clab 2016

XVI CONGRESO LATINOAMERICANO DE INNOVACIÓN TECNOLÓGICA

La biometría, a través de canales no presenciales, como herramienta de autenticación

Por: **José Ponce**, ***PCI QSA, C|CISO, CRISC, CGEIT, MBA***

Director para Latinoamérica

Jose.ponce@newcontrol.com.pe

newControl
IT & Risk Management

Agenda

- Control de acceso: Autenticación
- Introducción a la Biometría
- Biometría: Modalidades
- Biometría: Análisis comparativo
- Biometría: Factores claves de implementación
- Biometría: Casos de éxito
- Pronósticos de la Biometría en los servicios financieros

Control de acceso: Autenticación

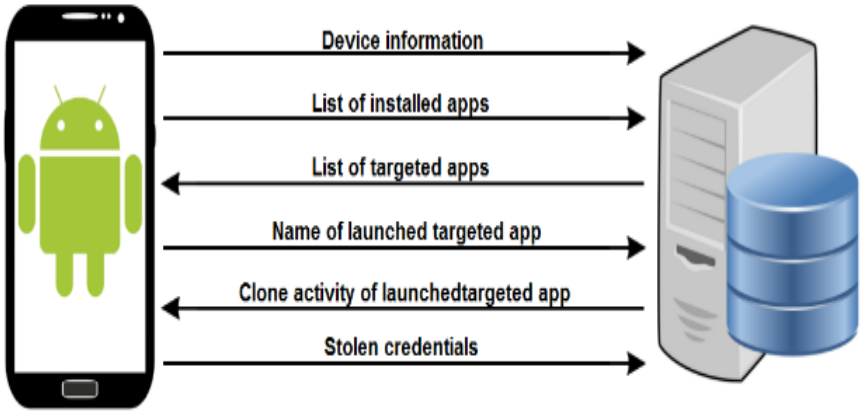
ISO/IEC 27001: Preservación de la **Confidencialidad**, **Integridad** y **Disponibilidad** de la Información.

Usuario:

- **Velocidad**
- **Seguridad**
- **No-repudio**

Ataques en la Banca Movil

TROYANO BANCARIO PARA ANDROID PRETENDE SER FLASH PLAYER Y EVADE DOBLE AUTENTICACIÓN



Marzo 2016

http://www.welivesecurity.com/la-es/2016/03/09/troyano-bancario-para-android-flash-player/

Los usuarios activos de banca móvil deben saber que hay una nueva campaña de malware dirigida a los bancos más importantes en Australia, Nueva Zelanda y Turquía. El troyano bancario para **Android roba las credenciales de inicio de sesión de 20 aplicaciones de banca móvil.**

Gracias a su capacidad de interceptar las comunicaciones SMS, el **malware también es capaz de eludir la autenticación en dos fases basada en SMS**

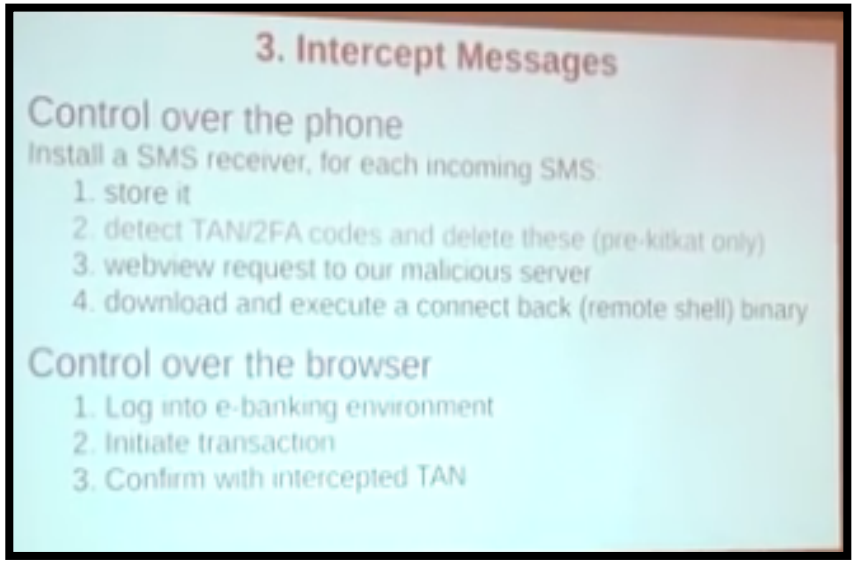
Ataques en la Autenticación: IOS y Android

Abril, 2016

How Google killed Two-Factor Authentication

La **sincronización entre las aplicaciones de diferentes sistemas operativos es el Talón de Aquiles de este sistema de verificación de la identidad**.

Como resultado, tenemos la posibilidad de **utilizar iTunes o la Google Play Store para enviar aplicaciones maliciosas a dispositivos iOS y Android** respectivamente sin que el usuario pueda hacer nada, y lo más importante, sin la necesidad de una autenticación en dos pasos.



MitB to MitMo

https://www.youtube.com/watch?v=7WiE0cpsxv4

Masivo robo de cuentas de Gmail, Hotmail y Yahoo

Cientos de millones de nombres de usuarios y contraseñas de correos electrónicos y otros sitios son ofrecidos por un hacker a criminales en foros de Internet en Rusia.

272,3 millones de cuentas robadas incluyen una mayoría de usuarios de Mail.ru, el servicio de correo electrónico más popular de Rusia.

Las cuentas de Yahoo Mail eran unas 40 millones, mientras que 33 millones pertenecían a usuarios de Microsoft Hotmail, y casi 24 millones, eran de Gmail, según Holden, que agregó que se hallaron miles de cuentas de proveedores de correo electrónicos alemanes y chinos.

cromo **5 Mayo 2016**

http://www.cromo.com.uy/masivo-robo-cuentas-gmail-hotmail-y-yahoo-n906345

Roban 167 millones de contraseñas de LinkedIn

El que podría ser el mayor robo de contraseñas de la historia tuvo lugar en 2012. Entonces sólo un reducido número de ellas salió a la luz, por lo que el verdadero tamaño del hackeo de contraseñas de LinkedIn quedó oculto.

Todos estos datos personales hackeados han sido puestos a la venta al mejor postor.

El hacker autor del robo se llama a sí mismo Peace

ComputerHoy.com

18 Mayo 2016

http://computerhoy.com/noticias/internet/roban-167-millones-contrasenas-linkedin-45176

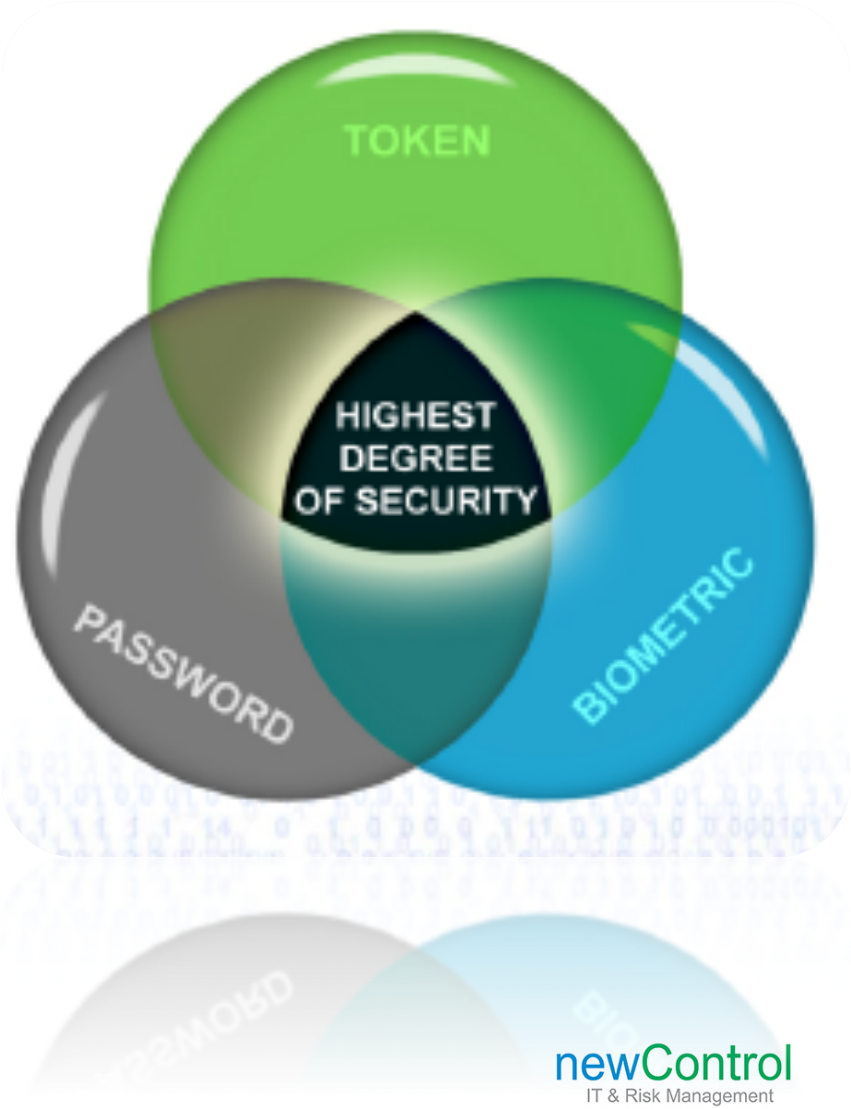
Métodos de Autenticación vulnerados con MITM

Metodo de AutenticaciÓn	Vulnerada con MITM
OTP / Tokens	El password pasa por el atacante antes del timeout del dispositivo.
IP Geolocacion	El atacante esta localizado en la misma red, usa el mismo ISP o un proxy.
Dispositivo/Hardware	El atacante simula la respuesta original del dispositivo.
Cookie del Navegador / Preguntas secretas	Las cookies pasan por el atacante, o si se pierden, se le solicitan preguntas al usuario que pasan por el atacante quedándose con las respuestas secretas.
Texto personalizado o imagen para identificación personal	Ya teniendo las respuestas secretas también es fácil conocer el texto personalizado o la imagen personal.
Teclado Virtual	La informacion es robada en transito al momento de ser enviada al servidor.
Fuera de banda (por otros medios como SMS o Email)	Después de tener el número de confirmación el usuario lo introduce a la página y este es robado al ser enviado al servidor.

Factores de Autenticación

Información utilizada para verificar la identidad de una persona.

- ✓ **Algo que el usuario conoce** (Password, PIN)
- ✓ **Algo que el usuario posee** (Tarjeta, Token)
- ✓ **Algo que el usuario es** (características biométricas: fisiológico y comportamiento)



Que es la Biometría ?

La biometría es un término general utilizado alternativamente para describir una característica o un proceso.

✓ **Como característica:**

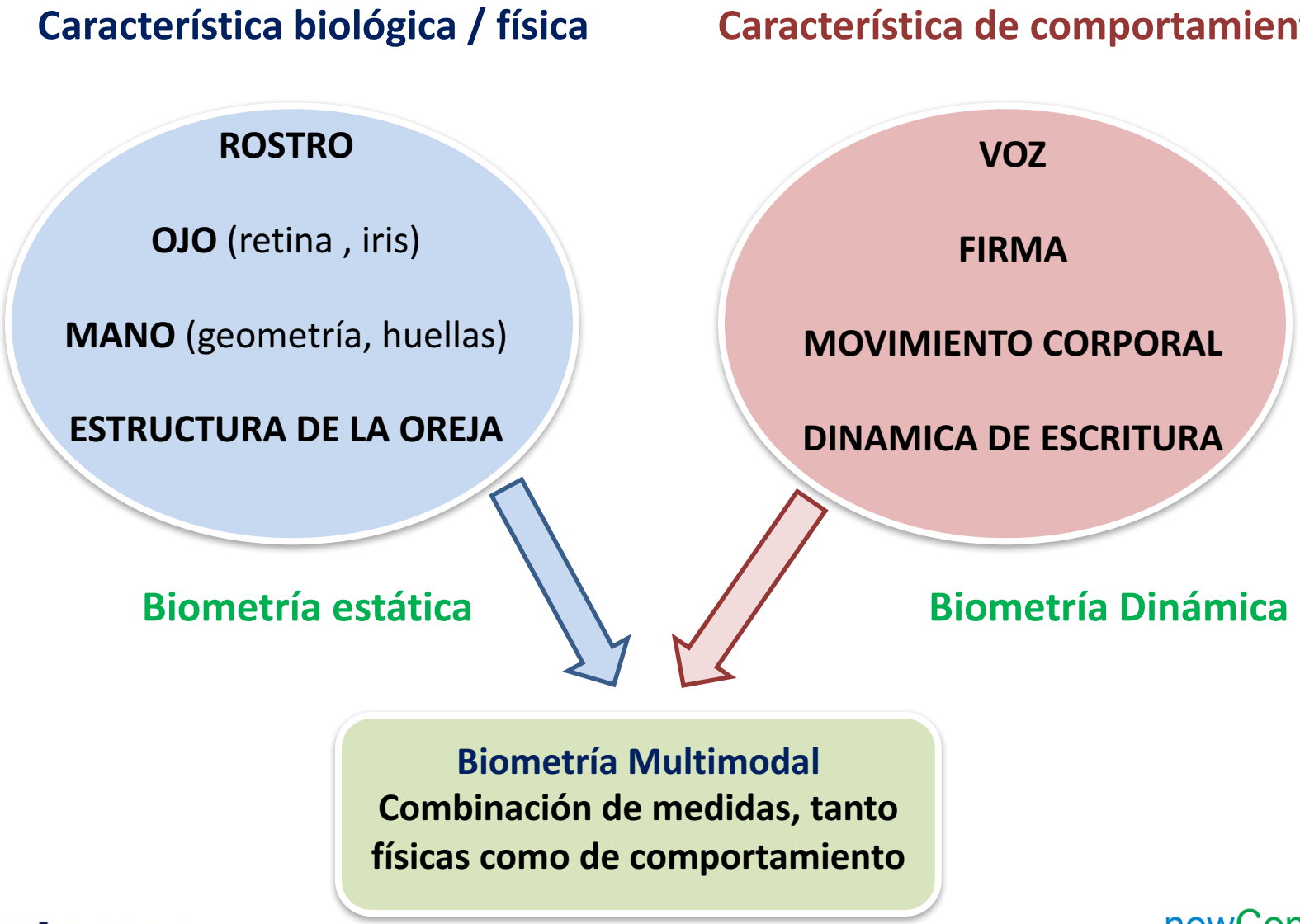
Es una característica biológica (anatómica y fisiológica) y de comportamiento medible que se puede utilizar para el reconocimiento automatizado.

✓ **Como proceso:**

Es un método automatizado de reconocimiento de un individuo basándose en las características biológicas **(estática)** y de comportamiento **(dinámica)** medibles.

National Science & Technology Council (NSTC)
Subcommittee on Biometrics and Identity Management

Soluciones Biométricas



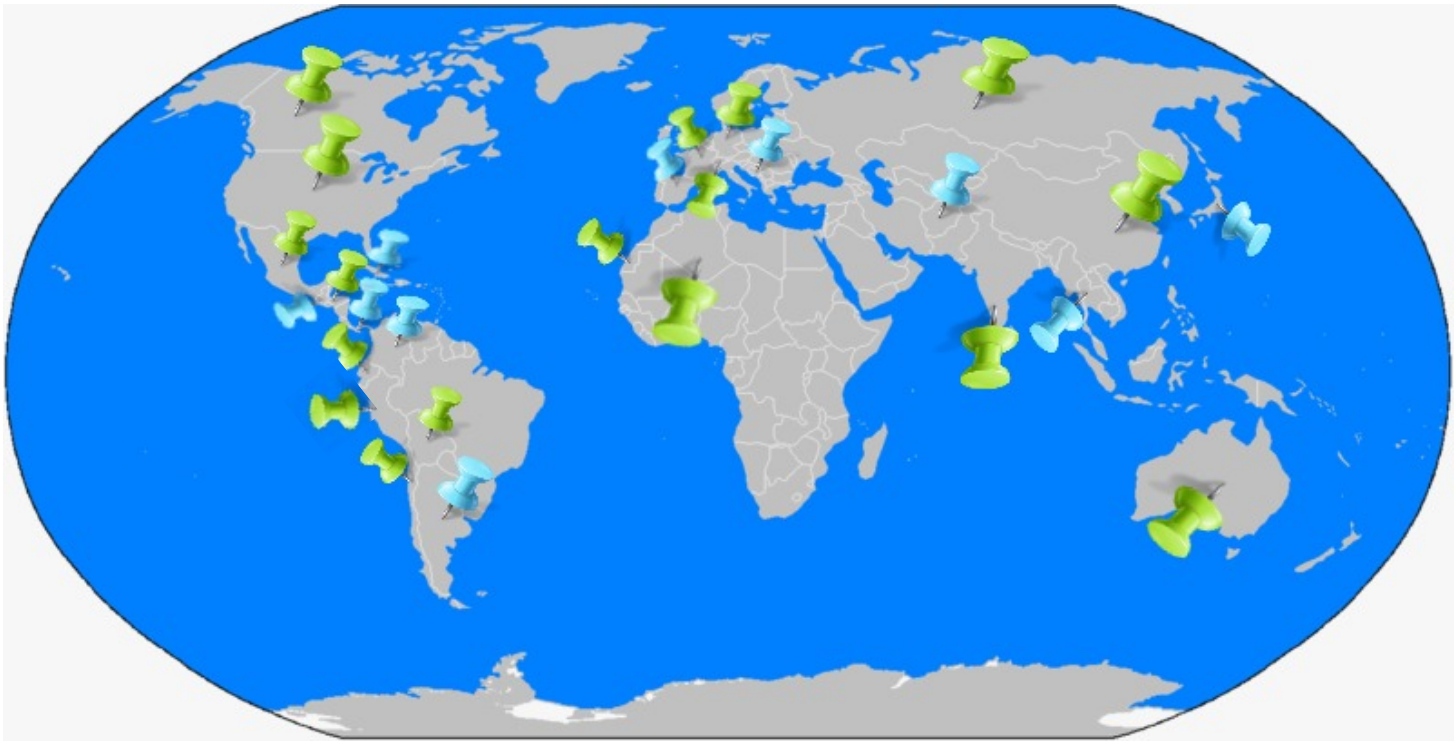
Biometría: características básicas

- ✓ **Universal:** todas las personas lo poseen.
- ✓ **Singular:** permite distinguir a una persona de otra.
- ✓ **Estable:** a lo largo del tiempo y en condiciones ambientales diversas.
- ✓ **Cuantificable:** tiene que ser medible cuantitativamente.
- ✓ **Aceptable:** por parte de los usuarios para ser considerada como parte de un sistema de identificación biométrico.
- ✓ **Rendimiento**: el nivel de exactitud elevado.
- ✓ **Usurpación:** capaz de resistir a técnicas fraudulentas.

Biometría: Estándares de la Industria

- ✓ **Estándar ANSI X.9.84:** define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.
- ✓ **Estándar NISTIR 6529:** propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.
- ✓ **Estándar ANSI 378:** establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias.
- ✓ **Estándar PIV-071006:** establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales (USA).

Bancos: Factores de Autenticación



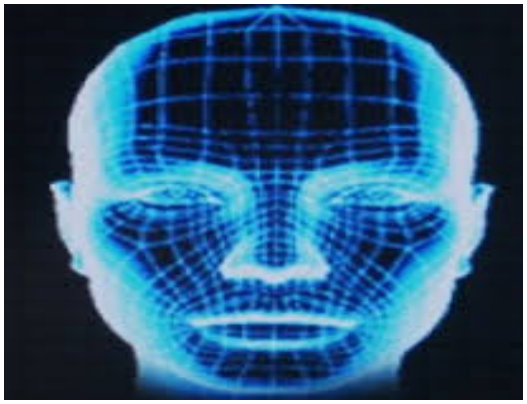
300 Bancos: 36% Token Físico, 28% Token Móvil, 22% Tarjeta, 14% Biometría

"Investigación Métodos de Autenticación", New Control, Junio 2016

Biometría en canales NO presenciales

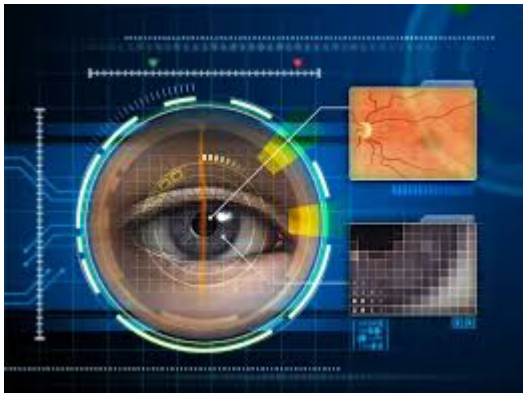
Internet, Call Center, IVR, Móvil

ROSTRO



VOZ

OJO (retina , iris)

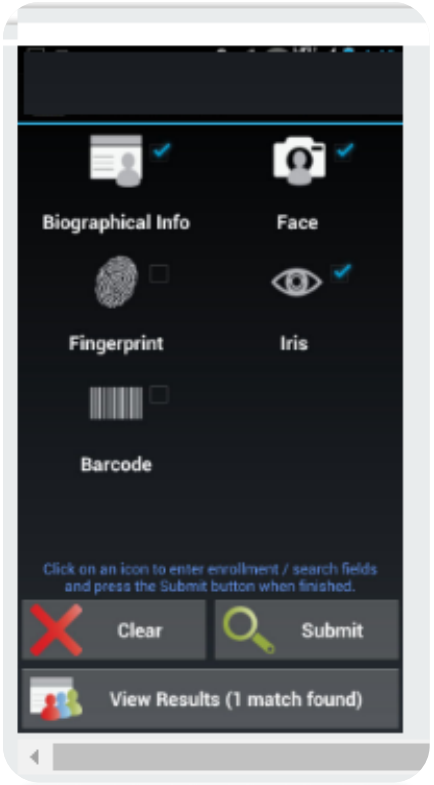


KEYSTROKES

Biometría: IRIS

- ✓ **Ventajas:**
  - No hay necesidad de tomar contacto
  - Órgano protegido con menor preponderancia a lesiones
  - Tiene una alta estabilidad a lo largo del tiempo

- ✓ **Desventajas:**
  - La captura en algunos individuos es muy difícil
  - Se la puede ocultar fácilmente con pestañas, parpados, lentes y reflejos de la córnea
  - La captura del iris requiere un mayor entrenamiento y una **mayor atención que los otros sistemas biométricos**
  - Ausencia de información que desalienta la posibilidad de utilizarlo como antecedente
  - **Los escáner del iris son relativamente caros**
  - **Los escáner pueden ser engañados por imagen de alta calidad**
  - **Requiere la cooperación de los usuarios**



National Science & Technology Council (NSTC) Subcommittee on Biometrics
International Journal of Advanced Research in Computer Science and Software Engineering , Abril 2014

Biometría: KEYSTROKES

Es la forma en que una persona escribe en el teclado.
Incluye velocidad, cómo se presiona y suelta las teclas.

- ✓ **Ventajas:**
  - Excepto el teclado, no se requiere hardware adicional
  - Fácil de implementar
  - No se requiere formación de los usuarios finales
  - Económico

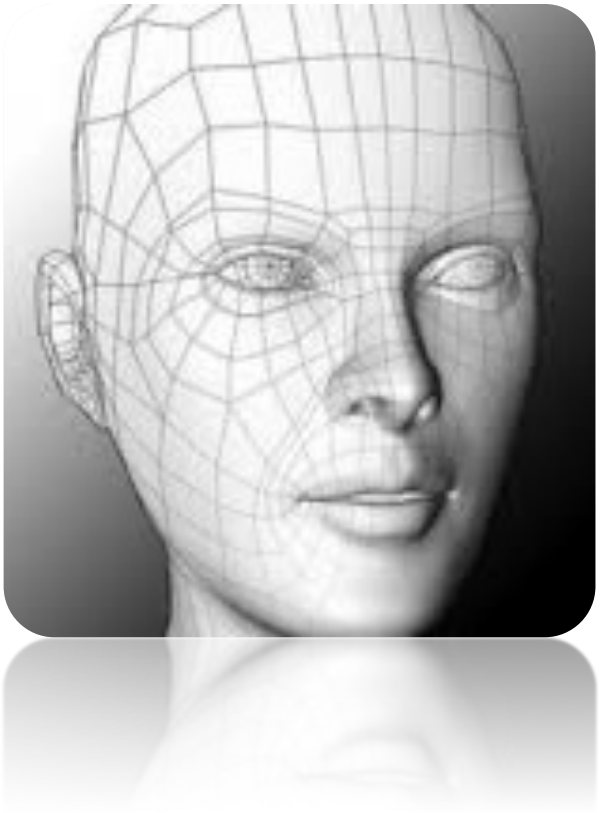
- ✓ **Desventajas:**
  - Los cambios dinámicos en “timing pattern”
  - Lesión en las manos
  - **Los cambios en el hardware del teclado (Móvil, PC)**

International Journal of Advanced Research in Computer Science and Software Engineering
Abril 2014

Biometría: ROSTRO

- **Ventajas:**
  - No requiere contacto
  - Sensores disponibles fácilmente (cámaras)
  - Grandes cantidades de datos existentes para permitir chequeos de antecedentes
  - Chequeo fácil por parte de los humanos para verificar resultados

- **Desventajas:**
  - El rostro puede ser obstruido por el pelo, anteojos, sombreros, pañuelos, etc.
  - Sensible a los cambios en la luz, la expresión y la pose
  - Los rostros se modifican conforme pasa el tiempo
  - Los usuarios son propensos a capturar imágenes de baja calidad aun esperando resultados de buena precisión



National Science & Technology Council (NSTC) Subcommittee on Biometrics

Biometría: VOZ

- ✓ **Ventajas:**
  - Aceptación pública
  - Sin necesidad de contacto
  - Sensores disponibles habitualmente (teléfonos, micrófonos)
  - **Confiable y barato**
  - **Fácil de usar y no requiere instrucciones especiales**

- ✓ **Desventajas:**
  - Dificultad para controlar las variaciones de sensores y de canales que impactan significativamente las capacidades
  - Insuficientemente distintivo para la identificación en bases de datos grandes
  - **Afectada por el ambiente ruidoso**
  - **Requiere grandes base de datos**
  - **Cambios en caso de personas que sufren de resfrío**
  - **Dependerá del estado emocional de las personas**

National Science & Technology Council (NSTC) Subcommittee on Biometrics
International Journal of Advanced Research in Computer Science and Software Engineering , Abril 2014

Biometría: Análisis comparativo

Basado en sus características básicas

	Universality	Uniqueness	Collectability	Permanence	Performance	Acceptability	circumvention
Fingerprint	M	H	M	M	M	H	M
Face	H	M	H	M	L	H	H
Iris	H	H	H	H	H	M	L
Hand Geometry	H	M	H	L	M	M	M
Retina	H	H	M	H	H	L	L
DNA	H	H	L	H	H	H	L
Gait	H	M	H	M	L	M	M
Signature	L	H	H	L	M	H	H
Keystroke	L	L	M	L	L	L	M
Voice	M	H	M	L	M	H	H

International Journal of Advanced Research in Computer Science and Software Engineering, 2014

H = High
M = Medium
L = Low

Biometría: Análisis comparativo

Basado desde un punto de vista social

	Socially introduced	Privacy concept	Hygiene factor	Safety	Cost	Popularity	Ease of use
Fingerprint	1981	H	M	M	L	H	H
Face	2000	H	L	M	M	H	H
Iris	1995	H	L	H	H	M	M
Hand Geometry	1986	L	H	M	H	L	H
Retina	1999	L	L	H	H	L	L
DNA	1965	L	M	H	H	H	L
Signature	1970`	H	H	H	M	H	H
Keystroke	2005	L	H	L	M	L	L
Voice	1998	M	L	H	L	H	H

International Journal of Advanced Research in Computer Science and Software Engineering, 2014

H = High
M = Medium
L = Low

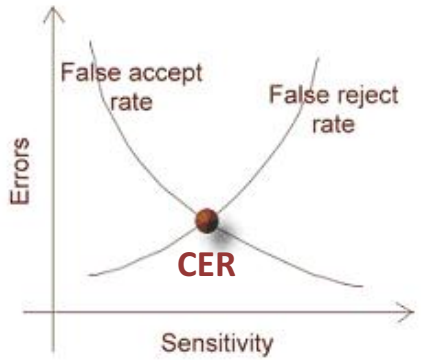
Biometría: Análisis comparativo

Basado en evaluaciones técnicas

	False accep-tance rate	False rejection rate	Crossover error rate	Failure to enroll rate	Failure to cap-ture rate	receiver operat-ing char.	Sensor subject distance
Fingerprint	2%	2%	2%	1%	-	-	30cm
Face	1%	20%	-	NA	NA	-	~20m
Iris	0.94%	0.99%	0.01%	0.5%	-	-	30cm
Hand Geometry	2%	2%	1%	NA	NA	-	10cm
Retina	0.91%	0.04%	0.8%	-	-	2cm	30cm
DNA	-	-	-	-	-	-	Zero
Signature	-	-	-	-	-	-	Zero
Keystroke	7%	0.1%	1.8%	-	-	-	Zero
Voice	2%	10%	6%	-	-	-	20cm

Cuanto más bajo es el CER, se considera que el sistema es más exacto

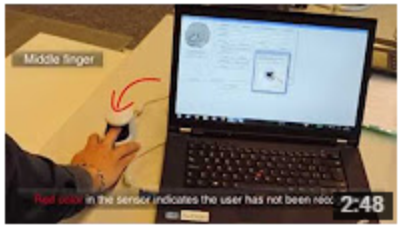
International Journal of Advanced Research in Computer Science and Software Engineering, 2014



H = High
M = Medium
L = Low

Trusted Biometrics under Spoofing Attacks (TABULA RASA)

Este proyecto es financiado por "***European Union's Seventh Framework Programme***" para la investigación, desarrollo tecnológico y demostración.

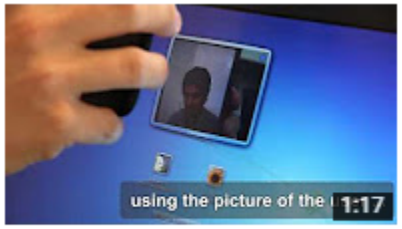


Spoofing a commercial finger vein recognition device

Spoofing FingerVein Recognition

Spoofing Face Recognition

Spoofing Near-Infrared Face Recognition



KeyLemon Countermeasures Improvement HD

BIO+EURECOM Voice AntiSpoofing Mobile

UOULU Anti-Spoofing to photo-attack in access control scenario

IDIAP anti-spoofing based on Local Binary Patterns (LBP):

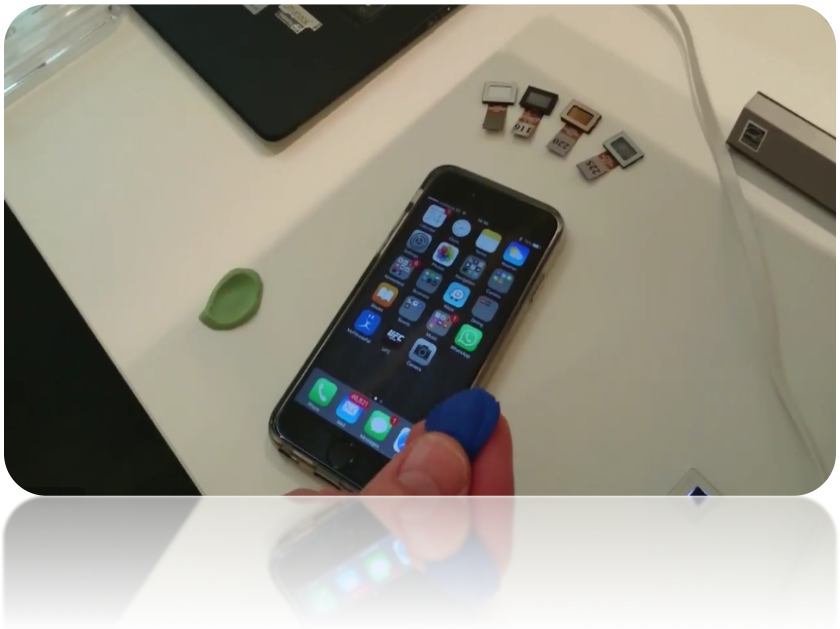
The TABULA RASA project brings together 12 research and industry partners from 5 EU Member States, from Switzerland and from China. It is led by the Idiap Research Institute (Switzerland) and also involves the University of Southampton (UK), University of Cagliari (Italy), University of Oulu (Finland), Universidad Autonoma de Madrid (Spain), EURECOM (France), Morpho (France), Starlab Barcelona (Spain), the Chinese Academy of Sciences (China), KeyLemon (Switzerland), BIOMETRY (Switzerland) and the Centre for Science, Society and Citizenship (Italy).

iPhone's Touch ID hacked with Play-Doh

Febrero 2016

Mobile World Congress, una empresa china mostró que es posible desbloquear un iPhone usando plastilina infantil.

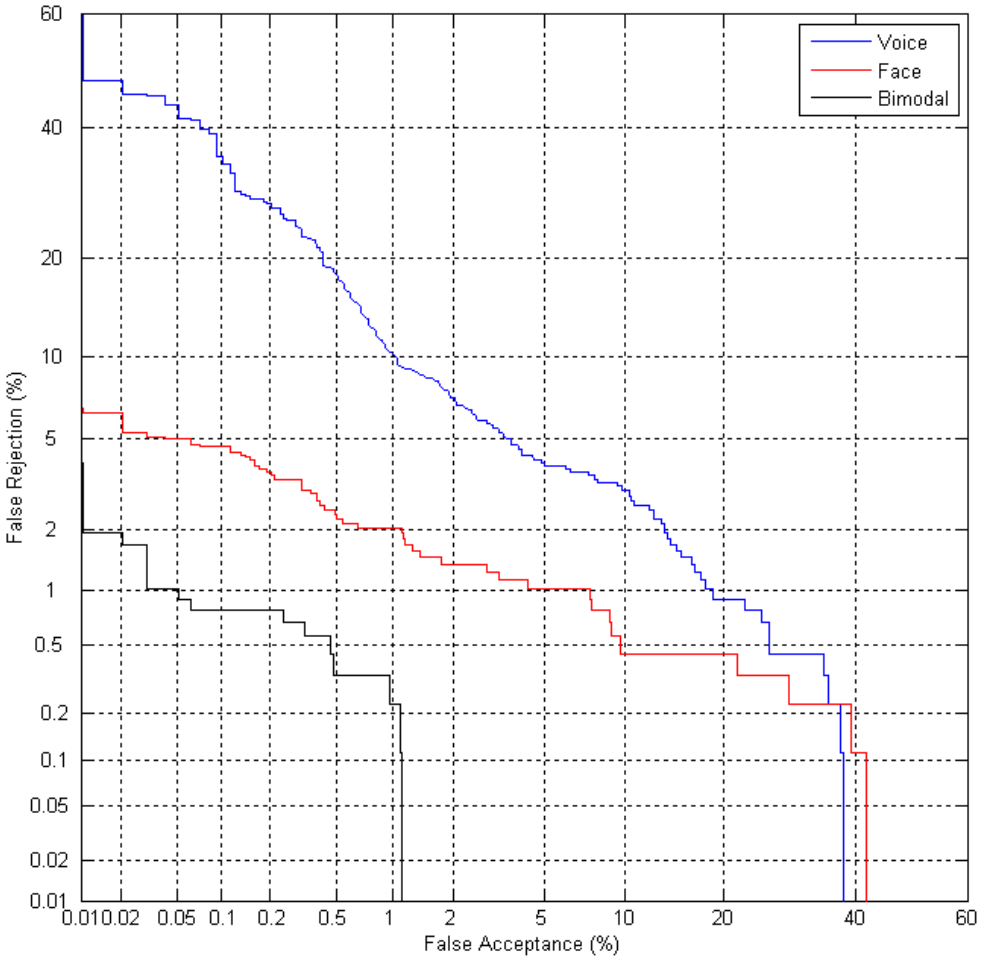
En el vídeo, Jason Chaikin, presidente de la firma de seguridad móvil Vkansee, muestra que es posible desbloquear uno de los últimos iPhones de Apple que utilizan una masa de plastilina.



http://www.iphonehacks.com/2016/02/iphone-touch-id-hacked-with-play-doh.html

Canal NO presencial: Biometría Multimodal

EL ENFOQUE MULTIMODAL REDUCE DRÁSTICAMENTE LA TASA CER



VOZ + ROSTRO

- Son fáciles de combinar
- La combinación es más precisa que un solo rasgo biométrico de cualquier otro tipo
- CER es menor a 0.5% para la verificación multimodal
- FA es de 0.01% siendo FR menos de 2%

Biometría: Análisis comparativo

Basado en la oferta de proveedores

Proveedor	Modalidad Biométrica		Detección de Vitalidad	CANAL			
	VOZ	ROSTRO		TELEFONO (solo voz)	MOVIL	WEB	PC
STC	✓	✓	✓	✓	✓	✓	✓
Nuance	✓			✓	✓	✓	✓
Sensory	✓	✓			✓	✓	✓
Daon	✓	✓					
BioID	✓	✓	✓		✓	✓	✓
Mobbeel	✓	✓			✓		

Biometría: Factores claves de implementación

La efectividad de una tecnología biométrica depende de cómo y dónde se la utiliza.

- ✓ **Ubicación**
- ✓ **Riesgos de seguridad**
- ✓ **Tarea (identificación o verificación)**
- ✓ **Numero esperado de usuarios**
- ✓ **Condiciones del usuario**
- ✓ **Datos existentes**

National Science & Technology Council (NSTC)
Subcommittee on Biometrics and Identity Management

Riesgos en la solución biométrica

Requerimientos adicionales de seguridad

- ✓ Prevenir la captura de datos biométricos que puedan ser reintroducidos de nuevo en el sistema de forma fraudulenta.
- ✓ Asegurar que los datos biométricos sean introducidos solamente a través de interfaces autorizadas.
- ✓ Considerar mecanismos de protección para **detectar** el fraude mediante el **uso de datos biométricos "falsos"**.
- ✓ Establecer mecanismos de protección para **prevenir la exposición o pérdida de datos biométricos**.
- ✓ Establecer mecanismos de protección para asegurar que el procedimiento de alta (enrolamiento) no permita la inscripción de falsas identidades

Atom Bank: Biometría y videojuegos aplicados a la banca

06 abril 2016

Atom Bank, el **banco de acceso exclusivamente móvil**, empieza a operar en **Reino Unido**.

A través de su aplicación móvil, el banco ofrecerá a finales de 2016 una amplia gama de productos bancarios como cuentas corrientes, hipotecas y tarjetas de crédito.

Atom Bank incluye novedades como:

- La utilización de **reconocimiento facial biométrico**, pionero en Reino Unido, para aumentar tanto la seguridad como la personalización a la hora de conectarse.
- La aplicación móvil está basada en la plataforma de desarrollo de **videojuegos** ***Unity*** para que la experiencia de cliente sea más atractiva.
- El uso por primera vez de un programa de **aprendizaje automático** para la atención al cliente, que permite dar respuestas de manera rápida.
- El alta de clientes **completamente *online***.

Santander

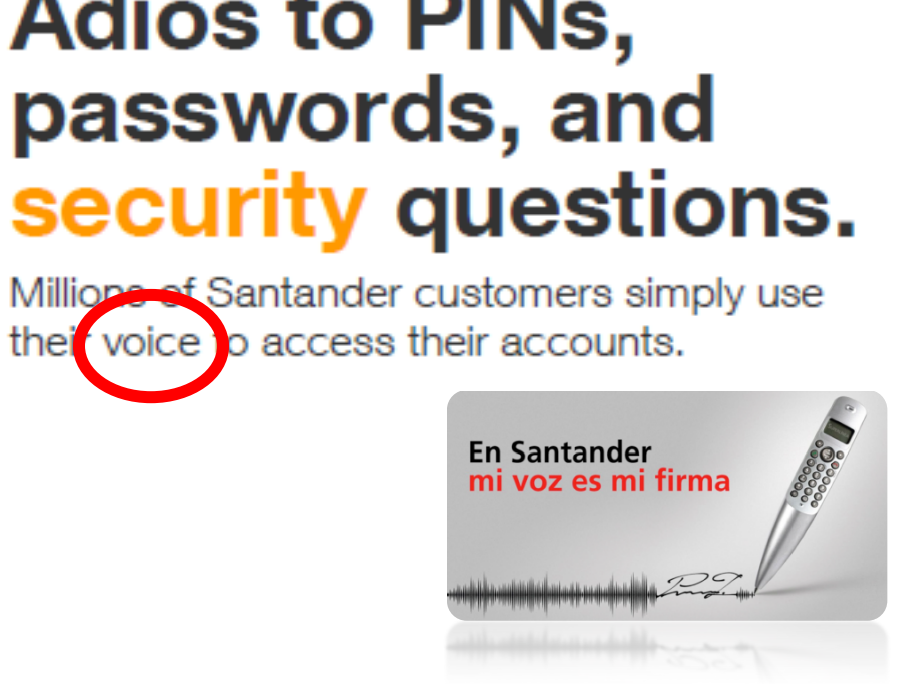
- **Cant. de operadores de Call Center:**

  4200 (en dos sedes)

- **Cant. de clientes:** +10 MM en México

- **Cant. de llamadas por mes:**

  +3 MM (55% IVR /45% operadores)



- El primer banco en México para desplegar una solución biométrica de voz.
- **Reducción de tiempo** en la identificación y verificación del cliente: de 72 segundos a 30 segundos.
- **Ahorro**: se ha logrado un ahorro anual de $ 1 millón.

HISTORIA DE ÉXITO

Implementación Piloto

- Verificación de los clientes actuales durante el registro inicial:
  - eliminar el fraude
  - eliminar registros duplicados

Itaú

Speech Technology Center

Itaú es es un banco internacional de Brasil que realiza operaciones en América del Norte y América del Sur, Europa y Asia, brindando servicios en un amplio abanico de segmentos de actividad

- ✓ Primera institución financiera de Estados Unidos que ofrece reconocimiento facial y de voz para la autenticación en una **aplicación móvil**.
- ✓ La biometría de rostro y de voz se captura durante la inscripción utilizando el dispositivo móvil propio del cliente.
- ✓ Para el reconocimiento de voz, los usuarios leen una frase corta.
- ✓ Los clientes de USAA que han aceptado hasta ahora la biometría, **prefieren el reconocimiento facial** por encima de la voz.

http://www.idnoticias.com/news-item/la-biometria-asegura-la-proxima-generacion-de-la-banca-movil/#sthash.Cl6YdSvZ.dpuf

- Que los clientes ingresaran largas contraseñas, había creado muchos inconvenientes y algunas otras tecnologías no eran fáciles de usar.
- La compañía eligió la biometría de voz para el *login* en la aplicación móvil
- El 2% del total de las sesiones fueron “falsos rechazos” y no hubo ningún caso de aceptación falsa.
- Un 88% de las sesiones fueron autenticadas en el primer o segundo intento.

http://www.idnoticias.com/news-item/la-biometria-asegura-la-proxima-generacion-de-la-banca-movil/#sthash.Cl6YdSvZ.dpuf

Tangerine

Forward Banking™

CANADA'S 10 MOST ADMIRED CORPORATE CULTURES™ 2015
Presented by Waterstone

NOTED PRODUCT OF THE YEAR CANADA Consumer Survey of Product Innovation 2016

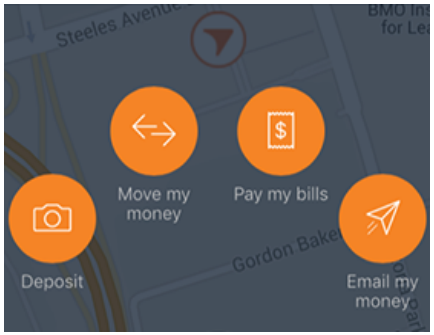
- Primer banco en Canadá en brindar una ***aplicación móvil*** controlada por voz desde el 2014.

- Desde el primer trimestre del 2016 su app móvil incluye el **primer chat seguro** en el que el cliente se comunica con un representante del banco.

Ipsos Best Banking 2015

Por undécimo año consecutivo, es reconocido como el líder de servicio al cliente en **Ipsos Best Banking** de Canadá, con seis premios en las siguientes categorías:

- Recommend to Friends or Family
- Interest Rates & Service Charges
- Products & Services Excellence
- Online Banking Excellence
- Mobile Banking Excellence
- Value for Money



Después de la voz, se incluyo la Huella digital (IOS y Android) y recientemente la autenticación del Iris

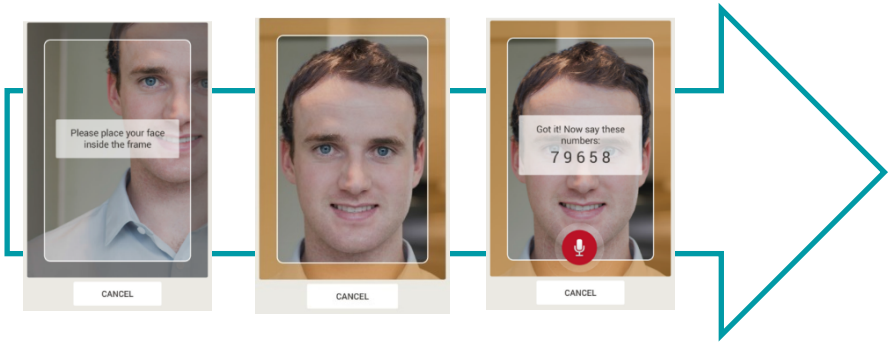
http://www.idnoticias.com/news-item/la-biometria-asegura-la-proxima-generacion-de-la-banca-movil/#sthash.Cl6YdSvZ.dpuf
http://www.newswire.ca/news-releases/tangerine-first-bank-in-canada-to-launch-eyeverify-vocalpassword-and-in-app-secure-chat-577123761.html

Exitosa implementación en Wells Fargo

FÁCIL Y SEGURO ACCESO BIOMÉTRICO VÍA MÓVIL

Speech Technology Center

Detección de vitalidad



Inicie la aplicación | **Mire a la cámara** | **Lea la contraseña**

- Banco Wells Fargo es TOP-5 en EEUU
- La combinación de **voz** y **rostro** se usa para la autorización de acceso de los clientes al sistema de **banca móvil**
- La prueba piloto presento una tasa de rechazo menor del 1%
- Descartaron la huella digital, porque los escáneres en dispositivos móviles solo dan un sí o no como respuesta, y no dan una calificación.

http://www.idnoticias.com/news-item/la-biometria-asegura-la-proxima-generacion-de-la-banca-movil/#sthash.CI6YdSvZ.dpuf

Reporte 2016

La biometría como método de pago impulsan europeos

- ✓ El 68%, **ya sea pagando desde su casa o en la tienda,** quiere usar la biometría como método de autenticación de pago.
- ✓ El 31% no se anima a comprar en comercios online porque **consideran insuficientes las medidas de seguridad** existentes en la actualidad.
- ✓ El 81% de los consumidores ve el sistema de huellas digitales como el método más seguro, seguido de la exploración del iris ocular (76%).
- ✓ El 51% afirma que la autenticación biométrica para pagos puede crear una **experiencia de pagos más ágil y fácil** que los métodos tradicionales.

Visa encargó a Populus la elaboración de este estudio de pagos biométricos, cuya muestra total ascendió a **14.236 encuestados**. El trabajo se realizó entre el **22 de abril y 6 de mayo de 2016** en siete países europeos: **Reino Unido, Suecia, España, Francia, Alemania, Italia y Polonia**.

http://www.pcworldenespanol.com/2016/08/29/la-biometria-metodo-pago-impulsan-europeos/

Tendencias de uso de la Biometría en los servicios financieros

Goode Intelligence identifica cinco tendencias sobre la adopción biométrica en diversas áreas de servicios financieros:

1. La biometría reemplazará los PIN de seguridad del ATM en cualquiera de estos escenarios:

- **Cardless utilizando un sensor biométrico integrado en el ATM.**
- **Cardless usando biometría basada en móviles como identificador para retirar efectivo.**
- **El uso de una tarjeta biométrica plástica, con:**
  - **Sensor biométrico integrado en la tarjeta para efectuar match-on-card.**
  - **Los datos biométricos almacenados en la tarjeta para que el cliente lo presente al sensor integrado del ATM y efectuar match-on-card.**

2. los pagos móviles sin contacto ofrecidos por Apple, Google, Samsung, PayPal, Alipay y los proveedores de esquemas tradicionales de pago, promoverán la biometría.

Goode Intelligence, "Biometrics for Financial Services analyst report series" Febrero 2016

Tendencias de uso de la Biometría en los servicios financieros

3. El aumento del fraude con tarjeta no presente (CNP) será enfrentado mediante la autenticación biométrica del móvil del usuario y la verificación de las transacciones con el apoyo de EMV Co y 3D Secure 2.0.

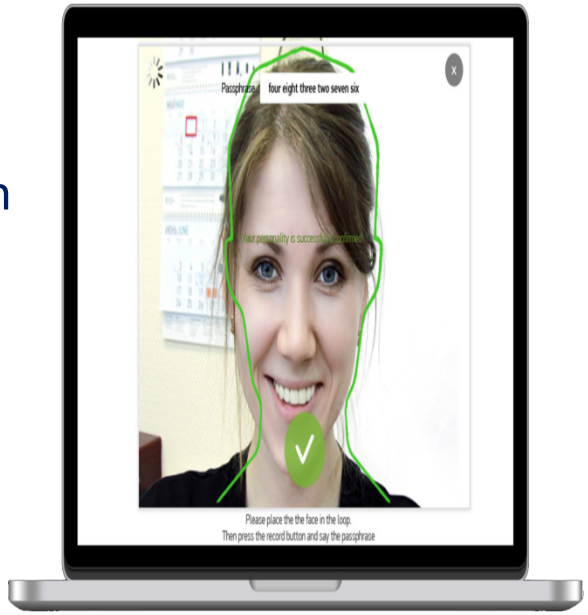
4. Uso de pagos para soportar modalidades biométricas que se ajustan al dispositivo, incluyendo las de ritmo cardiaco (ECG) y de conducta.

5. La autenticación biométrica multimodal se convertirá por defecto en las aplicaciones bancarias móviles.

Goode Intelligence, "Biometrics for Financial Services analyst report series", Febrero 2016

2020: Pronósticos de la Biometría en los servicios financieros

- ✓ Para el año 2020, habrá más de **622 millones de descargas** de aplicaciones de banca móvil que utilizaran la biometría para la autenticación del cliente y verificación de las transacciones.
- ✓ Casi **160 millones de dispositivos** portátiles soportaran biometría para la banca en 2020.
- ✓ En 2020, la biometría protegerá más **de $ 5.6 billones de pagos**.
- ✓ **350 millones de clientes** utilizaron la biometría para la seguridad de sus pago durante el año 2015.
- ✓ **Mil millones de usuarios de biometría móvil** para servicios financieros en el 2020.



Goode Intelligence, Febrero 2016

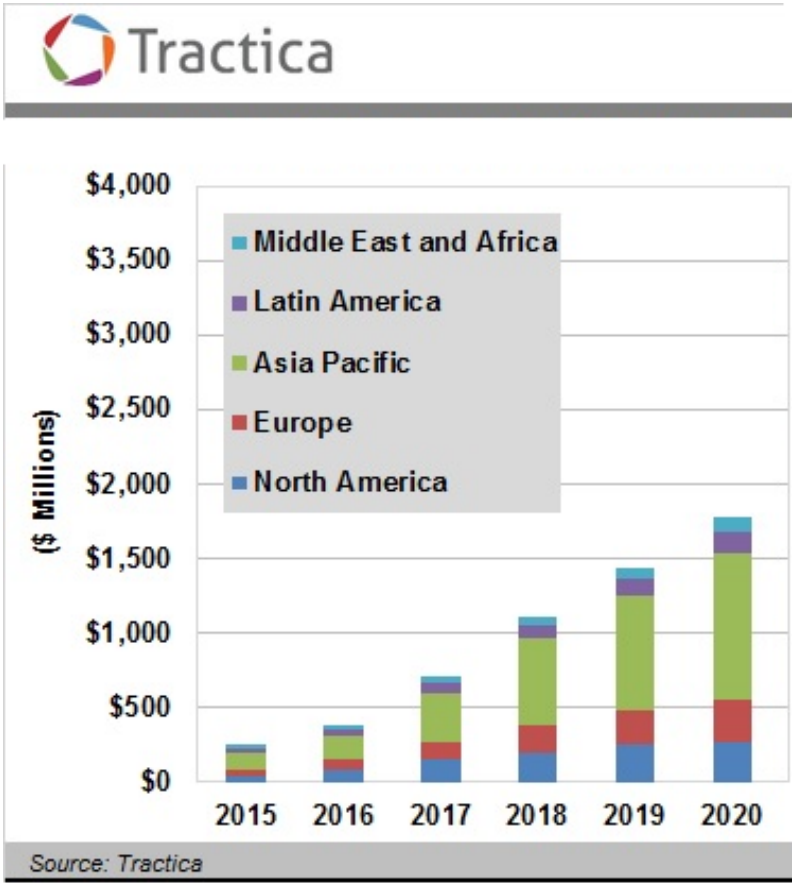
Biometrics for Banking; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020
Biometrics for Payments; Payment Security Gets Personal; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020
Mobile Biometrics for Financial Services; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020

BIOMETRÍA MULTIMODAL: TENDENCIAS DEL MERCADO

Análisis del mercado

Una tendencia firme del mercado es la **biometría multimodal**, por lo cual la producción se orienta hacia el mercado comercial, incluyendo los usuarios finales.

- ✓ Se estima que hacia el año 2020 el volumen del mercado mundial de la biometría llegará hasta 16,6 mil millones de dólares, de los cuales **1,8 mil millones de dólares corresponderán a la biometría móvil.**
- ✓ En la figura está representada la dinámica estimada del mercado de la biometría móvil y la distribución de ventas por regiones hacia el 2020.



*Fingerprint Recognition, Voice Recognition, Facial Recognition, and Other Biometric Modalities for Identification and Authentication Applications: Global Market Analysis and Forecasts. https://www.tractica.com/research/biometrics-for-mobile-devices/

Biometría en SmartCards

Jul-2016: Visa, MasterCard y PASA (Asociación de Pagos de Sudáfrica) Estándar de Biometría sobre chips EMV, como medio formal de autenticación

Jul-2016: FIDO Alliance junto a EMVCo Incorporan métodos Biométricos en el estándar EMV

Hay una **tendencia hacia la integración de validaciones Match-on-Card con Biometría**, con las siguientes ventajas:

- ✓ Desempeño, disponibilidad y conveniencia
- ✓ Flexibilidad y Escalabilidad

  Ejemplo: Biometría multi-modal MoC, actualización de parámetros

http://businesstech.co.za/news/banking/131500/fingerprint-technology-coming-to-sa-bank-cards/

http://findbiometrics.com/fido-emvco-collaborate-307131/

clab 2016

XVI CONGRESO LATINOAMERICANO DE INNOVACIÓN TECNOLÓGICA

La biometría, a través de canales no presenciales, como herramienta de autenticación

Por: **José Ponce**, ***PCI QSA, C|CISO, CRISC, CGEIT, MBA***

Director para Latinoamérica

Jose.ponce@newcontrol.com.pe

newControl
IT & Risk Management