**SEGURIDAD FÍSICA**

La seguridad física de los sistemas informáticos engloba los mecanismos destinados a proteger físicamente cualquier recurso del sistema

**Protección del hardware**

El hardware es frecuentemente el elemento más caro de todo sistema informático. La ubicación es un factor clave para su mantenimiento y protección

* **CPD:** Centro de Proceso de Datos

**Acceso físico:**

1. *Tarjetas:*

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

1. *Touch memories*
2. *Personal de vigilancia y control*
3. *Teclados*
4. *Sistemas biométricos*

**SEGURIDAD FISICA (2)**

**Instalación eléctrica**

**SAI:** Proporcionan al administrador el tiempo suficiente para guardar los datos y apagar el equipo de forma ordenada cuando se produzca un apagón

* **Standby:** Cuando existe corriente eléctrica, hay una línea directa que pasa a través del SAI hasta el ordenador. Cuando detecta que hay un fallo en el suministro activa la alimentación por baterías.
* **On line:** Proporciona constantemente su propia corriente al equipo a la vez que carga sus baterías. Ofrece una tensión de alimentación constante. (CPD)
* **Interactivo:** Ofrece más protección que los Standby, pero la batería dura menos tiempo, ya que ofrece su corriente con más frecuencia

**CONSUMICIÓN DEL SAI**

La potencia real consumida por un determinado equipo electrónico en vatios (W) es el

resultado de multiplicar la tensión (V) y la corriente instantánea (A).

**VA >= W la relación entre ellos es el factor de potencia.**

**FP=W/VA; su valor es siempre menor o igual que 1 (100%)**



**Calcular el tiempo de un SAI en modo baterías**

**Tiempo en min. de duración SAI = ((N x V x AH x Eff ) / VA ) x 60**

**N =** número de baterías en el SAI

**V =** voltaje de las baterías

**AH =** Amperios-Hora de las baterías

**Eff =** eficiencia del SAI

**VA =** Voltiamperios del SAI

**CARACTERÍSTICAS BIOMÉTRICAS:**

Las tecnologías biométricas se usan para reconocer a personas sobre la base del análisis de sus características físicas o de comportamiento

**Conceptos:**

* Universalidad: todos los individuos las tienen
* Singularidad: distinguen a cada individuo
* Permanencia en el tiempo y en distintas condiciones ambientales
* Medibles de forma cuantitativa
* Rendimiento: nivel de exactitud
* Aceptación: por parte del usuario
* Resistencia al fraude y usurpación

**Proceso de registro:**

* **Captura** de los parámetros biométricos.
* **Procesamiento** creando una plantilla con las características personales de los parámetros capturados.
* **Inscripción** de las personas autenticadas mediante el uso de la plantilla

**Proceso de autenticación:**

* **Identificación:** Consiste en la comparación de la muestra recogida del usuario con rasgos biométricos registrados previamente. Compara esta muestra para buscar una coincidencia
* **Verificación:** Identificación del usuario mediante algún nombre de usuario, tarjeta o algún otro método. El sistema recoge la característica biométrica y la compara con la que tiene almacenada. El resultado es positivo o negativo

**Sistemas de identificación biométrica**

* **Dinámicos:** Utilizan tecnologías de comportamiento que comparan acciones o movimientos
* **Estáticos:** Utilizan tecnologías fisiológicas que miden y comparan rasgos físicos
* **Multimodales:** Combinan técnicas estáticas y dinámicas

**2.1 Tecnologías biométricas fisiológicas**

Medición directa de algún rasgo estrictamente físico del cuerpo humano a la hora de identificar personas

**Huella Dactilar:**

Las huellas dactilares son únicas e inalterables.

Es el rasgo biométrico más utilizado para autenticación. Tiene como ventajas su alta tasa de precisión y su facilidad de uso

* **Basada en minucias:** Formas fácilmente identificables existentes en la huella dactilar.
* **Basada en correlaciones:** Analiza el patrón global seguido por la huella dactilar. Se ve afectada por la traslación y la rotación de la imagen



**Reconocimiento facial:**

Técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Se utilizan programas de cálculo que analizan imágenes de rostros humanos

* mediciones como la distancia entre los ojos
* la longitud de la nariz
* ángulo de la mandíbula

Cualquier persona puede modificar visualmente su cara de manera sencilla utilizando unas gafas de sol o dejándose crecer la barba

**Reconocimiento de iris:**

Los patrones de iris vienen marcados desde el nacimiento y rara vez cambian.

Cuenta con más de 200 propiedades únicas.

El escaneado del iris se lleva a cabo con una cámara de infrarrojos especializada que ilumina el ojo realizando una fotografía de alta resolución.

* No existe ningún riesgo para la salud
* Más resistentes al fraude

**Reconocimiento de la geometría de la mano:**

Utiliza la forma de la mano para confirmar la identidad del individuo. Las características extraídas incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general.

Una inflamación o una lesión, pueden variar la estructura básica de la mano dificultando la autenticación.

**Reconocimiento de retina**

Utilización del patrón de los vasos sanguíneos contenidos en la misma. Cada patrón es único y se mantiene invariable a lo largo del tiempo. Entornos de alta seguridad.

* Tasa de fallos prácticamente nula.
* Necesaria la total colaboración por parte del usuario

Requiere que el usuario permanezca inmóvil y muy cerca del sensor durante la captura de la imagen

**Reconocimiento vascular:**

Se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. Es interno, por esta razón no deja rastro y sólo se puede conseguir en presencia de la persona. Es por tanto muy difícil el robo de identidad.

Tiene una alta seguridad y se usa en las ocasiones que el dedo no esté limpio.

**2.2 Tecnologías biométricas de comportamiento**

Proceso de identificación de rasgos derivados de una acción realizada por una persona, Incluyen la variable tiempo, ya que toda acción tiene un comienzo, un desarrollo y un final

**Reconocimiento de firma:**

Analiza la firma manuscrita para confirmar la identidad del usuario firmante.

* **Comparación simple:** se considera el grado de parecido entre dos firmas, la original y la que está siendo verificada.
* **Verificación dinámica:** se hace un análisis de la forma, la velocidad, la presión de la pluma/bolígrafo y la duración del proceso de firma.

**Reconocimiento de escritor:**

Averigua o confirma la identidad del autor de un determinado texto manuscrito valiéndose de un software OCR. Cada persona tiene un grado de inclinación en la escritura y nivel de presión al escribir.

***Los sistemas dinámicos ofrecen mejores tasas que los estáticos***

* **Estático:** los usuarios escriben sobre papel; la imagen se sube al ordenador mediante una cámara de fotos. Esta modalidad también se conoce como «off-line».
* **Dinámico:** los usuarios escriben sobre una tableta digitalizadora, tablet, etc., que adquiere la escritura en tiempo real. Esta modalidad también recibe el nombre de «on-line»

**Reconocimiento de voz:**

Usan sistemas de inteligencia artificial para aprender a identificar voces. Miden y estiman la similitud entre las muestras para devolver un resultado o una lista de posibles candidatos.

La utilización de este método está más extendida en sistemas de respuesta por voz y en centros de atención de llamadas telefónicas

**Reconocimiento de escritura de teclado:**

Se basa en el hecho de la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. Se mide la fuerza de teclear, la duración de la pulsación y el periodo de tiempo que pasa entre que se presiona una tecla y otra.

De este modo el coste de implantación se centraría en el software

**Reconocimiento de la forma de andar:**

Toma como referencia la forma de caminar de una persona. Este acto se graba y se somete a un proceso analítico que genera una plantilla biométrica única de dicho comportamiento.

Aún está en desarrollo

**SISTEMAS BIOMÉTRICOS:**

