SEGURIDAD FÍSICA

Principios de la seguridad física

- La seguridad física esta enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico donde se encuentra ubicado el centro.

- Las principales amenazas que se ven en la seguridad física son amenazas ocasionadas por el hombre como robos destrucción de la información , disturbios, sabotajes internos y externos, incendios accidentales, tormentas e inundaciones.

Control de acceso

- El control de acceso no solo requiere la capacidad de identificación, sino también asociar la apertura o cierre de puertas, permitir o negar acceso, basado en restricciones de tiempo, área o sector dentro de una organización.

- El servicio de vigilancia es el encargado del control de acceso, de todas las personas al edificio, este servicio es el encargado de colocar a los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal. A cualquier personal ajeno a la planta se le solicitara completar un formulario de datos personales, los motivos de la visita, hora de ingreso y salida, etc.

- Teclados

- El uso de credenciales de identificación es uno de los puntos mas importantes del sistema de seguridad, a fin de poder efectuar un control eficaz de ingreso y salida del personal a los distintos sectores de la empresa.

Protección del hardware – Acceso físico

- Tarjetas

Las tarjetas presentan ciertas ventajas:

- Se puede configurar cada tarjeta para que abra ciertas puertas en alguna franja horario
- Tarjetas con caducidad
- Evitar que varios usuarios usen la misma tarjeta a la vez

Estas credenciales se pueden clasificar de la siguiente manera:

- ✓ Normal o definitiva
- ✓ Temporal
- ✓ Contratistas

Protección del hardware – Acceso físico

- Touch memories

Sistemas biométricos

- La biometría es una tecnología que realiza mediciones de forma electrónica, guardad compara características únicas, para la identificación de personas.

Beneficios de una tecnología biométrica:

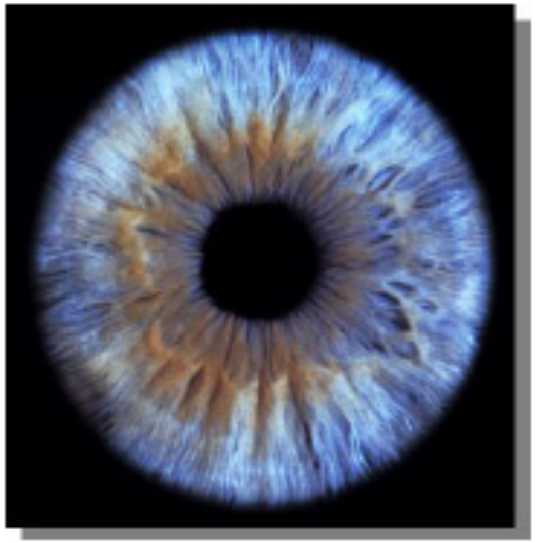
- Pueden eliminar la necesidad de poseer una tarjeta para acceder y de una contraseña difícil de recordar o que finalmente acabe escrita en una papel y visible para cualquier persona.

- Los coste de administración son mas pequeños se realizan un mantenimiento del lector y una persona se encarga de mantener una base de datos. Además las características biométricas son intransferibles a otra persona

- **La emisión de calor**
- **Huella digital**
- **Verificación de la voz**
- **Verificación de patrones oculares**
- **Verificación automática de firmas**

Protección del hardware – Acceso físico

- Sistemas biométricos



Protección del hardware – Acceso físico

- Sistemas biométricos

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Interferen-cias	Gafas	Irritaciones	Suciedad, heridas, asperezas .. .	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...

Protección electrónica

- Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectado los elementos de señalización que son los encargados de hacer saber al personal de una situación de emergencia.

- **Las barreras infrarrojas y de microondas**
- **Detector ultrasónico**
- **Circuitos cerrados de televisión (CCTV)**

Condiciones ambientales

- **Inundaciones**
- **Terremotos**

NMAP

- **Nmap (Network Mapper)** es una excelente herramienta de **seguridad informática** que permite escanear puertos y encontrar servicios y SO que se encuentren instalados en las máquinas analizadas. Esta herramienta es vital para cualquier administrador de red, para saber el estado de sus servidores y equipos y evitar a futuro ataques informáticos a gran escala por desconocimiento del estado de sus dispositivos.

ALGUNOS COMANDOS

- **ESCANEO DE PING**

Permite determinar los hosts que se encuentran activos en una red:

nmap -sP ip-255

- **ESCANEO TCP**

Lista los puertos abiertos y asequible:

Nmap –sT ip

- **ESCANEO TCP SYN**

Este tipo de escaneo se basa en no establecer una conexión completa con el *host* para descubrirlo, esto se logra al monitorear los primeros pasos al establecer una conexión conocidos como el **saludo de tres vías.**

Nmap –sS ip

ALGUNOS COMANDOS

- **Obtener el sistema operativo**

Habilita la detección de sistema operativo de la siguiente manera: nmap –O ip

- **Escaneo de lista**

Este comando permite conocer los nombres de los *hosts* o direcciones IP de aquella dirección que indiquemos, esto incluye la resolución de nombre DNS. Tengamos en cuenta que este tipo de escaneo no le hará *ping* a los hosts ni escaneará sus puertos.

Se obtiene una lista de *hosts* sobre los cuales está operando el **host escaneado** en este momento.

Nmap –sL ip

ALGUNOS COMANDOS

- **Detecta versiones**

Detecta versiones de aplicaciones instaladas.

Nmap –sV ip

- **Sondeo rápido**

Sondeo rápido de puertos

Nmap –F ip