Universidad del Gran Rosario

Tecnicatura en Ciberseguridad

Seguridad Física

Apuntes de Clase

Prof. Omar Cuarterolo

Introducción a la Seguridad en Datacenters

Introducción a la seguridad

Los tres pilares de la Seguridad Informática

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad



Confidencialidad

La confidencialidad en el contexto de la seguridad informática se refiere a la protección de la información sensible o privada contra el acceso, divulgación o uso no autorizado. En otras palabras, se trata de garantizar que solo las personas o entidades autorizadas puedan acceder a ciertos datos o recursos.

La confidencialidad en seguridad informática es fundamental para proteger la privacidad y la integridad de los datos, y se logra mediante una combinación de medidas técnicas, políticas y procedimientos diseñados para limitar el acceso no autorizado a la información sensible.

Para lograr la confidencialidad, se utilizan una variedad de técnicas y mecanismos de seguridad, que pueden incluir:

- ✓ **Cifrado de datos:** Consiste en convertir la información en un formato ilegible para cualquier persona que no posea la clave de cifrado correspondiente. Esto asegura que incluso si los datos son interceptados, no puedan ser interpretados sin la clave.
- ✓ **Controles de acceso:** Establecer políticas y procedimientos que regulen quién tiene permiso para acceder a ciertos recursos o información. Esto puede incluir la autenticación mediante contraseñas, biometría u otros métodos de verificación de identidad.

- ✓ **Segmentación de red:** Dividir una red en segmentos o zonas separadas, y controlar estrictamente el flujo de datos entre ellas. Esto ayuda a prevenir que usuarios no autorizados accedan a áreas sensibles de la red.
- ✓ **Políticas de manejo de información:** Establecer reglas claras sobre cómo se manejan y comparten los datos sensibles dentro de una organización. Esto puede incluir la clasificación de la información según su nivel de sensibilidad y la implementación de medidas para protegerla en consecuencia.
- ✓ **Auditorías y monitoreo:** Supervisar activamente el acceso y el uso de la información sensible, registrando las actividades y revisando los registros para detectar posibles violaciones de la confidencialidad.

Integridad

En el ámbito de la seguridad informática, la integridad se refiere a la garantía de que los datos no han sido alterados de manera no autorizada o accidentalmente durante su almacenamiento, procesamiento o transmisión. En otras palabras, se asegura de que la información permanezca precisa, completa y confiable a lo largo de su ciclo de vida.

La integridad en seguridad informática se centra en garantizar que los datos se mantengan precisos, completos y confiables, y se logra mediante una combinación de técnicas criptográficas, controles de acceso, monitoreo y prácticas de respaldo.

Para garantizar la integridad de los datos, se implementan una serie de medidas y controles, que pueden incluir:

- ✓ **Cifrado de datos:** El cifrado no solo protege la confidencialidad de los datos, sino que también puede garantizar su integridad al detectar cualquier intento de modificarlos ilegalmente. Si los datos cifrados son alterados, el proceso de descifrado no será exitoso, lo que indica una alteración.

- ✓ **Firmas digitales:** Las firmas digitales son técnicas criptográficas que permiten verificar la autenticidad e integridad de un mensaje o archivo. Se generan utilizando algoritmos criptográficos y claves privadas, y pueden ser verificadas utilizando claves públicas correspondientes.
- ✓ **Checksums y hashes:** Estos son valores numéricos únicos generados a partir de los datos originales utilizando algoritmos específicos. Son como "huellas digitales" de los datos. Al comparar el valor checksum o hash de un conjunto de datos con el valor original, es posible detectar cualquier cambio en los datos.
- ✓ **Control de acceso:** Limitar el acceso a los datos solo a usuarios autorizados ayuda a prevenir la manipulación no autorizada de los mismos. Además, llevar un registro de quién accede a los datos y cuándo puede ayudar a identificar cualquier actividad sospechosa.
- ✓ **Copias de seguridad y recuperación:** Mantener copias de seguridad de los datos importantes y utilizar procedimientos de recuperación en caso de corrupción o pérdida de datos. Esto ayuda a restaurar la integridad de los datos en caso de incidentes.

Disponibilidad

La disponibilidad se refiere a la garantía de que los recursos de tecnología de la información, como los sistemas, servicios y datos, estén accesibles y operativos cuando sea necesario para los usuarios autorizados. En otras palabras, la disponibilidad asegura que los usuarios puedan acceder a los recursos informáticos y utilizarlos de manera efectiva en el momento en que lo necesiten.

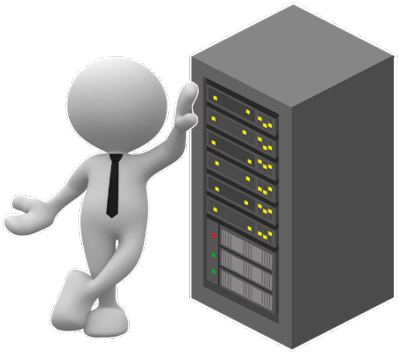
La disponibilidad en seguridad informática se refiere a asegurar que los recursos informáticos estén disponibles y accesibles cuando los usuarios los necesiten, y se logra mediante la implementación de medidas como la redundancia, el balanceo de carga, la escalabilidad y la gestión proactiva del rendimiento y los incidentes.

Para garantizar la disponibilidad de los sistemas y servicios de información, se implementan una serie de medidas y controles, que pueden incluir:

- ✓ **Redundancia:** Esta técnica implica tener duplicados de componentes críticos del sistema, como servidores, redes y dispositivos de almacenamiento. Si un componente falla, otro puede tomar su lugar de manera transparente para los usuarios, evitando interrupciones en el servicio.
- ✓ **Balanceo de carga:** Distribuir la carga de trabajo entre varios servidores o recursos de manera equitativa para evitar que un solo servidor se sobrecargue y afecte la disponibilidad del sistema.
- ✓ **Respuesta rápida a incidentes:** Implementar procedimientos y protocolos de respuesta rápida para abordar y mitigar rápidamente cualquier incidente que pueda afectar la disponibilidad de los sistemas, como ataques cibernéticos, fallos de hardware o desastres naturales.
- ✓ **Escalabilidad:** Diseñar sistemas y servicios informáticos de manera que puedan adaptarse fácilmente a cambios en la demanda, ya sea aumentando la capacidad de almacenamiento, agregando más servidores o utilizando recursos en la nube según sea necesario.
- ✓ **Monitoreo y gestión de rendimiento:** Supervisar de manera proactiva el rendimiento de los sistemas y servicios, identificando y abordando cualquier problema potencial antes de que afecte la disponibilidad para los usuarios finales.
- ✓ **Respaldos regulares:** Realizar copias de seguridad periódicas de datos críticos y mantener un plan de recuperación ante desastres para garantizar la disponibilidad de la información en caso de pérdida o corrupción de datos.

Que entendemos por DATACENTER

Un data center, también conocido como centro de datos, es una instalación física diseñada para alojar una gran cantidad de equipos informáticos y de red, así como para almacenar, procesar y distribuir datos de manera eficiente y segura. En esencia, es un espacio especialmente configurado y equipado para alojar servidores, sistemas de almacenamiento, equipos de red y otros componentes de infraestructura de tecnología de la información (TI).



Que incluye un data center

- ✓ **Infraestructura de energía:** El data center cuenta con sistemas de suministro eléctrico redundantes y sistemas de respaldo, como UPS (Sistemas de Alimentación Ininterrumpida) y generadores diésel, para garantizar un suministro continuo de energía y minimizar la posibilidad de interrupciones.
- ✓ **Sistemas de refrigeración:** Dado que los equipos informáticos generan calor, el data center está equipado con sistemas de refrigeración eficientes, como sistemas de aire acondicionado de precisión o refrigeración líquida, para mantener las temperaturas dentro de los límites operativos seguros.
- ✓ **Seguridad física:** Se implementan medidas de seguridad física, como sistemas de control de acceso, cámaras de vigilancia, sistemas de detección de intrusos y cercas perimetrales, para proteger los equipos y los datos almacenados en el data center contra amenazas físicas.
- ✓ **Conectividad de red:** El data center está conectado a redes de alta velocidad y redundantes para garantizar una conectividad confiable y de alto rendimiento tanto dentro del data center como hacia el exterior, permitiendo la comunicación rápida y eficiente entre los servidores y los usuarios finales.

- ✓ **Gestión de datos y servicios:** Los data centers suelen ofrecer una variedad de servicios relacionados con el almacenamiento y procesamiento de datos, como alojamiento de servidores dedicados, servicios de nube, almacenamiento en red (NAS) y almacenamiento en bloque (SAN).

En pocas palabras, podemos decir que un data center es una instalación crítica para la infraestructura de TI de una organización o proveedor de servicios, proporcionando un entorno seguro, confiable y escalable para alojar y gestionar equipos y datos informáticos.

Que son las "Facilities" en un datacenter

En el contexto de los centros de datos (data centers), el término "facilities" se refiere a las instalaciones físicas y los recursos necesarios para mantener en funcionamiento y asegurar la operatividad del centro de datos en su conjunto.

Estas instalaciones y recursos son fundamentales para garantizar que los equipos informáticos y de red operen de manera eficiente y segura. Algunos ejemplos de las facilities en un data center incluyen:

- ✓ **Infraestructura de energía:** Esto incluye sistemas de suministro eléctrico, como generadores de respaldo, UPS (Sistemas de Alimentación Ininterrumpida) y sistemas de distribución de energía redundante para garantizar un suministro continuo de electricidad sin interrupciones.
- ✓ **Sistemas de enfriamiento:** Dado que los equipos informáticos generan una cantidad significativa de calor, es crucial contar con sistemas de refrigeración eficientes para mantener las temperaturas dentro de los límites operativos seguros. Esto puede incluir sistemas de aire acondicionado de precisión, refrigeración por agua, o incluso sistemas de inmersión en líquido para enfriar los equipos.
- ✓ **Sistemas de seguridad física:** Para proteger los equipos y datos almacenados en el data center, se implementan medidas de seguridad

física, como sistemas de control de acceso, cámaras de vigilancia, cercas perimetrales y sistemas de detección de intrusos.

- ✓ **Sistemas contra incendios:** Los data centers suelen estar equipados con sistemas de detección y extinción de incendios, como rociadores automáticos, sistemas de supresión de incendios con gas inerte y sistemas de detección de humo, para mitigar cualquier riesgo de incendio que pueda surgir.
- ✓ **Sistemas de gestión de agua y humedad:** Para evitar daños por fugas de agua o problemas de humedad que puedan afectar a los equipos electrónicos sensibles, se utilizan sistemas de gestión de agua y humedad, que pueden incluir sistemas de detección de fugas y sistemas de deshumidificación.

Las facilities en un data center son las instalaciones físicas y los recursos necesarios para garantizar la operatividad y la seguridad del centro de datos, incluyendo el suministro de energía, la refrigeración, la seguridad física, la prevención de incendios y la gestión del agua y la humedad.

A continuación, vamos a detallar los diferentes sistemas y subsistemas que componen las "facilities" de un datacenter

Sistema Eléctrico

El suministro eléctrico en un datacenter es fundamental para garantizar el funcionamiento continuo y confiable de los equipos informáticos y los servicios alojados en él. Aquí están algunos puntos importantes a considerar en relación con el suministro eléctrico en un datacenter:

Fiabilidad y Redundancia: La fiabilidad es esencial en un datacenter. Se deben implementar sistemas de suministro eléctrico redundantes para evitar interrupciones en caso de fallos de energía. Esto implica la instalación de sistemas de alimentación ininterrumpida (UPS), generadores de respaldo y circuitos eléctricos redundantes para garantizar la continuidad del servicio incluso durante cortes de energía prolongados.

Capacidad y Escalabilidad: Es crucial dimensionar adecuadamente la capacidad eléctrica del datacenter para satisfacer las necesidades actuales y

futuras de energía. Se debe considerar no solo la carga eléctrica actual, sino también la capacidad de expansión para acomodar el crecimiento futuro de la demanda de energía.

Distribución de Energía: La distribución eficiente de energía dentro del datacenter es esencial para evitar puntos de congestión y garantizar un suministro uniforme a todos los equipos. Esto implica utilizar sistemas de distribución de energía inteligentes, como PDUs (Unidades de Distribución de Energía) con capacidad de monitoreo y gestión remota.

Refrigeración y Eficiencia Energética: La refrigeración es uno de los mayores consumidores de energía en un datacenter. Es importante implementar sistemas de refrigeración eficientes que minimicen el consumo de energía y reduzcan los costos operativos. Esto puede incluir el uso de tecnologías de enfriamiento de alta eficiencia, como la refrigeración por agua o por aire exterior, y el diseño de sistemas de gestión térmica que optimicen la distribución del aire frío y caliente dentro del datacenter.

Monitorización y Gestión: Se deben implementar sistemas de monitorización y gestión del suministro eléctrico para supervisar el consumo de energía, detectar anomalías y realizar ajustes en tiempo real para garantizar la eficiencia operativa y la disponibilidad del servicio. Esto puede incluir el uso de sistemas de gestión de energía (EMS) y sistemas de monitorización de infraestructura (DCIM) para obtener una visibilidad completa del rendimiento eléctrico del datacenter.

Seguridad y Protección: Es importante implementar medidas de seguridad física y protección contra sobretensiones para garantizar la integridad de los sistemas eléctricos y la seguridad de los equipos y del personal. Esto puede incluir la instalación de sistemas de supresión de incendios, sistemas de detección de intrusiones y protecciones contra sobrecargas y cortocircuitos.

El suministro eléctrico en un datacenter es un aspecto crítico que debe ser cuidadosamente planificado, gestionado y monitorizado para garantizar la fiabilidad, la eficiencia y la seguridad de las operaciones informáticas.

Detalle de subsistemas a considerar puntualmente:

Suministro Eléctrico:

- Garantizar un suministro eléctrico confiable y de alta calidad es fundamental para la operación de un datacenter.
- Se deben tener en cuenta fuentes de energía confiables y proveedores de servicios eléctricos que puedan cumplir con los requisitos de disponibilidad y calidad de energía.

Distribución de Energía:

- La distribución eficiente de energía implica diseñar y mantener una infraestructura eléctrica adecuada para llevar la energía desde las fuentes de suministro hasta los equipos informáticos.
- Esto incluye la instalación de tableros eléctricos, conductos y cables de distribución, así como la implementación de sistemas de distribución redundantes para garantizar la continuidad del servicio.

UPS (Sistemas de Alimentación Ininterrumpida):

- Los UPS proporcionan energía de respaldo instantánea en caso de interrupciones en el suministro eléctrico principal.
- Se deben seleccionar UPS con capacidad suficiente para mantener la carga del datacenter durante el tiempo necesario para que los generadores de respaldo entren en funcionamiento.

Grupos Electrógenos:

- Los grupos electrógenos son esenciales para proporcionar energía de respaldo a largo plazo en caso de cortes de energía prolongados.
- Deben estar dimensionados adecuadamente y mantenerse regularmente para garantizar su funcionamiento óptimo en caso de emergencia.

Automatización y Control:

- La automatización y el control de los sistemas eléctricos permiten supervisar y gestionar de manera eficiente el suministro de energía.
- Se pueden utilizar sistemas de gestión de energía (EMS) y sistemas de monitorización de infraestructura (DCIM) para automatizar procesos y realizar ajustes en tiempo real según las condiciones operativas.

Iluminación:

- La iluminación adecuada es importante para garantizar un entorno de trabajo seguro y cómodo dentro del datacenter.
- Se deben utilizar sistemas de iluminación eficientes y de bajo consumo energético, como luces LED, y se deben implementar controles de iluminación para minimizar el desperdicio de energía.

Protección Eléctrica:

- Se deben implementar medidas de protección eléctrica, como interruptores de circuito, fusibles y sistemas de supresión de sobretensiones, para proteger los equipos y la infraestructura eléctrica contra daños causados por fluctuaciones de voltaje, cortocircuitos o sobrecargas.

Etiquetado y Señalización:

- El etiquetado y la señalización adecuados de los equipos eléctricos y los circuitos son importantes para facilitar la identificación y el mantenimiento.
- Se deben seguir normativas y estándares de seguridad eléctrica para garantizar la correcta identificación de equipos, cables y dispositivos de protección.

La planificación, implementación y gestión efectivas del suministro eléctrico en un datacenter son críticas para garantizar la fiabilidad, la eficiencia y la seguridad de las operaciones informáticas. Cada aspecto mencionado

contribuye a mantener un entorno eléctrico robusto y confiable para el funcionamiento continuo del centro de datos.

Sistemas de Enfriamiento (Mecánico)

En el ámbito de los sistemas de enfriamiento para centros de datos, el término "enfriamiento en base a Chillers" y "enfriamiento en base a DX" se refieren a diferentes tecnologías de enfriamiento utilizadas para mantener las temperaturas dentro de los rangos adecuados en los centros de datos. Aquí tienes una explicación de cada uno:

Enfriamiento en base a Chillers (Chiller-based cooling): Los chillers son unidades de refrigeración que utilizan agua o un refrigerante para enfriar el aire. En el contexto de los centros de datos, los chillers a menudo se utilizan en sistemas de enfriamiento por agua. En estos sistemas, el agua se enfría en el chiller y luego se bombea a través de conductos o tuberías para absorber el calor de los equipos informáticos y enfriar el aire en el centro de datos. Este método de enfriamiento es efectivo para grandes instalaciones donde se requiere una gran capacidad de enfriamiento.

Enfriamiento en base a DX (Direct Expansion cooling): Este método de enfriamiento utiliza unidades de aire acondicionado que funcionan con un ciclo de refrigeración de compresión de vapor directo. En el caso de los centros de datos, las unidades DX a menudo se utilizan en sistemas de enfriamiento de precisión para enfriar áreas específicas, como salas de servidores o áreas de racks. Estas unidades funcionan enfriando el aire mediante la evaporación de un refrigerante dentro de una bobina de enfriamiento y luego distribuyendo el aire enfriado a través de conductos o difusores.

Ambos métodos tienen sus propias ventajas y desventajas y son utilizados en función de las necesidades específicas de enfriamiento, el tamaño y la configuración del centro de datos, así como consideraciones de eficiencia energética y costos de operación.

CRAH, InRow InRack y Overhead

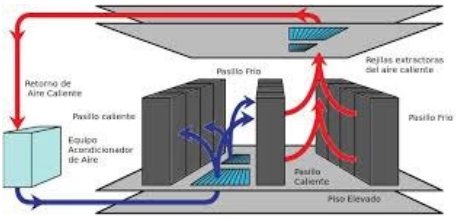
CRAHs, inRow, In Rack y Overhead son diferentes enfoques y configuraciones utilizados en sistemas de aire acondicionado para data centers, cada uno con sus propias ventajas y aplicaciones específicas en función de los requisitos de enfriamiento y diseño del centro de datos.

- ✓ **CRAH (Computer Room Air Handler):** Se trata de un tipo de unidad de manejo de aire diseñada específicamente para ambientes de centros de datos. Los CRAHs son responsables de tomar el aire caliente generado por los equipos informáticos y enfriarlo antes de recircularlo nuevamente en el centro de datos. Estas unidades suelen estar ubicadas en salas de máquinas o en áreas adyacentes a los racks de servidores.
- ✓ **inRow:** Este término se refiere a una configuración de enfriamiento en la que las unidades de aire acondicionado se colocan entre los racks de servidores, en lugar de ubicarse en los extremos de la sala. Esto ayuda a reducir la distancia que el aire refrigerado debe recorrer antes de llegar a los equipos, lo que puede mejorar la eficiencia del enfriamiento y reducir los problemas de recirculación de aire caliente.
- ✓ **In Rack:** Este término se refiere a sistemas de refrigeración que están integrados directamente en los racks de servidores. Estos sistemas pueden incluir ventiladores o unidades de refrigeración líquida que se instalan dentro de los racks para enfriar los equipos directamente. Esto puede ser útil en entornos donde se necesita un control preciso de la temperatura a nivel de rack.
- ✓ **Overhead:** Este término se refiere a sistemas de refrigeración que se montan en el techo o en la parte superior de la sala de servidores para distribuir el aire frío de manera uniforme sobre los racks de servidores. Estos sistemas pueden incluir conductos de aire frío y ventiladores de techo para dirigir el flujo de aire hacia los equipos informáticos.

Estrategias de gestión de aire en datacenters

Pasillo Frío/Caliente:

- **Pasillo Frío:** Es un área en un datacenter donde se suministra aire frío a los equipos informáticos. Los servidores toman este aire para enfriarse, y luego el aire caliente generado se expulsa hacia otro pasillo.



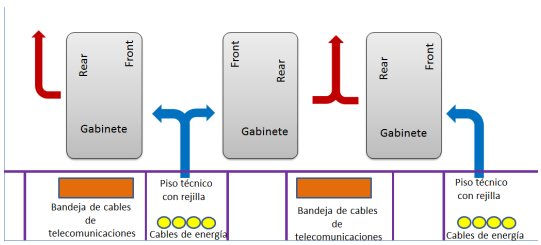
- **Pasillo Caliente:** Es el área donde se expulsa el aire caliente generado por los equipos informáticos. Los servidores liberan el calor en este espacio y luego el aire caliente se extrae del datacenter para su enfriamiento o expulsión al exterior.

Contención de Pasillo Frío/Caliente:

- **Contención de Pasillo Frío:** Consiste en utilizar barreras físicas para aislar el pasillo frío y mantener el aire fresco dentro de él. Esto se logra utilizando puertas o cortinas al final del pasillo y paneles laterales que separan el pasillo frío del resto del datacenter.
- **Contención de Pasillo Caliente:** Similar al pasillo frío, la contención de pasillo caliente implica usar barreras físicas para mantener el aire caliente dentro de este pasillo. Esto ayuda a dirigir el flujo de aire caliente hacia los sistemas de refrigeración o hacia las salidas de aire del datacenter.

Contención de Aire Caliente a través del Techo y Piso Falso

Piso Falso o Elevado: En muchos datacenters, se utiliza un piso falso o elevado para crear un espacio por debajo del nivel del suelo donde se pueden ocultar cables, conductos de aire y otras infraestructuras. Este espacio



también puede ser utilizado para la distribución del aire frío desde los sistemas de enfriamiento hacia los equipos informáticos.

Falso Techo: En combinación con el piso falso, el falso techo se utiliza para contener y dirigir el flujo de aire caliente generado por los equipos informáticos. Este falso techo puede estar diseñado para permitir el paso del aire caliente desde el pasillo caliente hacia los sistemas de enfriamiento, que pueden estar ubicados en el techo o en otra parte del centro de datos.

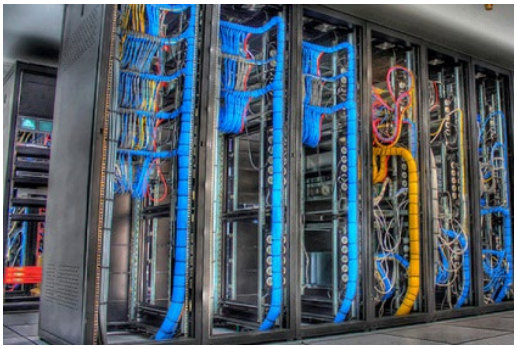
Uso Complementario: La combinación de un falso techo y un piso falso o elevado proporciona una vía eficiente para la contención del aire caliente. El aire caliente generado por los servidores puede ser dirigido hacia el falso techo a través de paneles o deflectores, mientras que el aire frío se suministra desde el piso falso hacia los pasillos fríos donde se encuentran los equipos informáticos.

Optimización del Flujo de Aire: Al utilizar un diseño que incluye tanto un falso techo como un piso falso o elevado, se puede optimizar el flujo de aire dentro del datacenter. Esto ayuda a mantener una separación efectiva entre el aire caliente y el aire frío, lo que contribuye a una refrigeración más eficiente y a un mejor rendimiento de los sistemas informáticos.

También se pueden instalar deflectores o barreras dentro del falso techo para dirigir el flujo de aire caliente de manera más eficiente hacia los sistemas de enfriamiento.

Además de estas estrategias, es importante tener en cuenta otros aspectos de diseño y gestión del datacenter, como la distribución adecuada de los equipos, la utilización de sistemas de enfriamiento eficientes, el monitoreo continuo de la temperatura y la humedad, y la implementación de prácticas de gestión de energía para optimizar el rendimiento y la eficiencia energética del centro de datos.

Cableado de Red



Cuando se trata del cableado de red y la infraestructura de telecomunicaciones en un edificio o centro de datos, Es común encontrarnos con acrónimos como ER, MDA, HDA, IDA, EDA y TR los cuales refieren a diferentes espacios físicos que se utilizan para albergar equipos de red, conexiones y cables, los cuales detallaremos a continuación.

- ✓ **Espacio de Equipos (Equipment Room - ER):** Es el área designada para albergar equipos de red activos, como conmutadores (switches), routers, servidores, y otros dispositivos de red. El ER es donde se concentra la infraestructura de red principal de un edificio o centro de datos.
- ✓ **Área de Distribución Principal (Main Distribution Area - MDA):** Es un espacio dentro del edificio o centro de datos donde se concentran las conexiones principales de cables de red y la distribución primaria de señales de red. El MDA conecta la infraestructura de red del edificio con la red de área amplia (WAN) o el proveedor de servicios de Internet (ISP).
- ✓ **Área de Distribución Horizontal (Horizontal Distribution Area - HDA):** Es el espacio donde se distribuyen los cables de red desde el MDA hacia los diferentes pisos o áreas del edificio. El HDA puede contener conmutadores de distribución de acceso (IDF) y equipos de parcheo para conectar los cables de red a las tomas de red en los pisos o áreas específicas.
- ✓ **Área de Distribución de Identificación (Intermediate Distribution Area - IDA):** Es un espacio intermedio entre el HDA y los dispositivos finales de red, como computadoras y teléfonos. El IDA puede contener conmutadores de distribución de piso (FDH) y equipos de parcheo para conectar los cables de red a los dispositivos finales.

- ✓ **Área de Entrada (Entrance Room - EDA):** Es el lugar donde ingresan los cables de telecomunicaciones desde el proveedor de servicios externo al edificio, como cables de fibra óptica o cables coaxiales. El EDA es el punto de entrada de la red en el edificio.
- ✓ **Telecommunications Room (TR):** Este término se utiliza para referirse a cualquier habitación o espacio dedicado al alojamiento de equipos de red, cables y dispositivos de telecomunicaciones en general. Puede utilizarse como un término genérico para cualquier área que albergue equipos de red y cableado.

Infraestructura de planta externa

La infraestructura de planta externa se refiere a los componentes y sistemas de cableado que se encuentran fuera del área de los racks de servidores y equipos de red.

Esta infraestructura abarca principalmente los cables y dispositivos que conectan el datacenter con el mundo exterior y con otros edificios o instalaciones.

A continuación, indicamos algunas características y componentes comunes de la infraestructura de planta externa en el contexto del cableado de red en datacenters:

- ✓ **Cables de Conexión Externa:** Estos cables son los que conectan el datacenter con proveedores de servicios de telecomunicaciones, proveedores de Internet u otras instalaciones externas. Pueden incluir cables de fibra óptica, cables de par trenzado o cables coaxiales, según las necesidades de conectividad y velocidad requeridas.
- ✓ **Conexiones a Red Externa:** Los datacenters suelen estar conectados a redes externas, como la red de Internet pública o redes privadas de empresas. La infraestructura de planta externa incluye los dispositivos de interconexión, como routers, switches y equipos de interconexión, que facilitan estas conexiones.

- ✓ **Distribución de Energía Externa:** Además del suministro eléctrico interno del datacenter, la infraestructura de planta externa también puede incluir la conexión a la red eléctrica pública y los dispositivos de distribución de energía externos, como transformadores y sistemas de distribución eléctrica secundaria.
- ✓ **Sistemas de Seguridad Externa:** Esto puede incluir sistemas de seguridad perimetral, como cámaras de vigilancia, sistemas de detección de intrusos y cercas perimetrales, que protegen las instalaciones del datacenter y la infraestructura externa asociada.
- ✓ **Acceso y Gestión de Servicios de Utilidad:** Además del suministro eléctrico y de datos, la infraestructura de planta externa puede incluir conexiones a servicios públicos como agua, gas o servicios de telecomunicaciones locales. La gestión adecuada de estos servicios es importante para garantizar el funcionamiento eficiente del datacenter.

La infraestructura de planta externa abarca todos los componentes y sistemas de cableado que conectan el datacenter con el entorno externo, incluyendo redes de datos, suministro eléctrico, servicios de utilidad y sistemas de seguridad. Estos elementos son fundamentales para asegurar la conectividad, la disponibilidad y la seguridad de las operaciones en el datacenter.

Canalizaciones



En el contexto del cableado de red en datacenters, las canalizaciones se refieren a los conductos físicos diseñados para alojar y proteger los cables de red y otros cables utilizados para la transmisión de datos, voz y otros servicios de comunicación. Estas canalizaciones proporcionan una ruta estructurada y ordenada para el tendido de cables, lo que facilita la instalación, mantenimiento y organización del cableado en el entorno del datacenter.

Son componentes estructurales clave que proporcionan una ruta organizada y protegida para el tendido de cables, contribuyendo a la eficiencia, la

seguridad y la fiabilidad de las operaciones de red en el entorno del datacenter.

Aquí hay algunos aspectos importantes sobre las canalizaciones en el contexto del cableado de red en datacenters:

- ✓ **Tipos de Canalizaciones:** pueden ser de diferentes tipos, como bandejas portacables, ductos de piso o techo, canaletas de pared, conductos subterráneos, entre otros. La elección del tipo de canalización depende de factores como la disposición física del datacenter, la capacidad de carga requerida, los requisitos de seguridad y los estándares de la industria.
- ✓ **Organización y Gestión del Cableado:** Proporcionan una estructura para organizar y gestionar el cableado de red de manera ordenada y eficiente. Esto ayuda a minimizar el desorden y el riesgo de daños en los cables, facilitando la identificación, el mantenimiento y la reparación cuando sea necesario.
- ✓ **Protección de los Cables:** Protegen los cables de la exposición a factores ambientales adversos, como la humedad, el polvo, los impactos físicos y el acceso no autorizado. Esto contribuye a la durabilidad y la integridad del cableado, reduciendo el riesgo de fallos y aumentando la vida útil de los equipos de red.
- ✓ **Facilitan la Instalación y Mantenimiento:** Proporcionan una ruta clara y accesible para la instalación inicial y el posterior mantenimiento del cableado de red. Esto facilita la identificación y el acceso a los cables, lo que simplifica las tareas de instalación, reparación y actualización en el datacenter.
- ✓ **Cumplimiento de Normativas y Estándares:** Deben cumplir con las normativas y estándares de la industria en cuanto a seguridad, capacidad de carga, protección contra incendios y acceso a los equipos. Es importante seleccionar y diseñar las canalizaciones de acuerdo con estos requisitos para garantizar la conformidad regulatoria y la seguridad del datacenter.

Medios de comunicación

En el contexto del cableado de red en datacenters, los medios de comunicación se refieren a los diferentes tipos de cables y tecnologías utilizadas para transmitir datos entre los equipos informáticos, servidores, dispositivos de red y otros componentes dentro del entorno del datacenter. Estos medios de comunicación proporcionan la infraestructura física necesaria para establecer conexiones de red y facilitar la transferencia de información.

los medios de comunicación en el contexto del cableado de red en datacenters son los diferentes tipos de cables y tecnologías utilizadas para establecer conexiones de red y facilitar la transferencia de datos entre los equipos y dispositivos dentro del entorno del datacenter. La elección del medio de comunicación adecuado dependerá de los requisitos de rendimiento, distancia, seguridad y coste de la red específica del datacenter.

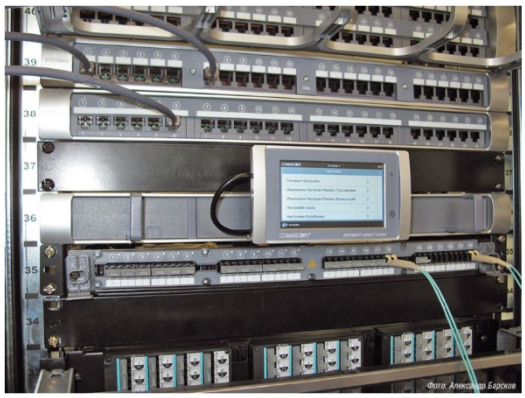
Indicamos a continuación algunos ejemplos comunes de medios de comunicación utilizados en el cableado de red en datacenters:

- ✓ **Cableado de Cobre:** El cableado de cobre, como el cable de par trenzado y el cable coaxial, ha sido tradicionalmente utilizado en redes de área local (LAN) y para la conexión de dispositivos dentro de un datacenter.
  Los cables de par trenzado, en particular, son ampliamente utilizados para la conexión de equipos informáticos y dispositivos de red, ya que ofrecen una buena relación coste-rendimiento y son adecuados para distancias cortas a medianas.
- ✓ **Fibra Óptica:** La fibra óptica es un medio de comunicación que utiliza hilos de vidrio o plástico para transmitir datos mediante pulsos electromagnéticos en el espectro infrarrojo (luz no visible para el ojo humano). En los datacenters, la fibra óptica se utiliza comúnmente para conexiones de alta velocidad y larga distancia, como enlaces de backbone de red, conexiones entre datacenters remotos y conexiones a proveedores de servicios de Internet.
- ✓ **Conexiones Inalámbricas:** Las tecnologías inalámbricas, como Wi-Fi y Bluetooth, también pueden ser consideradas como medios de

comunicación en el contexto del cableado de red en datacenters. Si bien las conexiones inalámbricas no son tan comunes en el cableado interno del datacenter debido a las limitaciones de velocidad y seguridad, pueden utilizarse para proporcionar conectividad en áreas específicas o para dispositivos móviles dentro del datacenter.

- ✓ **Conectividad de Alta Velocidad:** Para aplicaciones que requieren un rendimiento excepcionalmente alto y una latencia mínima, como la interconexión de servidores en clústeres de alta disponibilidad o sistemas de almacenamiento en red de alto rendimiento (SAN), se pueden utilizar medios de comunicación de alta velocidad y baja latencia, como InfiniBand o Ethernet de 10/25/40/100 Gbps y superiores.

Administración y Cableado Inteligente



El término "cableado inteligente" se refiere a una infraestructura de cableado de red que va más allá de simplemente conectar dispositivos mediante cables. Se caracteriza por la integración de tecnología y funcionalidades avanzadas que permiten una gestión más eficiente, segura y adaptable de la red.

El cableado inteligente va más allá de la simple conexión física de dispositivos y ofrece una serie de funcionalidades avanzadas que mejoran la gestión, la seguridad y la eficiencia de la red. Esto lo convierte en una opción atractiva para entornos empresariales y de centros de datos donde se requiere una infraestructura de red altamente adaptable y confiable.

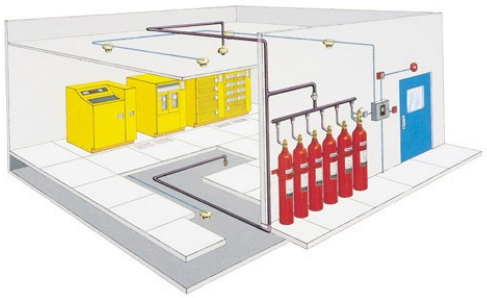
Algunas características comunes del cableado inteligente incluyen:

- ✓ **Gestión centralizada:** Los sistemas de cableado inteligente suelen incluir herramientas de gestión centralizada que permiten supervisar y administrar todos los componentes de la red desde una ubicación

central. Esto facilita la configuración, el monitoreo y el mantenimiento de la red.

- ✓ **Automatización:** Los sistemas de cableado inteligente pueden automatizar ciertas tareas, como la detección de problemas de conectividad, la reconfiguración de la red en respuesta a cambios en la demanda o la asignación dinámica de recursos de red según sea necesario.
- ✓ **Diagnóstico remoto:** Los cables inteligentes pueden incorporar tecnología que permite realizar diagnósticos remotos para identificar y solucionar problemas de red sin necesidad de intervención física en el lugar.
- ✓ **Gestión de energía:** Algunos sistemas de cableado inteligente pueden integrar funciones de gestión de energía que permiten monitorear y controlar el consumo de energía de los dispositivos conectados, lo que puede ayudar a optimizar el uso de la energía y reducir costos.
- ✓ **Seguridad mejorada:** Los sistemas de cableado inteligente pueden incorporar características de seguridad avanzadas, como la autenticación de usuarios, el cifrado de datos y la detección de intrusiones, para proteger la red contra amenazas internas y externas.

Sistema contra incendios



Los sistemas contra incendios en datacenters son críticos para proteger la infraestructura, los equipos y el personal contra los riesgos de incendio. Desde la detección temprana hasta la supresión eficaz y la evacuación segura, cada aspecto es fundamental para garantizar la seguridad y la continuidad de las operaciones en caso de emergencia.

- ✓ **Detección de Incendios:** Los sistemas de detección de incendios en datacenters son críticos para identificar cualquier signo de fuego en sus etapas iniciales. Utilizan detectores de humo, calor o llamas para alertar sobre la presencia de un incendio. La detección temprana es esencial para permitir una respuesta rápida y minimizar el riesgo de daños a los equipos y la infraestructura.
- ✓ **Supresión de Incendios:** Los sistemas de supresión de incendios están diseñados para controlar y extinguir incendios en caso de emergencia. Pueden incluir sistemas de rociadores automáticos, sistemas de extinción de agentes limpios (como el gas FM-200 o el gas inerte) y sistemas de extinción de agentes químicos. La elección del sistema de supresión depende de factores como el tamaño del datacenter, la carga de fuego y los requisitos de seguridad.
- ✓ **Sellado de Penetraciones:** Es importante sellar adecuadamente las penetraciones en paredes, techos y pisos para evitar la propagación del fuego y el humo a través del datacenter. Se utilizan materiales y selladores resistentes al fuego para asegurar que las penetraciones cumplan con los estándares de seguridad contra incendios.
- ✓ **Rutas de Evacuación:** Los datacenters deben contar con rutas de evacuación claramente señalizadas y libres de obstáculos para permitir la evacuación segura del personal en caso de emergencia. Se deben realizar simulacros periódicos de evacuación para garantizar que el personal esté familiarizado con los procedimientos de evacuación y las rutas de escape.
- ✓ **Plan de Emergencia:** Es fundamental contar con un plan de emergencia detallado que establezca los procedimientos y protocolos a seguir en caso de incendio u otras emergencias. El plan de emergencia debe incluir la asignación de roles y responsabilidades, la notificación de autoridades pertinentes, la coordinación con servicios de emergencia externos y la comunicación con el personal y los clientes afectados.

Seguridad

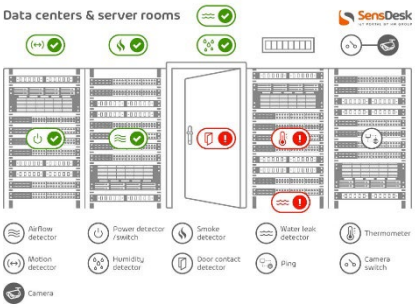
El control de accesos e intrusión, el CCTV y la administración de la seguridad son componentes clave de la seguridad física en datacenters. Estos sistemas y medidas ayudan a prevenir y detectar intrusiones, así como a proteger la infraestructura y los datos críticos almacenados en el datacenter.



- ✓ **Control de Accesos e Intrusión:** El control de accesos se refiere a los sistemas y medidas diseñados para regular quién puede entrar y salir de un datacenter, así como qué áreas pueden acceder dentro del mismo. Esto puede incluir el uso de tarjetas de acceso, lectores biométricos (como lectores de huellas dactilares o reconocimiento facial) y sistemas de autenticación de dos factores para garantizar la identidad de las personas que intentan acceder al datacenter. Los sistemas de intrusión detectan y responden a intentos no autorizados de acceso al datacenter. Estos pueden incluir sensores de movimiento, sensores de puertas y ventanas, y sistemas de alarma que alertan al personal de seguridad sobre posibles intrusiones.
- ✓ **CCTV (Circuito Cerrado de Televisión):** Los sistemas de CCTV consisten en cámaras de video ubicadas estratégicamente dentro y fuera del datacenter para monitorear y grabar actividades. Estas cámaras proporcionan vigilancia en tiempo real y grabaciones de eventos, lo que permite la identificación de intrusos, el seguimiento de movimientos sospechosos y la revisión de incidentes después de que ocurran. Los sistemas de CCTV también pueden integrarse con sistemas de análisis de video y software de gestión de seguridad para una vigilancia más avanzada y eficiente.
- ✓ **Administración de la Seguridad:** La administración de la seguridad implica la implementación y gestión de políticas, procedimientos y controles para proteger la infraestructura y los activos del datacenter. Esto puede incluir la creación y aplicación de políticas de acceso, la

capacitación del personal en prácticas de seguridad, la realización de evaluaciones de riesgos y vulnerabilidades, y el mantenimiento de registros de acceso y eventos de seguridad. La administración de la seguridad también implica la coordinación con equipos de seguridad física y cibernética para garantizar una protección integral del datacenter contra amenazas internas y externas.

Monitoreo



La monitorización de parámetros de operación y la automatización de sistemas son componentes esenciales para garantizar el rendimiento, la disponibilidad y la eficiencia operativa de los datacenters. Estas tecnologías ayudan a detectar y responder a problemas de manera proactiva, optimizar el uso de recursos y simplificar las operaciones diarias para mantener el datacenter funcionando de manera óptima.

- ✓ **Monitorización de Parámetros de Operación:** La monitorización de parámetros de operación implica el seguimiento continuo y la recopilación de datos sobre el rendimiento y el estado de los componentes críticos del datacenter. Esto incluye la supervisión de la temperatura, la humedad, la energía eléctrica, la utilización de recursos informáticos, el tráfico de red y otros indicadores clave de rendimiento (KPIs) que pueden afectar el funcionamiento del datacenter. Los sistemas de monitorización pueden utilizar sensores y dispositivos de supervisión distribuidos en todo el datacenter, así como software de gestión de infraestructura (DCIM) que recopila, procesa y presenta los datos en tiempo real para su análisis y toma de decisiones.
- ✓ **Automatización de Sistemas:** La automatización de sistemas implica la implementación de procesos y procedimientos automáticos para controlar y gestionar las operaciones del datacenter de manera

eficiente y sin intervención humana. Esto puede incluir la automatización de tareas rutinarias, como la gestión de energía, el balanceo de carga, la asignación de recursos informáticos y la gestión del ciclo de vida de los equipos. Los sistemas de automatización pueden basarse en reglas predefinidas, políticas de gestión y algoritmos de optimización para tomar decisiones y ejecutar acciones de manera autónoma, lo que ayuda a mejorar la eficiencia operativa y reducir los errores humanos.

- ✓ **Beneficios:** La monitorización de parámetros de operación y la automatización de sistemas ofrecen varios beneficios, incluyendo una mayor disponibilidad, fiabilidad y eficiencia del datacenter. Estos sistemas permiten detectar y responder rápidamente a problemas potenciales antes de que causen interrupciones en el servicio, optimizar el uso de recursos para maximizar el rendimiento y la eficiencia energética, y simplificar las operaciones diarias al minimizar la intervención manual y los tiempos de inactividad.
- ✓ **Tecnologías Utilizadas:** Las tecnologías utilizadas en la monitorización y automatización de sistemas incluyen software de monitorización de red y sistemas de gestión de infraestructura (como Nagios, Zabbix, Prometheus), así como herramientas de orquestación y automatización (como Ansible, Puppet, Chef) y sistemas de gestión de centros de datos (DCIM).