Nombre y apellidos: Víctor Suárez Cruz

-

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.

Un recurso de seguridad proactivo que se utiliza para reforzar la defensa de los sistemas informáticos implementados y prevenir la entrada de individuos no autorizados a los dispositivos en cuestión. Entre las estrategias de control de acceso se pueden incluir tarjetas de identificación, códigos PIN de seguridad, firmas electrónicas, entre otros métodos variados.

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 biométricos son sistemas tecnológicos que permiten reconocer a las personas por sus rasgos biológicos únicos e inalterables, como la huella dactilar, el iris, la voz, etc.

Estos sistemas se usan para verificar o identificar a las personas en diferentes ámbitos, como el control de accesos, la seguridad, la banca, etc.

Para funcionar, estos sistemas capturan el rasgo biométrico de la persona, lo convierten en un patrón digital y lo comparan con una base de datos previamente registrada. Si hay una coincidencia, el sistema confirma la identidad de la persona.

Los sistemas de identificación biométricos se clasifican en dos tipos: biometría física y biometría del comportamiento. La biometría física se basa en una característica estática del cuerpo, como la huella dactilar o el iris. La biometría del comportamiento se basa en una característica dinámica o del comportamiento, como la forma de andar o de firmar.

Los sistemas de identificación biométricos tienen ventajas y desventajas. Entre las ventajas, se destacan su seguridad, su facilidad de uso, su rapidez y su eficacia. Entre las desventajas, se encuentran su coste, su vulnerabilidad a posibles errores o ataques, su invasión a la privacidad y su falta de aceptación social.

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?

Los circuitos CCTV son un sistema de vigilancia que no se detiene mientras el edificio tenga electricidad y que puede detectar amenazas en todo momento. Para reforzar la seguridad,

se puede usar una cámara IP que permite ver lo que se graba desde otro lugar

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 es un Sistema de Alimentación Ininterrumpida que te permite mantener la energía de tus dispositivos electrónicos en caso de que haya un corte o una anomalía en la red eléctrica. Un SAI te puede servir para proteger tus equipos de posibles daños, pérdidas de datos o interrupciones de trabajo.

Al seleccionar y utilizar un SAI, debes tener en cuenta el tipo de SAI, la potencia del SAI y la autonomía del SAI. El tipo de SAI determina el nivel de protección y el rendimiento que ofrece. La potencia del SAI debe ser suficiente para alimentar todos los dispositivos que quieres conectarle. La autonomía del SAI es el tiempo que puede suministrar energía sin recurrir a la red eléctrica.

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

Un rack es una estructura metálica que sirve para alojar y organizar los dispositivos del sistema informático, como switches, routers, bandejas, patch panels y regletas de alimentación. Los racks se pueden clasificar según dos características principales: el ancho y el número de U. El ancho del rack se mide en pulgadas y suele ser de 19, que es el estándar. El número de U indica la cantidad de unidades que caben en el rack y determina

el espacio disponible para los dispositivos. Cuanto mayor sea el número de U, más dispositivos se podrán instalar. Por eso, es conveniente planificar el número de U que se necesitará en el futuro para evitar quedarse sin espacio.

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?

Los CPD son instalaciones que alojan los sistemas informáticos de diferentes sectores y que necesitan una gran inversión y mantenimiento. Para protegerlos de las amenazas ambientales, se deben implementar medidas como: SAI, sistemas de detección y extinción de fuego, sistemas de drenaje y bombeo, sistemas de climatización y control ambiental, sistemas de limpieza y filtrado de aire, sistemas de pararrayos y puesta a tierra, y jaulas de Faraday. Además, se debe elegir una ubicación adecuada para el CPD, que evite riesgos como incendios, inundaciones o terremotos.

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.

Gracias a las distintas certificaciones y normas dirigidas a estandarizar los dispositivos y prácticas relacionadas con los GPD, se puede evitar situaciones donde obtener los materiales necesarios para la implementación cause problemas por fallos de compatibilidad entre dispositivos. Además las regulaciones de seguridad ayudan a crear GPD que eviten problemas para las personas que lo utilizan, evitando la pérdida de datos, como para los demás usuarios que trabajen en el mismo edificio donde se encuentre uno por ejemplo:

Evitando que causen un incendio en un edificio de oficinas y pongan en peligro vidas.Una regulación en este entorno es por ejemplo: La Orden ECE/983/2019 del 26 de Septiembre, la cual regula las características de reacción al fuego de los cables de telecomunicaciones dentro de edificios. La norma ANSI/EIA 310 D_92 que estandariza los gabinetes y racks