## Interacciones crecen exponencialmente

Hoy en día, ya usamos nuestras identidades varias veces al día; en el futuro, serán innumerables.

IDEMIA

## Nuestro mundo es cada vez más vulnerable – Crece el riesgo de Fraude

La privacidad del usuario y la seguridad de los datos son clave para que las personas se sientan seguras

Análisis de Datos - Un requisito indispensable para generar cadenas de confianza

**Era ULTRA CONECTADA**

**Equilibrar - Sin Fricción - Seguridad**

1

## Estamos seguros que la identidad es la clave para….

IDEMIA Feb. 2023 | Group presentation

### conectarnos con nuestro entorno

A través del crecimiento de dispositivos conectados

### Reducir la brecha entre en mundo físico y el mundo digital

Reinventando la forma como interactuamos, mas fluida y sin fricción

### Es el corazón de nuestras interacciones diarias

Cada vez que pagamos, que nos conectamos, accedemos, viajamos, pagamos, rentamos, compramos, pedimos….

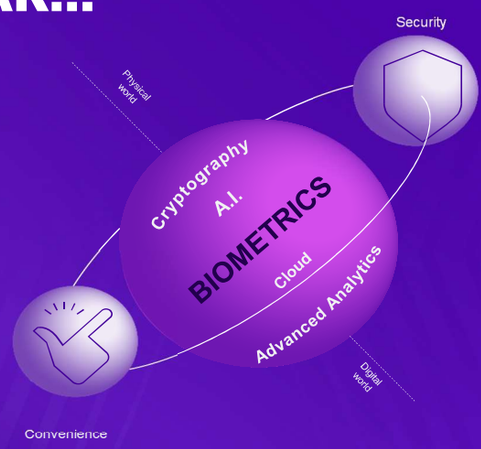
2

**LA IDENTIDAD es el único y mas Preciado activo de una persona**

**En la medida que las interacciones sean mas fáciles y seguras, se genera un sentimiento de libertad y tranquilidad para viajar, pagar, acceder, comprar, rentar…..**



# APALANCANDONOS EN NUESTRA HABILIDAD PARA COMBINAR…



## Sensores para detección de huella dactilar sencillo: MorphoSmart™ 1300 Series


Customer Video IDFC Aadhaar Pay Cashless purchases
https://youtu.be/y_FcQGgrpSo

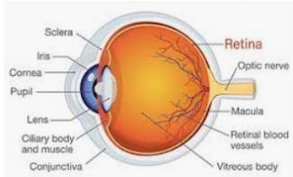
January 2018

## Principios de biometría

**Que es? Uso de tecnologías para analizar características del cuerpo humano**

Una tarjeta de acceso es lo que usted lleva
Una Credencial Virtual / QR es lo que usted lleva en su Teléfono
Un PIN es lo que usted sabe y debe recordar

**BIOMETRÍA ES LO QUE USTED ES**




## Biometría sin Contacto

https://youtu.be/5ugup7BIznc



# VISION GENERAL

## Evaluaciones externas, objetivas y neutrales

**A diferencia de otras industrias no existen certificaciones externas obligatorias para dispositivos de biometría**

**...Significa**
**Los departamento de compras de Seguridad deben creer en los cuadros de datos y publicaciones de marketing...**
**O hacer sus propios test POC**

**Ejemplo en sistemas de pagos**

Tarjetas y sistemas POS deben aprobar certificaciones de seguridad
La lista de vendors certificados es publica y los **Bancos** solo deben adquirir este tipo de sistemas

**Con Cuidado**

Los test o pruebas de concepto no prueban lo que un laboratorio certificado puede validar

IDEMIA

8

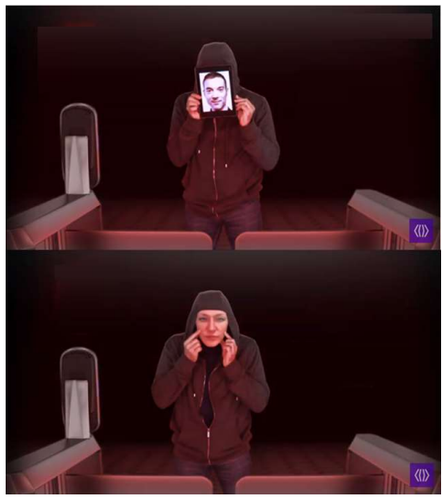
# RESISTENTE A INTENTOS DE SUPLANTACIÓN

## Resistencia a falsear los sitemas

*¿Quien desearía que sus terminales sean fácilmente vulneradas y la identidad sea suplantada con imágenes impresas o en celulares o tabletas?*

Que tan robustos son los mecanismos para garantizar estos niveles de seguridad implementados en la terminal

¿como medir la eficiencia?



IDEMIA



## Certificado PIV IQS

Productos certificados **FBI PIV IQS**, estándar de referencia para calidad óptica de los dispositivos

https://fbibiospecs.fbi.gov/certifications-1/cpl

CERTIFICATION OF COMPLIANCE

for

MORPHO

Model *CBM-E3, MSO 1300 E3, MSO 1350 E3* single finger livescan capture devices without membrane at 500ppi.

The FBI certifies that the equipment described above is in compliance with the following FBI CJIS Division's Next Generation Identification System Image Quality Specifications (IQS):

Personal Identity Verification (PIV)
Single Finger Capture Device Specifications

This certification process does not constitute an endorsement, but only attests that the product meets FBI standards. Continued acceptance of the images created by an installed system, for retention in the FBI Master Fingerprint files, is contingent on the ability of the product to meet the IQS over time. As equipment can degrade, the FBI recommends that your company assist customers in the establishment of quality assurance programs and appropriate maintenance schedules for your products.

*This certification process is not intended to endorse one entity or implementation over another, but merely to certify that the implementation meets FBI standards. The authenticity of this certificate can be confirmed by checking the online registry at <fbibiospecs.cjis.gov>.*

Date: July 28, 2015

January 2018

## Calidad de la adquisición

- **Calidad de imagen de huella**
  - La alta calidad es CLAVE
  - FBI PIV IQS requerimientos relacionados con
    - →nitidez y detalles de interpretación de la huella
    - →Precisión Geométrica (distorsión)
    - →Nivel de grises uniforme
    - →Contraste
    - →Relación señal a ruido (noisy background)
    - →Carencia de características, malformaciones etc.….
  - STQC Certificado

## Seguridad En redes y dispositivos

❑ SEGURIDAD EN BORDE

✓ Enrolamiento propietario en borde

✓ Templates protegidos encriptación AES 128 / 256

✓ Dispositivos protegidos por contraseña

✓ Actualizaciones de Firmware

✓ Interruptor de sabotaje

✓ Sistema FFD (Fake Finger/Face Detection)

## Seguridad En redes y dispositivos

- ❑ SEGURIDAD EN COMUNICACIONES
  - ✓ CIFRADOS Y SEGUROS
  - ✓ OSDP V2
    - ✓ Security Industry Association (SIA)
    - ✓ https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/
  - ✓ Autenticación TLS 1.2 / SSL


May 2019

## Seguridad En redes y dispositivos

- ❑ SEGURIDAD EN SERVIDOR
  - ✓ Templates Cifrados en Lugar de imágenes
  - ✓ Perfiles de Usuario
  - ✓ Software protegido con Contraseña
  - ✓ Canales de comunicación protegidos

May 2019

# GDPR

**Reglamento General de Protección de Datos**

**Política de protección de datos**

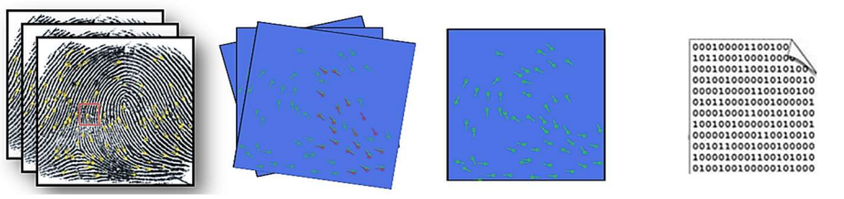
**Imágenes de la biometría?**


IDEMIA

## Almacenamiento de datos y privacidad

**No es necesario almacenar imágenes o datos biométricos puros**

* El template es una representación matemática de los puntos característicos.



Adquisición y detección de minucias

Imagen descartada – comparación y validación de minucias

Consolidación final de el template de enrolamiento

Template almacenado como un archivo de código digital

January 2018

## SEGURIDAD Y PRECISIÓN

False Negative Identification Rates (FNIR)

Falso Aceptación

Falso Rechazo

False Match Rate

False Non-Match Rates

AGILIDAD

EER

%

+ Conveniencia

Threshold – Umbral

+ seguridad

TASA DE FALSA ACEPTACIÓN Ajustable de 1/100 a 1/100,000,000

False Positive Identification Rate (FPIR)

January 2018

## Estándares de comparación NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



281 algoritmos de 75 vendors has sido probados desde el inicio

January 2018

## Estándares de comparación NIST

**99,88% de precisión**
en la prueba NIST FRVT

Face Recognition Vendor Test

**Ranked #1**
en el desafío NIST mFIT

Mobile Fingerprint Information Technologies

**Ranked #1** en tecnologías de reconocimiento de tatuaje
(Tatt-E)

Tattoo Recognition Technology Evaluation

January 2018

**Ranked #1** en coincidencia de huellas dactilares NIST

**MINEX TEST Results**
False Non-Match rates at a fixed False Match Rate of .01
Table 1:Results for all ongoing MINEX vendors

NIST National Institute of Standards and Technology U.S. Department of Commerce

*fijando un % de falsa aceptación
Da como resultado un % de falsos rechazos

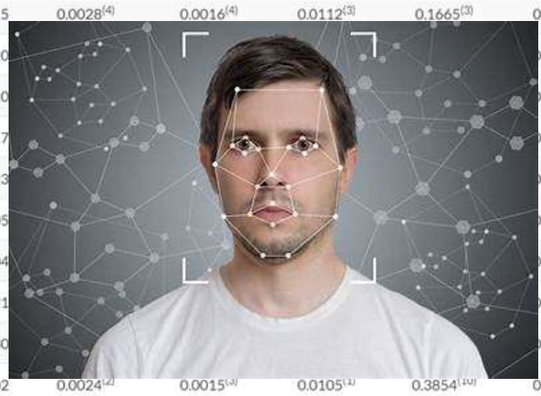
January 2018

NIST National Institute of Standards and Technology U.S. Department of Commerce

https://www.nist.gov/itl/iad/image-group/ongoing-minex-evaluation-results

## FRVT 1:N Identification Face Recognition Vendor Test (FRVT) | NIST

| Algorithm | Date | Mugshot Mugshot N = 12000000 | Mugshot Mugshot N = 1600000 | Mugshot Webcam N = 1600000 | Mugshot Profile N = 1600000 | Visa Border N = 1600000 |
|---|---|---|---|---|---|---|
| idemia_008 | 2021_03_15 | 0.0028(4) | 0.0016(4) | 0.0112(3) | 0.1665(3) | 0.0035(1) |
| | 2021_02_10 | | | | | 0.0041(2) |
| | 2020_08_10 | | | | | 0.0046(3) |
| | 2020_12_17 | | | | | 0.0048(4) |
| | 2020_07_23 | | | | | 0.0051(5) |
| | 2021_02_05 | | | | | 0.0055(6) |
| | 2020_08_04 | | | | | 0.0061(7) |
| | 2021_01_21 | | | | | 0.0065(8) |
| | 2018_10_30 | | | | | 0.0065(9) |
| | 2019_12_02 | 0.0024(2) | 0.0015(3) | 0.0105(1) | 0.3854(10) | 0.0065(9) |



https://pages.nist.gov/frvt/html/frvt1N.html

January 2018

## Top performer en el rally biométrico del DHS

2020 Biometric Technology Rally prueba sistemas biométricos de la industria para identificar personas con sistemas de alto tráfico usando mascarilla

Sistema de Captura

1:582 identification

Algoritmo

Homeland Security

Science and Technology

The Maryland Test Facility

https://mdtf.org/

January 2018

- https://mdtf.org/Downloads/MatchingSystemResults.pdf

# ESTANDARES DE LA INDUSTRIA


- Asegurémonos que los sistemas se evalúen ante NIST / DHS y más especialmente que los resultado iBeta PAD sean requeridos

***Genuine***
*Bona fide presentation*

***Impostor***
*Attack presentations L1*

***Impostor***
*Attack presentations L2*



# ACERCA DE iBeta

## Y la evaluación PAD

iBeta QUALITY ASSURANCE

- Laboratorio de Estados Unidos
- Pruebas de software de servicios críticos desde1999
- Ha desarrollado habilidades y especializado en pruebas de Sistemas biométricos
- laboratorio para pruebas en biometría acreditado por el NIST NVLAP

## PAD

### Presentation Attack Detection

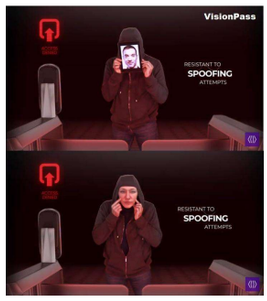
- Evaluación de referencia en la industria biométrica en cuanto mecanismos para evitar la suplantación de identidad (antispoofing)
- De conformidad con los estándares ISO/IEC 30107-3, alineado con los marcos de referencia ISO/IEC 30107-1
- Varios cientos de intentos de usando distintos métodos:
  - **Level 1** : 2D/3D Fotografías presentadas desde impresiones o pantallas de celulares o tabletas
  - **Level 2** : Intentos usando mascaras 3D

https://www.ibeta.com/biometric-testing/

**Test method** : https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/

## Sistema de detección de Rostro / huella Falsos - FFD

- En un sistema biométrico el factor de precisión es mandatorio a fin de asegurar que los impostores no son permitidos en un sistema.
  - NONE → FFD deactivated
  - LOW → FFD Low security level / FRR = 0,5%
  - MEDIUM → FFD Medium security level / FRR = 1,5 %
  - HIGH → FFD High security level / FRR = 5%




- Función de dedo o rostro falso:
- Algoritmo de detección
  - Agilidad
- Calidad de Imagen

* Wikipedia

January 2018

IDEMIA

# COMO AUMENTAR LA SEGURIDAD DE SU SISTEMA DE CONTROL DE ACCESO

# CIBERSEGURIDAD

- Debido a diferentes tensiones y casos a nivel mundial, diferentes agencias han recomendado a las empresas el refuerzo de sus sistemas de Cibersegurdad-1.
- El sistema de control de acceso es uno de estos sistemas que se deben proteger, dado que este restringe el acceso de las personas a los sistemas de IT.
- Como las terminales biométricas hacen parte del sistema de control de acceso, se recomienda reevaluar su configuración, ambiente y caso de uso. Acá listamos algunos Consejos para su configuración.

- 1-French Agence Nationale de Sécurité des Systèmes d'Information and the UK National Cyber Security Centre

IDEMIA



# SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

- **Buenas practicas:**
  - Se recomienda incrementar la seguridad de su sistema instalado terminales biométricas IP, resguardadas en sistemas de protección de red y de preferencia **aisladas de la red corporativa y de la Internet.**
  - Seguir las guías de Idemia de **buenas practicas de seguridad y protección de datos personales y recomendaciones de instalaciones seguras:**

    → https://biometricdevices.idemia.com/sfc/servlet.shepherd/document/download/0690X00000DqNJEQA3


IDEMIA

# MONITOREO

- **Se recomienda que los *puntos de accesos sensibles sean supervisado*, por ejemplo con cámaras de vigilancia o sensores.**

- **Eventos de accesos negados repetidos reportados desde un mismo puntos de acceso en cortos de periodos de tiempo o durante horas valle, pueden indicar intentos de intrusión, que deben ser monitoreados y aplicados los protocolos de cada institución.**



# TECNOLOGIA BIOMETRICA

- **Todas las terminales Idemia tiene dos parámetros que pueden ser configurados de manera independiente:**

  - Umbral biométrico que configura la tasa de falsa aceptación
  - Detección de biometría falsa, que cuenta con varios niveles de configuración.

IDEMIA

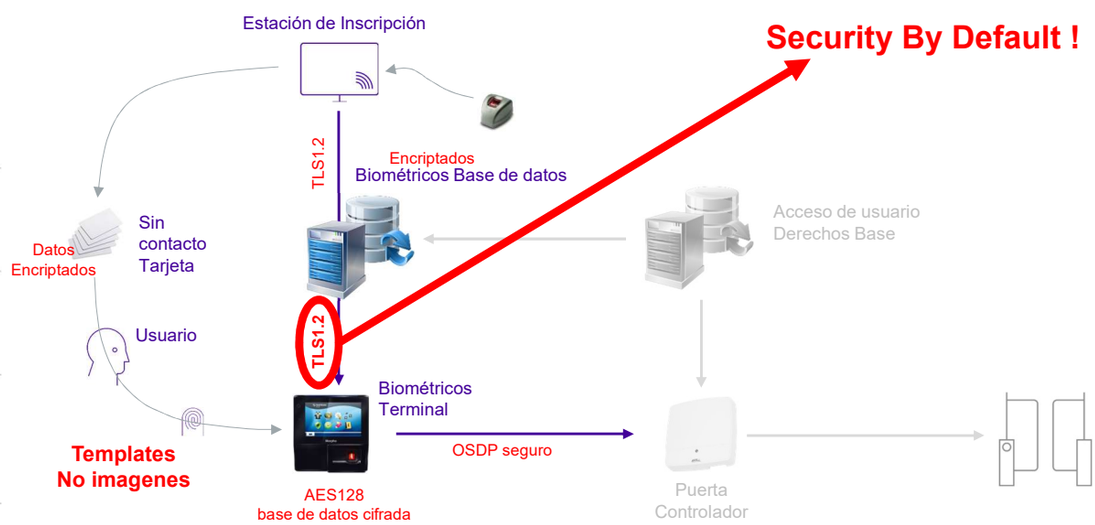
# SECURITY BY DEFAULT



## SECURITY BY DEFAULT



12-Apr-23



# SECURITY BY DEFAULT

› **Las nuevas terminales vienen con un certificado de seguridad que incrementa la seguridad de la aplicación y de las comunicaciones entre el software y las terminales.**

› **Este certificado de seguridad bloquea:**

- Web server
- Acceso MBTB*
- Administracion en pantalla
- Programación por USB

› **Con este certificado se establece una comunicación segura y permanente.**

IDEMIA



## Puntos clave dipositivos de huella

### Rendimiento

› Tecnología óptica robusta con el mejor rendimiento probado en campo
› Algoritmo con mas de 30 años de experiencia y mejor calificado en pruebas NIST
› Amplia superficie para adquisición de datos
› Certificado FBI PIV IQS calidad de imagen

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

### Seguridad

› Encriptación de la comunicación desde el dispositivo
› Fake Finger Detection
› Llaves de Seguridad
› Security by Default

CONTACT

**Nelson RODRIGUEZ**
Regional Sales Manager – Andean Region
Terminals Business Line

Nelson.rodriguez@idemia.com

P. +57 1 6468600 Ext 1029
M. +57 318 707 3437

IDEMIA

Join us on

www.idemia.com