SEGURIDAD FISICA-CPD

Ubicación y Protección Física

Instalación física	Suministro eléctrico	Climatización y control de incendios	Diseño de red	Sistemas de seguridad
■ Obra ■ Ubicación ■ Paredes y suelos ■ Acústica ■ Iluminación	■ Distribución ■ Protección ■ Sistemas de alimentación ininterrumpida	■ Aires acondicionados ■ Sensores detectores ■ Sistemas de apagado ■ Gas y agua	■ Racks ■ Servidores tipo blade ■ Topologías core/acceso	■ Videovigilancia ■ Control de acceso

CENTRO DE PROCESOS DE DATOS

Sala con la tecnología informática de una organización

UBICACIÓN DE UN CPD

UBICACIÓN DEL CPD

Espacio y sus accesos
Accesos para operaciones
Accesos centralizados
Salidas emergencias
Evitar interferencia electromagnética
Control inundación
Idoneidad del sótano

INFRAESTRUCTURA

Obra
Energía
Climatización
Protección contra incendio
Cableado
Seguridad

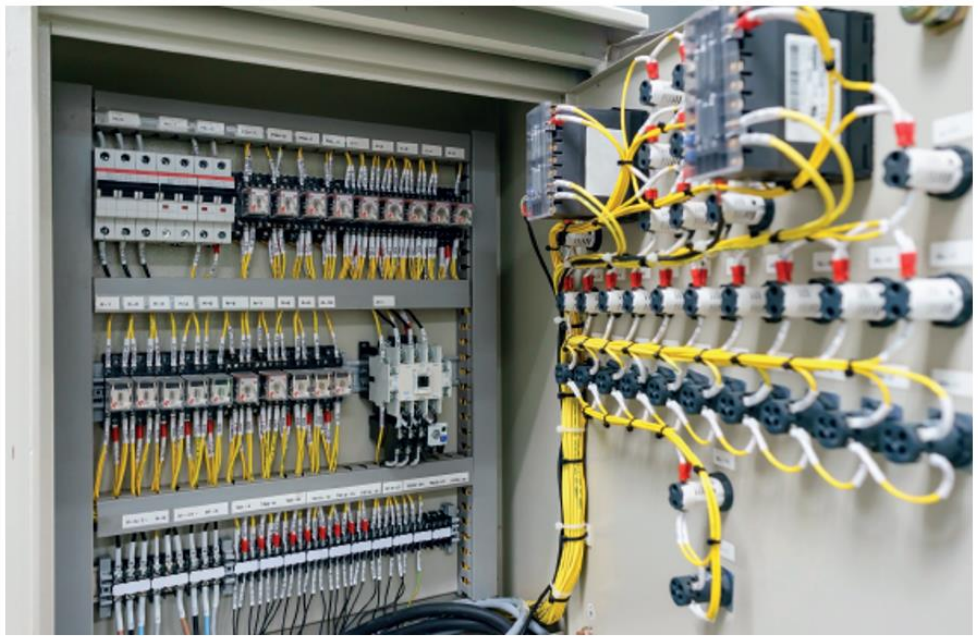
CONTRUCCIÓN DEL CPD

Enchufes
Acometidas telefónicas
Climatización
Salida de emergencia
Autoprotección
Elementos voluminosos y pesados
Vías, suelos, espacios y divisiones

CONSIDERACIONES AMBIENTALES

Temperatura (21-23 °C)
Humedad (40-50 %)

Evitar fallos componentes
Corrosión
Descargas estáticas



CONSIDERACIONES ELÉCTRICAS

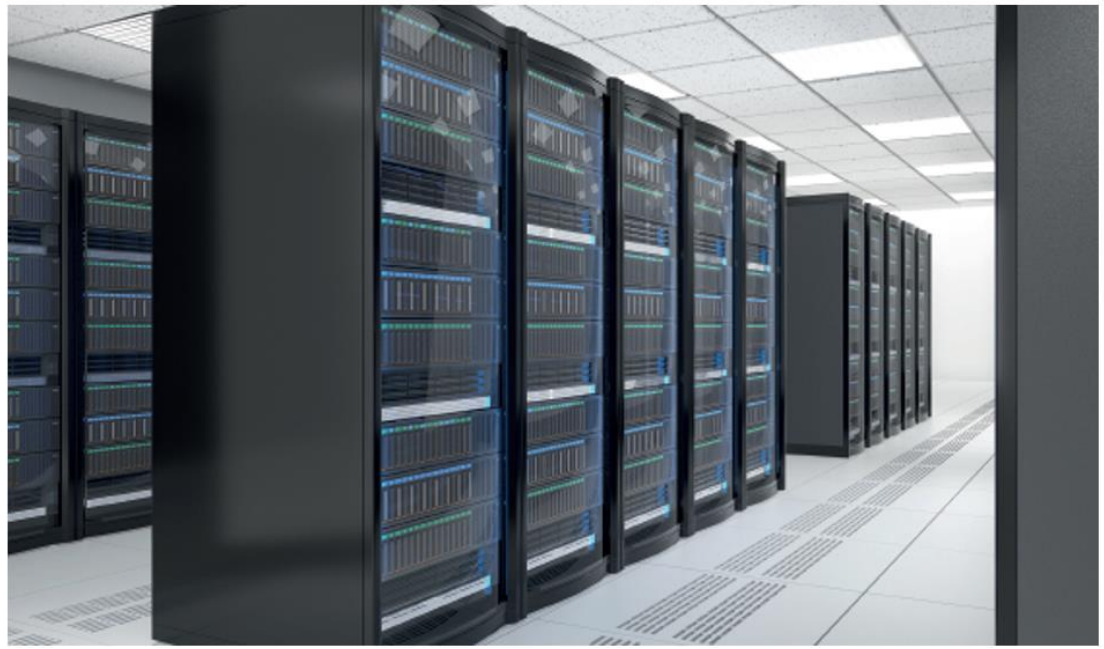
Apagado de emergencia
Cableado
Conductos eléctricos
Diferenciales
PDU
Toma de tierra
Transitorios
Control del voltaje

DETECCIÓN DE INCENDIOS

Pasamuros
Alarmas
Central, detectores, líneas, pulsadores
Extinción por gas
Por agua nebulizada
Estanqueidad
Refrigeración

DISEÑO

Switches y Routers en topologías Núcleo/Acceso
Racks: refrigeración y seguridad



DISEÑO

RACKS: Puertas, paneles y cerraduras

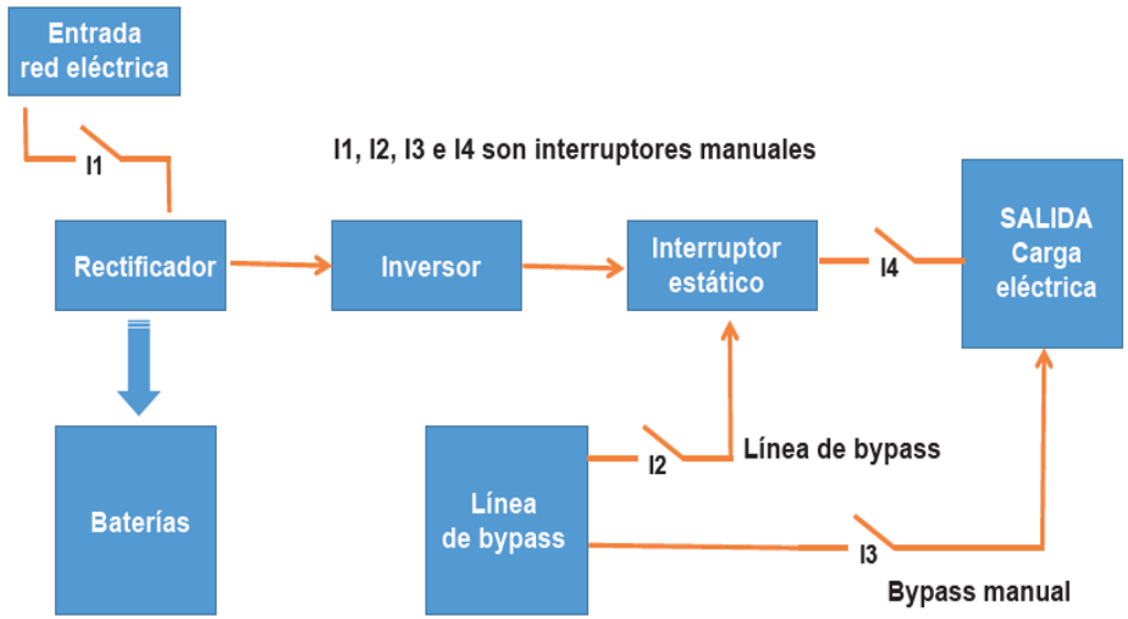
Sistema de cableado

Servidor tipo RACK

Servidor tipo BLADE

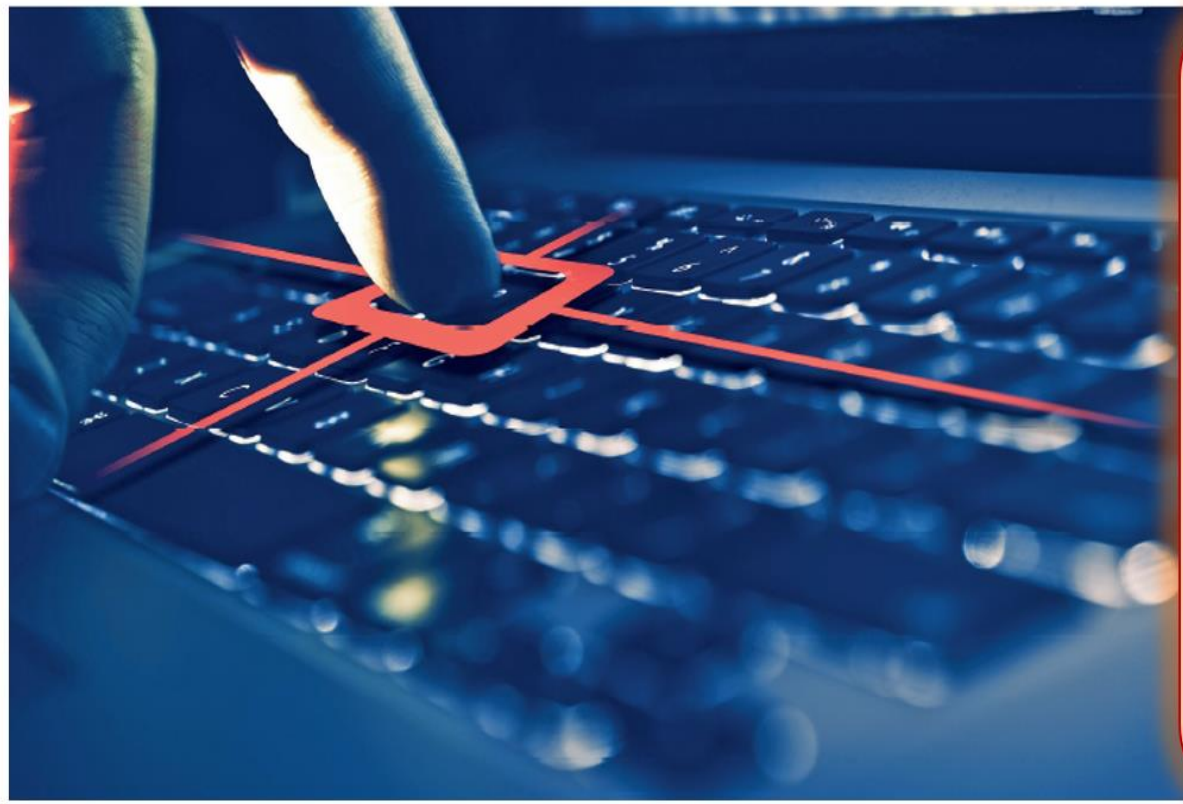
SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Cortes, microcortes, micropicos
Distorsión y Ruido eléctrico
Sobretensiones y subtensiones
Variaciones en frecuencia



SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Batería
Bypass manual y automático
Inversor
Rectificador
Filtro
Panel, pulsadores, software



ESPIONAJE

KEYLOGGER
Módulos hardware que espían
También productos software
Chequear procesos
HijackThis, tasklist, taskkill

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.

SEGURIDAD EN SISTEMAS DE ALMACENEMIENTO

Confidencialidad, integridad y disponibilidad
Responsabilidad, no repudio
Cifrado, control de acceso, de uso de dispositivos externos y en la nube
Destrucción segura
Copias de seguridad
Registrar la actividad (cumplimiento normativa)

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 encargas 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 *(bring your own device)* 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.

POLÍTICAS

Garantizar accesos
Plan de recuperación
Control pérdida y deterioro
Borrado

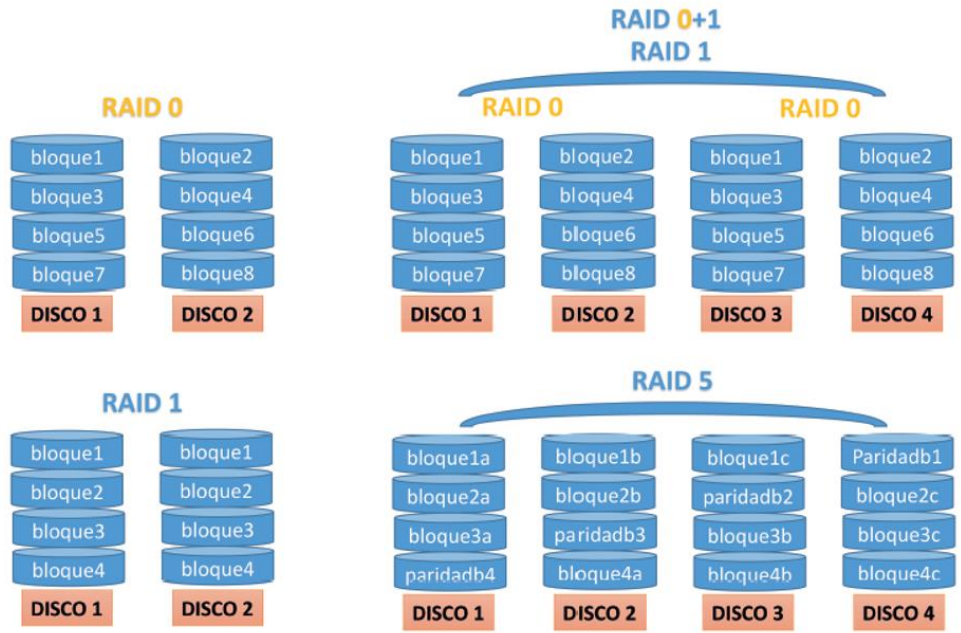
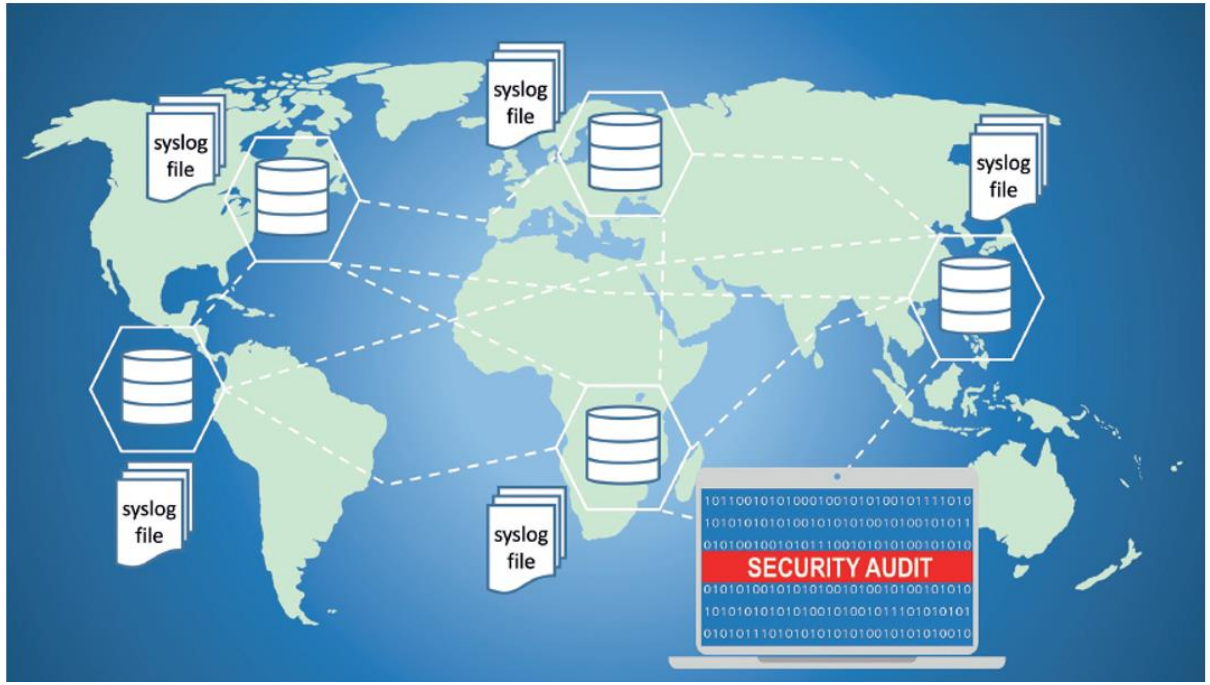


Figura 2.14. Los sistemas de matrices de **discos redundantes** usan diferentes discos con el fin de distribuir o replicar los datos contenidos en ellos. Los más conocidos son **RAID** nivel **0**, RAID nivel **1**, RAID nivel **0+1** y RAID nivel **5**.



GESTIÓN DE EVENTOS

De acceso, de autenticación, de errores, de intrusión, de contra-políticas, de cambios, de estados, de rendimiento, de depuración

CPD en la nube

Microsoft SCCM
Soluciones Azure
Amazon Web Services
Google Cloud Platform
Seguridad en la nube