UT3: Control de acceso en el entorno físico.

2º Curso CFGM SMR

Índice.

1. Sistemas de control de acceso.

* Continuamos con la seguridad en el entorno físico …

Entorno físico:
espacio donde se encuentra el sistema de información (locales y edificios).

* En este tema veremos:
  * Mecanismos de SEGURIDAD FÍSICA que tienen relación con el control de acceso, algunos de ellos utilizables también en la protección directa del equipamiento hardware.
  * Los dispositivos dependen:
    - Nivel de seguridad requerido.
    - Impacto de una amenaza.
    - Pérdidas económicas, daños a personas o a la imagen social de la organización.

1. Sistemas de control de acceso.

Tipos de sistemas de control de acceso:

SISTEMAS DEPENDIENTES:
También llamados online, conectados por red y que permiten la supervisión a través de internet. Son los que necesitan la conexión a un ordenador que los gestione.

SISTEMAS AUTÓNOMOS:
Se autogestionan o lo hacen mediante un dispositivo adjunto, con el inconveniente de estar aislados de la red y la ventaja de que se reducen los costes de conexión.
Sistemas autónomos convertibles: son sistemas autónomos que permiten ser configurados para su conexión a un ordenador que controla sus funciones. La conexión será cableada o inalámbrica.

1.1. Personal de vigilancia y control.

* La vigilancia y el control de seguridad pueden asignarse a personal auxiliar de la plantilla de la organización, a vigilantes de seguridad privados u potar por un sistema mixto de vigilancia entre el personal propio de la empresa y externo.

1.2.Teclados.

- Sirven para abrir puertas tras introducir la contraseña correcta.
- Contraseña común a todos los usuarios y se cambia con frecuencia.
- Disponen d una batería y de un sistema atutmático de cierre y apertura de la puerta , que tendrá una cerradura eléctrica.
- Pueden ser de interior o de exterior.
- Los avanzados, permiten personalizar contraseñas por usuario.
- Tienen una limitación en cuanto a número de usuarios (precio).
- Algunos modelos se pueden conectar a un ordenador para registrar las entradas y salidas e intentos fallidos.

1.2.Teclados.

1.3. Tarjetas de proximidad.

- Tienen dos misiones:
  1. Acceso: permitir la entrada al portador de la tarjeta.
  2. Identificación: conocer la identidad del titular de la tarjeta.
- Tarjetas de proximidad: si se acerca la tarjeta al lector, este procede a la identificación y permite el acceso.
- Otros modelos:
  - De banda magnética: sufren más deterioro por el uso.
  - Con código de barras.
- En general son sistemas autónomos.
- Algunos están conectados a un ordenador para dar de alta y de baja las tarjetas.

1.3.Tarjetas de proximidad.

1.3. Tarjetas de proximidad.

- Limitaciones por número de usuarios: hasta miles.
- Hay que borrar a las personas que se han ido de la empresa.
- Se basan en tecnología de identificación por radiofrecuencia (RFID): distancias que van de los 15 cm a los 2 o 3 metros.
- Tipos de tarjetas:
  - Antipassback por áreas: acceso a ciertas zonas.
  - Antipassback por tiempo: tiempo restringido.
  - Antipassback de acceso: impide que varios usuarios utilizan la misma tarjeta a la vez.
  - Fecha de caducidad: fecha y hora a partir de la cual la tarjeta no funcionará.

1.4. Llaves electrónicas de contacto.

- También llamadas touch memories o iButton.
- Es una pastilla electrónica incluida dentro de una carcasa de acero inoxidable y montada en un soporte de material plástico.
- Invulnerable a: polvo, suciedad, calor, agua, campos magnéticos o arañazos.
- Se utiliza poniendo en contacto la parte metálica con el equivalente del lector, que debe estar colocado junto a la puerta de acceso correspondiente.
- Mismas restricciones que las tarjetas de proximidad.

1.4.Touch memories.

1. Sistema de control de accesos.

* ACTIVIDADES 7 – 16.

1.5. Sistemas biométricos.

* Biometría: estudio de métodos que permiten reconocer a seres humanos basándose en factores genéticos o en determinados rasgos físicos o de conducta.

* En los Sistemas de Información: autenticación de personas utilizando tecnologías que usan fórmulas matemáticas complejas para asegurar, con un margen de error nulo o insignificantes que la persona que solicita la entrada a un recurso o a un espacio físico, es quien dice ser.

1.5. Sistemas biométricos.

- Características físicas:
  - Iris, huellas dactilares, palma de la mano, rasgos faciales.
  - ADN, indudable fiabilidad (si no contaminado).
- Hábitos de comportamiento:
  - Forma de andar, firma, escritura manual.
  - Voz: mezcla de característica física y de comportamiento (varía según el momento).
- Historia:
  - China: siglo XIV identificación infantil estampando huellas mano
  - Babilonia y Persia: firmas en papiros con huellas dactilares.
  - Occidente: siglo XIX inventa antropometría. Francis Galton 1892 descubre que las huellas dactilares son irrepetibles e invariables a lo largo de la vida.

1.5.Sistemas biométricos.

- Los métodos de identificación vistos se basan en:
  - Algo que conoces: Ej las contraseñas.
  - Algo que posees: Ej la tarjeta de proximidad.
- Gracias a la biometría, añadimos:
  - Algo que eres o haces (una característica personal).
    - Ventaja: no se olvida, "la clave se lleva encima".
    - La fiabilidad puede acercarse al 100% (huella dactilar).
- Se pueden combinar:
  - Ej: para acceder pasar la mano e introducir un código.
  - Ej: cajeros automáticos: algo que posees (tarjeta) y algo que conoces (la clave secreta).

Proporción uso de sistemas de reconocimiento biométricos.

1.5. Sistemas biométricos.

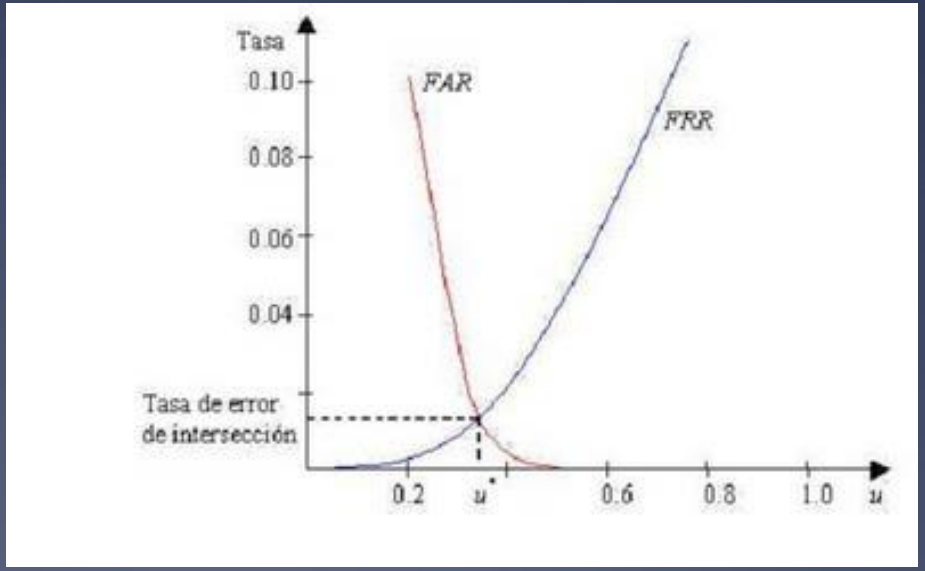
- Indicadores biométricos:
  - Para que un control de acceso con tecnología biométrica sea fiable debe crearse un torno a características humanas que tengan los siguientes indicadores:
    - **Universalidad:** todos los individuos deben poseer la característica.
    - **Unicidad:** esa característica es distinta en cada individuo.
    - **Permanencia:** no se modifica en el tiempo ni a corto ni a largo plazo.
    - **Cuantificación:** puede medirse.

1.5. Sistemas biométricos.

- Características exigibles a un sistema biométrico.
  - **Efectividad:** uso cómodo y rápido para los usuarios.
  - **Aceptabilidad:** no debe provocar rechazo ni poner en peligro la salud ni la integridad física.
  - **Fiabilidad:** ha de ser robusto en el sentido de que los resultados sean fiables y no se pueda trucar ni usar de manera fraudulenta.
- Funcionamiento de un sistema biométrico:
  - El reconocimiento biométrico personal puede utilizarse de dos maneras distintas:
    - Identificación: uso de bases de datos (ADN).
    - Verificación: para verificar que alguien es quien dice (por ej tras introducir user/password, pasar el dedo por lector de huellas dactilares).

1.6.Sistemas biométricos.

- Nivel de exigencia.
  - Alto nivel: alta probabilidad de falsos rechazos (FRR).
  - Bajo nivel: alta probabilidad de falsas aceptaciones (FAR).
  - Gráfica: relación entre ambos.
  - Punto de corte: equilibrio.



1.6.Sistemas biométricos.

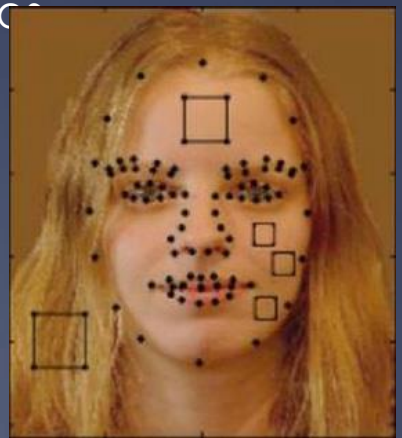
- Iris.
  - Parte que otorga color a los ojos y es inalterable a lo largo de la vida.
  - El lector identificador de iris se colocará próximo a los accesos.
  - Es difícil de falsear.
  - Realiza captura de datos, tras lo cual el software procesa la imagen aplicándole una serie de algoritmos de los que se obtienen unos parámetros que se guardan y se utilizarán posteriormente para permitir o denegar el acceso.

1.6.Sistemas biométricos.

- Manos.
  - Se considera de fiabilidad alta.
  - Consisten en captar el entramado de las venas que discurren por las palmas.
  - La captación se hace desde un dispositivo que emite rayos casi-infrarrojos que al reflejarse en las manos, a causa de una propiedad de la hemoglobina, hace que en la imagen obtenida las venas se muestren de color negro.
  - Del entramado se realizar una imagen digital y se conserva en una base de datos, que servirá para la posterior identificación y permiso de acceso de la persona registrada.
  - Fujistsu es el creador del sistema Palm Secure de identificación para palmas de las manos.

1.6.Sistemas biométricos.

- Reconocimiento facial.
  - **Base:** colocación de puntos sobre la imagen del rostro y en la medición de las distancias entre ellos, como por ejemplo la distancia que hay entre las dos pupilas de un sujeto.
  - Se han comenzado a usar técnicas 3D: añade profundidad.
  - **Funcionamiento:** la persona se pone frente a una cámara de vídeo que capta su imagen, el software de la cámara reconoce los puntos clave del rostro y hace el cálculo de las distancias. Luego los valores se compara con la base de datos para identificar a la persona y permitir o denegar el acceso.
  - **Fiabilidad:** media-baja. Se pueden usar prótesis o añadidos con los años el rostro cambia, la iluminación hace que aparezcan sombras que confundan al sistema.



1.6.Sistemas biométricos.

- Huellas dactilares.
  - Es el sistema más utilizado en todo el mundo.
  - Facilita la tarea de identificar y comparar huellas con bases de datos sin tener que emplear el reconocimiento visual.
  - El sistema empleado para extraer el patrón de las huellas es similar al del iris.
  - La identificación posterior, al contrario que en el iris, se realiza por contacto de dedo identificador sobre la superficie lectora del dispositivo.
  - Se considera de fiabilidad media.

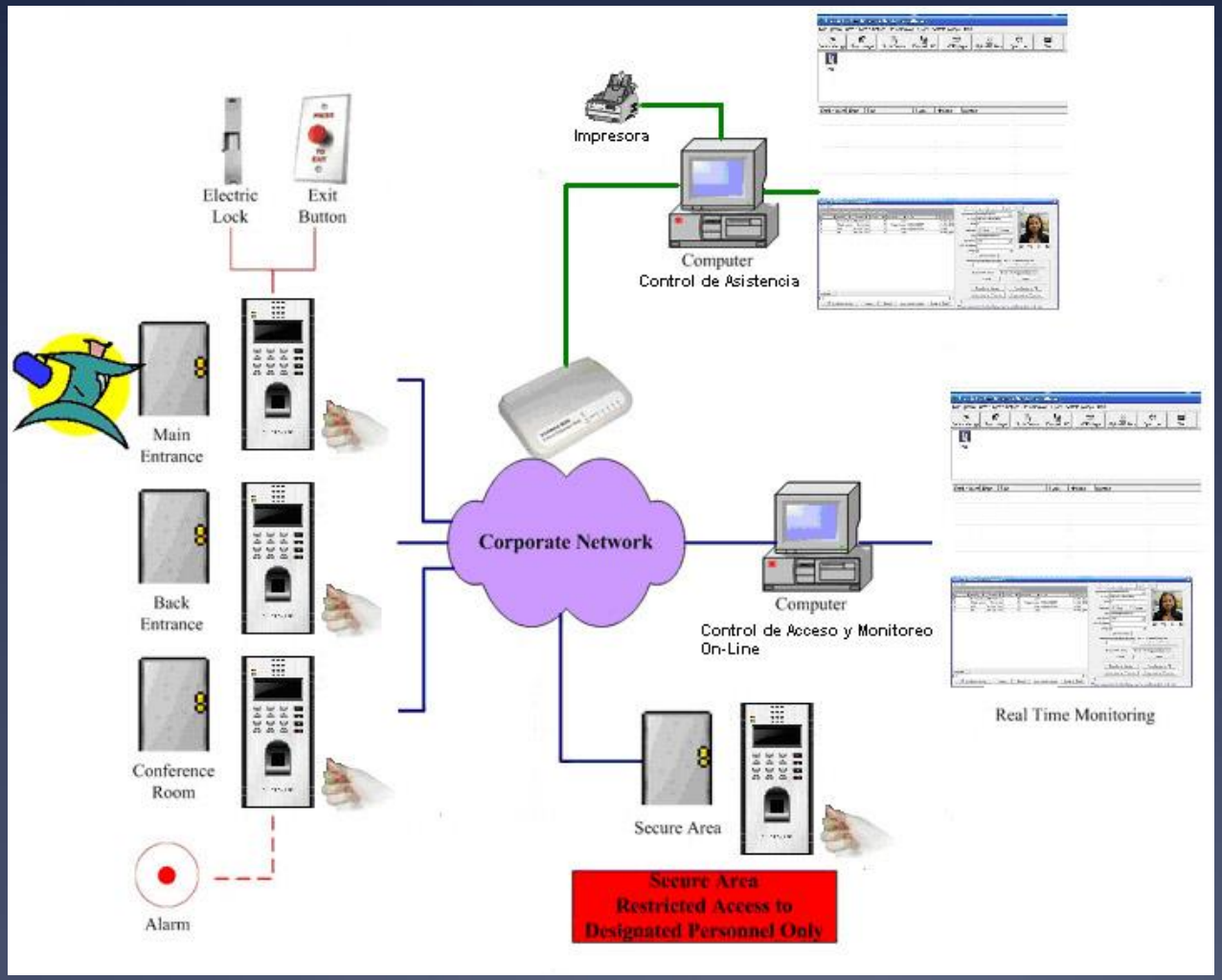
1.5.Sistemas biométricos.

* ACTIVIDADES 17-29.

2. Integración y centralización de sistemas de control de acceso.

- Otros sistemas: tornos, portillas, lector de matrículas de vehículos, etc.
- Todos los sistemas (dependientes y autónomos convertibles) **se pueden centralizar** en un potente ordenador al que estarán conectados y que gestionará esos recursos mediante un software dedicado.
- El software suele ser un **paquete de aplicaciones** integradas que proporciona todas las utilidades necesarias para la gestión y el control de accesos: altas, bajas, modificaciones de usuarios, configuración de tarjetas, confección de nóminas en función de las horas trabajadas, ausencias, retrasos, etc.

2.Integración y centralización de sistemas de control de accesos.



2.Integración y centralización de sistemas de control de accesos.

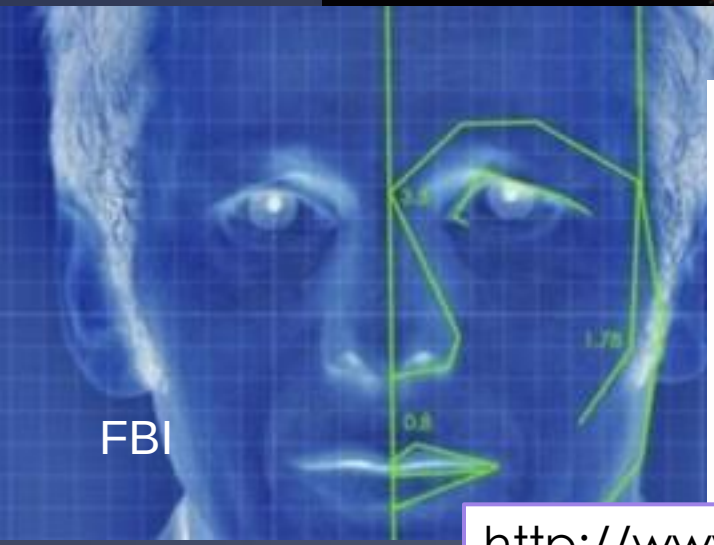
- Algunas empresas que crean o distribuyen en España sistemas de control de acceso físico:
  - Bytech. www.by.com.es Sistema IMBY
  - Fermax www.fermax.es
  - Grupo SDI www.sisdid.com
  - CTS www.controltime.net
  - Inditar www.inditar.com
  - Kimaldi www.kimaldi.com
  - Aike www.aike.com
  - Bodet www.bodet.es Sistema Kelux
  - MMSistemas www.mmsistemas.es

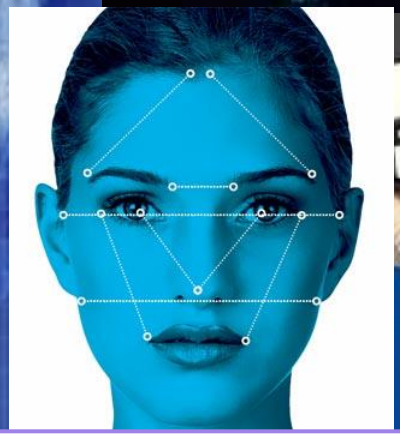
3. Competencias del técnico en SMR.

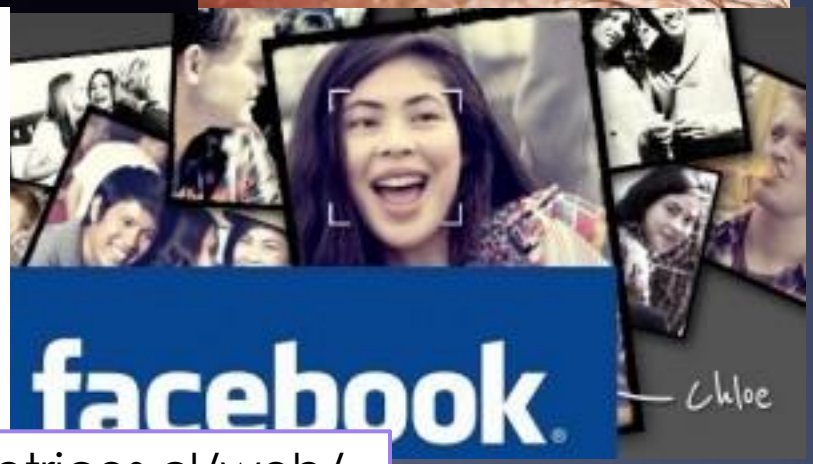
- El estudio de necesidades de cada caso en particular, el presupuesto y la instalación de los sistemas de acceso son realizados por las empresas que los distribuyen o por profesiones de la electrónica.

- La persona que se ocupe de la instalación y mantenimiento del sistema informático y de las redes ha de tener conocimiento de cuáles son las medidas de seguridad que protegen el entorno físico, tanto las que se vieron en la unidad anterior como las relativas al control de acceso, y en la medida de lo posibles, asesorea sobre la conveniencia o no de instalar algunos de estos sistemas.

3. ALGUNOS ARTÍCULOS SOBRE BIOMETRÍA







http://www.sistemasbiometricos.cl/web/