

# Seguridad de la Información

## Sistemas de Control de Accesos

**Federico Pacheco**



@FedeQuark



[www.federicopacheco.com.ar](http://www.federicopacheco.com.ar)



[info@federicopacheco.com.ar](mailto:info@federicopacheco.com.ar)

# Contenidos

---

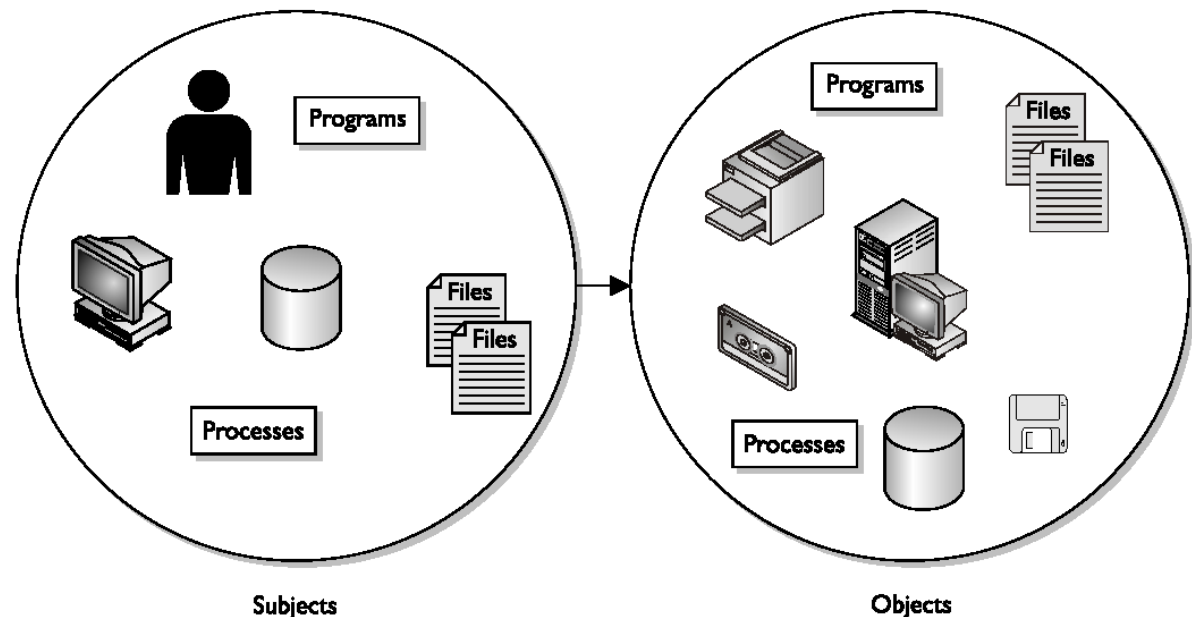
- Conceptos
- Mecanismos de autenticación
- Administración centralizada
- Modelos de control de acceso
- Gestión de logs



# Control de accesos

- Concepto
  - Capacidad de permitir acciones a entidades autorizadas de forma autorizada
  - Se busca proteger datos y sistemas

- Elementos
  - Sujeto
  - Objeto
  - Acceso
  - Dominio
  - Grupo



# Ciclo de vida de un Sistema de Control de Accesos

---



# Clasificación de controles

## Por su naturaleza



- ☐ Administrativos
- ☐ Lógicos (Técnicos)
- ☐ Físicos



Administrative



Physical



## Por el momento de acción



- ☐ Preventivo
- ☐ Detectivo
- ☐ Correctivo



Technical

# Matriz de controles

Type of Control:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
	Avoid undesirable events from occurring	Identify undesirable events that have occurred	Correct undesirable events that have occurred	Discourage security violations	Restore resources and capabilities	Provide alternatives to other controls
<b>Category of Control:</b>						
<b>Physical</b>						
Fences	X			X		
Locks	X			X		
Badge system	X			X		
Security guard	X	X		X		
Biometric system	X					
Mantrap doors	X			X		
Lighting	X					
Motion detectors		X				
Closed-circuit TVs		X		X		
Alarms	X	X		X		
Backups					X	

# Matriz de controles

Type of Control:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
Information classification	X					
<b>Technical</b>						
ACLs	X					
Routers	X					
Encryption	X					
Audit logs		X				
IDS		X				
Antivirus software	X	X	X		X	
Firewalls	X			X		
Smart cards	X					
Dial-up call-back systems	X					
Alarms and alerts		X				

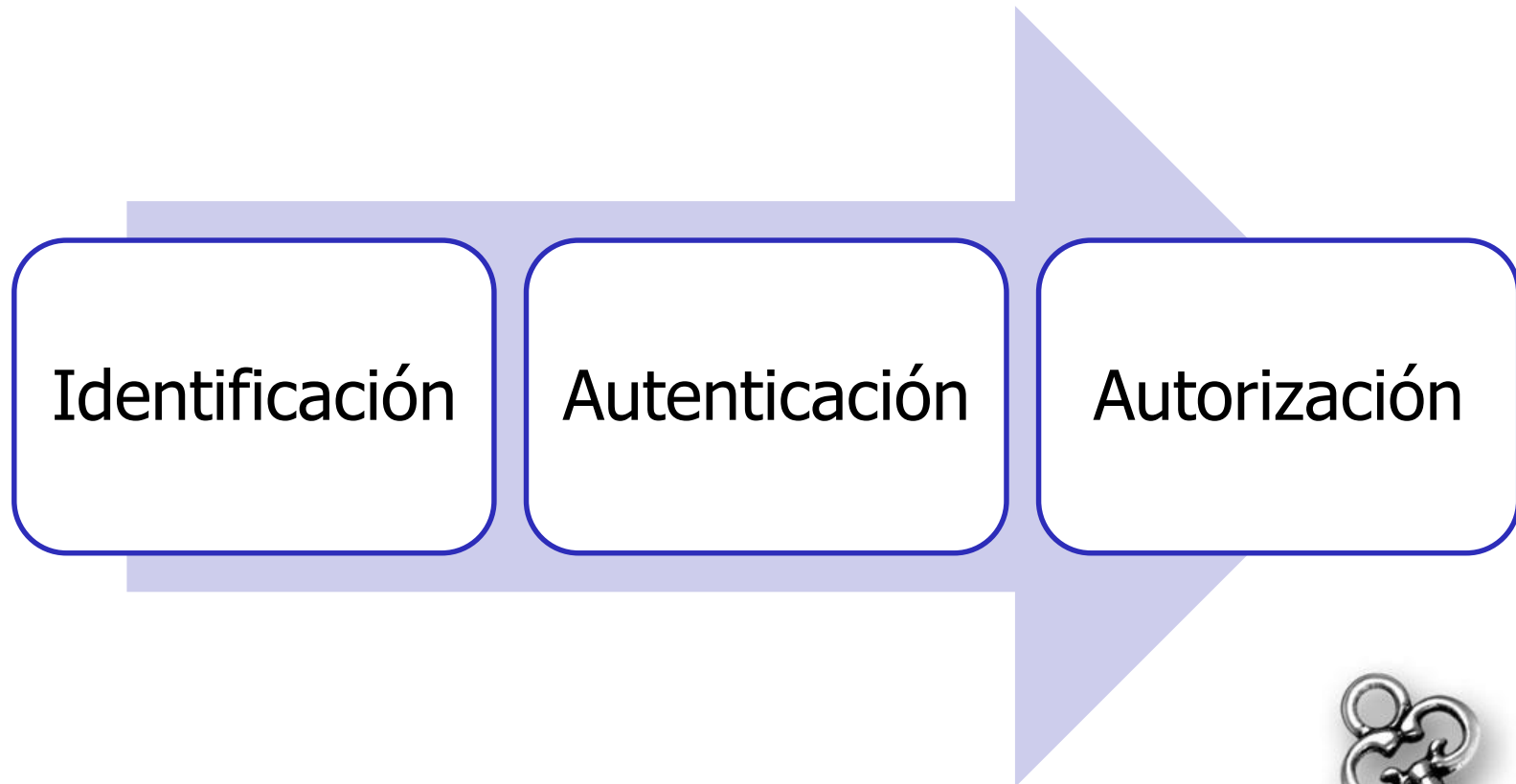
# Matriz de controles

Type of Control:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
Information classification	X					
<b>Administrative</b>						
Security policy	X					
Monitoring and supervising	X	X		X		X
Separation of duties	X					
Job rotation		X				
Personnel procedures	X			X		X
Investigations		X				
Testing	X					
Security-awareness training	X			X		



# Control de accesos – Fases

---



# Control de accesos – Conceptos

---

Trazabilidad  
(Accounting)

Anonimidad

Profiling

Privacidad y  
expectativa

No repudio

Mínimo  
privilegio

Separación de  
tareas

Rotación de  
tareas

Multi Factors

Default No  
Access

SPOF  
(Single Point  
of Failure)

Need to Know

# Factores de autenticación

## Lo que uno sabe

- Passwords
- Passphrase
- PIN

## Lo que uno tiene

- Tokens
- Tarjetas
- Llaves

## Lo que uno es

- Biometría

Dos factores distintos: autenticación fuerte

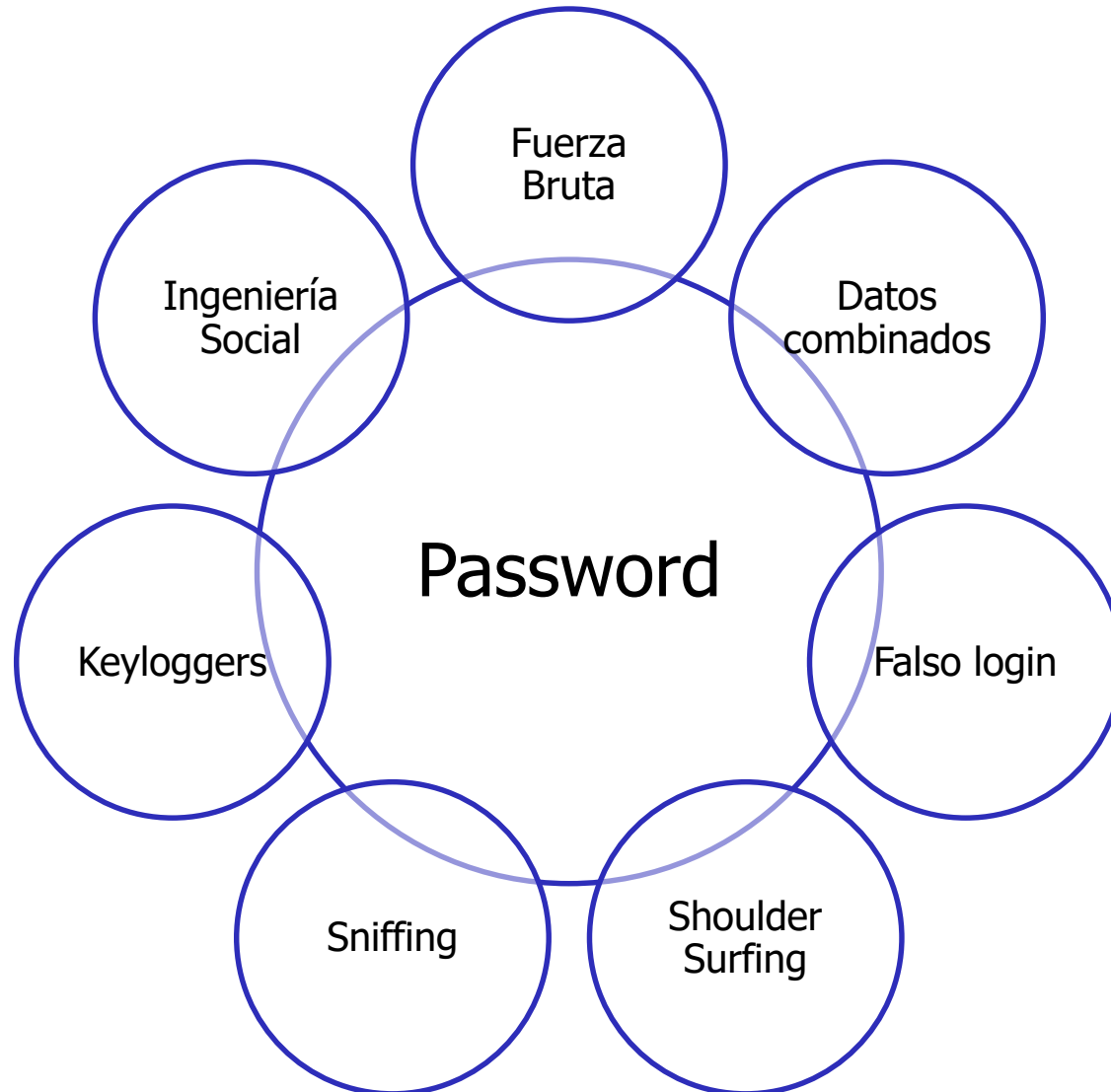
# Algo que uno sabe: Contraseñas

- El modelo de autenticación más básico y barato
  - Es el sistema más vulnerable a ataques
  - Se utiliza como complemento a otros mecanismos
  - Caso ideal: OTP (one-time password)
- Suele ser elegido por el usuario
  - Reutilización
  - Elección débil
  - No cambio
- Se utilizan en diferentes entornos
  - Servicios online
  - Sistemas operativos y aplicaciones
  - Dispositivos de hardware y BIOS
  - Cifrado de archivos y discos



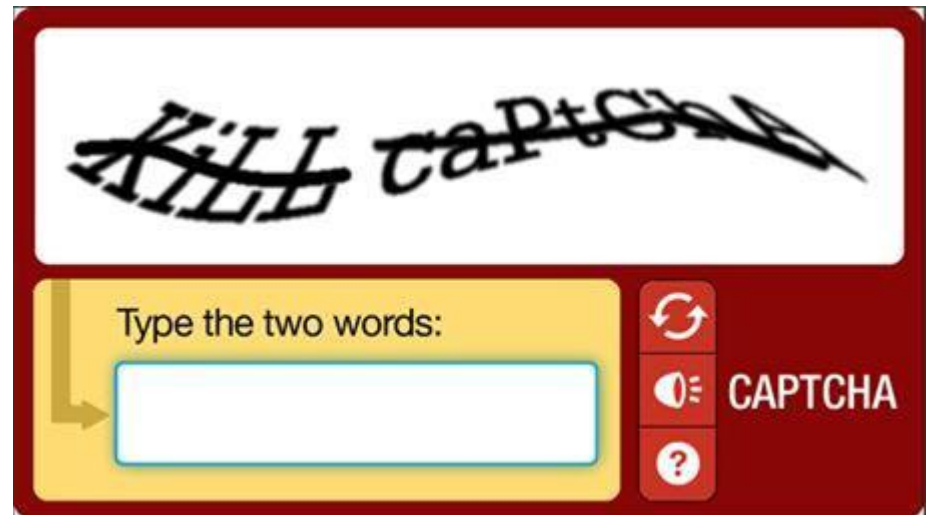
# Contraseñas – Ataques

---



# Contraseñas – Ataques online: Contramedidas

- Captcha
  - Elemento reconocible por un humano y difícil por un software
  - Formatos
    - Texto escritos
    - Texto hablado
    - Imágenes
- Bloqueo por cantidad de intentos
- Introducir demoras entre intentos



# Contraseñas – Ataques offline: Contramedidas

- Fortaleza en los hashes
  - Algoritmos fuertes
  - Uso de “salt”
    - Valor aleatorio que se concatena a la contraseña antes de calcular el hash
    - Se almacena junto al hash: UserID|salt|hash(pass+salt)
- Requerimientos fuertes
  - Complejidad
  - Longitud



# Contraseñas – Contramedidas generales

---

- Implementar políticas que prohíban usos inseguros
  - Complejidad
  - Longitud mínima
  - Por defecto o trivial
  - De diccionario
  - Información personal
- Implementar tiempos de expiración
  - No muy corto: el usuario lo olvida y se debe resetear
  - No muy largos: aumenta la probabilidad de compromiso
  - Regla general: Más cantidad de usos, menor tiempo de expiración
- Implementar autenticación de 2 factores
- Evitar la reutilización entre períodos



# Contraseñas – Test de fortaleza

Test Your Password		Minimum Requirements
Password:	<input type="password"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li></ul></li></ul>
Hide:	<input checked="" type="checkbox"/>	
Score:	0%	
Complexity:	Too Short	

## Additions

- |   |                           |
|---|---------------------------|
| ✗ | Number of Characters      |
| ✗ | Uppercase Letters         |
| ✗ | Lowercase Letters         |
| ✗ | Numbers                   |
| ✗ | Symbols                   |
| ✗ | Middle Numbers or Symbols |
| ✗ | Requirements              |

## Deductions

- |   |              |
|---|--------------|
| ✓ | Letters Only |
| ✓ | Numbers Only |

Microsoft®

## Safety & Security Center

Computer Security, Digital Privacy, and Online Safety

[Home](#) | [Security](#) | [Privacy](#) | [Family Safety](#) | [Resources](#)

### Check your password—is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords.

**Test the strength of your passwords:** Type a password into the box.

Password:

Strength: 

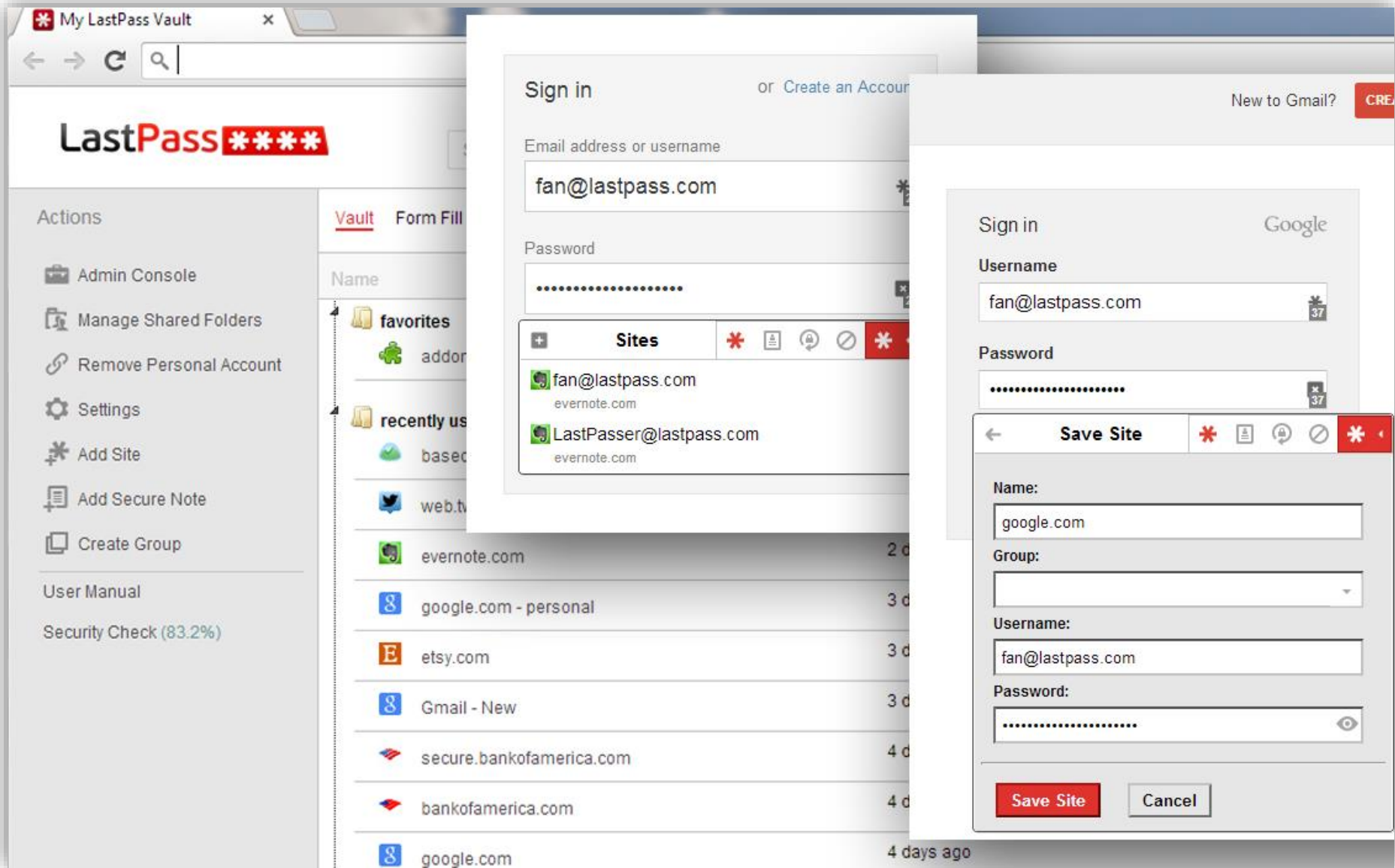
Strong

# Gestores de contraseñas

---

- Es recomendable el uso de password managers en las organizaciones
  - Como todo software, conviene definir uno para estandarizar su uso
- Hay diversas opciones pagas y gratuitas
  - KeePass
  - LastPass
  - PasswordGorilla
  - PasswordSafe
  - RoboForm
  - 1Password
  - Dashlane
- Existen versiones portables y para varios S.O.
- Algunos permiten sincronización entre dispositivos

# LastPass



# Dashlane

Search...

PASSWORD MANAGER

Passwords

Security Dashboard

Secure Notes

PERSONAL INFO

Contact

IDs

WALLET

Payments

Receipts

dashlane

Your security score:

81.7%

You are super safe!  
Get even closer to 100% and stay on top of the game with these quick wins:

3%

bankofamerica.com:  
weak or reused  
password! Replace it with  
a strong one.

Replace now

3%

gap.com: weak or reused  
password! Replace it with  
a strong one.

Replace now

3%

paypal.com: weak or  
reused password!  
Replace it with a strong  
one.

Replace now

5%

Activate Google  
Authenticator to get even  
more secure.

Activate now

DETAILED PASSWORD ANALYSIS

48

All  
accounts

6

Weak  
passwords

0

Compromised  
passwords

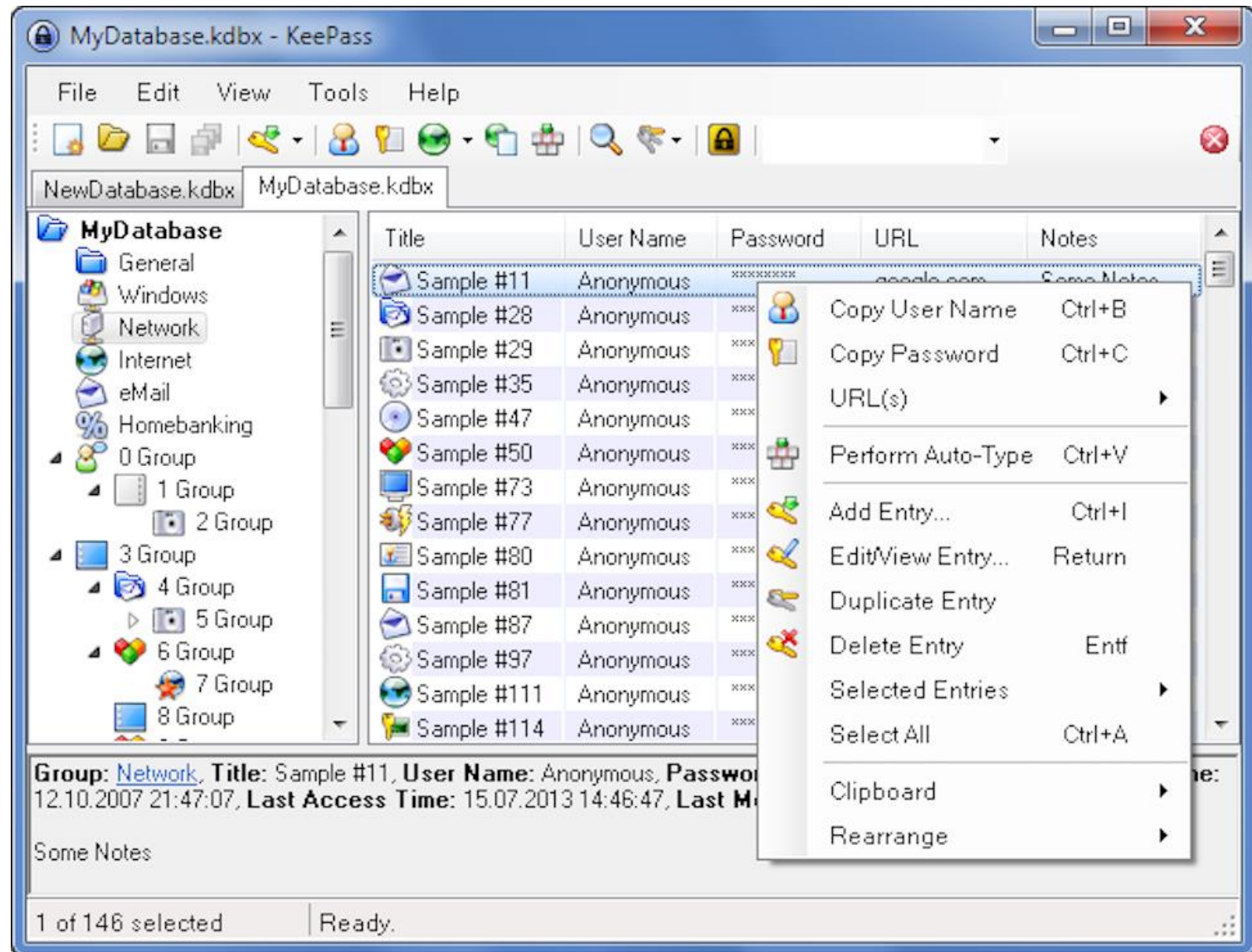
6

Reused  
passwords

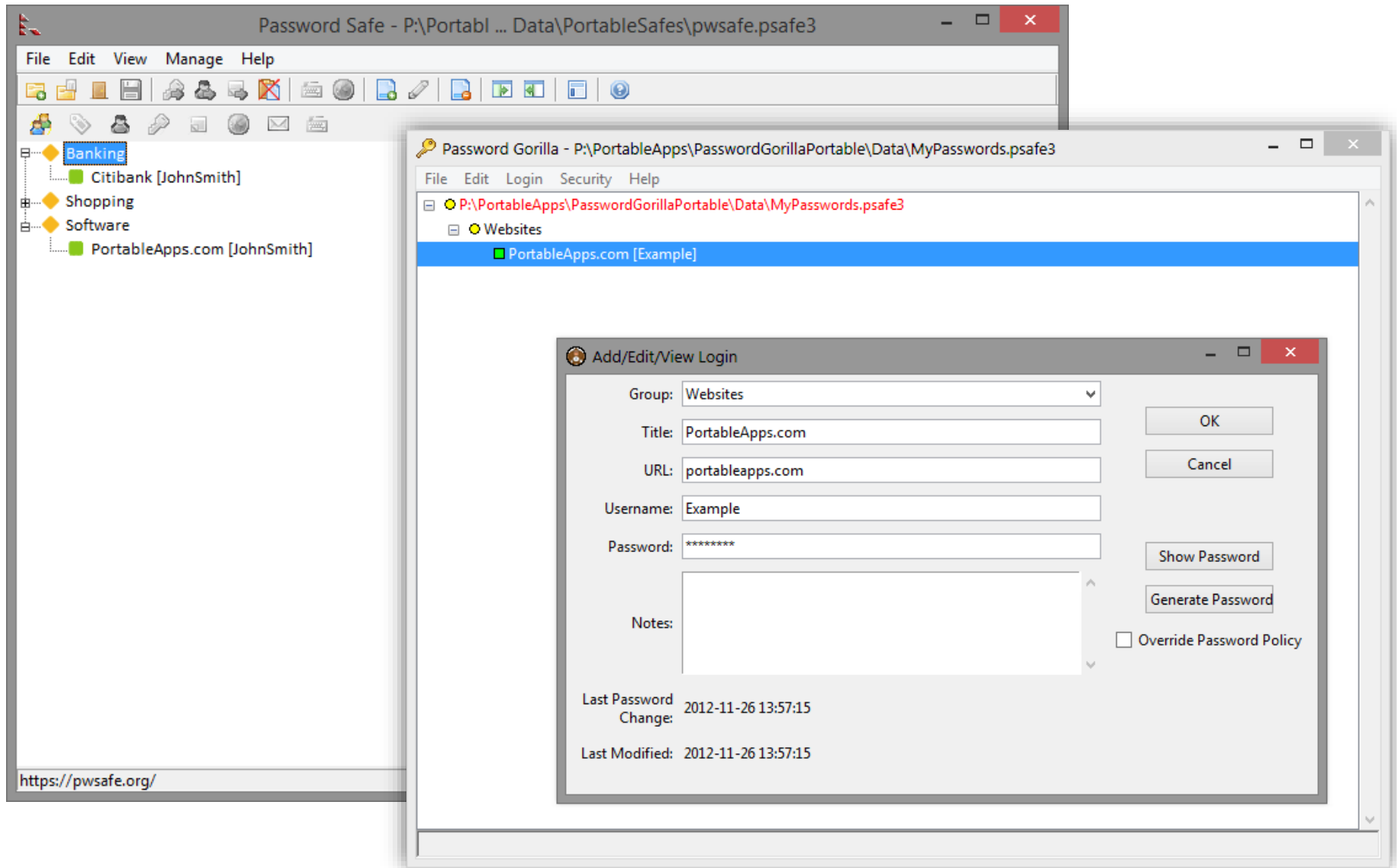
Website	Login	Password	Reused?	Password strength	Action
soundcloud.com	dashlane@rocketmail.com	.....	2 times	<div>Very unsafe, 0%</div>	

Go Premium

# KeePass

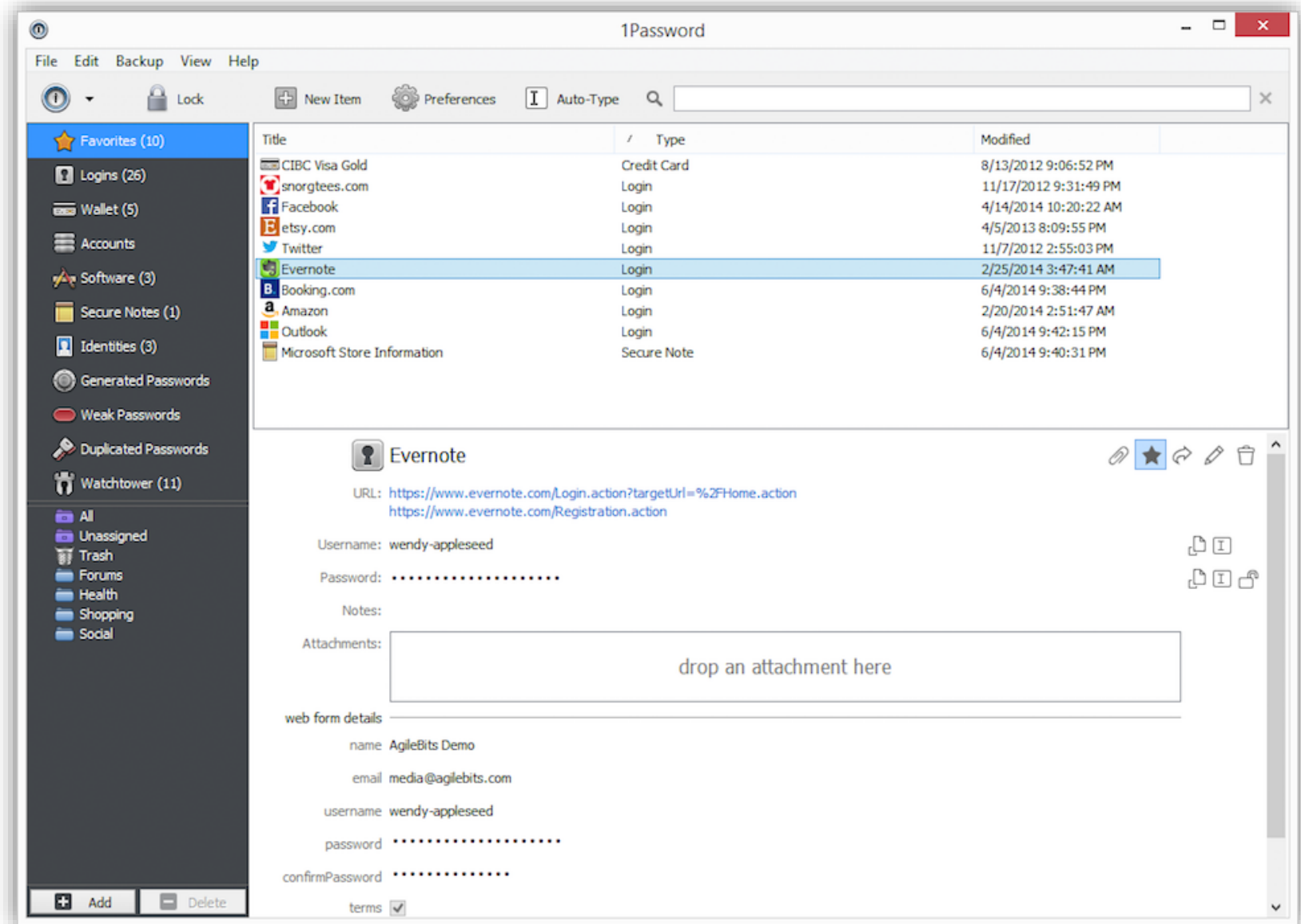


# Password Safe y Password Gorilla

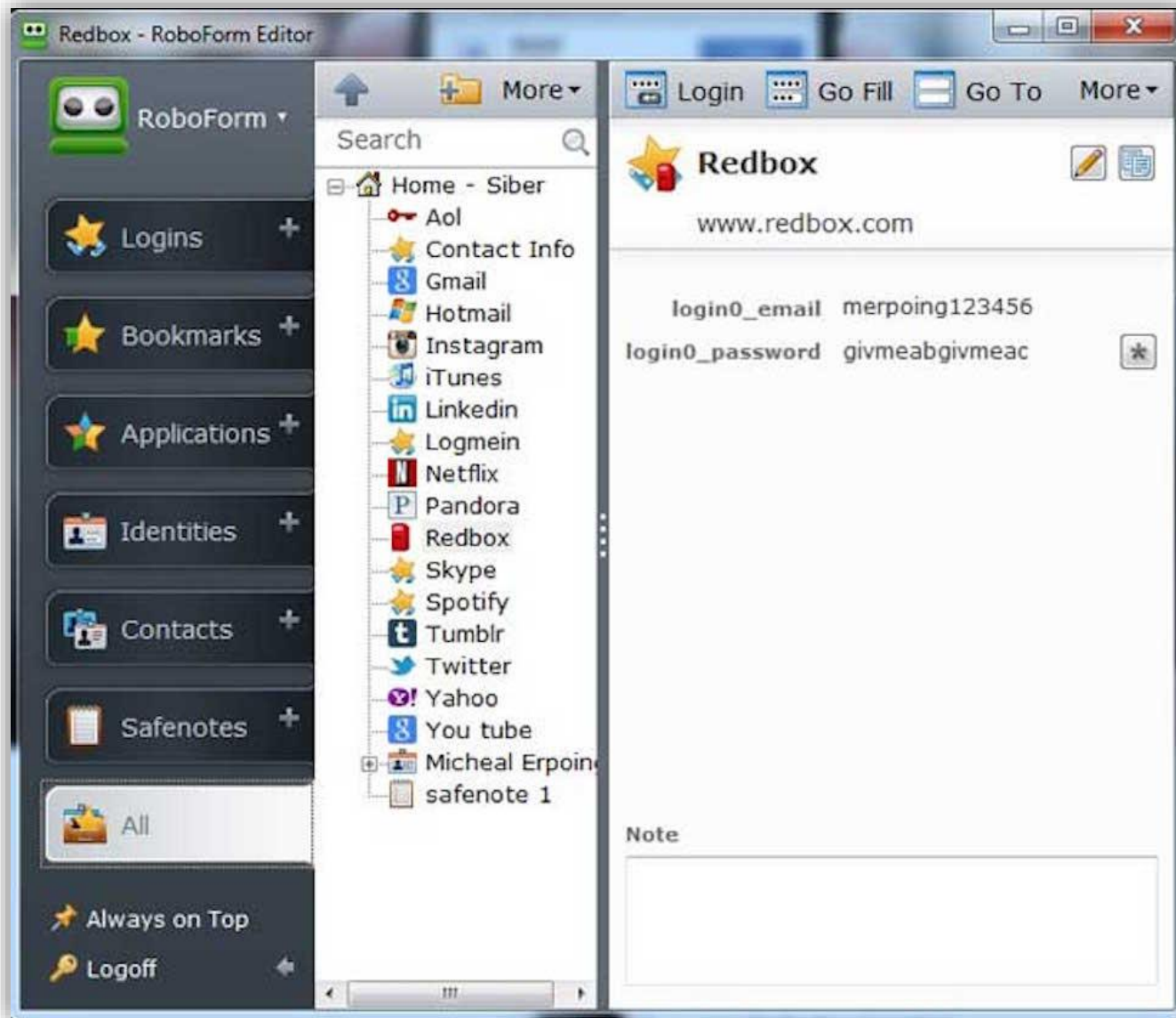




# 1Password



# RoboForm





# Algo que uno tiene - Tokens

- Sincrónicos

- por tiempo
- por contador



- Asincrónicos (Desafío / Respuesta)



# Algo que uno tiene - Tarjetas

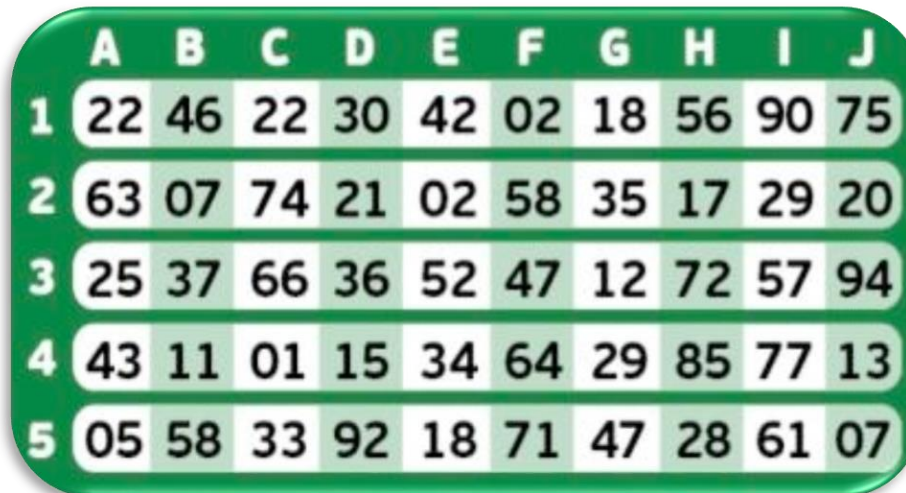
---

- Las tarjetas tienen múltiples usos
  - Firma digital mediante en entornos WEB
  - Presencia e identificación personal
  - Monedero electrónico
  - Autenticación
- Existen diversas tecnologías
  - Tarjetas de coordenadas
  - Banda magnética
  - Proximidad
  - Chip (con o sin procesamiento)
  - RFID



# Tarjetas de coordenadas

- Elementos predefinidos en una matriz
- Uso manual por parte del usuario
- Desventaja: puede ser fotocopiada o fotografiada



A green-bordered coordinate card with a grid of numbers. The card has a green border and rounded corners. The grid consists of 5 rows and 10 columns. The columns are labeled A through J, and the rows are labeled 1 through 5. Each cell contains a two-digit number.

	A	B	C	D	E	F	G	H	I	J
1	22	46	22	30	42	02	18	56	90	75
2	63	07	74	21	02	58	35	17	29	20
3	25	37	66	36	52	47	12	72	57	94
4	43	11	01	15	34	64	29	85	77	13
5	05	58	33	92	18	71	47	28	61	07

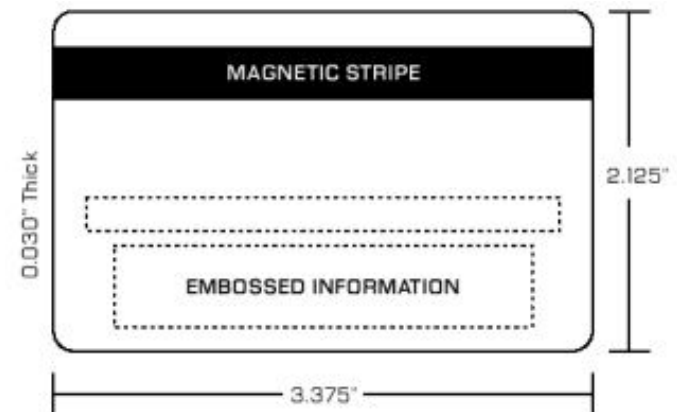
# Tarjetas de banda magnética

- Características

- Compuesta por partículas ferromagnéticas incrustadas en una matriz de resina
- Almacenan datos por polarización
- La información se organiza en diferentes pistas (1 a 3)
- La banda magnética es grabada o leída mediante contacto físico
- Se utiliza una cabeza lectora/grabadora
- Formato y estructura de datos estándar (ISO7810 a 7813 pistas 1 y 2 e ISO4909 pista 3)

- Desventajas

- Baja seguridad y capacidad
- Baja resistencia a la fricción
- Incapacidad para firma digital y cifrado
- Equipos de lectura y escritura costosos



# Tarjetas de proximidad

---

- El chip se comunica con el lector mediante inducción eléctrica sin contacto directo
- Utilizan un circuito integrado y un circuito LC (bobina y capacitor) en serie
  - El lector excita la bobina con un campo magnético y carga el capacitor
  - El capacitor energiza la bobina y la bobina energiza el integrado
  - El integrado transmite la información (en general un número) al lector vía la bobina
- Características físicas, eléctricas e informáticas definidas en ISO/IEC 14443 (2001)
  - Define tipos A y B para distancias de hasta 10cm (C,D,E y F, aun no estandarizados)
  - Se comunican mediante el protocolo Wiegand
  - Tasa de transferencia de 106 a 848 Kb/s
- Un estándar alternativo es ISO 15693
  - Permite distancias de hasta 150 cm
  - Opera en la frecuencia 13.56 MHz

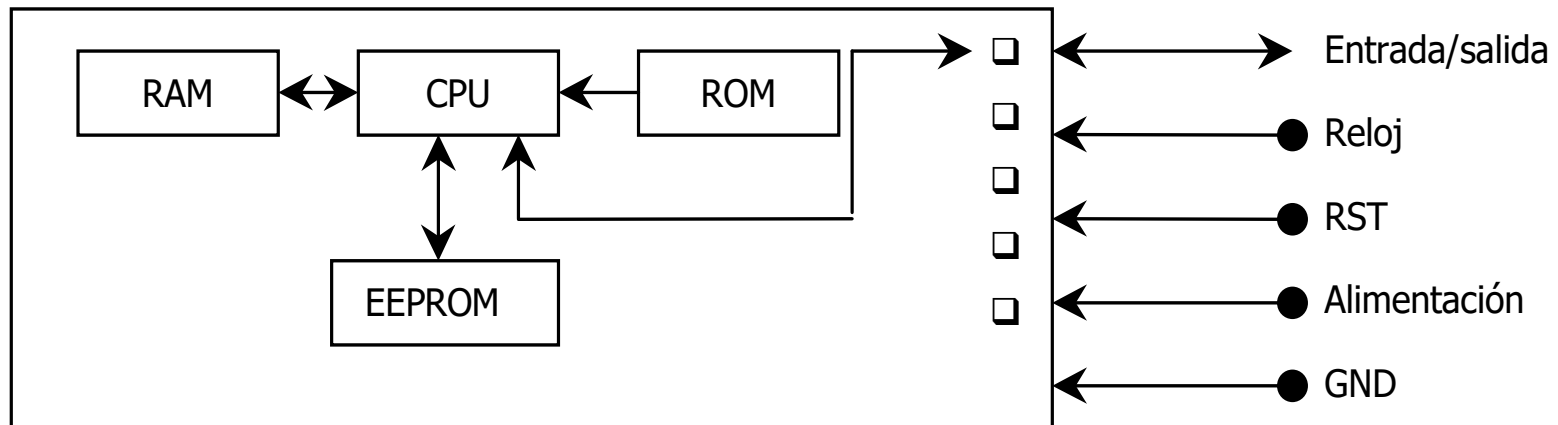
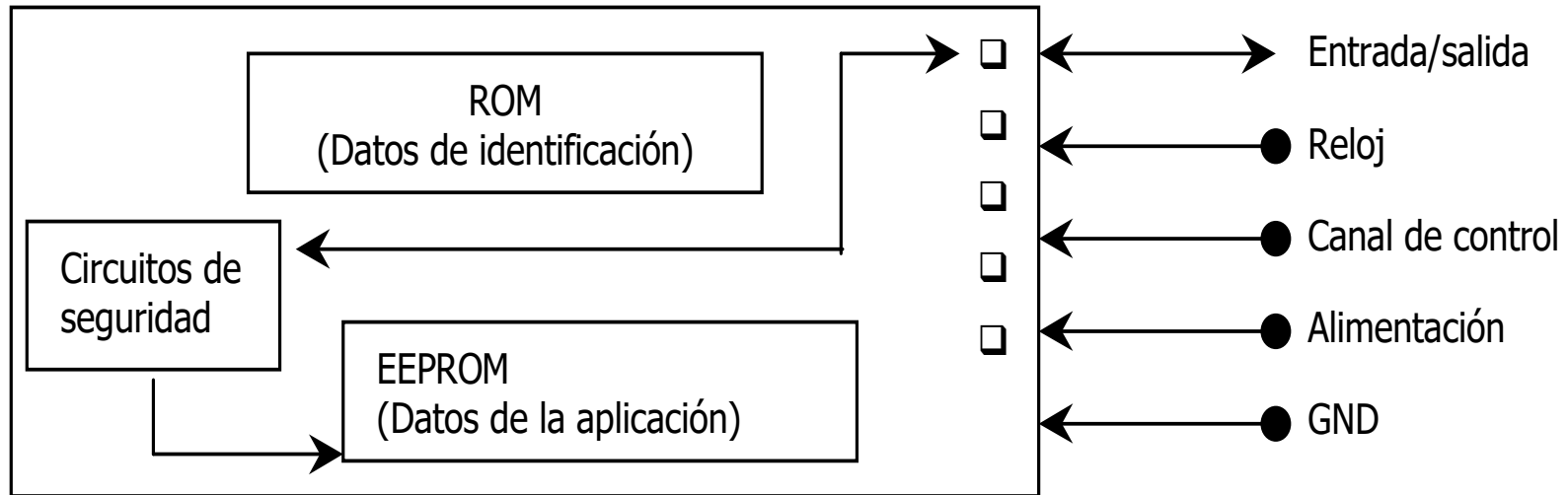


# Tarjetas chip

- Incluyen circuitos integrados y la energía es suministrada por los lectores
- Cronología
  - Inventadas en los 70 (creador en discusión)
  - Primer uso masivo en teléfonos públicos en Francia (1983)
  - Auge en los 90 por las tarjetas SIM (GSM)
  - Probado en tarjetas de crédito en los 90s (EMV) sin lograr reemplazar las magnéticas
- Características físicas, eléctricas e informáticas definidas en ISO/IEC 7816/7810
  - Físicas y eléctricas: forma, dureza, posición y forma de contactos, niveles de corrientes
  - Informáticas: protocolos, comandos, funcionalidades y sistema de archivos
- Pueden clasificarse según capacidades
  - Sin capacidad de procesamiento (solo memoria)
  - Con capacidad de procesamiento (uso de algoritmos)



# Tarjetas chip – Con y sin procesamiento



# RFID (Radio Frequency Identification)

---

- Sistema de almacenamiento y lectura de datos remoto
  - Idea básica: transmitir la identidad de un objeto
  - Pensadas conceptualmente desde la década del 40
  - Se incluye dentro de las llamadas tecnologías de Auto ID (Automatic Identification)
- Componentes
  - Etiqueta pasiva, semi pasiva o activa
    - Incluye antena y memoria (solo lectura, lectoescritura y lectura múltiple anticolisión)
  - Lector de RFID
  - Subsistema de procesamiento de datos
- Hay polémica por la privacidad para el uso en ID de productos
  - El comprador de un artículo no sabe de su presencia ni puede eliminar la etiqueta
  - Puede ser leído a distancia sin autorización
  - Al realizar un pago, es posible relacionar IDs con la identidad del comprador
  - EPCGlobal pretende crear números de serie globales únicos



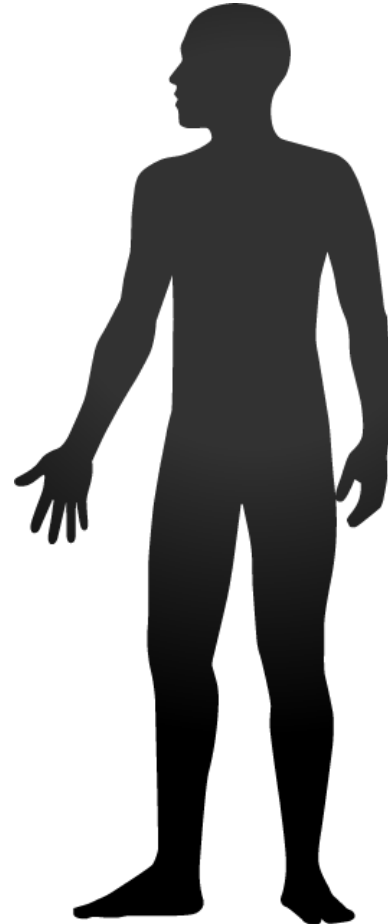
# RFID – Estandarización

- Áreas de estandarización
  - Protocolo en la interfaz aérea
  - Contenido de los datos
  - Certificaciones para interoperabilidad
  - Aplicaciones del sistema
- Existen varios grupos de especificaciones (competidoras)
  - ISO (serie 18000, estrictamente relacionada RFID)
  - EPCglobal (propone 2 estándares no interoperables e incompatibles con ISO)
- Clasificación según frecuencias (las regulaciones son nacionales)
  - Baja frecuencia: 125 a 134,2 KHz
  - Alta frecuencia: 13,56 MHz
  - Ultra alta frecuencia (UHF): 868 a 956 MHz
  - Microondas: 2,45 GHz



# Algo que uno es – Sistemas Biométricos

- Concepto: características físicas o psicológicas únicas del ser humano
- Ventajas
  - Difíciles de falsificar
  - No pueden ser prestados ni olvidados
  - No requieren esfuerzo de uso
- Desventajas
  - Costo elevado
  - Posible rechazo de los usuarios
- Proceso de autenticación
  - Captura de datos de la persona
  - Extracción de características de la muestra
  - Comparación con las muestras guardadas
  - Decisión sobre la validez del usuario



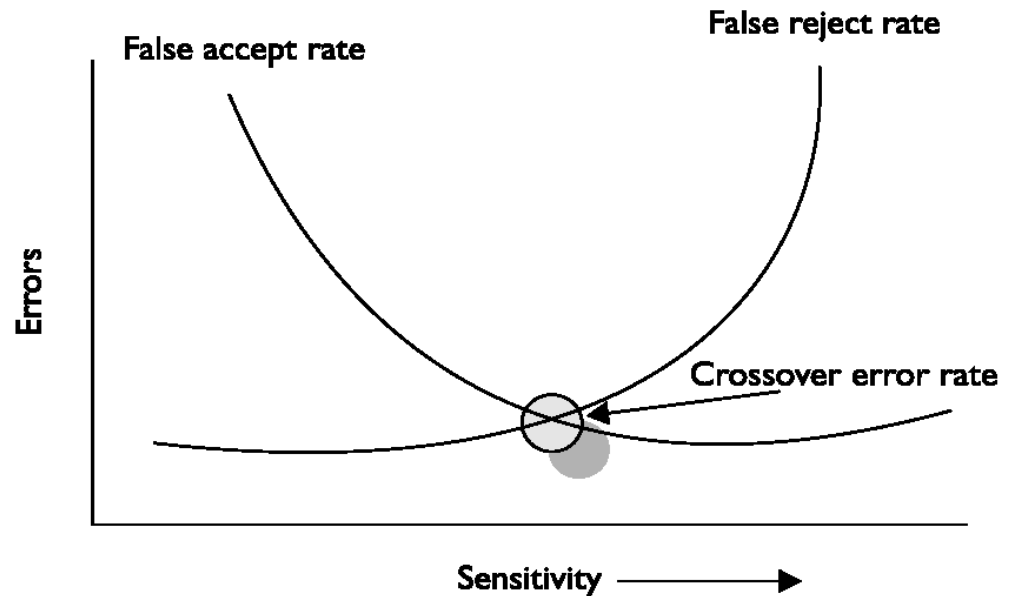
# Sistemas Biométricos – Características

- Factores característicos

- Tiempo de enrolamiento inicial
- Tasa de procesamiento
- Aceptabilidad
- Exactitud y precisión

- Tasas de error

- FRR (False Rejection Rate) - Error Tipo I: Tasa de rechazo de un sujeto válido
- FAR (False Acceptance Rate) - Error Tipo II: Tasa de aceptación de sujeto no válido
- CER (Crossover Error Rate) - Equal Error Rate (EER): Punto en que se igualan FAR y FRR



# Sistemas Biométricos – Organizaciones y estándares

- Organizaciones internacionales
  - Biometrics Consortium
  - BioAPI Consortium (ISO/IEC)
  - International Biometric Society
  - International Biometrics & Identification Association
- Estándares más importantes
  - ISO/IEC 7816 (Sub-Comité 17, Joint Technical Committee)
  - ANSI X.9.84 (USA)
  - ANSI/INCITS 358 (ANSI y BioApi, USA)
  - NIST IR 6529 (USA)



# Sistemas Biométricos – Elementos

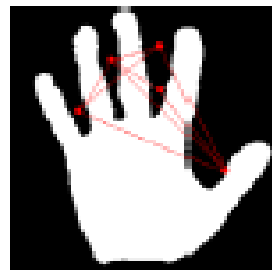
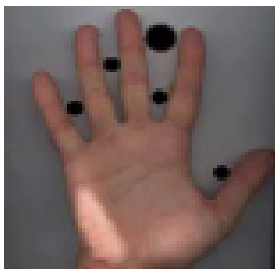
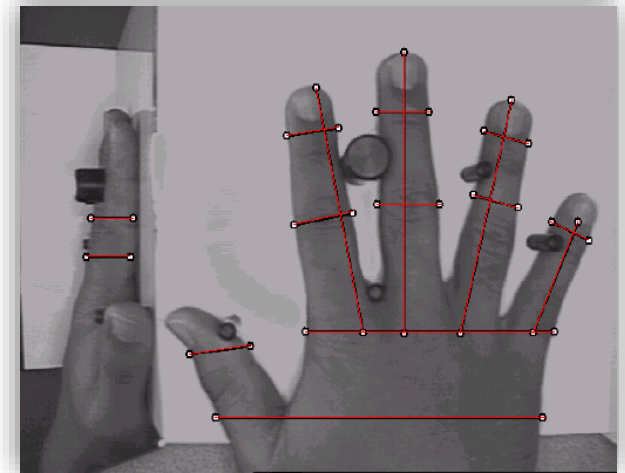
---

- Físicos
  - Mano: Geometría, Huella Digital, Huella Palmar,
  - Ojos: Iris y Retina
  - Cabeza: Topología y Rostro
  - ADN
- Psicológicos
  - Firma
  - Típeo
  - Voz



# Sistemas Biométricos – Geometría de la mano

- Método: determinar puntos característicos de la geometría de la mano en 2D
  - Son rápidos pero con alto FAR
  - Pueden aprender percibiendo variaciones
  - Puede aplicarse con 1 o 2 dedos, a menor precisión
- Proceso
  - Se sitúa la mano sobre un dispositivo lector con guías
  - Se toma una imagen superior y otra lateral
  - Se extraen datos geométricos (puntos característicos)
  - Se crea la muestra con su código correspondiente

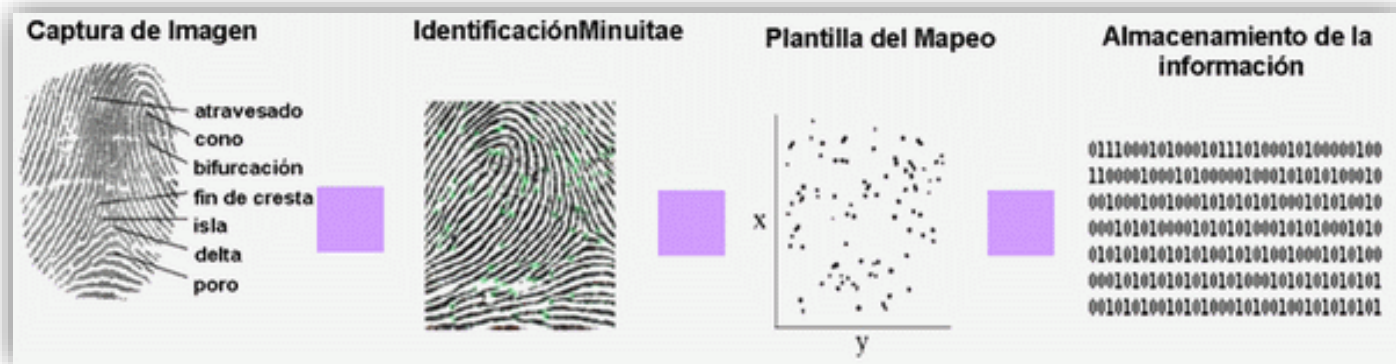


Código de la mano

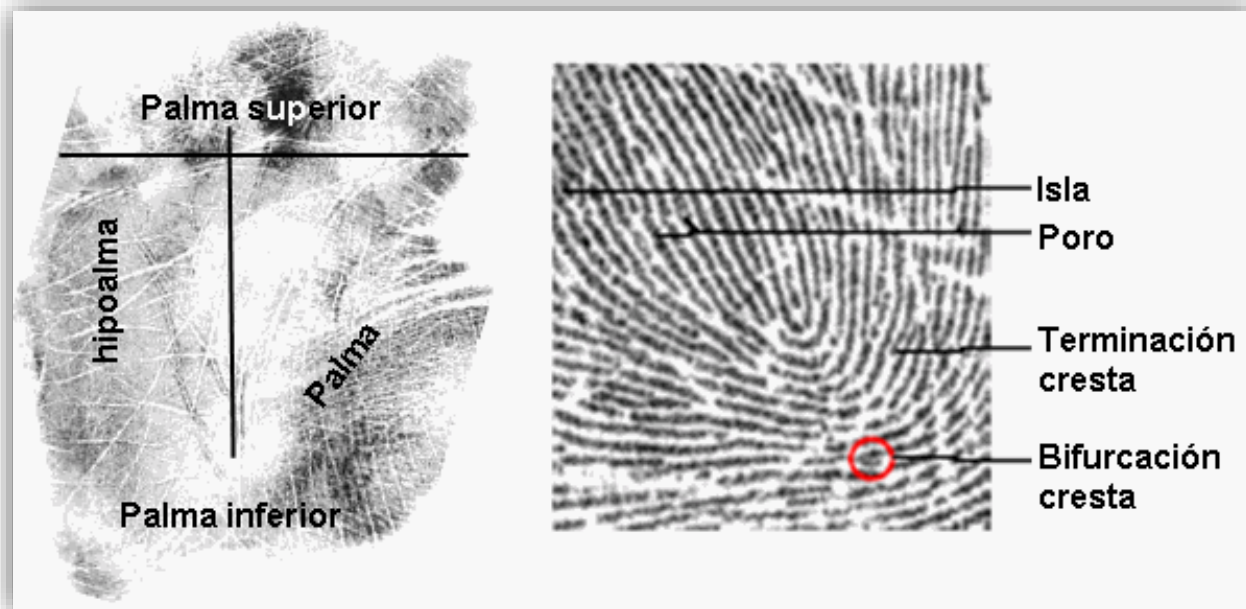
43BFFFA60

# Sistemas Biométricos – Huella Dactilar

- Método: determinar puntos característicos (patrones y minucias) de la huella
  - Cada dedo tiene al menos 40 minucias
  - Dos dedos no poseen más de ocho minucias comunes
  - Puede complicarse con heridas en el dedo
- Proceso
  - Se toma de una imagen de la huella con un lector
  - Se procesa y extraen características
  - Se mapean los puntos según un modelo matemático
  - Se crea la muestra con su código correspondiente



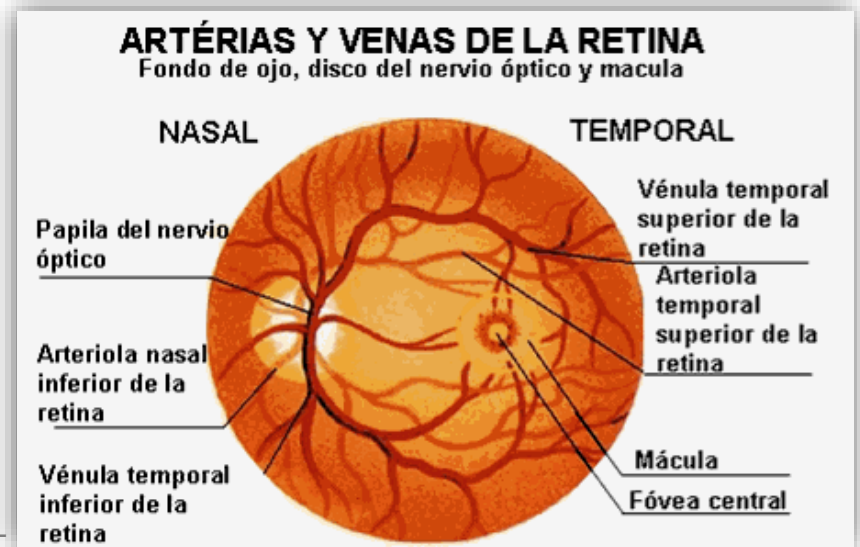
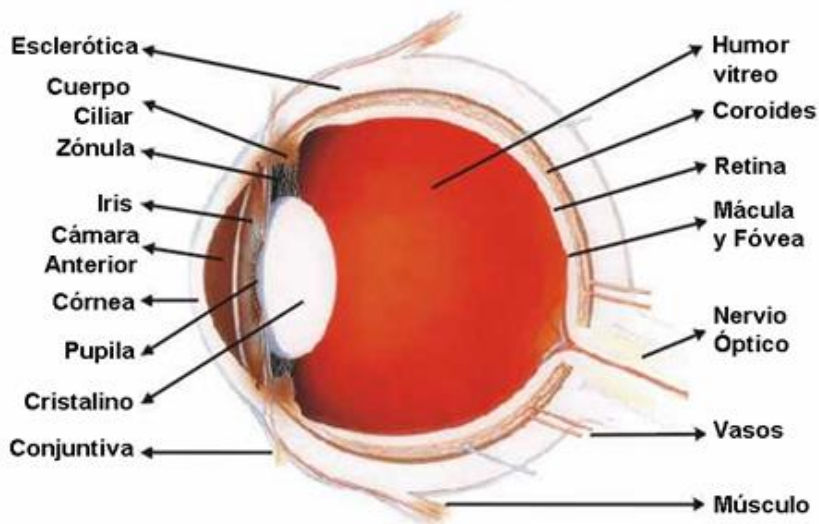
# Sistemas Biométricos – Huella Palmar





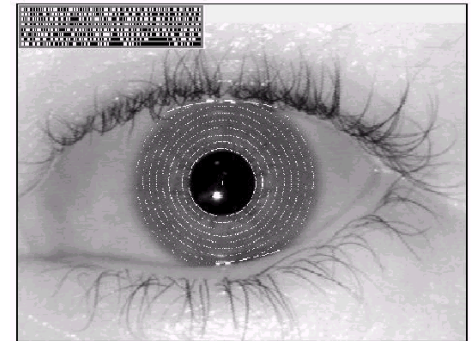
# Sistemas Biométricos – Retina

- Método: determinar la vasculatura de la retina (forma de los vasos sanguíneos)
  - La empresa EyeDentify tiene la patente mundial sobre esta tecnología
- 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 crea la muestra con su código correspondiente

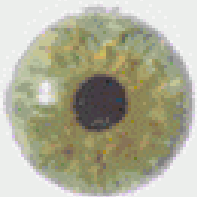


# Sistemas Biométricos – Iris

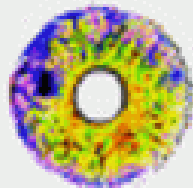
- Método: determinar patrones del iris (más moderno que el de retina)
  - La empresa IriScan tiene la patente mundial sobre esta tecnología
- Proceso
  - Se captura una imagen o video del iris en blanco y negro
  - Se somete a deformaciones pupilares
  - Se extraen patrones y realizan transformaciones matemáticas
  - Se crea la muestra con su código correspondiente (iriscode)



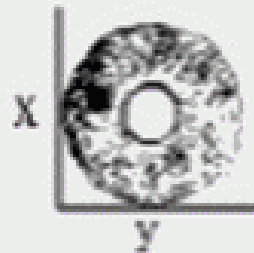
Captura de video



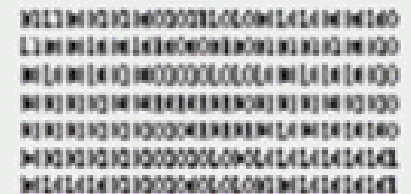
Trabecular Meshwork



“Huella digital” óptica



Record del código del iris



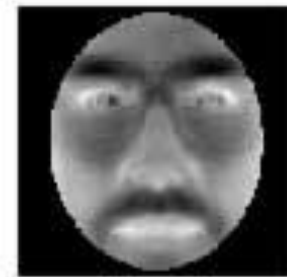
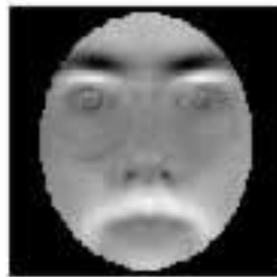
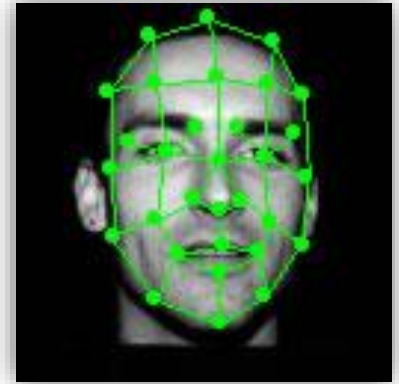
# Sistemas Biométricos – Rostro

---

- Método: determinar patrones en la cara (2D y 3D)
  - Tasas de reconocimiento limitadas: patrones no estables
  - Uso principalmente en autenticación
- Buena aceptación social
  - Es la manera en que identificamos visualmente a la gente
  - Poco invasivo
  - Poco costoso
- Registro del usuario
  - Captación de imágenes
  - Procesamiento y obtención de un código digital
  - Almacenamiento en base de datos

# Sistemas Biométricos – Rostro - Técnicas

- Análisis del contenido de la imagen (Gabor Analysis)
  - Elastic graph matching (EGM)
- Obtención de valores característicos
  - Eigenfaces



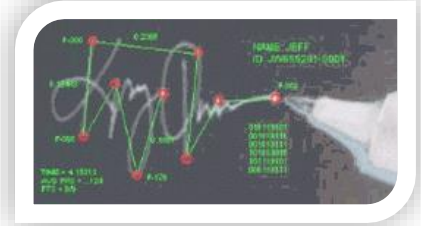
# Sistemas Biométricos – ADN

- Reconocimiento de una característica genética
  - Solo 4 ácidos nucleicos comprenden el código genético (ACTG)
  - Solo gemelos idénticos tienen mismo ADN
- Ventajas
  - Sumamente confiable y difícil de vulnerar
  - Puede identificar y autenticar
- Desventajas
  - Requiere de una muestra física (pelo, piel, fluido)
  - Es muy invasivo
  - Sin procesamiento en tiempo real
  - Costo elevado



# Sistemas Biométricos – La Firma

- Detección de características de la firma hológrafa
  - Gran aceptación (costumbre de firmar para identificarnos)
- Existen dos sistemas
  - Reconocimiento de firma estática (off-line)
    - Se parte de firmas realizadas previamente
    - Se extraen las características extraídas de la firma (geometría en 2D)
  - Reconocimiento de firma dinámica (on-line)
    - La información se adquiere durante el firmado
    - Se tiene información temporal (duración, posición, velocidad)
    - La información dinámica es más difícil de falsificar
    - Requiere dispositivos digitalizadores



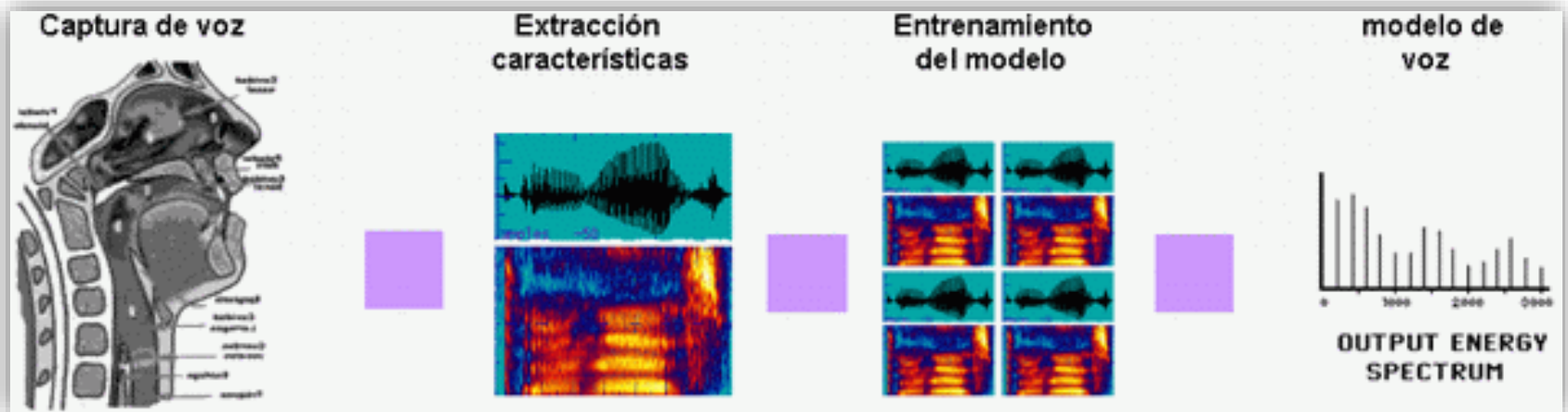
# Sistemas Biométricos – Típeo

- Detección de características del típeo
  - Velocidad
  - Ritmo
  - Cadencia
  - Presión
- Uso en autenticación
- Puede requerir un teclado especial



# Sistemas Biométricos – La Voz

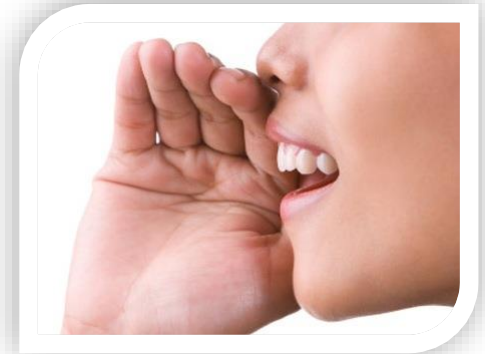
- Método: detectar patrones en la señal vocal
  - Usos en identificación y autenticación
  - Se soporta sobre la estructura física y psicológica de la voz
  - Requiere entrenamiento de un modelo de referencia (representación)
  - Se aplican técnicas matemáticas avanzadas
    - Modelos ocultos de Markov (HMM)
    - Modelos de mezclas Gaussianas (GMM)
- Existen sistemas dependientes e independientes del texto





# Sistemas Biométricos – La Voz: Etapas

- Captura
  - Sensado con micrófonos comunes u ópticos
- Pre-procesamiento
  - Cancelación de ruido, filtro anti-aliasing, Conversión A/D, detección inicio-fin, pre-énfasis
- Extracción de parámetros y generación de patrón
  - División de la señal en cuadros (frames) y ponderación de cuadros por ventana
- Comparación de patrones y verificación (límite de decisión)
  - Verosimilitud calculada > Umbral definido



# Comparación de tecnologías

<b>Tecnología</b>	<b>Tamaño plantilla (bytes)</b>	<b>Fiabilidad</b>	<b>Facilidad De Uso</b>	<b>Costo</b>	<b>Aceptación</b>
<b>Huella digital</b>	250 – 1000	Muy alta	Alta	Bajo	Alta
<b>Geometría de la mano</b>	9	Baja	Alta	Bajo	Alta
<b>Retina</b>	96	Baja	Baja	Alto	Baja
<b>Iris</b>	512	Baja	Baja	Muy alto	Baja
<b>Geometría facial</b>	84 – 1300	Baja	Baja	Medio	Baja
<b>Voz</b>	10000 – 20000	Alta	Media	Alto	Media
<b>Firma</b>	1000 – 3000	Alta	Media	Alto	Media

# ¿Preguntas?

**Federico Pacheco**



@FedeQuark



[www.federicopacheco.com.ar](http://www.federicopacheco.com.ar)



[info@federicopacheco.com.ar](mailto:info@federicopacheco.com.ar)