

「**Biometría**
Fintechgración」

CÁPSULA

1

RECONOCIMIENTO:

DE LO ANÁLOGO A LO DIGITAL





**CONOCERSE A SÍ MISMO ES EL
PRINCIPIO DE TODA SABIDURÍA**

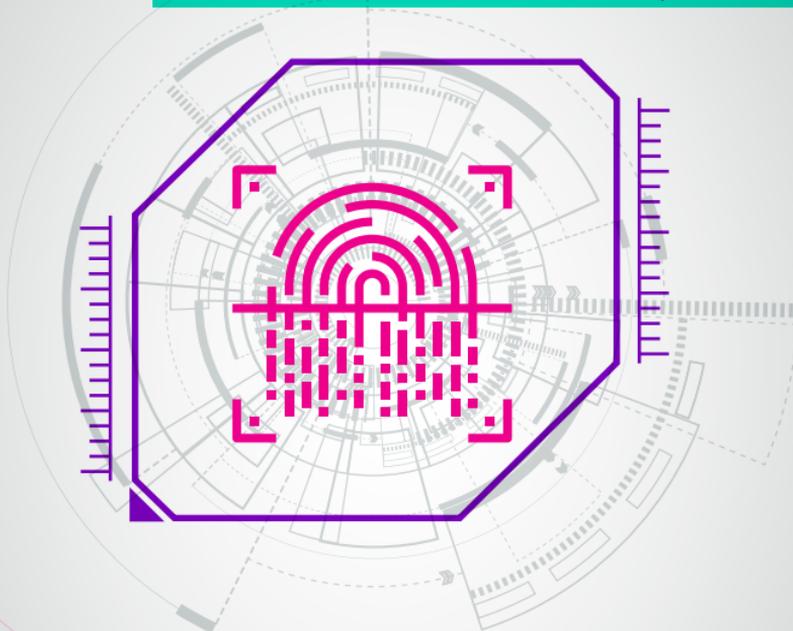


ARISTÓTELES



DESDE HACE

MILES DE AÑOS,



**LAS SOCIEDADES HAN USADO
LA BIOMETRÍA PARA DEJAR SU FIRMA
EN OBJETOS Y PARA IDENTIFICAR INDIVIDUOS.**

**HAY EVIDENCIA DE QUE LAS
HUELLAS DACTILARES SE USARON
EN TABLETAS DE ARCILLA EN EL**

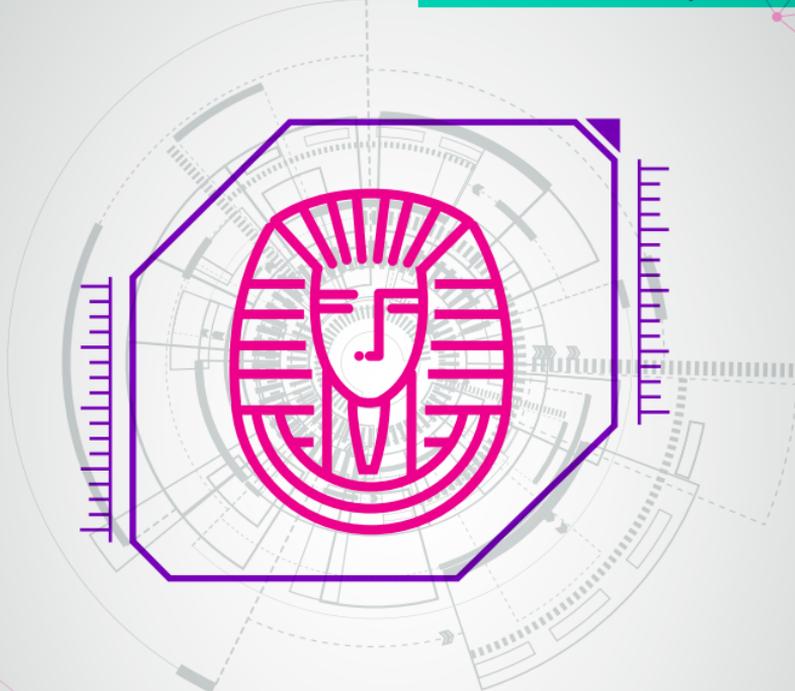
AÑO 500 A.C.



**DURANTE LAS TRANSACCIONES
COMERCIALES DE BABILONIA¹.**

1- Govtech, 2012. Tracing the History of Biometrics.
Disponible en <http://www.govtech.com/Tracing-the-History-of-Biometrics.html>

TAMBIÉN SE ENCONTRÓ QUE,
A PRINCIPIOS DE LA HISTORIA EGIPCIA,

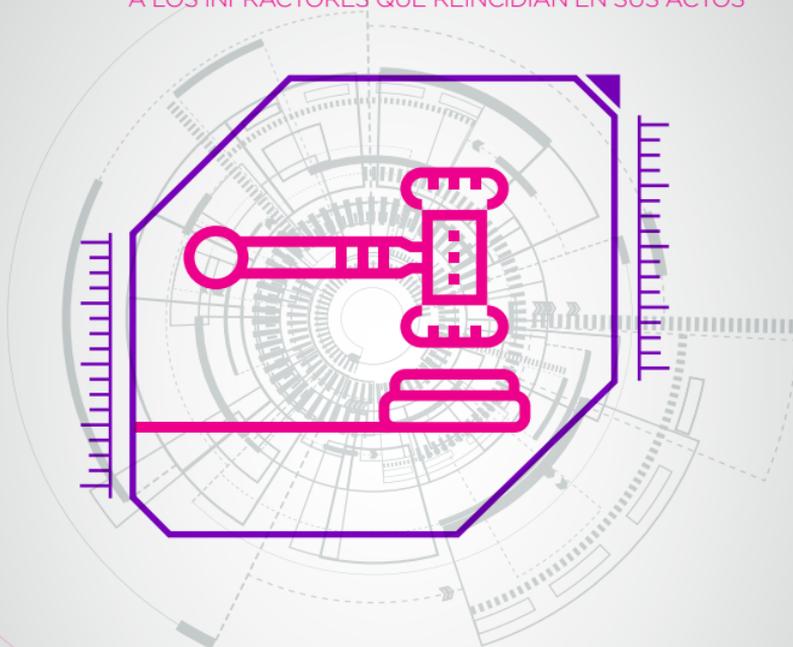


LOS COMERCIANTES SE DIFERENCIABAN
POR SUS CARACTERÍSTICAS FÍSICAS PARA
IDENTIFICAR AQUELLOS CON BUENA
REPUTACIÓN CON LOS RECIÉN LLEGADOS.





EN UN TIEMPO NO TAN LEJANO, A MEDIADOS DEL SIGLO XIX, LOS SISTEMAS DE JUSTICIA BUSCARON CASTIGAR CON MAYOR SEVERIDAD A LOS INFRACTORES QUE REINCIDÍAN EN SUS ACTOS

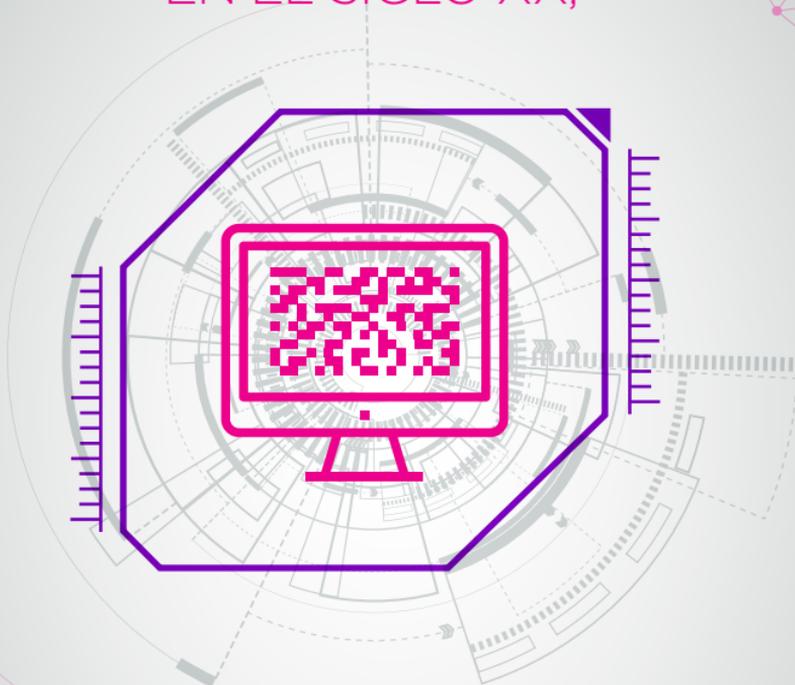


Y PARA ELLO ERA INDISPENSABLE UN SISTEMA FORMAL QUE MIEDIRA LOS RASGOS DE IDENTIDAD DE LOS DELINCUENTES².

2- Stephen Mayhew, 2015. History of Biometrics.
Disponible en <http://www.biometricupdate.com/201501/history-of-biometrics>



AÑOS DESPUÉS, EN EL SIGLO XX,



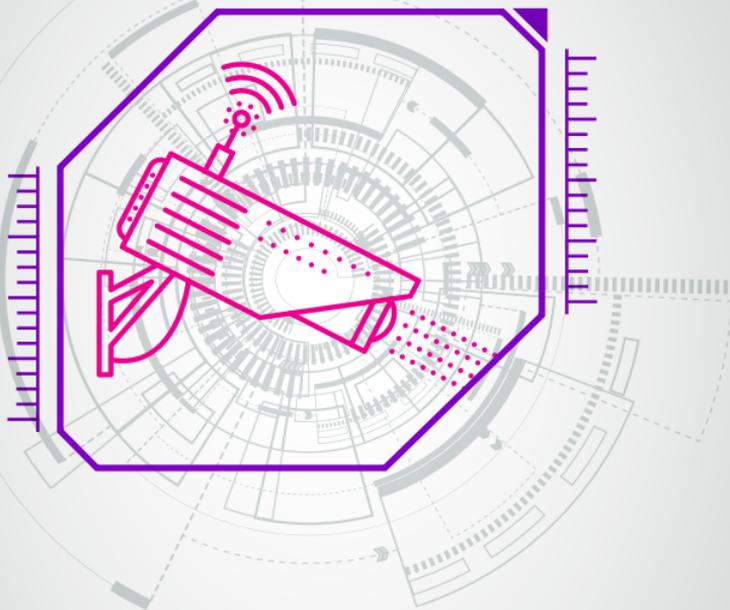
EL SURGIMIENTO DE SISTEMAS DE COMPUTACIÓN PERMITIÓ DIGITALIZAR LAS TÉCNICAS BIOMÉTRICAS Y DARLES PASO A LOS SISTEMAS DE BIOMETRÍA AUTOMATIZADOS.



LA IDENTIFICACIÓN BIOMÉTRICA

PRIMERO CAPTURA UNA IMAGEN O LAS MÉTRICAS DE UN INDIVIDUO A TRAVÉS DE UN DISPOSITIVO

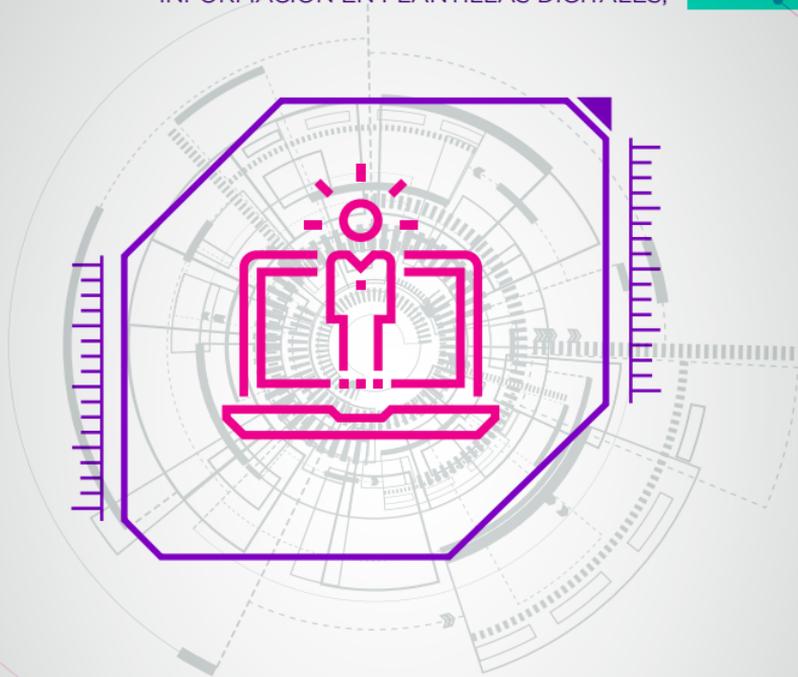
(POR EJEMPLO, UNA CÁMARA O UN SENSOR),



Y, CON LA AYUDA DE UN ALGORITMO, **APOYADO EN HARDWARE Y SOFTWARE COMPUTACIONAL, EXTRAE, CODIFICA, ALMACENA Y COMPARA ESAS CARACTERÍSTICAS**



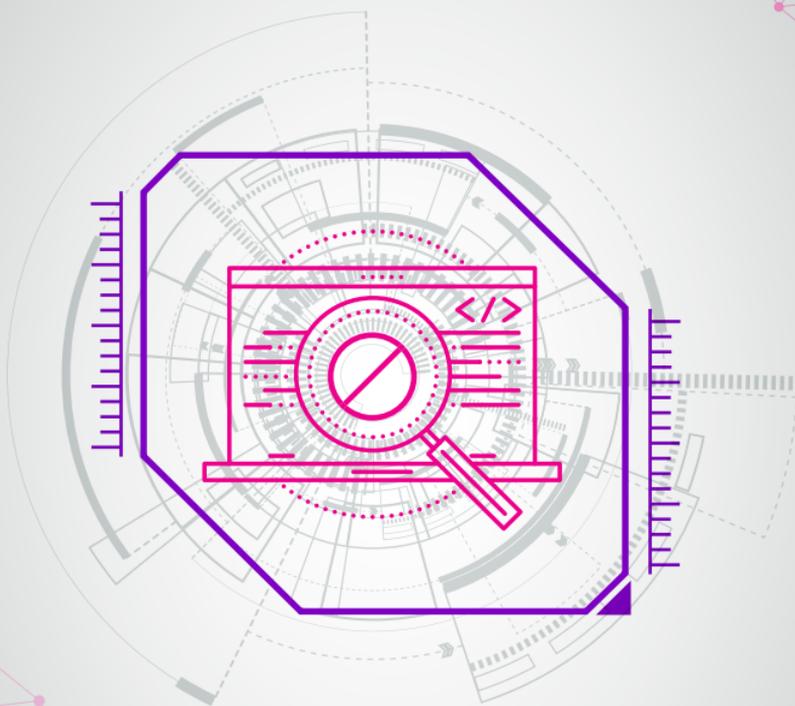
UNA VEZ REALIZADO EL REGISTRO
Y ALMACENAMIENTO DE ESTA
INFORMACIÓN EN PLANTILLAS DIGITALES,



EL SISTEMA BIOMÉTRICO ES CAPAZ
DE IDENTIFICAR AL USUARIO
DE MANERA AUTOMÁTICA.



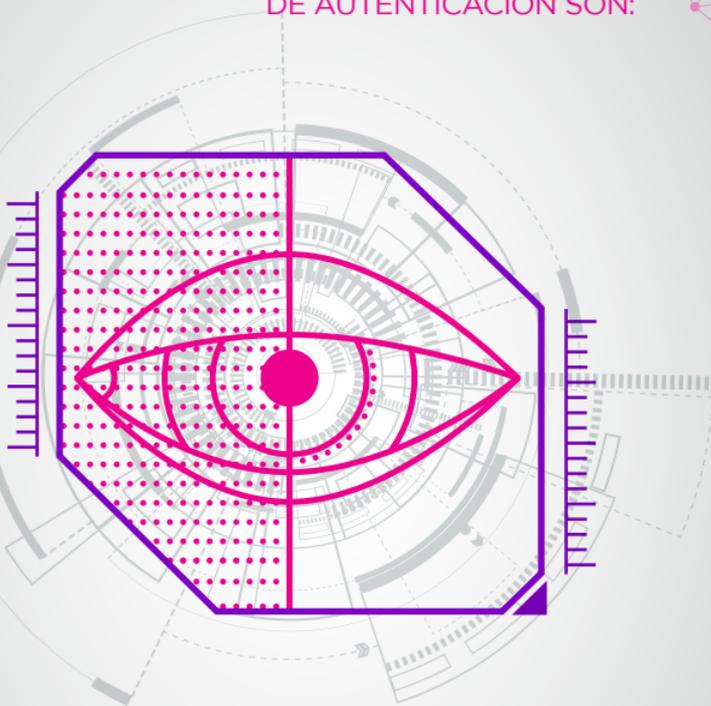
DE NO HABER UNA COINCIDENCIA
AL COMPARAR LA INFORMACIÓN BIOMÉTRICA
CON AQUELLA DE LAS PLANTILLAS,



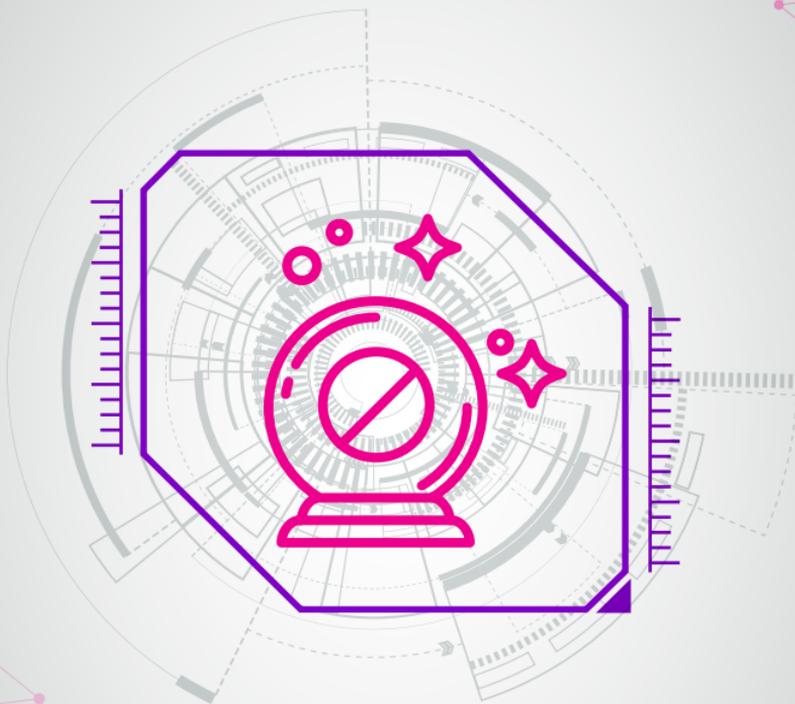
LA AUTENTICACIÓN DEL USUARIO ES
RECHAZADA Y, DEPENDIENDO DEL
CONTEXTO, SU ACCESO ES DENEGADO.



LAS VENTAJAS DE LA UTILIZACIÓN
DE RASGOS BIOMÉTRICOS COMO MÉTODOS
DE AUTENTICACIÓN SON:



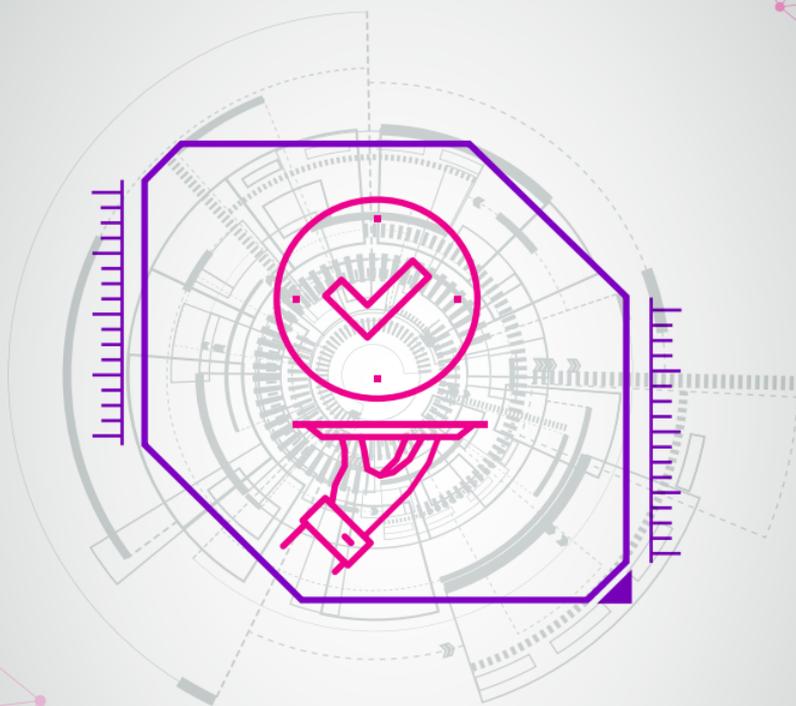
**NO SE PUEDEN
DESCONOCER**



NO SE PUEDEN ADIVINAR



NO SON TRANSFERIBLES



DISPONIBILIDAD



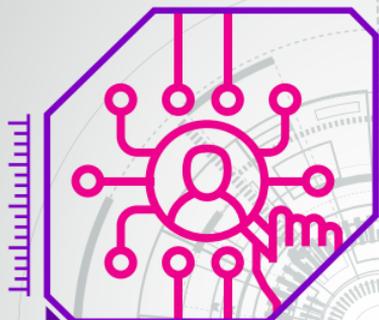
ES MÁS, SE ESPERA QUE,
PARA EL AÑO 2020,



LA BIOMETRÍA SEA EL MÉTODO
PREDOMINANTE DE IDENTIFICACIÓN PARA
ACCEDER A SERVICIOS BANCARIOS.



CADA VEZ MÁS,
LAS INSTITUCIONES TIENDEN
AL USO DE LA BIOMETRÍA MULTIMODAL,

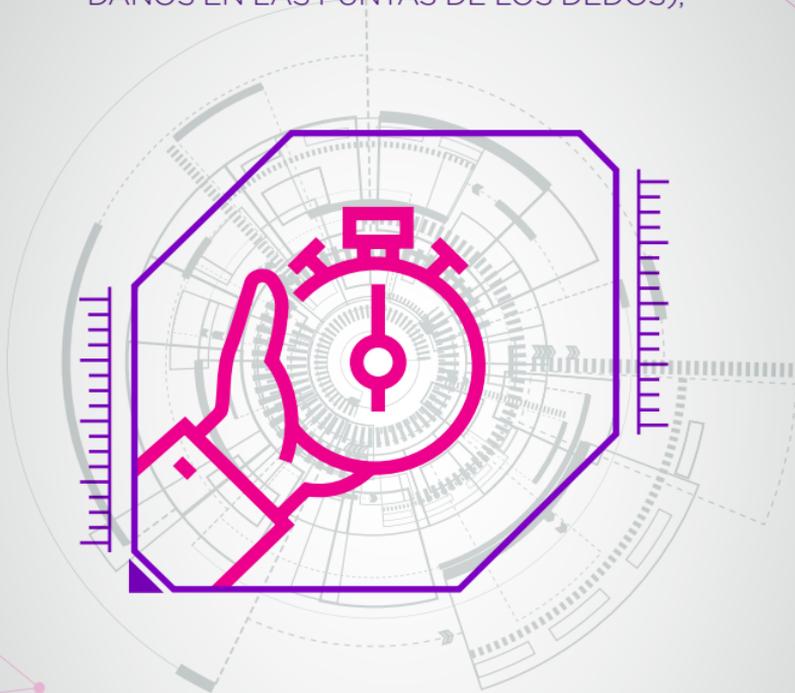


DONDE MÁS DE UN
IDENTIFICADOR **BIOMÉTRICO**
ES UTILIZADO EN EL PROCESO DE
VERIFICACIÓN.



**DE ESTA MANERA, EXISTE MAYOR
PRECISIÓN Y FLEXIBILIDAD QUE AL
USAR UNA SOLA MODALIDAD**

**ESTO NO SOLO PERMITE ABARCAR
MAYOR POBLACIÓN** (PUES ES POSIBLE
**COMPENSAR EN CASO DE QUE HAYA
DAÑOS EN LAS PUNTAS DE LOS DEDOS),**



**SINO QUE TAMBIÉN OFRECE
MAYOR EFICIENCIA**



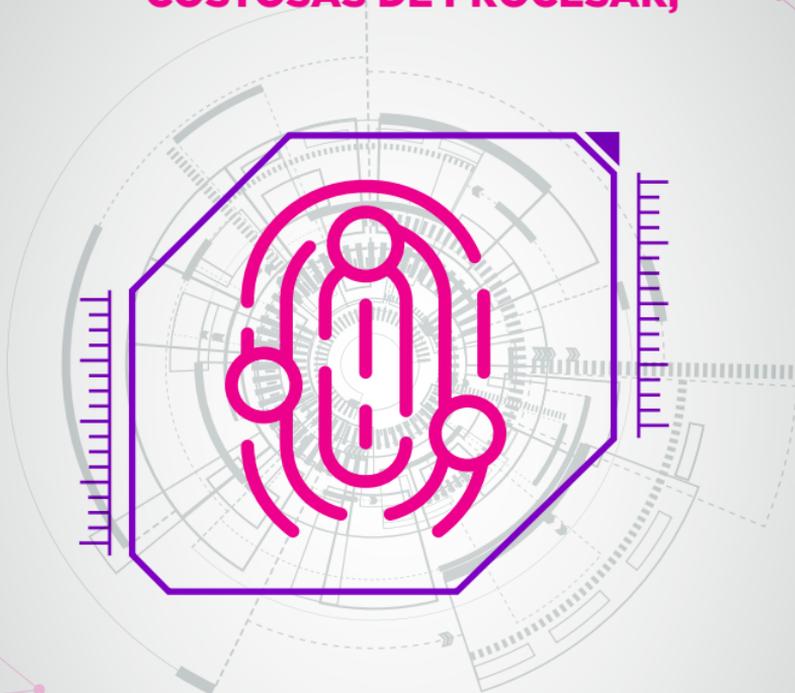
**POR EJEMPLO, EL RECONOCIMIENTO
DE IRIS ES IDEAL CUANDO SE BUSCA
IDENTIFICAR UN USUARIO DENTRO DE
MILLONES DE OPCIONES,**



**PUES ESTA BIOMETRÍA ES
LA QUE MÁS PUNTOS DE
COMPARACIÓN OFRECE.**



**EN CAMBIO, LAS HUELLAS DACTILARES,
AL SER MÁS RÁPIDAS Y MENOS
COSTOSAS DE PROCESAR,**



**SON ÓPTIMAS PARA CORROBORAR AL INSTANTE
QUE EL INDIVIDUO ES QUIEN DICE SER.**



POR OTRO LADO, SU USO SIMULTÁNEO
LOGRA AUMENTAR LA RESISTENCIA
A TÉCNICAS FRAUDULENTAS.

**ESTO PUEDE OBSERVARSE AL USAR EL
RECONOCIMIENTO FACIAL JUNTO A LA VOZ,**



**PUES LAS ORGANIZACIONES PUEDEN
PREVENIR EL ACCESO NO PRESENCIAL DE
INDIVIDUOS QUE UTILIZAN MÁSCARAS
EN 3D O FOTOS DEL GENUINO USUARIO³.**

3- WIRED, 2016. Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?). Disponible en <https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/>



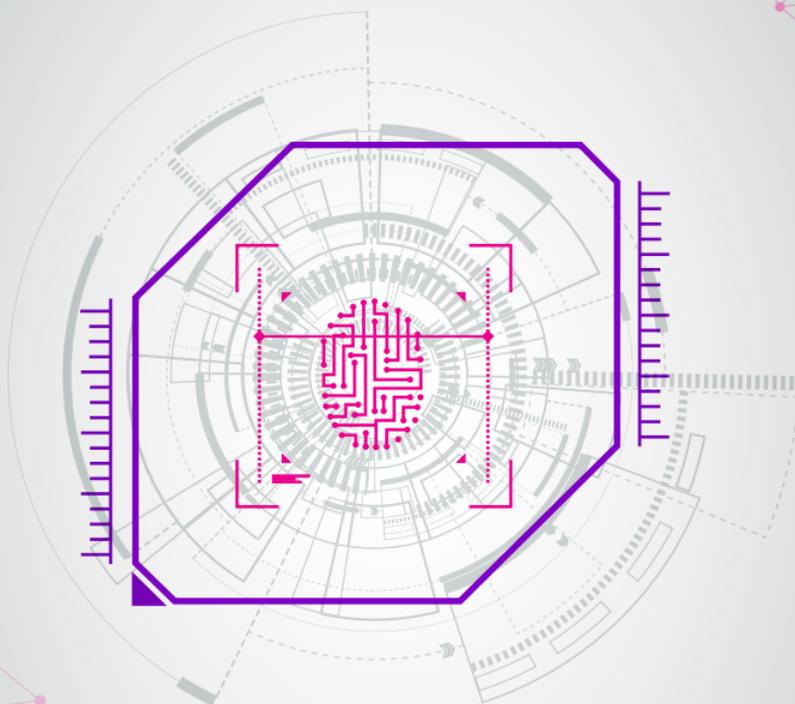
EN ÚLTIMAS, LA BIOMETRÍA ES LA ÚNICA TECNOLOGÍA QUE ASEGURA LA IDENTIDAD DE LA PERSONA EN UN GRADO IMPORTANTE DE CONFIANZA.



CON ELLA, LAS PERSONAS NO NECESITAN CORROBORAR SU IDENTIDAD POR MEDIO DE LO QUE SABEN O TIENEN (CONTRASEÑAS O DOCUMENTO DE IDENTIDAD), SINO QUE SON RECONOCIDAS POR LO QUE SON.



LA DECISIÓN DE CUÁL MODALIDAD BIOMÉTRICA
UTILIZAR DEPENDERÁ DEL CONTEXTO,



DE LOS RIESGOS EN SEGURIDAD Y
DE FACTORES PRÁCTICOS, COMO:





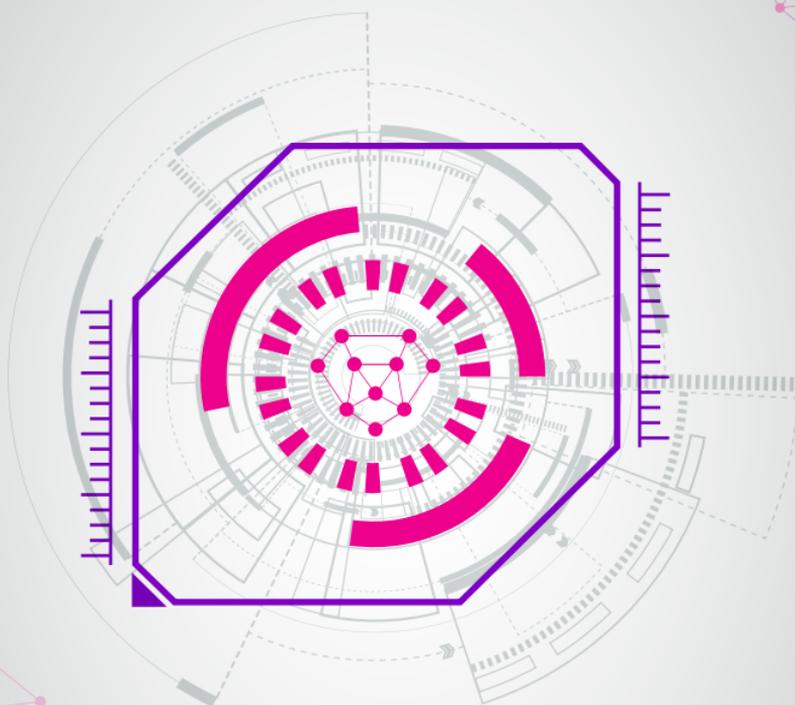
RECOLECCIÓN:



FACILIDAD DE CAPTURA



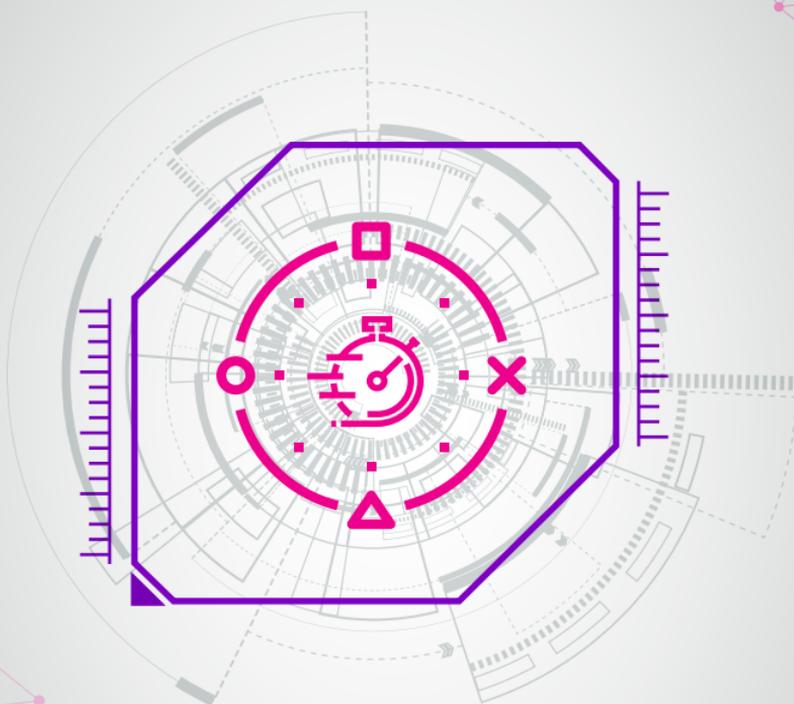
ESTÁNDARES:



**EXISTENCIA DE ACUERDOS
SOBRE PARÁMETROS**



COSTO EFICIENTE:



**EFICIENCIA ENTRE
IMPLEMENTACIÓN Y USOS**

Biometría

| CÁPSULA 1



SEGURO:



**DIFICULTAD DE FALSIFICACIÓN,
TASA DE FALSO POSITIVO, ENTRE OTROS.**

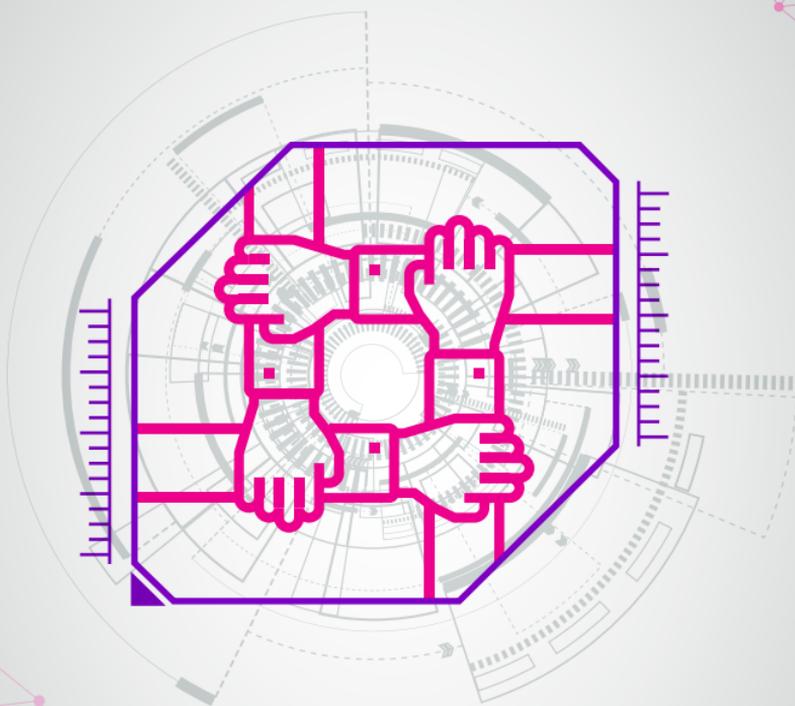


FACILIDAD DE USO:



**USABILIDAD Y
PRACTICIDAD**

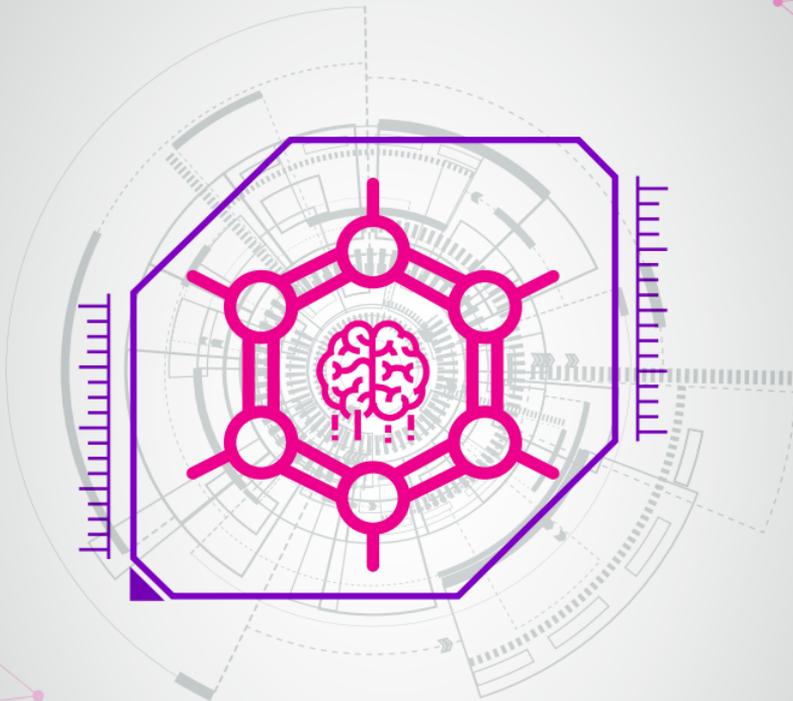
ACEPTABILIDAD:



**SOCIALMENTE
ACEPTADA**



OTROS:



**SINGULARIDAD, PERMANENCIA, CUANTIFICABLE,
VELOCIDAD DE PROCESAMIENTO, EXACTITUD,
ESTABILIDAD, PRIVACIDAD O POPULARIDAD.**

"La disrupción del sistema financiero no va a suceder, está sucediendo"

Bienvenidos a la Fintechgración



Nuestros Aliados

