CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN REDES

FUNDAMENTOS DE HARDWARE

Tema 4. Implantación de un Sistema Informático

Nombre y apellidos: Wuke Zhang
1-ASIR

1. Explica qué es el control de acceso y por qué es importante para la seguridad física de los sistemas informáticos. Describe algunas técnicas de control de acceso que se utilizan en los CPD.

Básicamente, el control de acceso es una forma de controlar quién entra a un lugar y cuándo lo hace. La persona que accede puede ser un empleado, un contratista o un visitante, y puede hacerlo a pie, en coche o en otro medio de transporte.

Solemos llamarlo control de acceso físico para diferenciarlo del control de acceso de espacios virtuales cómo, por ejemplo, cuando se inicia una sesión en cualquier página web.

Algunas técnicas comunes incluyen la autenticación de usuarios, la autorización basada en roles, el control de acceso basado en políticas, y la auditoría y registro de acceso. Estas medidas ayudan a prevenir intrusiones no autorizadas y proteger la integridad, confidencialidad y disponibilidad de la información crítica en los Centros de Procesamiento de Datos (CPD).

2. Describe las características principales de los sistemas de identificación biométrica y su aplicación en la seguridad física de los sistemas informáticos.

Los sistemas de identificación biométrica utilizan características físicas o comportamentales únicas de un individuo para verificar su identidad. Algunas características principales de estos sistemas incluyen:

Unicidad: Cada persona tiene características biométricas únicas, como huellas dactilares, rasgos faciales o patrones de voz.

Inmutabilidad: Las características biométricas tienden a ser estables a lo largo del tiempo y difíciles de alterar o falsificar.

Conveniencia: Los usuarios no necesitan recordar contraseñas o llevar consigo dispositivos de autenticación; simplemente utilizan sus características biométricas naturales.

Precisión: Los sistemas biométricos pueden proporcionar una alta precisión en la verificación de identidad, especialmente cuando se combinan con otras formas de autenticación.

Seguridad: La utilización de características únicas y difíciles de falsificar aumenta la seguridad del sistema.

En cuanto a su aplicación en la seguridad física de los sistemas informáticos, los sistemas de identificación biométrica se utilizan para autenticar y controlar el acceso de usuarios a recursos sensibles. Por ejemplo, las huellas dactilares pueden usarse para desbloquear dispositivos o acceder a áreas restringidas dentro de un Centro de Procesamiento de Datos (CPD). Esto ayuda a prevenir la intrusión no autorizada y fortalece la seguridad física del sistema informático al garantizar que solo usuarios autorizados puedan acceder a recursos críticos.

3. ¿Cuáles son las ventajas y desventajas de utilizar circuitos cerrados de televisión (CCTV) en la seguridad física? ¿Qué medidas adicionales se pueden implementar para mejorar la seguridad?

Las ventajas de utilizar circuitos cerrados de televisión (CCTV) en la seguridad física incluyen:

Disuasión de delitos: La presencia visible de cámaras de CCTV puede disuadir a los delincuentes de cometer actos delictivos en áreas vigiladas.

Vigilancia continua: Las cámaras de CCTV pueden monitorear continuamente áreas específicas, lo que permite una respuesta rápida a incidentes de seguridad.

Recopilación de pruebas: Las grabaciones de video de CCTV pueden proporcionar pruebas útiles para investigaciones posteriores de incidentes, como robos o

vandalismo.

Supervisión remota: Algunos sistemas de CCTV permiten la supervisión remota a través de Internet, lo que facilita la vigilancia de ubicaciones desde cualquier lugar en cualquier momento.

Sin embargo, también existen algunas desventajas, como:

Costo inicial y mantenimiento: La instalación y el mantenimiento de sistemas de CCTV pueden ser costosos, especialmente para grandes áreas o instalaciones.

Privacidad: El uso de cámaras de CCTV puede plantear preocupaciones sobre la privacidad, especialmente si las cámaras graban áreas donde las personas tienen una expectativa razonable de privacidad, como áreas residenciales.

Limitaciones técnicas: Los sistemas de CCTV pueden ser vulnerables a fallos técnicos, como la pérdida de alimentación o el mal funcionamiento de las cámaras, lo que puede comprometer la efectividad del sistema.

Para mejorar la seguridad, se pueden implementar algunas medidas adicionales, como:

Iluminación adecuada: Asegurarse de que las áreas vigiladas estén bien iluminadas puede mejorar la calidad de las imágenes captadas por las cámaras de CCTV y disuadir la actividad delictiva.

Integración con otros sistemas de seguridad: Integrar el sistema de CCTV con otros sistemas de seguridad, como alarmas y sistemas de control de acceso, puede proporcionar una respuesta más completa a los incidentes de seguridad.

Capacitación del personal: Proporcionar capacitación al personal sobre cómo usar y responder adecuadamente a las alertas generadas por el sistema de CCTV puede mejorar la eficacia de la seguridad física.

4. ¿Qué es un SAI y para qué se utiliza? ¿Cuáles son las consideraciones importantes a tener en cuenta al seleccionar y utilizar un SAI?

Un SAI (Sistema de Alimentación Ininterrumpida) es un dispositivo que protege tus equipos electrónicos de los problemas de suministro eléctrico, como cortes, bajadas o subidas de tensión, ruido o picos. Un SAI proporciona una energía limpia y estable a tus

dispositivos, evitando daños, pérdidas de datos o averías.

Al seleccionar y utilizar un SAI, es importante tener en cuenta las siguientes consideraciones:

Capacidad de carga: El SAI debe tener la capacidad suficiente para alimentar todos los equipos que se consideren críticos durante un período de tiempo determinado. Es importante calcular la carga total que se conectará al SAI para garantizar que no se exceda su capacidad.

Tiempo de respaldo: Evaluar el tiempo de respaldo que proporciona el SAI durante un corte de energía. Este tiempo debe ser suficiente para permitir un cierre ordenado de sistemas y dispositivos críticos o para activar una fuente de energía alternativa.

Tipo de onda de salida: Los SAI pueden generar una onda sinusoidal pura, una onda cuadrada o una onda modificada. Es importante seleccionar el tipo de onda de salida adecuado según los requisitos de los equipos conectados. Los equipos sensibles, como servidores y equipos de comunicaciones, suelen requerir una onda sinusoidal pura para un funcionamiento óptimo.

Capacidad de gestión y monitoreo: Algunos SAI ofrecen capacidades de gestión remota y monitoreo que permiten supervisar el estado del dispositivo, la carga de la batería y recibir alertas en tiempo real sobre eventos importantes, lo que facilita el mantenimiento y la administración del sistema.

Protección contra sobretensiones y filtrado de ruido: Buscar un SAI que ofrezca protección contra sobretensiones y filtros de ruido para proteger los equipos conectados contra daños causados por fluctuaciones de voltaje y interferencias eléctricas.

En resumen, al seleccionar y utilizar un SAI, es esencial considerar la capacidad de carga, el tiempo de respaldo, el tipo de onda de salida, las capacidades de gestión y monitoreo, así como la protección contra sobretensiones y el filtrado de ruido para garantizar una protección efectiva de los equipos críticos durante cortes de energía.

5. Describe las características principales de los racks y su aplicación en la organización y seguridad física de los equipos.

Los racks son estructuras diseñadas para organizar y montar equipos electrónicos de manera eficiente en entornos de centro de datos, salas de servidores, redes de telecomunicaciones y otros espacios similares. Algunas características principales de los racks y su aplicación en la organización y seguridad física de los equipos son:

Organización del espacio: Los racks proporcionan un medio para organizar los equipos de TI de manera ordenada y compacta, lo que maximiza el espacio disponible y facilita la gestión de cables.

Montaje en altura: Los equipos se montan en el interior del rack, utilizando unidades de altura estándar, conocidas como "unidades de rack" (U), que facilitan la instalación y la sustitución de equipos de manera uniforme y eficiente.

Ventilación: Los racks suelen estar diseñados con orificios de ventilación en los paneles laterales y traseros para permitir la circulación de aire y evitar el sobrecalentamiento de los equipos.

Seguridad física: Los racks pueden estar equipados con cerraduras en las puertas frontales y laterales para evitar el acceso no autorizado a los equipos. Esto ayuda a proteger los dispositivos contra el robo y la manipulación no autorizada.

Gestión de cables: Los racks suelen incluir canales y ganchos para gestionar los cables de manera ordenada, lo que facilita la identificación, el seguimiento y el mantenimiento de las conexiones.

Acceso y mantenimiento: Los racks están diseñados para facilitar el acceso a los equipos para realizar tareas de mantenimiento, actualización y reparación de manera rápida y sencilla.

6. ¿Cuáles son las principales amenazas ambientales que pueden afectar a la seguridad de los sistemas informáticos en un CPD? ¿Qué medidas se pueden implementar para prevenirlas?

Las principales amenazas ambientales que pueden afectar la seguridad de los sistemas informáticos en un Centro de Procesamiento de Datos (CPD) incluyen:

Incendios: Los incendios pueden dañar equipos y causar pérdida de datos si no se controlan adecuadamente.

Inundaciones: Las inundaciones pueden causar daños graves a equipos electrónicos y sistemas de almacenamiento de datos.

Cortes de energía: Interrupciones en el suministro eléctrico pueden provocar la pérdida de datos y causar daños en equipos sensibles.

Sobrecalentamiento: El sobrecalentamiento puede dañar los equipos electrónicos y provocar fallos en el sistema si no se controla adecuadamente la temperatura ambiente.

Vibraciones y golpes: Vibraciones y golpes pueden afectar negativamente el rendimiento y la integridad de los equipos.

Para prevenir estas amenazas ambientales, se pueden implementar varias medidas, como:

Sistemas de detección y extinción de incendios: Instalar sistemas de detección de incendios, alarmas y extinción automática de incendios para controlar y extinguir rápidamente cualquier incendio que se produzca en el CPD.

Sellado y elevación del suelo: Sellado adecuado de puertas y ventanas para proteger contra inundaciones, y elevación del suelo para evitar el daño por agua en caso de inundaciones.

Sistemas de alimentación ininterrumpida (SAI): Utilizar Sistemas de Alimentación Ininterrumpida para proteger contra cortes de energía y mantener la continuidad de

la energía durante cortes eléctricos.

Sistemas de enfriamiento y ventilación: Implementar sistemas de enfriamiento y ventilación adecuados para controlar la temperatura y prevenir el sobrecalentamiento de los equipos.

Instalaciones físicas seguras: Utilizar armarios y racks resistentes para proteger los equipos contra vibraciones y golpes, y ubicar el CPD en una ubicación segura y protegida.

7. ¿Cuál es el papel de la certificación y las normas de seguridad en la implementación de un CPD seguro y confiable? Enumera algunas de las normas y estándares más importantes en esta área.

La certificación y las normas de seguridad juegan un papel fundamental en la implementación de un Centro de Procesamiento de Datos (CPD) seguro y confiable al proporcionar directrices y requisitos para asegurar la integridad, confidencialidad y disponibilidad de los datos y sistemas. Algunas normas y estándares importantes en esta área incluyen:

ISO/IEC 27001: Es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI). Ayuda a las organizaciones a proteger sus activos de información y gestionar los riesgos de seguridad de manera efectiva.

PCI DSS (Payment Card Industry Data Security Standard): Es un conjunto de estándares de seguridad diseñados para garantizar que las empresas que procesan, almacenan o transmiten datos de tarjetas de pago mantengan un entorno seguro. Es especialmente relevante para los CPD que manejan transacciones con tarjetas de crédito.

ANSI/TIA-942: Es una norma desarrollada por la Asociación de Industrias de Telecomunicaciones (TIA) que establece los requisitos para el diseño y la operación

de un CPD, incluyendo aspectos como la infraestructura física, la seguridad, la capacidad de energía y refrigeración, entre otros.

Uptime Institute Tier Standard: Es un conjunto de estándares desarrollados por el Uptime Institute que clasifica los CPD según su nivel de disponibilidad, desde Tier I (básico) hasta Tier IV (concurrentemente mantenible), lo que ayuda a garantizar la disponibilidad de servicios críticos.

BS 25999 / ISO 22301: Estándar de gestión de la continuidad del negocio que proporciona un marco para desarrollar, implementar y mantener un sistema de gestión de la continuidad del negocio (SGCN), lo que garantiza que las organizaciones puedan mantener operaciones críticas durante interrupciones.