de muchos tipos, pero, principalmente, son los registros de aplicación, los registros de seguridad, los registros del sistema, los eventos administrativos y los registros de web server.

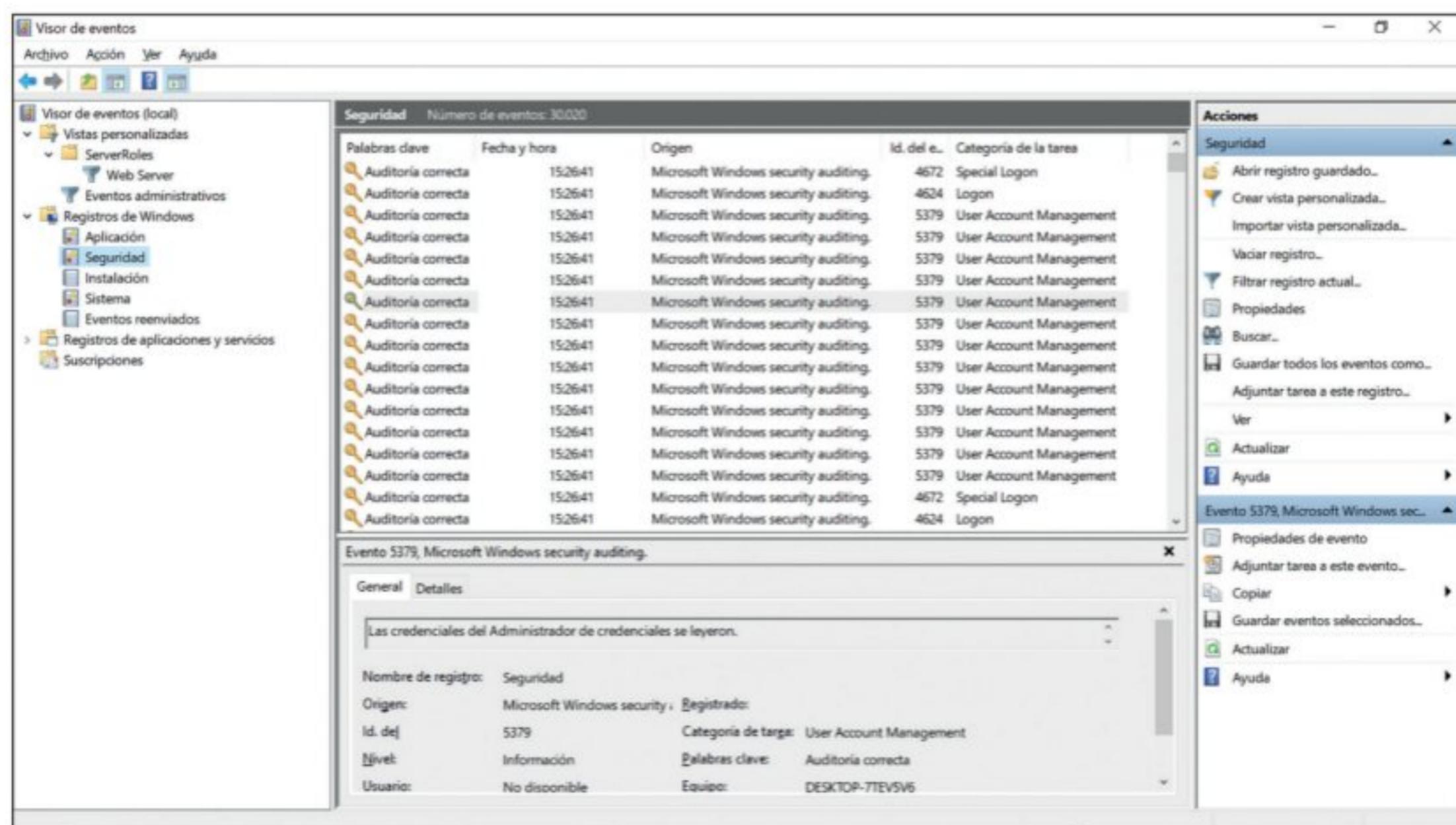


Figura 2.17. El visor de eventos de Windows provee una colección de herramientas muy potentes para supervisar cualquier acontecimiento que ocurra en un servidor local.

■ ■ ■ 2.8.1. System Center Configuration Manager de Microsoft

Es un producto de Microsoft que permite gestionar centros de datos en entornos de cloud híbridos de una forma más cómoda y centralizada: supervisión de la infraestructura, administración de copias de seguridad y servicios avanzados de tecnología de la información.

Las herramientas más completas de System Center son:

- **Data Protection Manager:** para la protección completa de los datos, a través de copias de seguridad, almacenamiento y recuperación, en entornos de máquinas físicas-servidores y cloud privado.
- **EndPoint Protection:** protección de malware para clientes y servidores.
- **Orchestrator:** para automatizar tareas y gestionar *runbooks* a través de scripts Powershell.
- **Operations Manager:** gestiona la capacidad, el estado y el uso de las aplicaciones, cargas de trabajo e infraestructura.
- **Service Manager:** para la gestión de la actualización de los sistemas, a través de políticas de configuración, supervisión del sistema y seguridad.
- **Virtual Machine Manager:** para la gestión de software de virtualización orientado a almacenamiento, computación, redes y seguridad.

Actividad propuesta 2.14

La consola Windows Admin Center

Evaluá la herramienta de Microsoft Windows Admin Center. Esta consola muestra una colección de herramientas muy potentes para la administración del sistema, tanto para la gestión de la máquina local como para la gestión de los recursos compartidos.

Se trata de una herramienta basada en explorador implementada localmente, sin necesitar conexión a internet ni soluciones Azure, y ofrece control total sobre la implementación incluso en redes privadas sin conexión a internet.

Descárgala desde la página oficial de Microsoft, instálala y evalúa su potencia.

■ ■ ■ 2.8.2. Soluciones Azure

Los servicios ofrecidos están alojados en la nube, ya sean tanto los propios servidores como los sistemas de almacenamiento, redes o aplicaciones. Son más económicos, seguras, flexibles y confiables que los servidores locales. El escalado de los recursos es mucho más rápido, ya que la solución se adapta a las necesidades propias de la organización conforme los recursos son o no necesarios, con la premisa que solo se paga lo que se usa.

Azure es una tecnología de Microsoft para ofrecer servicios de informática híbridos que combinan la tecnología local con la contratada en la nube, asegurando todos los requisitos de cumplimiento normativo y privacidad.

■ ■ ■ 2.8.3. Amazon Web Services

Amazon Web Services, también llamado AWS, se ha convertido en una de las plataformas en la nube más completa en la actualidad, compuesta por multitud de servicios integrales de centro de datos. Ofrece tecnología muy avanzada en infraestructuras de cómputo, bases de datos, almacenamiento, lagos de datos y análisis, aprendizaje automático, inteligencia artificial e internet de las cosas.

Una de claves del éxito de AWS es la integración de una red de socios muy extensa que permiten la unión de sistemas especializados en sus servicios y un conjunto de proveedores independientes que adaptan sus tecnologías para que también funcionen en AWS.

■ ■ ■ 2.8.4. Google Cloud Platform

La plataforma **Google Cloud** reúne todas las aplicaciones de desarrollo web de Google a través de arquitecturas basadas en la nube, siendo esta tecnología la única forma de acceso, almacenamiento y gestión de datos de estas aplicaciones. Cuando se desactiva este servicio, se puede acceder a los proyectos ya creados, pero no se pueden crear nuevos.

G Suite es un servicio de Google que aglutina varios productos bajo un nombre de dominio que Google personaliza para el cliente que contrata este servicio.

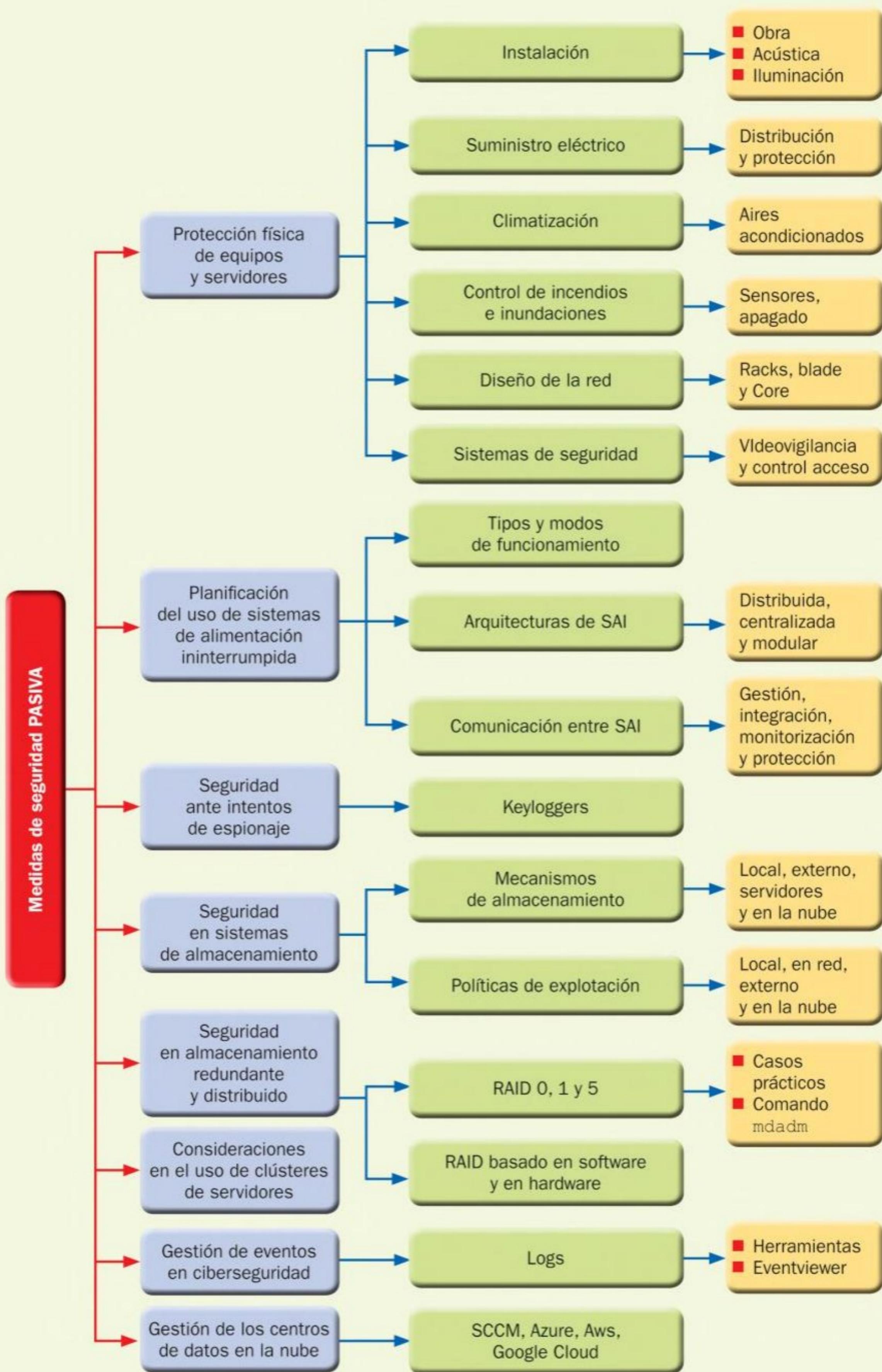
■ ■ ■ 2.8.5. Seguridad en la nube

La gestión en la nube no está exenta de protocolos de seguridad por el hecho de no estar ubicada en la infraestructura de la organización. Más bien todo lo contrario. Aparecerán nuevas situaciones derivadas de la propia naturaleza de estos sistemas, ya que deja de estar bajo el control de la organización. Evidentemente, las ventajas son muchas, pero también las desventajas. Se deben preservar la autenticidad, la fiabilidad, la usabilidad y la confidencialidad de la información, y las políticas de actuación dependerán de los servicios contratados, de su forma y de su despliegue. A continuación, se enumeran algunas de las amenazas y riesgos asociados a la gestión en la nube:

- Control de los accesos no autorizados para evitar robos, inyección de código malicioso, etcétera.
- En tecnologías compartidas, un fallo podría acarrear la difusión de información confidencial de la organización.
- La interfaz provista por el proveedor debe ser segura y no contener errores.
- La suplantación de identidad y el desconocimiento del entorno en la nube puede acarrear riesgos potenciales si las políticas de seguridad no son las adecuadas.
- Las transferencias de datos deben estar cifradas, ya que las tecnologías en la nube no están exentas de ataques de ingeniería social o de infección con malware.
- Se debe solicitar al proveedor del servicio dar de baja a los agentes que ya no trabajan en la organización y que tienen acceso a dichos servicios.

MAPA CONCEPTUAL

2. MEDIDAS DE SEGURIDAD PASIVA



Actividades de comprobación

2.1. Para la recuperación de un centro de procesos de datos en caso de desastres, las mejores opciones son:

- a) No es necesario actuar según el plan de contingencia, ya que, al ser un caso especial, es vital recuperarse lo antes posible.
- b) Lo último será la recuperación de las bases de datos, ya que prima la seguridad del personal, que debe abandonar la sala de computadores cuanto antes.
- c) Lo primero es usar el protocolo de recuperación de datos y mecanismos de acceso a los mismos.
- d) Debe evitarse desviar las comunicaciones a un centro alternativo.

2.2. Los tipos de sistemas de alimentación ininterrumpida más conocidos son:

- a) De corriente continua y de corriente alterna, en función del modo de trabajo.
- b) SAI estático, rotativo o mixto, según la corriente de carga que soporta.
- c) Mixtos o alternos, según el modo de trabajo o el modo de corriente de carga.
- d) Ninguna de las anteriores es correcta.

2.3. ¿Los SAI pueden trabajar de forma modular?

- a) Sí, centralizándose para controlar y vigilar varias cargas simultáneamente.
- b) Sí, actuando cada uno de ellos de forma independiente, aumentando así la autonomía y su potencia.
- c) No, ya que cada carga se conecta a su propio SAI.
- d) No, ya que lo que se pretende es proteger un sistema importante y distribuir sus cargas.

2.4. Los factores que suelen causar variaciones del suministro eléctrico son:

- a) Errores humanos.
- b) Catástrofes naturales.
- c) Interferencias que generan otros subsistemas del CPD.
- d) Todas las anteriores son correctas.

2.5. En cuanto al uso de las tarjetas de comunicación y de red, ¿cuál de las respuestas es incorrecta?

- a) Se usa para sistemas de equipos individuales.
- b) En cualquier configuración, solo un ordenador tiene instalado una aplicación especial de gestión de los SAI, el servidor central.
- c) Pueden existir sensores que miden parámetros ambientales que intercepta la interfaz de red.
- d) Cuando se usa un servidor central, se comunica con otros servidores locales, y estos, con los SAI.

2.6. En cuanto a las medidas de seguridad de la información almacenada en los sistemas de almacenamiento masivo, ¿cuál de las siguientes respuestas es correcta?

- a) No es necesario controlar la pérdida o robo, ya que no es culpa de la organización.
- b) La información compartida en la nube no puede ser manipulada, destruida o divulgada, ya que los datos están en otros soportes alojados en servidores remotos.
- c) Los soportes de almacenamiento no se deterioran con facilidad. La mayoría de ellos pueden durar varias décadas.
- d) El acceso por entidades no autorizadas puede dar lugar a la modificación o eliminación de la información.

2.7. Respecto a los sistemas RAID (Redundant Array of Independent Disks), es correcto afirmar que:

- a) En el nivel 1, los datos están distribuidos equitativamente.
- b) En el nivel 1, se accede a los datos de forma independiente usando la técnica de paridad distribuida.
- c) En el nivel 5, los datos están distribuidos equitativamente.
- d) En el nivel 1, los datos se copian de forma idéntica en cada disco.

2.8. Con respecto a las unidades de registro de evento, ¿cuál de las siguientes respuestas no es correcta?

- a) Pueden ser alertas de intrusión.
- b) Pueden ser registros de acceso a datos.
- c) Pueden ser registros de cambios de sistema, componentes y cuentas de usuario.
- d) Se diferencian de los logs en que estos registran mensajes usados para comprobar la funcionalidad de las aplicaciones y del sistema.

2.9. En cuanto a los clústeres de servidores, ¿cuál de las respuestas es correcta?

- a) Son un conjunto de clústeres de discos apilados y conectados a un servidor.
- b) Todos los nodos del clúster deben tener la misma arquitectura.
- c) El objetivo es conseguir alta disponibilidad, pero se disminuye el balanceo de carga.
- d) Se consigue mayor balanceo de carga, una alta disponibilidad y mayor rendimiento.

2.10. Con respecto a los sistemas RSyslog, ¿cuál de las respuestas no es correcta?

- a) Recolectan los logs y los centralizan en un servidor.
- b) Son de código abierto.
- c) Recolectan eventos Windows.
- d) Las fuentes pueden ser diversas.

Actividades de aplicación

- 2.11.** Averigua qué son los códigos IP que hacen referencia a los grados de protección. ¿Qué tipo de grados existen? ¿Qué significa su cifra?
- 2.12.** El código IK también se trata de un sistema de codificación para indicar grados de protección. ¿Cuáles son sus posibles valores y qué indican?
- 2.13.** Los indicadores WK indican la resistencia antirrobo. ¿Cuál es el que más protege, ante qué protege y cuánto tiempo?
- 2.14.** ¿Qué son los servidores tipo blade?
- 2.15.** ¿Para qué se usan los centros de proceso de datos de respaldo?
- 2.16.** Indica las especificaciones técnicas de los sistemas de alimentación ininterrumpida. Averigua cuál puede ser el precio de un SAI con seis horas de autonomía.
- 2.17.** Configura tu máquina Windows para que evite la ejecución de aplicaciones en segundo plano cuando estas no son necesarias.

- 2.18. Visita el sitio web de NextCloud e investiga sobre su utilidad. Compara NextCloud con OwnCloud y despliega un servidor NextCloud/OwnCloud en una máquina Linux.
- 2.19. Consulta las pequeñas aplicaciones que se pueden ejecutar desde Windows a través de la consola MMC (Microsoft Management Console).
- 2.20. Visita los sitios webs de Azure, Amazon Web Services y Google Cloud y confecciona un documento que describa las diferencias y similitudes entre estas plataformas.

Actividades de ampliación

- 2.21. ¿Qué es DCIM integrado, para qué se usa y cuáles son sus especificaciones? Enumera algunos fabricantes y analiza los precios de mercado.
- 2.22. Investiga sobre productos como Chilled Water inRow Cooling, Rack Air Distribution Systems, Direct Expansion inRow Cooling e InRow Cooling Accesories. Elabora un documento técnico con las especificaciones estándares de estos productos y precios de mercado.
- 2.23. Investiga sobre los siguientes conceptos relacionados con los sistemas de detección y extinción de incendios en centro de procesos de datos: central automática de detección de incendios, sensores ópticos o iónicos de incendios, agua nebulizada, reducción de oxígeno. Confecciona una lista sobre algunos fabricantes y los productos que tienen en el mercado.
- 2.24. ¿En qué consiste la refrigeración por salas, la refrigeración por racks y la refrigeración por filas?
- 2.25. La descarga en sistemas de extinción que usa extintores de tipo halocarbonato tiene ciertos riesgos. ¿Cuáles son y cómo se miden?
- 2.26. ¿En qué consiste el uso de jaulas en un CPD?
- 2.27. Indica la utilidad de los comandos `sfc`, `dism` y `findstr`.

Enlaces web de interés

■ **Herramientas de Microsoft** - <http://technet.microsoft.com/en-us/sysinternals>

Plataforma en la que se pueden encontrar pequeñas herramientas muy útiles para sistemas operativos Windows.

■ **Plataforma Azure** - <https://azure.microsoft.com/es-es>

Plataforma de Microsoft que se presenta como su opción para la gestión de centros de datos en la nube.

■ **Plataforma Amazon Web Services** - <https://aws.amazon.com/es/>

Plataforma de Amazon que da soporte a las tecnologías de gestión de centros de datos en la nube orientados a sitios web.

■ **Plataforma Google Cloud** - <https://cloud.google.com/>

Plataforma de Google para desarrolladores de aplicaciones de tecnologías basadas en la nube.

■ **Plataforma Next Cloud** - <https://nextcloud.com/>

Plataforma posterior a OwnCloud que permite desplegar servidores de almacenamiento de datos en la nube, entre otras funciones.