

Ingeniería en Sistemas de Información

Ciberseguridad

Docente: Ing. Gabriela Nicolao
Ayudantes: Ing. Luciano Sebastianelli,
Matías Baghdassarian



Sistemas y Metodologías de Control de Acceso



Introducción a los sistemas y metodologías de control de acceso

► Requisitos:

- Evitar proveer información sensible a usuarios no autorizados. (Confidencialidad)
- Proveer información sensible a usuarios autorizados. (Disponibilidad)
- Confiable (integridad)
- Escalable (Duradero)

► Tipos:

- Administrativos
- Físicos
- Técnicos

Introducción a los sistemas y metodologías de control de acceso

- ▶ **Sujeto:** Es una entidad activa que solicita acceso a un objeto.
 - Ejemplos: usuarios, programas, procesos, computadoras, etc.

- ▶ **Objeto:** Es una entidad pasiva que contiene información o realiza una función.
 - Ejemplos: archivos, programas, documentos, impresoras, etc.

Introducción a los sistemas y metodologías de control de acceso

- ▶ La transferencia de información desde un **objeto** a un **sujeto** es llamada **acceso**.
 - El control de acceso es la habilidad de otorgar el acceso a un sistema u otro recurso que se desea controlar.
- ▶ El control de acceso se implementa para asegurar la confidencialidad, integridad y disponibilidad.



Identificación, Autenticación y Autorización

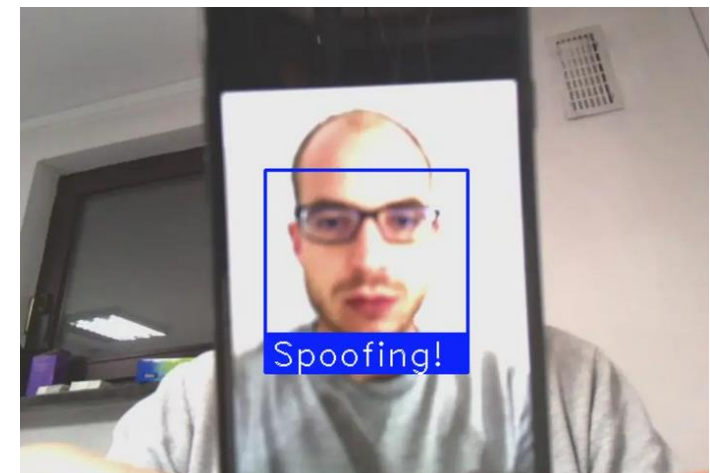
- ▶ **Identificación:** Es un mecanismo para diferenciar los sujetos.
 - Por ejemplo: Nombre de usuario, numero de proceso, etc.
- ▶ **Autenticación:** Permite asegurar (con un determinado nivel de certeza) que el sujeto es quien dice ser.
- ▶ **Autorización:** Es el mecanismo utilizado para definir si el sujeto tiene o no acceso a determinados objetos.
 - Ejemplo: Listas de control de acceso, Control de acceso mandatorio, etc.



Identificación, Autenticación y Autorización

- ▶ **Trazabilidad (Accountability):** Habilidad para determinar las acciones individuales de un usuario dentro de un sistema. Esta soportado por logs de auditoría.
- ▶ **No repudio:** El sujeto no puede negar que realizó cierta acción. Por ejemplo: En el envío de mensajes el no repudio del origen el emisor no puede negar que envió el mensaje.

ReportResults				
Audit Trail report was run on 23 Jan 2020 12:57 PM by DIANA HUDSON				
Date/Time ^	Patient	User	Section	Action
22 Jan 2020 11:24 AM	STACEY JAY	dianahudson@kareotest.com	Patient Chart	View
22 Jan 2020 11:24 AM	REBECCA AN	dianahudson@kareotest.com	Patient Chart	View
22 Jan 2020 11:25 AM	CHRISTY ARNETT	dianahudson@kareotest.com	Patient Chart	View
22 Jan 2020 11:25 AM	SAVANNAH CANNON	dianahudson@kareotest.com	Patient Chart	View
22 Jan 2020 12:11 PM	SAVANNAH CANNON	dianahudson@kareotest.com	Demographics	View
22 Jan 2020 12:11 PM	SAVANNAH CANNON	dianahudson@kareotest.com	Demographics - Address	View
22 Jan 2020 12:11 PM	SAVANNAH CANNON	dianahudson@kareotest.com	Patient Chart	View
22 Jan 2020 01:07 PM	SHIRLEY BISHOP	dianahudson@kareotest.com	Demographics	View
22 Jan 2020 01:07 PM	SHIRLEY BISHOP	dianahudson@kareotest.com	Demographics - Address	View
22 Jan 2020 01:07 PM	SHIRLEY BISHOP	dianahudson@kareotest.com	Demographics - Address	View



Tipos o factores de autenticación

▶ Autenticación basada en Secretos

- “Algo que uno conoce”
- Ejemplo: contraseñas, pin, etc.



▶ Autenticación basada en la posesión de elementos

- “Algo que uno tiene”
- Ejemplo: tarjeta, token, llaves, etc.



▶ Autenticación basada en elementos biométricos

- “Algo que uno es”
- Ejemplo: huella, voz, etc.



Autenticación Fuerte

- ▶ Aquellos sistemas que requieren la autenticación de 2 factores diferentes de forma conjunta.
 - Ejemplo: Contraseña + Tarjeta de coordenadas

INGRESE DESDE AQUÍ PARA OPERAR

Su número de Documento

Su clave Santander Río

Su usuario

ACEPTAR **TECLADO VIRTUAL**

PRIMER INGRESO

SI YA OPERA CON ONLINE BANKING

CAMBIÓ SU CLAVE SANTANDER RÍO

OLVIDÓ SU USUARIO

OLVIDÓ SU CLAVE SANTANDER RÍO

	A	B	C	D	E	F	G	H	I
1	07	45	77	85	23	23	24	23	24
2	94	78	83	68	75	75	44	75	44
3	75	09	93	16	16	16	51	16	51
4	63	40	65	39	39	39	92	39	92
5	20	75	13	38	38	38	58	38	58
6	85	54	38	45	45	45	76	45	76
7	74	51	77	86	86	86	07	86	07
8	18	42	85	61	61	61	54	61	54
9	76	96	98	03	03	03	12	03	12

C4 D8

- ▶ Se considera fuerte porque las debilidades de un factor son mitigadas por el segundo factor.

Autenticación basada en hashes

1. El sujeto configura sus credenciales por primera vez y se calcula y guarda el hash (“H1”) de la contraseña en el servidor de autenticación.
2. El sujeto informa sus credenciales (ID + Contraseña).
3. El autenticador calcula el hash de la contraseña, obteniendo “H2”.
4. El autenticador busca el hash almacenado correspondiente al ID del usuario, obteniendo “H1”.
5. El autenticador compara “H1” con “H2”. Si son iguales, entonces la autenticación es correcta.

Si un atacante pudiera robarse el almacenamiento de credenciales, obtendría hashes y no las contraseñas en plano (al menos inicialmente).

No es necesario y no se sugiere almacenar la contraseña.

Amenazas a la autenticación basada en Secretos

- ▶ Ataques de diccionario / fuerza bruta.
 - Probar opciones de contraseñas hasta dar con la correcta.
- ▶ Password Spray.
 - Probar múltiples usuarios con la misma contraseñas débiles o default.
- ▶ Análisis de tráfico de red.
 - Buscar credenciales observando los protocolos.
- ▶ “Spoofing” del dispositivo autenticado.
 - Engañar al sujeto para que se autentique en un objeto falso.
- ▶ Intentar obtener acceso a los mecanismos de autenticación basado en secretos, por ejemplo:
 - Archivo “/etc/shadow” de Linux.
 - SAM (Security Access Manager) de Windows.
 - Base de datos de usuarios, por ejemplo Directorio IDM.

Contramedidas a las amenazas a la autenticación basada en Secretos

- ▶ No utilizar palabras de diccionario.
- ▶ No utilizar contraseñas triviales.
- ▶ Bloqueo de la cuenta tras ciertos intentos fallidos.
- ▶ Implementar retraso luego de ciertos intentos fallidos.
- ▶ Implementación de captchas.
- ▶ Forzar el uso de contraseñas con números, mayúsculas, minúsculas, establecer longitud mínima, etc.
- ▶ Forzar el cambio de contraseña periódico.
- ▶ No permitir el uso de credenciales anteriores.

- ▶ Son dispositivos generadores de contraseñas que un sujeto lleva con él.
- ▶ Existen 4 tipos de Tokens:
 - Tokens estáticos
 - Tokens sincrónicos basados en tiempo
 - Tokens sincronicos basados en eventos
 - Tokens asincronicos basados en desafío respuesta
- ▶ Pueden ser dispositivos físicos o “software Tokens”



Token estáticos

- ▶ Pueden requerir una contraseña.
- ▶ Pueden almacenar una clave, credenciales de login encriptadas, etc.
- ▶ Son utilizados principalmente como técnica de identificación en lugar de autenticación.
- ▶ Ejemplos:
 - Dispositivo USB
 - Tarjeta inteligente



Token sincrónicos basado en tiempo

- ▶ Los dispositivos y el servidor tienen relojes que miden el tiempo transcurrido desde la inicialización.
- ▶ Cada cierto tiempo la clave generada se muestra en la pantalla del dispositivo. El usuario ingresa su clave en el sistema al cual se quiere autenticar.
- ▶ Como el servidor esta sincronizado con el dispositivo, la clave generada por el servidor debe coincidir con la clave generada por el dispositivo para que el usuario sea aceptado.



Token sincrónicos basado en eventos

- ▶ Las claves se generan en el dispositivo debido a la ocurrencia de un evento.
 - Ejemplo: Botón presionado en el dispositivo.
- ▶ El usuario debe ingresar la clave en el sistema al cual se quiere autenticar.
- ▶ El servidor compara la clave con un listado de claves que tiene.
 - Si esta, el usuario se autentica y esa clave se elimina.
 - Si no está, el usuario no se autentica.



Token asincrónicos Desafío – Respuesta

- ▶ El servidor de tokens genera una cadena de dígitos aleatoria (desafío).
- ▶ El sujeto ingresa esa cadena en el dispositivo, la cual le aplica un algoritmo y genera la clave (respuesta).
- ▶ El resultado de esa función es enviado nuevamente al servidor de token, quien realiza la misma operación. Si el resultado es igual, el usuario es autenticado.

	A	B	C	D	E	F	G	H	I
1	07	45	55	85	34	20	73	79	70
2	08	46	25	44	39	90	83	89	75
3	01	55	15	65	38	99	93	69	50
4	87	48	05	35	74	69	27	87	55
5	07	35	55	25	84	25	26	59	29
6	09	43	55	82	24	24	26	80	30
7	77	25	55	15	44	23	53	39	79
8	67	42	55	80	14	19	43	78	78
9	57	15	55	95	94	09	23	23	76

Nro. de serie: 0192 070 0223

B6: 43 H8: 83



Amenazas en los Tokens físicos

- ▶ Robo del token físico
- ▶ Clonado del token
- ▶ Ataques a la tarjeta de coordenadas mediante phishing:
 - Se le solicita al usuario que complete todos los casilleros de la tarjeta de coordenadas en un sistema que tiene el atacante.
 - Se solicita foto de la tarjeta.

Contramedidas a la amenaza a la Autenticación basada en la posesión de elementos

- ▶ Capacitación
- ▶ Denuncia del token
- ▶ Autenticación Fuerte

Software Tokens

- ▶ Hay distintas implementaciones que permiten agregar un segundo factor de autenticación sin una alta inversión de hardware y aumenta la seguridad del sistema.
 - Ejemplo: JWT (Json Web Token)

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "HS256",  "typ": "JWT"}
```

PAYLOAD: DATA

```
{  "sub": "1234567890",  "name": "John Doe",  "iat": 1516239022}
```

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  your-256-bit-secret)
```

your-256-bit-secret

☐ secret base64 encoded

✔ Signature Verified

SHARE JWT

Amenazas en los Software Tokens

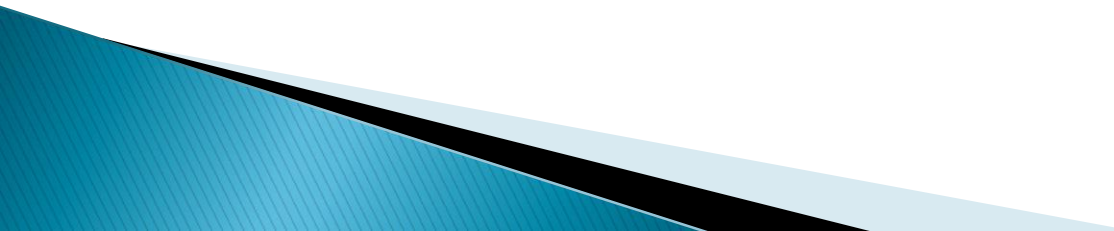
- ▶ Mala implementación.
- ▶ Falta de firma.
- ▶ Manipulación de los campos que generan el Token.

Contramedidas a la amenaza a la Autenticación basada en Software Tokens

- ▶ Utilización de firma para los tokens.
- ▶ Agregar en el JWT solo los datos necesarios.
- ▶ Validar en backend los datos del JWT.

Sistema Biométrico – Proceso

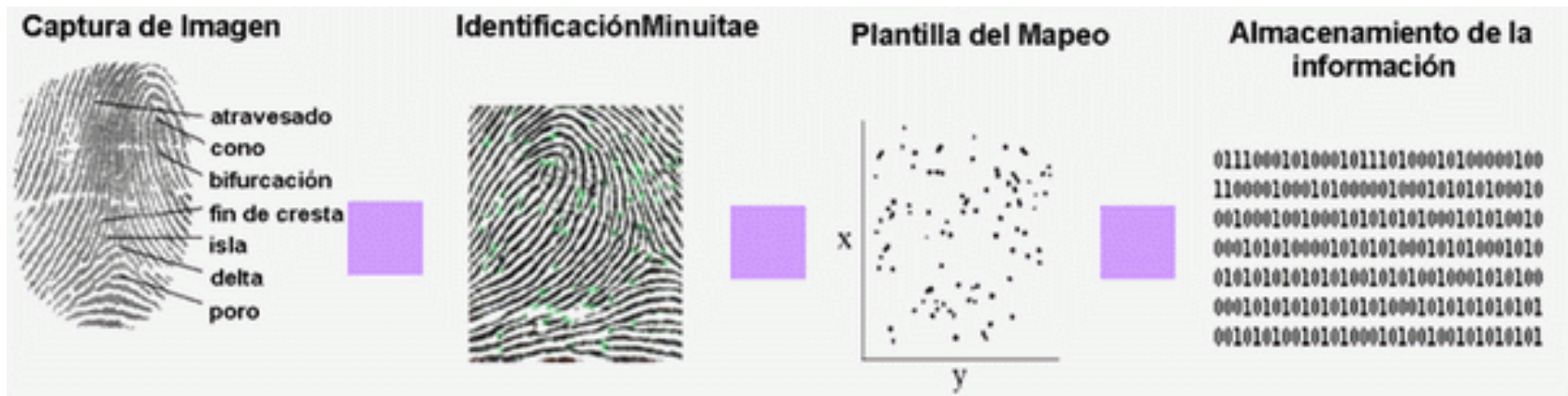
Los sistemas biométricos se basan en características físicas del sujeto a identificar (Huellas digitales, Reconocimiento retina/iris, geometría de mano) o en patrones de conducta/comportamiento (registro vocal, firma a mano alzada).

1. Extracción de ciertas características de la muestra.
 2. Comparación de ciertas características con las almacenadas en la base de datos.
 3. Finalmente la decisión de si el usuario es válido o no.
- 

Sistemas biométricos – Huella Dactilar

► Proceso

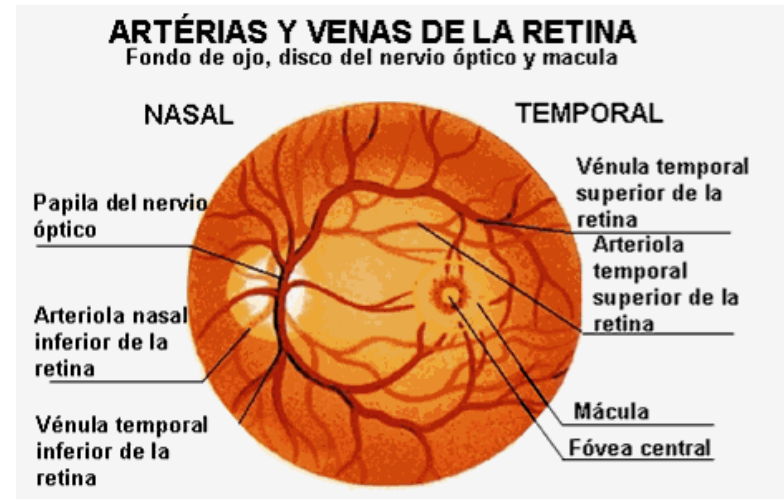
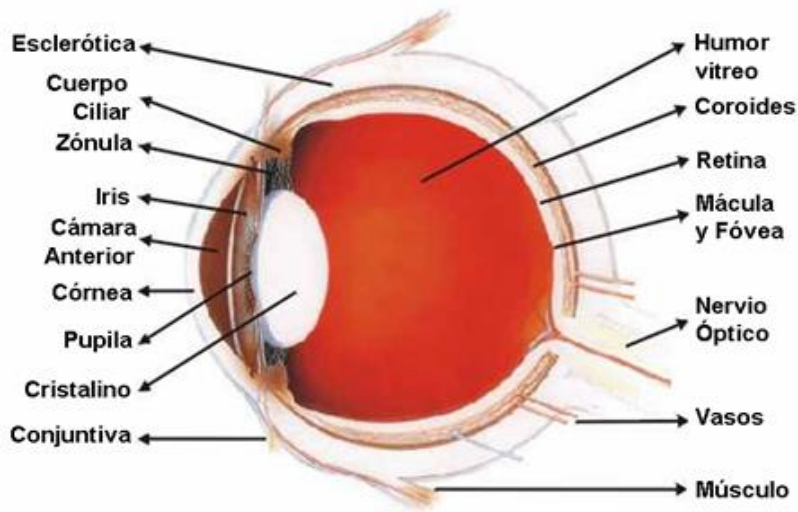
- Toma de una imagen.
- Procesamiento y guardado en una base de datos.
- Extracción de puntos característicos.
 - Arcos, bucles, remolinos.
- Comparación contra la base de datos.
 - Basada en minucias.
 - Basada en patrones.



Sistemas biométricos – Retina

► Proceso

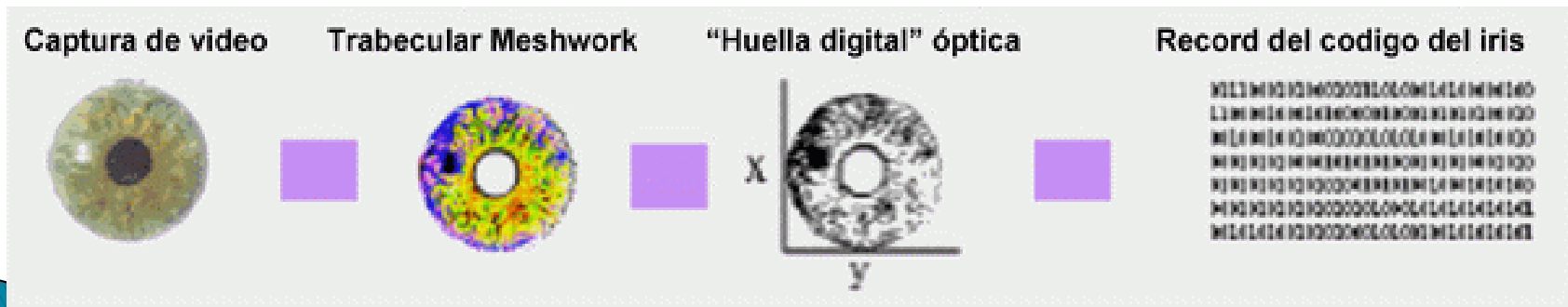
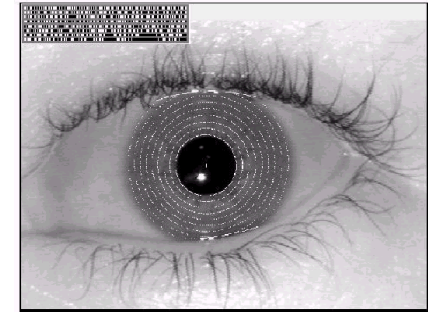
- Se mira a través de binoculares a un punto (existen dispositivos de mayor distancia).
- Se escanea la retina con radiación infrarroja de baja intensidad en forma de espiral.
- Se detectan nodos y ramas del área retinal.
- Se comparan con la base de datos.



Sistemas biométricos – Iris

► Proceso

- Se captura una imagen del iris en blanco y negro.
- Se somete a deformaciones pupilares.
- Se extraen patrones y realizan transformaciones matemáticas.
- Esa muestra se denominada iriscode.



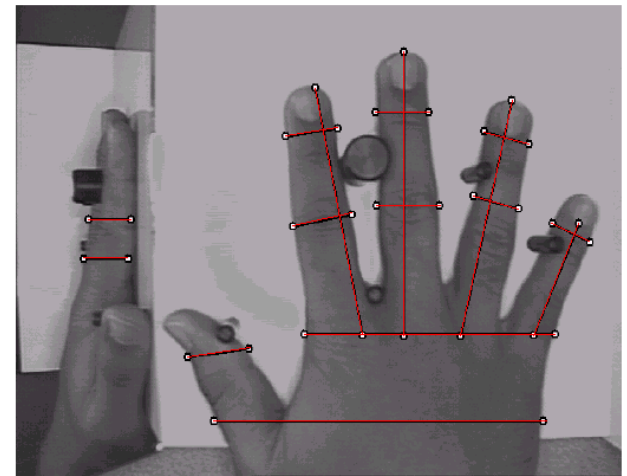
► Proceso

- Se sitúa la mano sobre un dispositivo lector con guías que marcan la posición correcta
- Se toma una imagen superior y otra lateral, de las que se extraen los datos
- Se transforman los datos en un modelo matemático que se contrasta contra una base de patrones



Código de la mano

43BFFFA60

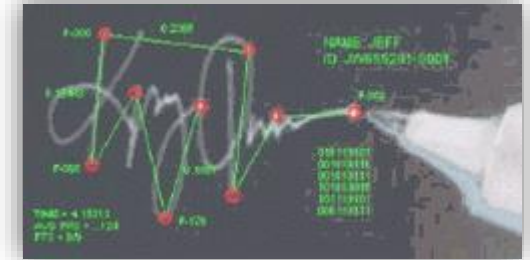


Sistemas biométricos – La firma

- ▶ Estamos acostumbradas a firmar para identificarnos:
 - Alta aceptación social.

- ▶ Existen dos líneas de investigación
 - Reconocimiento de firma estática (offline)
 - Se parte de firmas realizadas previamente.
 - Se extraen las características extraídas de la firma (geometría en 2D).

- ▶ Reconocimiento de firma dinámica (online)
 - La información se adquiere durante el firmado
 - La información dinámica es más difícil de falsificar
 - Requiere dispositivos digitalizadores
 - Se dispone de información temporal (duración, posición, velocidad)



Elección de Sistemas biométricos

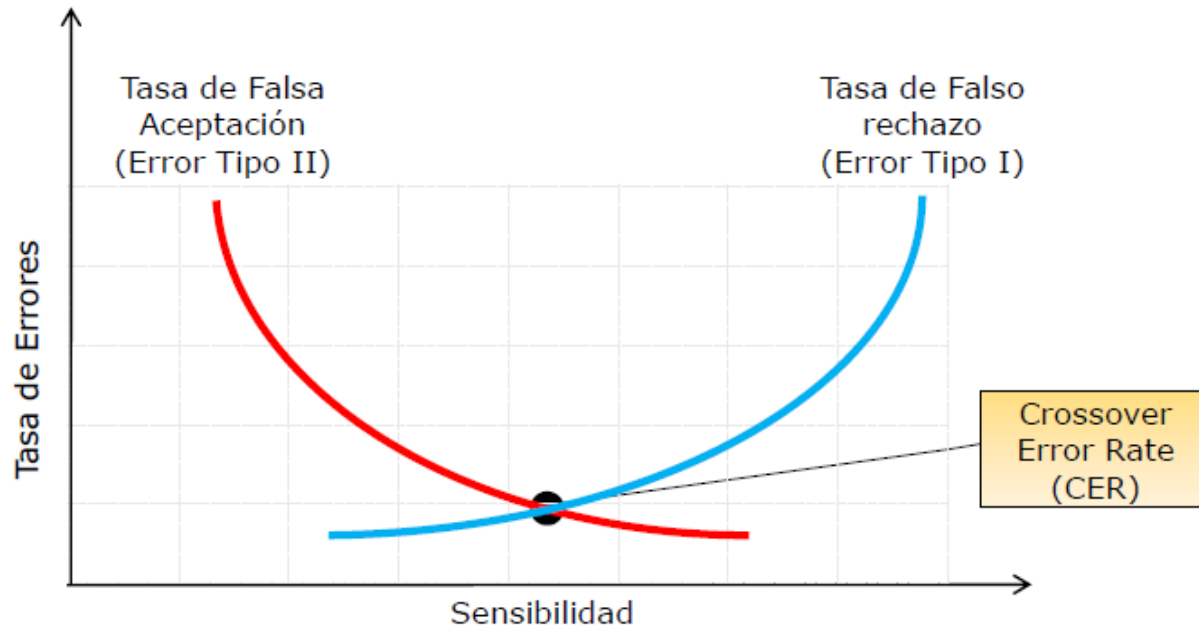
- ▶ Además de los costos hay ciertos puntos críticos a determinar a la hora de elegir un sistema biométrico como método de control de acceso:
 - Aceptación del usuario.
 - Tiempo de registración (la toma de la muestra inicial).
 - Tiempo de ingreso.
 - Precisión.
 - Facilidad de implementación.
 - Tamaño y manejo de las muestras.

Amenazas a la Autenticación basada en elementos biométricos

- ▶ Dispositivos muy sensibles.
 - Error tipo 1: Tasa de falsos rechazos.
- ▶ Dispositivos poco sensibles.
 - Error tipo 2: Tasa de falsas aceptaciones.

Contramedidas a las amenazas a la Autenticación basada en elementos biométricos

- ▶ Contar con dispositivos bien configurados.
 - El punto CER es usado como estándar para evaluar la performance de los dispositivos biométricos.



Gestión de Identidades

- ▶ Tecnologías usadas para gestionar la información de un sujeto.
- ▶ Centralización de la administración de usuarios/contraseñas.
- ▶ Ejemplos de proveedores:
 - CyberArk, ForgeRock, IBM, Microsoft, Okta, Oracle.
- ▶ Ventajas:
 - Sincronización y utilización de contraseñas fuertes.
 - ABM de usuarios automatizada.
 - Workflows de aprobación.
 - Disminución de costos de administración.
- ▶ Desventajas:
 - Punto único de entrada.
 - Tiempo de desarrollo para sincronizar las aplicaciones.

Acceso Unificado (Single Sign On)

- ▶ Logueo único para diferentes sistemas.
- ▶ Ejemplos de protocolos:
 - Kerberos.
 - Oauth.
 - SAML.
 - OpenID.
 - LDAP.
- ▶ Ventajas:
 - Facilidad de administración.
 - Uso de contraseñas fuertes.
- ▶ Desventajas:
 - Punto único de entrada.
 - Difícil de implantar y operar.
 - Al dejar la PC desbloqueada se puede acceder a cualquier sistema.

- ▶ **Control de Acceso Discrecional (DAC)**
 - Cada objeto tiene un dueño.
 - Normalmente se implementa con Listas de Control de Acceso.

- ▶ **Control de Acceso Obligatorio (MAC)**
 - El sistema impone sus reglas.
 - Se implementa con el uso de etiquetas.

- ▶ **Control de Acceso Basado en Roles (RBAC)**
 - Asignación indirecta de permisos.
 - Se basa en una descripción de puesto que ocupa en vez de la identidad del sujeto.
 - Facilita la implementación de Segregación de Funciones.

► Dependiente del Contexto (CBAC)

- El sistema toma su decisión de acceso basado en el estado de una determinada cantidad de variables que conforman el contexto.

► Ejemplos:

- Control de Acceso de Red (NAC).
- Firewall de Red.



You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[Sign out and sign in with a different account](#)

[More details](#)

► Dependiente del Contenido

- Las decisiones de acceso se basan en la sensibilidad del dato y su contenido.
- Los cambios en el contenido pueden provocar cambios en las decisiones de acceso. No obstante, las reglas de acceso definidas permanecen constantes.

► Ejemplos:

- Firewall a nivel de Aplicación.
- Filtros Antispam.
- Antivirus.

PREGUNTAS?

