Biometría

Conveniente, ¿pero seguro?

Nuestros Aliados

CRÉDITOS

RECONOCIMIENTOS

Los autores desean agradecerle a Asobancaria por la información y apoyo en la construcción de este documento, y en especial a las siguientes personas:

- Jonathan Malagón
- Nicolás Rodríguez
- Marcela Rey
- Lorena García
- Alan García

ACERCA DEL DOCUMENTO

La naturaleza de los servicios financieros está cambiando y los bancos deben estar en capacidad de afrontar este proceso. Por tal razón, **Asobancaria** y el **TicTac de la CCIT** se han asociado para generar un espacio en la web con información sobre las tendencias digitales del mundo financiero, más conocidas como **FinTech**.

Este editorial forma parte de una serie de investigaciones acerca de las últimas innovaciones y tendencias en la disrupción de los servicios financieros. En general, el proyecto incursiona en distintos aspectos FinTech y sus implicaciones en la manera como las personas se relacionan con el sistema financiero.

ACERCA DEL TICTAC

El TicTac es el primer tanque de análisis y creatividad del sector TIC en Colombia, establecido con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social y la eficiencia gubernamental.

ACERCA DE LOS AUTORES

Felipe Buitrago - Director del TicTac
felipe.buitrago@ccit.org.co

Carlos Romero - Investigador asociado al TicTac
carlos.romero@ccit.org.co

Cualquier error u omisión es únicamente responsabilidad de los autores y no refleja de ninguna manera una posición oficial de la CCIT , de Asobancaria o de las entidades aliadas.

Para más información, visite la página
www.fintechgracion.com

.Puntoaparte bookvertising

WWW.PUNTOAPARTE.COM.CO

Dirección editorial: Andrés Barragán
Dirección de arte: Mateo L. Zúñiga
y Jeisson Reyes
Diseño y diagramación: Hansel Martínez

PRESENTACIÓN

Según una encuesta de MasterCard[1], 1 de cada 2 compradores olvida su contraseña al menos una vez por semana, perdiendo más de 10 minutos restableciéndola. Esto resulta en que 1 de cada 3 termine abandonando su compra. Por esa y otras razones, nuevas técnicas para la verificación de usuarios están siendo exploradas y acondicionadas a en el entorno digital. Aunque la biometría no es nada nuevo para la industria financiera, la implementación extendida de esta tecnología promete habilitar la siguiente generación de mecanismos de autenticación.

¿SE PUEDE SALVAR VIDAS CON UNA SONRISA?

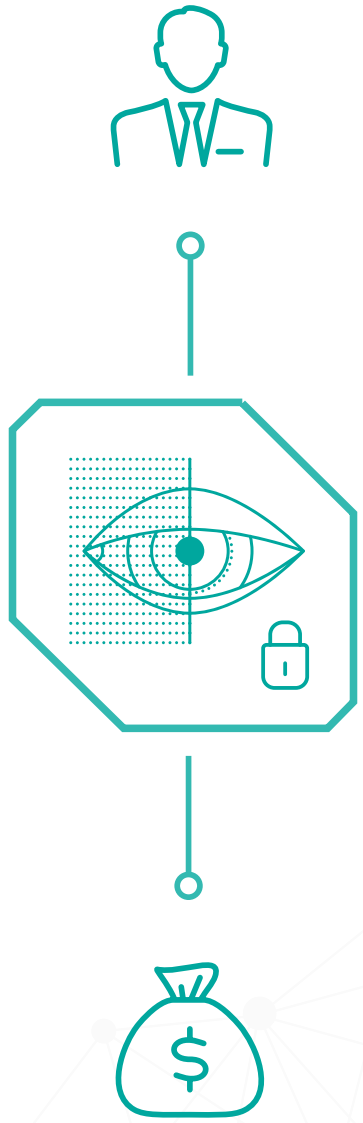
En cualquier momento puede ocurrir una tragedia. Desastres naturales como un terremoto, un tsunami, un incendio o un deslizamiento – como el que dejó sin nada a centenares de familias en Mocoa el 31 de marzo de 2017 – no dejan de sorprendernos. En momentos así, las donaciones y subsidios son cruciales para salir a apoyar a las víctimas y procurar devolverles la esperanza. Sin embargo, además de destruir los enseres y casas de las personas, los desastres naturales también se roban la identidad de sus víctimas: las dejan sin la documentación para identificarse o demostrar las propiedades perdidas.

Esto significa que, para recibir la solidaridad de los colombianos y la comunidad internacional, miles de mocoanos quedaron excluidos de la ayuda de emergencia. No era posible determinar que en efecto se tratara de víctimas. Peor aún, también les era imposible reclamar los subsidios de Familias en Acción de los cuales dependían para complementar sus magros ingresos familiares. Afortunadamente, gracias a la iniciativa de una importante empresa colombiana de tecnología, fue posible comparar los registros biométricos de estos miles de colombianos en tiempo récord y determinar que en efecto se trataba de habitantes de las zonas afectadas. De esta manera se reestablecieron de inmediato sus identidades, dignidad y derechos.

Ahora imagine, que esta misma tecnología de identificación biométrica empleada para devolver la esperanza a quienes lo habían perdido todo, también pudiera utilizase para enviarles el apoyo económico y emocional de manera personalizada. ¿Qué tal una campaña humanitaria de sonrisas de apoyo para las víctimas? Aprovechar que su smartphone cuenta con la capacidad de reconocer su cara, su huella dactilar, su iris y sus expresiones para determinar con seguridad su identidad e intenciones, e invitarle a sonreír para activar la autorización de hacer una transferencia de $5.000 para contribuir a las necesidades más inmedia-

tas de las víctimas. De manera simultánea, el mismo sistema toma su foto sonriendo, la comparte en redes sociales invitando a otros a sonreír para donar, y la envía a un álbum para que tanto las víctimas como los voluntarios comprometidos en las tareas de rescate y reconstrucción sepan que no están solos, que cuentan con su apoyo.

Todo esto, con total conveniencia, seguridad y confianza, garantizando la trazabilidad de su dinero, desde la cuenta de ahorros hasta el agua que quita la sed a una familia que lucha por salir adelante. Todo esto, con su sonrisa.



La identificación y autenticación de las personas son mecanismos fundamentales para la sociedad moderna, pues permiten interacciones seguras mientras previenen el fraude y la criminalidad. La biometría, por su parte, verifica la identidad de un individuo en función de sus características fisiológicas y de comportamiento únicas, lo que ofrece ventajas de seguridad, conveniencia y eficiencia en la autenticación de transacciones. Asimismo, no solo las instituciones financieras se benefician, sino también el consumidor ya que obtiene protección y tranquilidad.

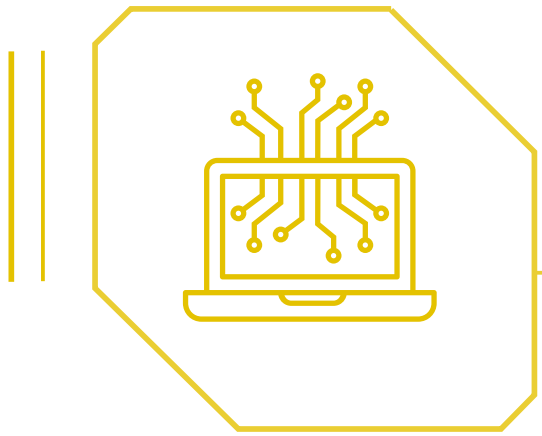
Estos beneficios son cada vez más relevantes en un mundo en el que la movilidad digital y el comercio electrónico son cada vez más importantes. Como lo han demostrado eventos pasados, mantener un sistema de seguridad basado únicamente en usuarios y contraseñas presenta un riesgo a las instituciones, y expone a los usuarios a prácticas vulnerables para proteger su información. Es importante entender que estamos entrando a una nueva era de seguridad digital - si las personas no usan contraseñas, entonces ellos son la contraseña.

Este editorial explorará las implicaciones que tiene el uso extendido de la biometría en la banca, sus alcances y tendencias.

SECCIONES DEL DOCUMENTO

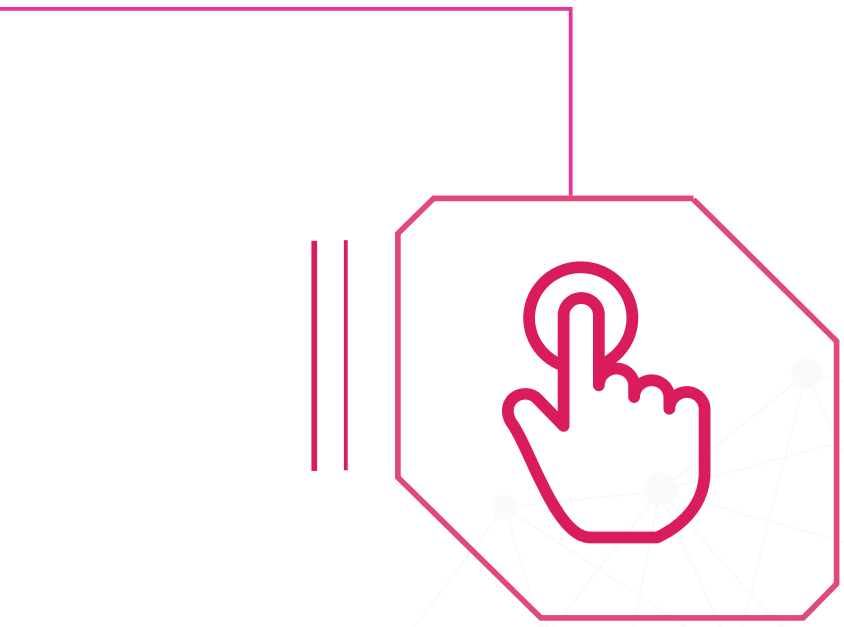
1. RECONOCIMIENTO: DE LO ANÁLOGO A LO DIGITAL

El uso de técnicas biométricas para el reconocimiento de individuos ha tenido lugar por miles de años, pero no es sino hasta hace pocas décadas que ha sido posible utilizarlas en procesos automáticos. Como resultado, la verificación e identificación de las personas se facilita, abriendo una nueva dimensión de posibilidades para la industria de servicios financieros.



2. AUTENTICACIÓN: DESBLOQUEANDO EL POTENCIAL BANCARIO EN UN MUNDO HIPERCONECTADO

El incremento en el número de incidentes de fraude financiero, robo de identidades y ciber-amenazas ha hecho que las instituciones financieras se encuentren bajo la constante presión de adaptar sus prácticas en la identificación de usuarios. El uso de la biometría por parte del sistema financiero ofrece una solución a estos retos.



3. CIBERESPACIO: TU IDENTIDAD MÁS ALLÁ DE LAS CONTRASEÑAS

Los mecanismos de autenticación que no están basados en biometría inevitablemente solucionan el problema incorrecto. Al estar basados en usuarios y contraseñas, tokens de seguridad, o verificación de dispositivos, esos sistemas estarían autenticando secretos, tokens o dispositivos, mas no a las personas. En cambio, un sistema biométrico asegura que del otro lado del dispositivo de acceso esté la persona indicada. Un aspecto cada vez más importante para la economía móvil.

4. SEGURIDAD: UN TOQUE HUMANO PARA CADA DISPOSITIVO

La manera en que los humanos se reconocen unos a otros, también se denota en la biometría del comportamiento. Por ejemplo, esta identifica características como la forma de caminar y la voz para reconocer a cada individuo. Integrar estas capacidades al funcionamiento de cada dispositivo y al acompañamiento de cada compra permitirá una autenticación continua y no restringida solo al momento de ingreso.

“Conocerse a sí mismo es el principio de toda sabiduría”.

–Aristóteles

RECONOCIMIENTO: DE LO ANÁLOGO A LO DIGITAL

RECONOCIMIENTO: DE LO ANÁLOGO A LO DIGITAL

Cuando se habla de biometría, en su forma literal y más simple, se hace alusión a la medición del cuerpo humano. Desde hace miles de años, las sociedades han usado esta ciencia para dejar su firma en objetos y para identificar individuos. Pues, hay evidencia de que las huellas dactilares se usaron en tabletas de arcilla en el año 500 a.C. durante las transacciones comerciales de Babilonia, y 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.[2]

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 midiera los rasgos de identidad de los delincuentes.[3] Uno de dos avances que tuvo lugar en esa época, fue el sistema Bertillon -también conocido como antropometría– donde se recopilaba información en tarjetas sobre la dimensión de varias partes del cuerpo (por ejemplo, la altura, la longitud del brazo, entre otras medidas). A finales de ese mismo siglo tuvo mejor acogida el segundo avance que proporcionaba una sola métrica: las huellas dactilares. Este sistema de clasificación llamado Henry, es el que se utiliza hoy en día.[4]

Años después se comenzó a investigar sobre otras modalidades biométricas como el iris y el reconocimiento facial. Al coincidir con el surgimiento de sistemas de computación en el Siglo XX, no solo fue posible digitalizar las técnicas biométricas, sino también darles paso a los sistemas de biometría automatizados. Desde entonces, fue posible realizar el reconocimiento de individuos bajo un esquema digital.

Tabla 1. Ejemplos de identificadores biométricos (modalidades)

IDENTIFICADORES FISIOLÓGICOS	IDENTIFICADORES DE COMPORTAMIENTO
Huellas dactilares/manos/pies	La firma
Iris y retina de los ojos	Gestos
Venas y patrones vasculares	Forma de caminar/escribir
Cara, oreja	
Voz para ambos	

Fuente: Elaboración propia.

Así las cosas, 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. Mejor dicho, después de la captura de los datos, un sistema biométrico automatizado está diseñado para realizar el registro y almacenamiento de esa información en plantillas digitales, para luego 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.

01

VENTAJAS DE LA BIOMETRÍA FRENTE A OTROS MÉTODOS DE AUTENTICACIÓN DE USUARIOS.[5]

En un día cotidiano, desde desbloquear el teléfono hasta para realizar una transacción bancaria, las personas necesitan comprobar quiénes son. En este sentido, los métodos de autenticación e identificación de usuarios son indispensables.

Por un lado, varios de los procesos convencionales de verificación están basados en secretos (por ejemplo, contraseñas o un PIN de cuatro a seis dígitos) o en la posesión de objetos (como *tokens* o documentos de identificación). Pero el problema con estos métodos es que las contraseñas pueden ser vulneradas, los documentos de identidad pueden ser robados o falsificados, y el PIN se puede olvidar.

En cambio, la utilización de rasgos biométricos como métodos de autenticación promete solucionar esos inconvenientes gracias a sus ventajas. Estas serían:

- **NO SE PUEDEN DESCONOCER**
- **NO SE PUEDEN ADIVINAR**
- **NO SON TRANSFERIBLES**
- **NO SE PUEDEN OLVIDAR**
- **DISPONIBILIDAD**

La propiedad más importante de un rasgo biométrico es el nivel en que permite distinguir a una persona de otra. Por ejemplo, se estima que dos personas pueden compartir el mismo patrón de iris con una probabilidad de 1 en 10^{78} (prácticamente 0%).

Hoy en día, el continuo avance tecnológico y su mayor habilidad de reconocimiento, junto con el incremento en la capacidad de almacenamiento y en la velocidad de procesamiento computacional, han hecho que el uso de la biometría sea posible en una variedad de aplicaciones para distintas industrias. Es más, se espera que para el año 2020, la biometría sea el método predominante de identificación para acceder a servicios bancarios.[6]

A finales del año 2017, el gigante digital – Alibaba – implementó su tecnología "Sonríe para Pagar" en la cadena de restaurantes KFC en China.[7] Gracias a su sistema de reconocimiento facial, ahora los clientes pueden pagar su comida sonriéndole a una cámara 3D. En cuanto a Apple, otro gigante digital, este lanzó su nuevo sistema operativo (iOS 11) que permite transferir dinero desde su aplicación de mensajes o preguntándole a Siri.[8] Claro está, siempre y cuando la persona esté autorizada para hacer la transferencia. Para ello, Apple dispone de un mecanismo de autenticación en sus teléfonos como FaceID y TouchID, que utilizan el reconocimiento facial y de huellas dactilares, respectivamente.

Por su lado, las instituciones financieras han implementado tecnologías biométricas en una amplia gama de canales bancarios, incluyendo cajeros automáticos, sucursales bancarias, como respaldo de la banca telefónica, la banca en línea, y en el interior de aplicaciones de la banca móvil. Por otra parte, han comenzado a trabajar en pilotos y pruebas de conceptos con proveedores de tecnologías biométricas innovadoras sobre dispositivos portátiles *(wearables)*.[9]

En la era digital, es imposible no pensar que desde el efectivo hasta el bitcoin pueden tener protección basada en biometría. A continuación, se presentan algunos de esos ejemplos y una visión general de distintos identificadores biométricos:

IDENTIFICADOR BIOMÉTRICO	VISIÓN GENERAL	TENDENCIAS DE USO (EJEMPLOS)
 **HUELLAS DACTILARES**	Las crestas epidérmicas en las puntas de los dedos forman un patrón único de cada huella. Para su identificación existen técnicas manuales y distintos sensores tecnológicos que permiten su recolección. Hoy en día, el reconocimiento de huellas dactilares es el identificador biométrico más utilizado en el mercado, pero se estima que otro tipo de biometría dominará en el año 2020.[10]	**Tarjetas de Pago Biométricas:** Mientras que los consumidores tienen un medio de pago conveniente y ágil gracias a las tarjetas *contactless*, al incluirle biometría se mantiene la seguridad sin necesidad de un PIN. Esto no solo promueve la confianza, sino que también ahorra tiempo. Barclaycard estima un ahorro mayor a siete segundos por cada compra contactless en vez de usar "Chip & PIN"; y, de 15 segundos, en comparación con el efectivo.[11]
 **OJOS**	Los ojos tienen características con una gran singularidad, lo que incluye (i) el iris, (ii) la retina y (iii) el patrón de vasos sanguíneos en el blanco de los ojos: es decir el reconocimiento de la vasculatura escleral (o eyeprint en inglés). Recientemente, el reconocimiento ocular ha comenzado a abrirse paso en la autenticación biométrica móvil.	**Acceso simple a la cuenta bancaria:** Bancos como Wells Fargo comenzaron a utilizar la biometría *eyeprint* para la autenticación rápida de sus clientes. A diferencia del iris y la retina, *eyeprint* no necesita de hardware especializado, sino que con una cámara de al menos un megapixel de resolución es suficiente.[12] Lo importante es que *eyeprint* igual utiliza el inmenso universo de características del ojo para mantener una seguridad óptima.

CARA

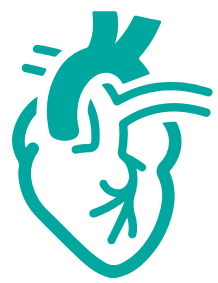
El rostro tiene múltiples rasgos que en conjunto logran ser usados para identificar a una persona (por ejemplo, la forma de la nariz o la distancia entre los ojos). Alrededor de 80 características pueden ser leídas en el rostro, lo que a su agrupación se le denomina puntos nodales.[13] Las personas usan esas características, tal vez de forma inconsciente, para reconocer individuos de manera cotidiana. Algo similar ocurriría con las conductas de comportamiento.

Reconocimiento facial en cajeros automáticos: Ahora las personas no necesitan obligatoriamente tener su tarjeta para sacar plata del cajero automático. Hoy se han habilitado cajeros que al acercarse se genera un código legible por un celular y este último ayude a verificar el rostro de la persona dándole acceso a la cuenta. Bancolombia traería esta tecnología a Colombia a inicios del año 2019.[14]

VOZ

La voz como biometría conductual puede cambiar según el estado emocional de las personas al igual que por su edad o estado de salud. Sin embargo, como biometría fisiológica esta es constante ya que depende del tamaño o forma de la boca, labios, cuerdas vocales y de las cavidades nasales, entre otras. Debido a que su implementación es relativamente facíl y barata, el reconocimiento por voz es ampliamente usado por centros de servicio al cliente.

Identificación en llamadas telefónicas: En el año 2014, el Banco Santander en México incorporó el reconocimiento de voz a sus canales telefónicos. Esto permitió que la identificación de sus usuarios tomara 30 segundos, bajando el promedio anterior de 72 segundos. De esta manera, la satisfacción de sus clientes aumentó y el banco obtuvo ahorros anuales de un millón de dólares.[15]



RITMO CARDIACO

La biometría según el ritmo cardiaco único de cada persona es una tecnología en sus primeras etapas de desarrollo. Aun así, se piensa que jugará un papel importante en la banca cuando el mundo avance a la siguiente generación de dispositivos vestibles (wearables) y el Internet de las Cosas (IoT).[16] Aquellos que defienden esta tecnología aseguran que es muy dificil de falsificar.

Wearables para proteger tus bitcoins: Algunos *wearables* incorporan sensores para electrocardiograma. Así, la identificación creada por Nymi tiene la capacidad de ser usada para guardar los bitcoins de un usuario en una billetera móvil teniendo la llave privada sujeta a su particular ritmo cardiaco. El ID de Nymi aún está en pruebas de concepto y en pilotos de varias instituciones financieras.[17]

CONDUCTUALES

La biometría conductual identifica patrones de comportamiento de las personas, incluyendo la forma de escribir, los gestos manuales, entre otros. Por ejemplo, cuando se quiere observar un patrón en la forma de caminar de una persona se analiza una composición de parámetros tanto espacio-temporales (longitud del paso, rápidez para caminar, ciclos de tiempo) como también cinemáticos (rotación de las articulaciones de la cadera, rodilla y tobillo, ángulos promedio entre estas, etc.)

Autenticación continua después del ingreso: Por ejemplo, BioCatch puede analizar más de 500 patrones de comportamiento diferentes durante una sesión bancaria (post-inicio de sesión) para determinar si el consumidor es realmente el usuario genuino y no un impostor humano/robot. Cada perfil de sus usuarios se basa en los 20 parámetros más exclusivos de ellos (como temblor de manos, coordinación mano-ojo, y demás).[18]

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 quién dice ser (por ejemplo, verificar quien accede a la oficina corresponda verdaderamente al empleado).[19]

Por otro lado, su uso simultáneo logra aumentar la resistencia a técnicas fraudulentas. Esto ocurre, por ejemplo, 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 usuario.[20] Así, al añadir una técnica biométrica adicional, el intruso enfrentaría una mayor dificultad. Otra medida para combatir el fraude está en manos de los desarrolladores de tecnología, puesto que los dispositivos puedan hacerse más seguros incluyendo sensores con la capacidad de detectar vida.

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 reconocidos por lo que son. Las instituciones financieras deben valerse de todos estos recursos para autenticar a sus usuarios con las mejores y más seguras herramientas, mientras procuran no causarles fricciones en su vida cotidiana.

Además, dado que la tecnología biométrica está en constante desarrollo, con el tiempo se volverá cada vez más segura y accesible para los usuarios. Por ahora, la decisión de cuál modalidad biométrica utilizar dependerá del contexto, de los riesgos en seguridad y de factores prácticos, como:

ACEPTABILIDAD:
Socialmente aceptada.

COSTO EFICIENTE:
Eficiencia entre implementación y usos.

FACILIDAD DE USO:
Usabilidad y practicidad.

OTROS:
Singularidad, permanencia, cuantificable, velocidad de procesamiento, exactitud, estabilidad, privacidad o popularidad.

ESTÁNDARES:
Existencia de acuerdos sobre parámetros.

SEGURO:
Dificultad de falsificación, tasa de falso positivo, entre otros.

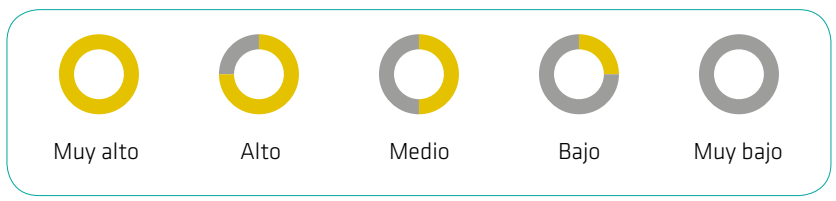
RECOLECCIÓN:
Facilidad de captura.

PARA HABLAR DE UN CASO CONCRETO, EL RECONOCIMIENTO FACIAL CONTRIBUYE A PRESERVAR LA SEGURIDAD EN EL ESTADIO ATANASIO GIRARDOT EN MEDELLÍN, COLOMBIA (NEC, 2018). LAS AUTORIDADES DE LA CIUDAD JUNTO CON NEC HAN INSTALADO CÁMARAS QUE IDENTIFICAN, MEDIANTE SENSORES DE RECONOCIMIENTO FACIAL A LOS INDIVIDUOS QUE INGRESAN AL ESTADIO. CON ESTA INFORMACIÓN SE CREA UNA LISTA DONDE SE REGISTRA EL HISTORIAL DE LOS ASISTENTES, ASÍ, UNA PERSONA QUE HA ESTADO INVOLUCRADA EN DISTURBIOS PREVIAMENTE, ES RECONOCIDA POR EL SISTEMA QUE ALERTA AL PERSONAL ENCARGADO DEL LUGAR.

Tabla 2. Características y factores sociales de distintas modalidades biométricas (comparativo)[21,22]

		HUELLAS DACTILARES	VENAS (VASCULAR)	IRIS	VOZ	RETINA	CARA	VASCULATURA ESCLERAL (EYEPRINT)
PROPIEDADES	**RECOLECCIÓN** Facilidad de captura	Muy alto	Alto	Medio	Medio	Bajo	Alto	Medio
	ESTÁNDARES Existencia de acuerdos sobre parámetros	Muy alto	Bajo	Medio	Alto	Bajo	Alto	Bajo
DESEMPEÑO	**COSTO EFICIENTE** Eficiencia entre implementación y usos	Medio	Bajo	Medio	Muy alto	Bajo	Muy alto	Muy alto
	SEGURO Dificultad de falsificación, FAR, entre otros	Medio	Muy alto	Muy alto	Bajo	Muy alto	Bajo	Muy alto
SOCIAL	**FACILIDAD DE USO** Usabilidad y practicidad	Muy alto	Muy alto	Medio	Muy alto	Bajo	Muy alto	Muy alto
	ACEPTABILIDAD Socialmente aceptada	Muy alto	Bajo	Medio	Muy alto	Bajo	Muy alto	Bajo
	AÑO INTRODUCIDO	1981	1994	1995	1998	1999	2000	2008

Fuente: Adaptado de Redeye, 2016 y IJARCSSE, 2014.
Nota: Las fechas correspondientes al "Año Introducido" fueron tomadas de IJARCSSE, pero no se encontró consenso entre distintas fuentes literarias. Estas fechas corresponderían a cuando se usaron bajo un sistema automatizado



“Nada más intenso que el terror de perder la identidad”.

- Alejandra Pizarnik

AUTENTICACIÓN: DESBLOQUEANDO EL POTENCIAL BANCARIO EN UN MUNDO HIPERCONECTADO

AUTENTICACIÓN: DESBLOQUEANDO EL POTENCIAL BANCARIO EN UN MUNDO HIPERCONECTADO

Con la banca electrónica, las instituciones financieras pudieron llegar a nuevos consumidores alrededor del mundo y realizar negocios transnacionales. Desde entonces, las interacciones digitales han crecido en protagonismo, en especial a través de dispositivos móviles. Hoy en día, los usuarios realizan más de la mitad de sus operaciones bancarias por medio de canales digitales[23], y se estima que, en el transcurso del año 2018, el mundo llegará a 2.000 millones de usuarios de banca móvil (alrededor del 40% de la población adulta globalmente).[24]

Se trata de una gran oportunidad para los bancos si se considera que cada interacción de los usuarios con un asesor telefónico o un cajero le cuesta al banco en promedio USD$4, frente a $10 centavos de dólar cuando la interacción es hecha a través de dispositivos móviles.[25]

De esta manera, en el proceso de digitalización las instituciones financieras tienen la oportunidad de seguir bajando costos (debido a una menor dependencia de las sucursales físicas) y ofrecer nuevos productos (como créditos totalmente en línea). Sin embargo, a medida que los usuarios se acostumbran a la tecnología, la industria financiera experimenta nuevos desafíos:

Omnicanalidad: A diferencia de la multicanalidad, donde los clientes pueden realizar diferentes transacciones a través de múltiples canales, la omnicanalidad se refiere a la posibilidad de interactuar de manera fluida y consistente a través de cualquier canal.[26] En este sentido, el reto para las instituciones financieras es asegurar una experiencia del usuario unificada donde la calidad de los servicios y la información presentada no dependan del canal utilizado.

Seguridad digital: Al digitalizar el ecosistema de pagos, este se vuelve un objetivo de ataques de fraude electrónico. Con el tiempo, su valor ha aumentado y las medidas de seguridad deben mantenerse alerta para contrarrestar cualquier amenaza. En países como Kenia, se estima que el 40% de su PIB pasa cada día por el sistema de dinero móvil M-Pesa.[27] En Europa, siete de cada ocho compras se hicieron de forma electrónica en el año 2015.[28]

Legitimidad de las interacciones: Verificar que el acceso, el intercambio de mensajes, las transacciones y la identidad pertenezcan al genuino usuario demanda vigilancia. Además, con el crecimiento del comercio digital y con la eliminación de servicios cara a cara, los métodos de identificación deben replantearse frente a un panorama digital. Por tal razón, un sistema de autenticación útil hoy en día debe asegurar que la persona sea el legítimo usuario ya sea de forma presencial o en línea.

Es así como los bancos tienen el reto de simplificar el acercamiento de los usuarios a sus canales mientras garantizan la seguridad de sus finanzas. De no lograrlo, los clien-

tes tendrían motivos para seguir usando sucursales físicas o podrían sentirse insatisfechos y nunca establecer una relación duradera con su proveedor financiero. De hecho, en el mundo, 3 de cada 10 personas (29%) estaría dispuesta a cambiar de banco si fuera fácil hacerlo.[29] Un sentimiento que es aún más pronunciado en clientes jóvenes.

Además, a medida que las interacciones se vuelven digitales, el ciberespacio se vuelve una mina de oro para los atacantes. En los últimos seis años, se han perdido USD$112.000 millones en el mundo por robos de identidad. Esto equivale a una pérdida de USD$35.600 cada minuto.[30] Y lo que es peor, según la Comisión Federal de Comercio de los Estados Unidos, hay una nueva víctima de robo de identidad cada 3 segundos.[31] Por ello, las medidas de seguridad deben fortalecerse y estar acordes al panorama digital. La prioridad será prevenir la suplantación de identidad y el uso indebido de las credenciales, pues el impacto no es solo financiero sino elementos como la difamación tienen un impacto negativo incalculable.

En este sentido, el número de credenciales de acceso que han sido comprometidas por ataques fraudulentos es enorme. Según el portal web "have I been pwned"[32] alrededor de 5.000 millones de cuentas han sido vulneradas. Entre las formas más usadas de fraude electrónico para conseguir la información personal y financiera que guardan los usuarios en sus dispositivos, se encuentran el Ataque de Intermediario (MitM por sus siglas en inglés), el Phishing, el Malware (por ejemplo, WannaCry o Petya) y el Fraude de Tarjeta (por ejemplo, el *shimming* y el uso de la ingeniería social).

Hoy en día, los esfuerzos de los bancos y demás instituciones para reducir la fricción y el fraude a través de sus canales, se manifiesta en un cambio de actitud frente a los mecanismos de identificación. Al enfocar sus energías hacia los sistemas biométricos automatizados, tienen la oportunidad de enfrentar varios de los retos digitales y aprovechar los beneficios de esta tecnología:

NUEVAS POSIBILIDADES	RETOS Y OPORTUNIDADES
Conveniencia: Al usar los rasgos biométricos para autorizar pagos o acceder a distintos servicios, los consumidores ahora tienen más opciones que nunca para liberar espacio en sus bolsillos.	**Experiencia del Usuario:** La evolución de las opciones de pago es cada vez más importante para aumentar la fidelización y retención de los clientes pues al hacer los pagos simples y fáciles gracias a la biometría, la satisfacción de los usuarios aumenta. Según un estudio de Visa, 2 de cada 3 consumidores (68%) en Europa quieren utilizar la biometría como método de autenticación para pagos en distintas situaciones, desde la casa o en la calle.
Trazabilidad: En el caso de créditos, la tecnología biométrica haría creíble la posibilidad de denegar futuros préstamos ya que les facilita a las instituciones financieras identificar las personas en mora y por otro lado premiar a los prestatarios responsable aumentándoles el crédito.	**Reducción del Fraude:** En general, Biometric Research Group, Inc. estima que la implicación de las nuevas tecnologías biométricas tiene el potencial de recortar los riesgos operacionales de las instituciones financieras por lo menos 20 por ciento en los próximos 10 años.[33] Por ejemplo, al atar los pagos a la biometría de una persona, se puede asegurar que los subsidios sean desembolsados únicamente por solicitud del genuino acreedor y no por alguien suplantando su identidad con documentos falsos.

NUEVAS POSIBILIDADES	RETOS Y OPORTUNIDADES
Dinamismo: Desde que los datos biométricos estén vinculados a una cuenta bancaria, existe tanto la posibilidad de autenticación como de facilitador de transacciones. Según Barclayscard, el tiempo ahorrado por compra usando biometría llegaría a ser mayor que al pagar con tarjetas *contactless* que de por si se estima en 15 segundos más rápido que usando efectivo. En la vida de un usuario se trata de un ahorro considerable, pues se estima en hasta nueve días.[34]	**Estimula el Comercio:** En países como Brasil (46%), Chile (44%) y Colombia (41%), existe entusiasmo entre los usuarios de internet por realizar pagos móviles.[35] Sin embargo, el comercio digital ha visto que en promedio 6 de cada 10 personas abandonan su compra debido a que encuentran el proceso de pago muy complicado, largo o muy intrusivo al solicitar información sensible.[36] Por su lado, la biometría ofrece mayor privacidad cuando reemplaza información como la dirección de vivienda, el correo electrónico o el número telefónico. Además, al brindar mayor dinamismo en los procesos de pago promete cambiar el panorama del comercio pues cuando se agiliza el tiempo de compra de los consumidores esto normalmente tiende a generar mayor gasto y menos tiempo para cambiar de parecer.

02

USO DE LA BIOMETRÍA EN DESASTRES NATURALES.[37]

Tras la avalancha del 30 de marzo del año 2016 en Mocoa, Colombia, muchas personas se vieron afectadas y entre ellas cerca de tres mil personas beneficiarias de subsidios del Estado perdieron sus documentos. Con el uso de cinco mil datafonos, la compañía AssendaRed – empresa de Carvajal Tecnología y Servicios y operador del Banco Agrario – realizó una jornada de identificación biométrica con el fin de que estas personas pudieran volver a cobrar las ayudas. Valiéndose de la base de datos de la Registraduría Nacional y la autenticación de la huella dactilar, se permitió evitar el robo de dineros utilizando la modalidad de suplantación de identidad, por parte de personas inescrupulosas que puedan tener en su poder tarjetas y documentos de beneficiarios afectados, desaparecidos o fallecidos en la tragedia.

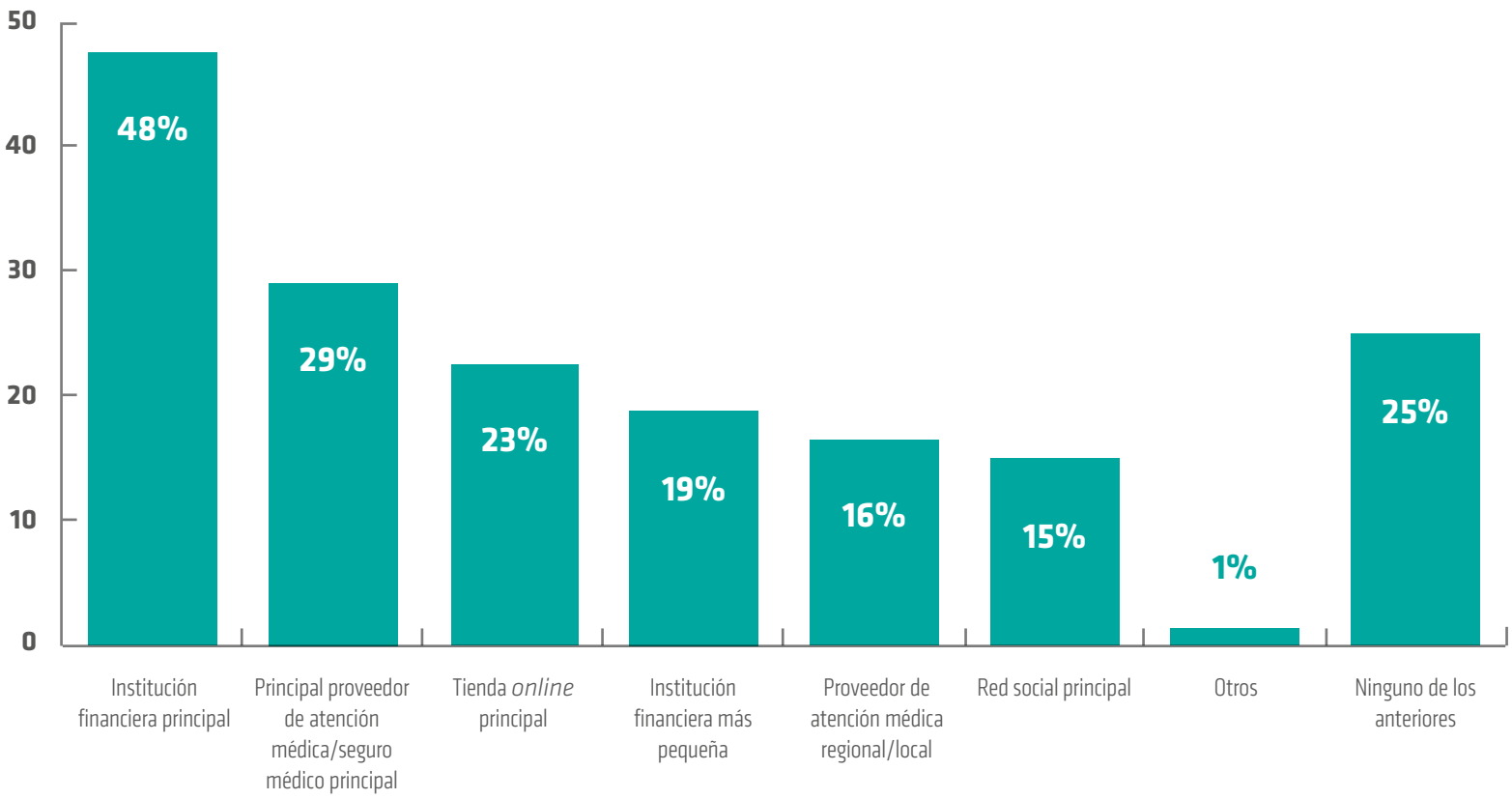
03

LA BIOMETRÍA COMO SISTEMA DE IDENTIFICACIÓN NACIONAL[38]

En el año 2017, India alcanzó la inscripción de más del 99% de sus ciudadanos mayores a 18 años – es decir más de 1,000 millones de personas – en su programa de identificación digital respaldada por biometría de huellas dactilares e iris. A principios del 2018, una nueva modalidad biométrica es instaurada, el reconocimiento facial, para extender las opciones de identificación.[39] Una vez puesto en funcionamiento, la base de datos conocida como Adhaar, permitió que una buena proporción de los indios participara en la economía formal, ya sea consiguiendo empleo o recibiendo prestamos de los bancos. El sistema también permite que el gobierno desembolse subsidios directa e instantáneamente a los beneficiarios poseedores de una cuenta bancaria o billetera móvil asociada con su identificación, lo que ahorra meses de obstáculos burocráticos y elimina la "comisión" de intermediarios.

Hasta ahora, la implementación de los sistemas biométricos no se ha dado en su totalidad debido a los costos en los que deben incurrir los comerciantes para utilizar estos métodos de verificación y por las preocupaciones que aún tienen los consumidores sobre la protección de su información. Sin embargo, con el surgimiento del móvil como canal bancario predominante y de estrategias bancarias que plantean el uso de dispositivos vestibles *(wearables)*, se espera que en los próximos años el despliegue de estos sistemas tome mucho mayor protagonismo.

Figura 1. Tipos de organización en las que las personas confían más para proteger su información biométrica (perspectiva global)



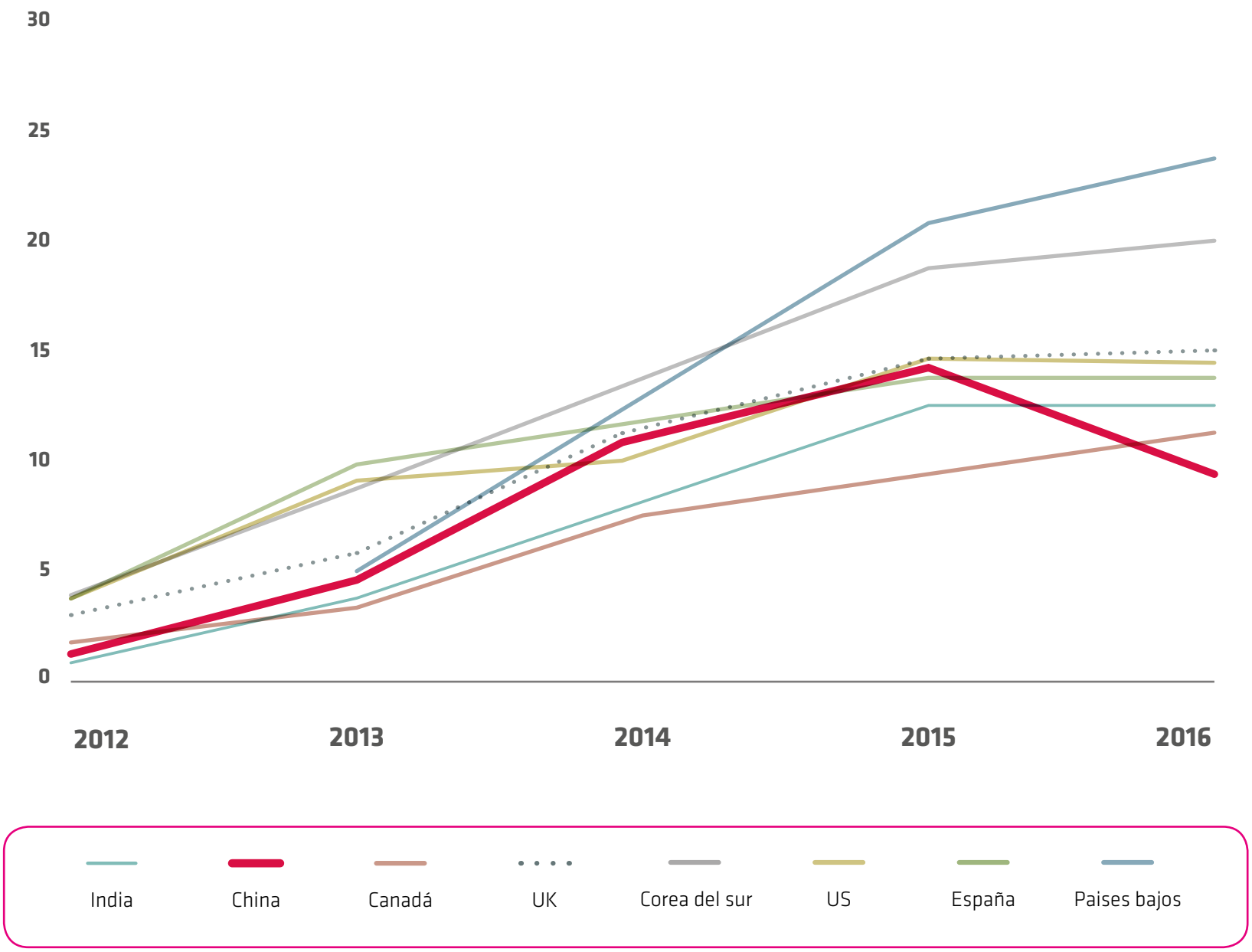
Fuente: IBM, 2018[40]

En particular, los bancos deben aprovechar su posición como las instituciones más confiables en la protección de los datos biométricos de los usuarios de tal manera que se consoliden como líderes en los servicios de autenticación y como los facilitadores de medios de pago. En contraste, es importante reconocer que la entrada de los gigantes digitales como Amazon, Apple y Alibaba en el ámbito financiero traerá un nivel de competencia mucho más alto. Según un reporte de Bain & Company, más de una cuarta parte de estadounidenses estarían dispuestos a utilizar asistentes de voz como Alexa, Siri o Cortana para realizar sus actividades bancarias diarias.[41]

Es más, los acontecimientos en China pueden dar una idea del futuro en la industria financiera. Según un análisis de Bain & Company, en China hubo un menor uso móvil para las interacciones bancarias rutinarias en el año 2016 debido a que los consumidores utilizan con mayor frecuencia plataformas no bancarias que consideran más convenientes y prácticas como WeChat y Alipay para pagos, ahorros y otras transacciones financieras.

Puesto que los usuarios están cada vez más abiertos a comprar productos financieros de empresas digitales y ya que la experiencia del usuario ha mostrado ser mayor en estas, los bancos deben enfocarse principalmente en el relacionamiento con sus clientes y en bajar significativamente sus costos.

Figura 2. Número de interacciones móviles promedio por usuario en varios países



Fuente: Bain & Company, 2016.
Nota: No hay datos para Holanda en el año 2012.

“El diseño no es solo cómo se ve o cómo se siente. El diseño es cómo funciona”.

– Steve Jobs

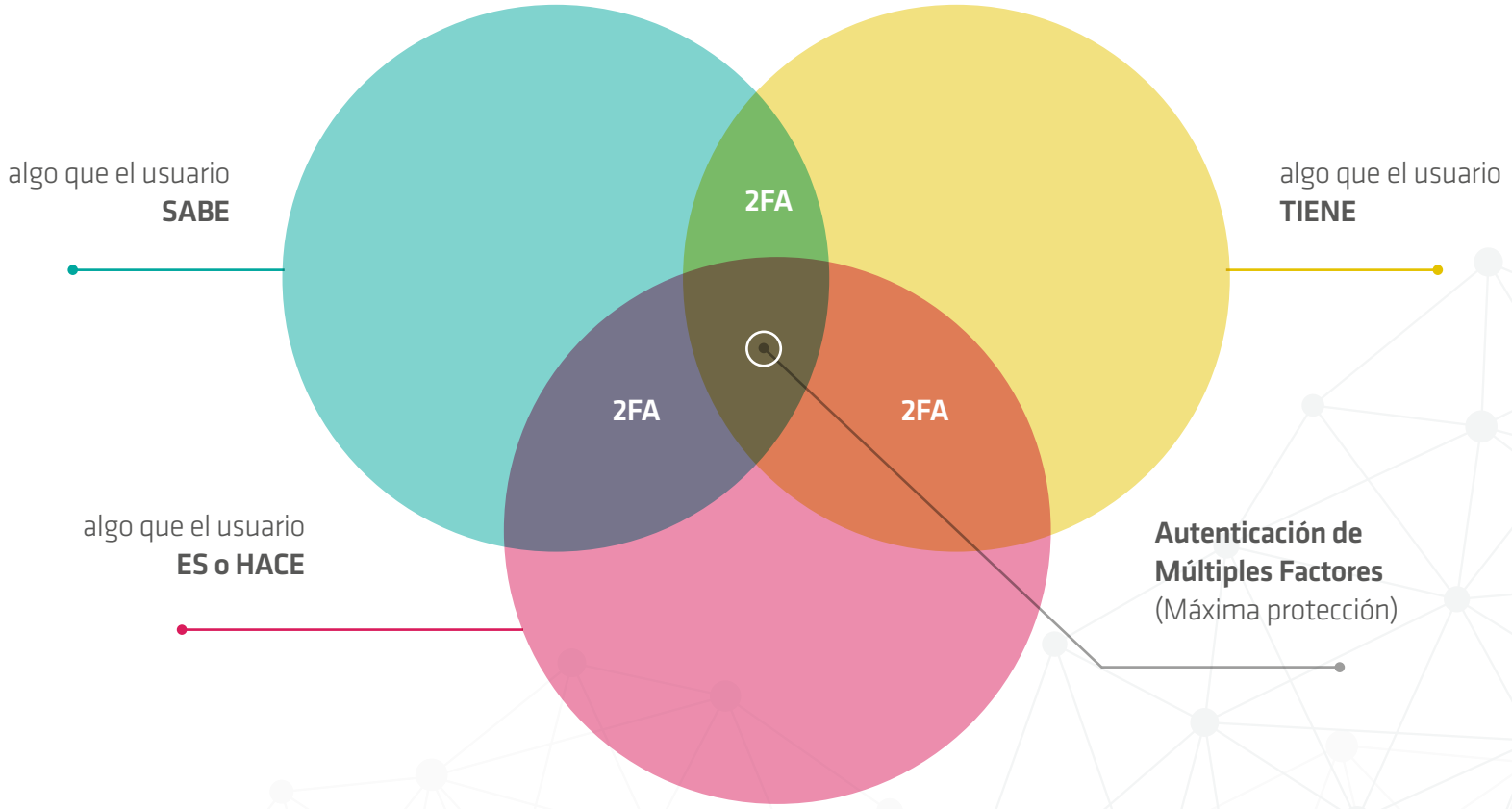
CIBERESPACIO: TU IDENTIDAD MÁS ALLÁ DE LAS CONTRASEÑAS

CIBERESPACIO: TU IDENTIDAD MÁS ALLÁ DE LAS CONTRASEÑAS

La manera en que las personas logran corroborar su identidad se puede agrupar en tres categorías: i) algo que el usuario sabe, ii) algo que el usuario tiene, y iii) algo que el usuario es o hace.

i. **Factor de Conocimiento:** contraseña, código PIN, respuestas a preguntas de seguridad, etc.
ii. **Factor Físico:** Documento de identidad, *token* de seguridad, teléfono celular, llave física, etc.
iii. **Factor Inherente:** huella, firma, voz, etc.

Figura 3. Tres factores de autenticación



Fuente: Elaboración propia.
Nota: 2FA hace referencia al término en inglés *Two-Factor-Authentication*, que en español significa autenticación de dos factores.

Cada uno de estos factores de autenticación cubre un rango de elementos que son usados para verificar la identidad de una persona antes de aprobar una transacción, proporcionar ingreso, firmar un documento u otorgar autoridad a otros usuarios, y demás. Como se ha mencionado en párrafos anteriores, existen varios inconvenientes en el uso de claves u objetos como método de identificación ya que suelen olvidarse o perderse. Estos problemas en particular se acrecientan a medida que las redes se expanden y las personas se conectan.

Debido a la explosión de las redes sociales y el aumento en la oferta de servicios por internet se estima que para el año 2020 el usuario promedio podría contar con 200 cuentas en línea.[43] En ese sentido, se vuelve inconcebible que los usuarios administren contraseñas robustas y únicas para cada una de ellas. Al contrario, por simplicidad, hoy más de dos tercios de las personas usan la misma contraseña repetidas veces.[44]

04

LA BIOMETRÍA A 2020 EN LOS SERVICIOS FINANCIEROS.[45,46]

Según predicciones de Goode Intelligence, para el año 2020 el papel que tomará la biometría dentro el sistema financiero será de gran importancia. Estas serían algunas de sus implicaciones:

La biometría como el método predominante de identificación.

622 millones de descargas de aplicaciones móviles bancarias habilitadas con biometría.

Más de 3.000 millones de clientes utilizarán la biometría para la seguridad de sus pagos. **En 2015 solo lo hicieron 350 millones.**

Protegerá USD$5,6 billones en pagos

Según un estudio comisionado por Telesign,[47] más de la mitad de los consumidores (54%) en Estados Unidos y el Reino Unido usan cinco o menos contraseñas en toda su vida en línea. Además, también encontró que los consumidores raramente cambian sus contraseñas, pues casi la mitad (47%) de ellos dependen de una clave que no se ha modificado durante cinco o más años.

El núcleo del problema para la seguridad digital de las personas y las instituciones recae en que la principal fuente de pérdida de datos se atribuye a contraseñas débiles y al robo de identidades. Sólo en el año 2016, el 81 por ciento de las principales vulneraciones de información se remonta a una sola identidad comprometida de las personas.[48] Es decir, a una sola cuenta víctima de fraude electrónico.

Las contraseñas robadas son tan comunes entre los delincuentes que con facilidad logran comprar 1.000 nombres de usuario y contraseñas por menos de USD$20 en la 'Dark Web'.[49] Con ellas pueden infligir una cantidad de daño financiero considerable por una inversión muy pequeña. Por eso, no es posible pensar que las contraseñas por sí solas sean suficientes para garantizar seguridad. En el año 2004, Bill Gates ya establecía la necesidad de migrar a otros sistemas de autenticación.[50]

Pero, no es hasta el año 2013 cuando el mundo empieza a adoptar masivamente los mecanismos de au-

tenticación de la siguiente generación: los sistemas biométricos. A partir de ese año, el número de modelos de smartphones que incorporan sensores de huellas creció significativamente y las personas comenzaron a familiarizarse con la biometría. Si para el año 2014 se estimó que el 3% de los modelos incorporaban estos sensores, para el año 2017 más de dos tercios los tenían.[51] Este cambio sustancial se asocia con el lanzamiento del sistema de reconocimiento de huellas de Apple (TouchID), que debutó en el iPhone 5s y continuo en los siguientes dispositivos iOS. Con el lanzamiento a finales del año 2017 por parte de Apple de su nuevo sistema FaceID, se espera un nuevo impulso a la biometría de reconocimiento facial.

En este sentido, gracias a la adopción masiva de dispositivos móviles habilitados para usar tecnología biométrica, los bancos han podido implementar este tipo de autenticación para millones de usuarios sin mayor inversión en hardware adicional. Aquí, el principal desafío para las instituciones financieras es tener la capacidad de soportar y facilitar los múltiples factores de autenticación que utilicen sus usuarios, ya sea reconocimiento facial, de huellas u otros. No obstante, en Colombia ya varias entidades han demostrado ser particularmente innovadoras:

- Nequi, una empresa que ofrece servicios bancarios móviles, es la primera firma colombiana que incorpora el reconocimiento facial para la autenticación móvil de sus usuarios. Aparte de implementar técnicas de detección de vida, también incorpora el reconocimiento de voz como una modalidad biométrica adicional.[52]

- A principios del 2017, el Banco Colpatria ya tenía en operación una plataforma multi-biométrica en sus oficinas. Esta plataforma, llamada ReconoSer, valida en tiempo real la identidad del ciudadano logrando mitigar la suplantación o robo de identidad.[53]

- Redeban MultiColor está trabajando para traer la solución de Pago Facial a Colombia. Con ella, los usuarios podrían realizar pagos utilizando únicamente su rostro, esto gracias a una aplicación en sus dispositivos móviles habilitados para escanear la cara de las personas.[54]

Dado que los dispositivos habilitados con biometría no están equipados para capturar información de todas las modalidades biométricas sino solo de algunas (dependiendo de los sensores incluidos en cada dispositivo), resulta importante que las entidades financieras avancen en la oferta de productos que contemplen varias opciones de autenticación. En esa misma línea, también es importante verlo como complemento en caso de que los datos biométricos de un usuario puedan verse comprometidos a causa de un accidente. Por ejemplo, cuando hay quemaduras en la punta de los dedos, el usuario podría experimentar inconvenientes para incorporarse a un sistema de identificación basado en huellas dactilares y sería oportuno contar con otro identificador biométrico.

Por otra parte, todavía persisten retos para la implementación de la tecnología biométrica cuando esta se utiliza como la única forma de autenticación. A diferencia de las contraseñas, donde estas son correctas o equivocadas, los mecanismos de verificación biométricos funcionan

EN UN AEROPUERTO (NEC, 2018),SISTEMAS DE AUTENTICACIÓN BIOMÉTRICA FACILITAN BASTANTE LOS PROCEDIMIENTOS. DE ESTA MANERA, USTED PUEDE EVITARSE LOS TEDIOSOS TRÁMITES. LUEGO DEL CHECKIN, EN EL ÁREA DE SEGURIDAD, UNA ENTRADA CON DISPOSITIVOS DE IDENTIFICACIÓN BIOMÉTRICA INTEGRADOS VERIFICA SU PASAPORTE Y ESCANEA SU ROSTRO PARA VALIDAR SU INFORMACIÓN. POSTERIORMENTE SU FOTO ES BORRADA PARA PRESERVAR SU PRIVACIDAD Y USTED PUEDE PROCEDER A ABORDAR EL AVIÓN.

con puntajes que describen la probabilidad de coincidencia. De esta manera, se tiene en cuenta que tan parecidos son los datos biométricos de un usuario con aquellos registrados previamente en una plantilla digital. Teniendo eso en mente, su resultado puede terminar en falsos positivos (identificando incorrectamente a alguien como el genuino usuario sin éste serlo) o en falsos negativos (diciendo incorrectamente que el legítimo usuario no es verdadero). Esto quiere decir que, si el rendimiento de la tecnología biométrica no es confiable, esto se reflejaría negativamente en los bancos pues podrían estar aceptando frecuentemente usuarios ilegítimos o identificando erróneamente como sospechosos a usuarios genuinos. Tanto la regulación como los consumidores no aceptarían que eso ocurriera.

La biometría funciona mejor si se vincula con un segundo factor de autenticación, cómo un teléfono celular o una contraseña, entre otros. Así las cosas, existe un *trade-off* entre conveniencia y seguridad, pues a medida que más factores de autenticación se incluyan, el usuario necesita más pasos para corroborar su identidad. Sin embargo, es importante reconocer que por unos años más la biometría, por sí sola, será un tema más de conveniencia que de seguridad.

Así las cosas, un banco podría escoger un mecanismo de autenticación conveniente como el uso de la huella dactilar para que sus usuarios puedan consultar su saldo bancario desde el móvil. Sin embargo, no escogería el mismo método para aprobar una transacción internacional multimillonaria. Seguramente, el proceso de autenticación que podría ser más pertinente es aquel que incorpore un sistema biométrico multi-modal atado a una sucursal bancaria con fuertes protocolos de seguridad.

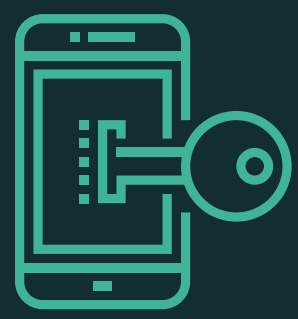
Lamentablemente, los delincuentes no se detendrán en la búsqueda de nuevas formas de adquirir dinero. Incluso después que las instituciones toman medidas que logran disminuir un cierto tipo de criminalidad, es posible que las cifras aumenten nuevamente a medida que los atacantes encuentran nuevas técnicas y canales para cometer fraudes. Por ejemplo, en la transición hacía tarjetas de crédito y débito más seguras gracias al chip EMV, el fraude electrónico se fue dirigiendo de lo físico a lo digital.w[55] Mientras que en el 2014 el 70 por ciento del fraude de tarjeta se realizaba por canales como datáfonos o cajeros automáticos, en la actualidad el 80 por ciento se materializa en compras no presenciales (internet o teléfono).[56]

Hoy, el principal enfoque de los mecanismos de autenticación debe estar en mitigar el riesgo de fraude por canales digitales. No obstante, las instituciones financieras tienen el reto de no poner medidas de seguridad ni muy complejas ni muy sencillas, pues deben incentivar al usuario al uso cotidiano de estos canales digitales, pero también deben hacerles sentir protegidos para que los sigan usando en el futuro. Los bancos deberán resolver el *trade-off* de conveniencia versus seguridad con ayuda de la tecnología biométrica.

“La seguridad siempre es excesiva hasta que no es suficiente”.

– Robbie Sinclair

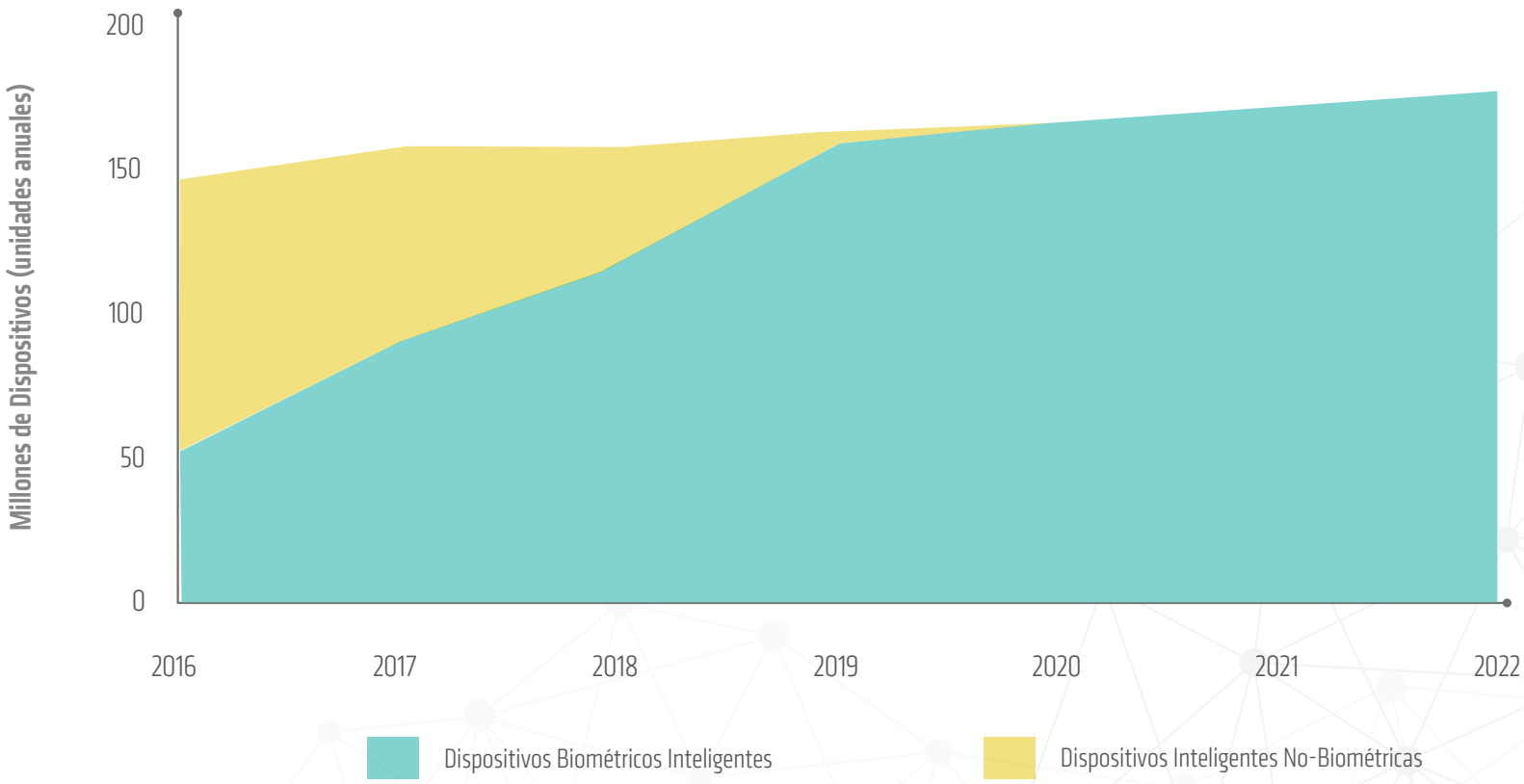
SEGURIDAD: UN TOQUE HUMANO PARA CADA DISPOSITIVO



SEGURIDAD: UN TOQUE HUMANO PARA CADA DISPOSITIVO

Si las principales preocupaciones en la implementación de sistemas biométricos por parte de las instituciones son los costos asociados y la confiabilidad de la tecnología, la primordial preocupación a considerar por los usuarios recae en la privacidad de su información. Por un lado, con la correcta implementación de estos sistemas las personas pueden ver su privacidad beneficiada cuando la biometría sirve de sustituto a datos sensibles (como el correo electrónico o el número telefónico) que son exigidos en procesos de compra por internet, entre otros. Y, gracias a la fuerte ola de dispositivos móviles habilitados con lectores biométricos en el mercado, los usuarios podrán escoger este mecanismo de autenticación con mayor facilidad.

Figura 4. Número de dispositivos móviles biométricos vs. no-biométricos en Latinoamérica (millones)



Fuente: Acuity Market Intelligence, 2017.[57]
Nota: Los dispositivos móviles incluyen *smartphones*, tabletas y *wearables*.

Sin embargo, los usuarios cada vez son más conscientes de que es normal que sus rasgos biométricos estén expuestos, a diferencia de las contraseñas que permanecen secretas. Esto facilita que las personas puedan ser identificadas fácilmente con o sin su permiso. Como es el caso del reconocimiento facial, ahora es posible encontrar el perfil de una persona en redes sociales con solo tomarle una foto y usando una aplicación, tal y como sucede en Rusia con la app FindFace.[58] O, por ejemplo, Facebook podría obtener imágenes del interior de un concesionario e identificar a los visitantes para luego enviarles publicidad relacionada con carros. Se tiene entonces que, una vez los datos biométricos son capturados, no hay manera fácil de cambiarlos como sí se puede hacer con las contraseñas.

Por tal razón, para que las interacciones migren a lo digital, los usuarios deben primero tener la tranquilidad de que sus datos son usados correctamente y segundo deben tener garantías de que están bien protegidos. Un estudio de Capgemini[59] encontró que las preocupaciones de seguridad impiden que casi la mitad de los consumidores (47%) usen canales digitales, y también concluyó que el 74 por ciento cambiaría su banco o aseguradora en caso de una vulneración de datos.

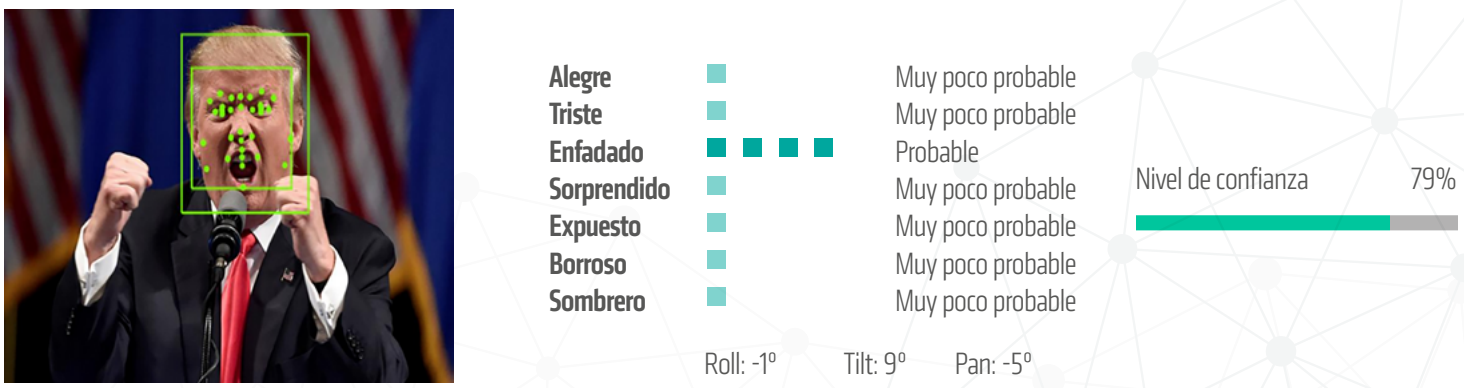
En este sentido, el sistema de protección de la información que utilicen las organizaciones debe contar con varios niveles de seguridad, que logren mitigar el riesgo de sufrir ataques fraudulentos o que delincuentes puedan pasarlos por alto. Por ejemplo, si el proceso de registro es fácil, los *hackers* encontrarían la manera de adjuntar información ajena a sus propios datos biométricos, lo que les permitiría iniciar sesión fácilmente como otra persona o configurar una cuenta a nombre de alguien más. Al fin y al cabo, la plantilla digital donde se registran los datos biométricos es simplemente una representación matemática de esa

05

¿QUÉ PUEDE DECIR LA TECNOLOGÍA SOBRE TI?

Mucha gente se frustra fácilmente cuando la tecnología no funciona bien o es contra-intuitiva. Lo que menos esperan es que esta misma tecnología entienda sus emociones y se relacione con ellos de diferente manera como resultado. Pues gracias a los avances en la ciencia biométrica y la inteligencia artificial, la tecnología se está volviendo emocionalmente inteligente, y esto puede cambiar muchas percepciones.

Figura Análisis Biométrico según expresiones faciales.



Fuente: Adaptado de Edgar Helou (GoogleCloud), 2017.[60]

Al analizar los distintos rasgos biométricos (como la entonación de la voz o la lectura del rostro) con ayuda de la tecnología, las instituciones podrían prestar un mejor servicio al cliente al entender mejor el estado anímico del usuario en tiempo real.

- En china, el restaurante KFC lanzó su primer restaurante inteligente que utiliza el reconocimiento facial para recordar y predecir el plato que el usuario probablemente quiere, según su edad estimada y "humor" dependiendo del día.[61]

Pensar que la tecnología puede engancharse emocionalmente con las personas es sorprendente y necesario en el futuro, si se toma en cuenta la predicción de Gartner para 2020, donde los clientes administrarán el 85% de su relación con las empresas sin interactuar con otro ser humano.[62]

información y está sujeta a los peligros asociados al robo de identidad.

Con los ataques cibernéticos cada vez más sofisticados, las medidas de seguridad también deben ser más inteligentes. Un siguiente paso se encuentra con la incorporación de la biometría conductual, pues la clave está en implementar medidas de seguridad que monitoreen y prueben continuamente la autenticidad de los usuarios mediante características difíciles de replicar. Sin embargo, técnicas como la geolocalización también son importantes, pues la creciente inclusión de la funcionalidad de GPS en los dispositivos móviles, ha permitido que la ubicación sea tomada en cuenta para la seguridad.

De esta forma, si un cliente quiere revisar su saldo y se encuentra en casa, con el uso de reconocimiento facial desde su celular podría ser suficiente. Pero, si el cliente se encuentra en Venezuela y está intentado transferir USD$10.000, el sistema podría requerir dos o tres tipos de autenticación diferentes.

Aquí, hay que considerar que ninguna tecnología ha probado ser inquebrantable. Con el tiempo y dinero suficientes es posible vulnerar cualquier sistema de seguridad. Incluso Blockchain –"la tecnología más segura"- se ve amenazada ante el alcance aún desconocido de la computación cuántica.[63] La única medida preventiva que queda para la protección de la información es hacer la vulneración del sistema tan costosa de realizar que los beneficios de un ataque exitoso no valgan la pena.

Entonces, para avanzar en ese cometido hay que estar siempre alerta frente a nuevos riesgos y, ante todo, contar con la colaboración de todas las partes involucradas. Esto concierne a los bancos y organizaciones, en relación con los sistemas de seguridad implementados; a los clientes, a través del uso consciente de internet y de sus dispositivos; a la policía y la ley con avances en la judicialización adecuada de delitos cibernéticos; y, por último, a los desarrolladores de tecnología en relación con la sofisticación, estandarización y confiabilidad de la tecnología. Por ahora, en un horizonte de tiempo cercano la autenticación de múltiples factores (siempre y cuando involucre la biometría) es el método más robusto para acceder a distintos servicios.[66] Sin embargo, es

06

¿CÓMO ASEGURAR QUE LOS DATOS BIOMÉTRICOS SEAN INÚTILES ANTE EL ROBO DE IDENTIDAD?[64]

Uno de los casos más populares y recientes de robo de identidad lo sufrió el "Office of Personnel Management" (OPM) en Estados Unidos. Siendo víctimas de un ciberataque, más de cinco millones de registros biométricos quedaron comprometidos.[65] En casos como estos dónde la información biométrica de los usuarios ya está en manos de los delincuentes, es importante tener en cuenta buenas prácticas y tácticas que vuelvan inútil esa información salvo para el usuario genuino.

Entre ellas estarían:

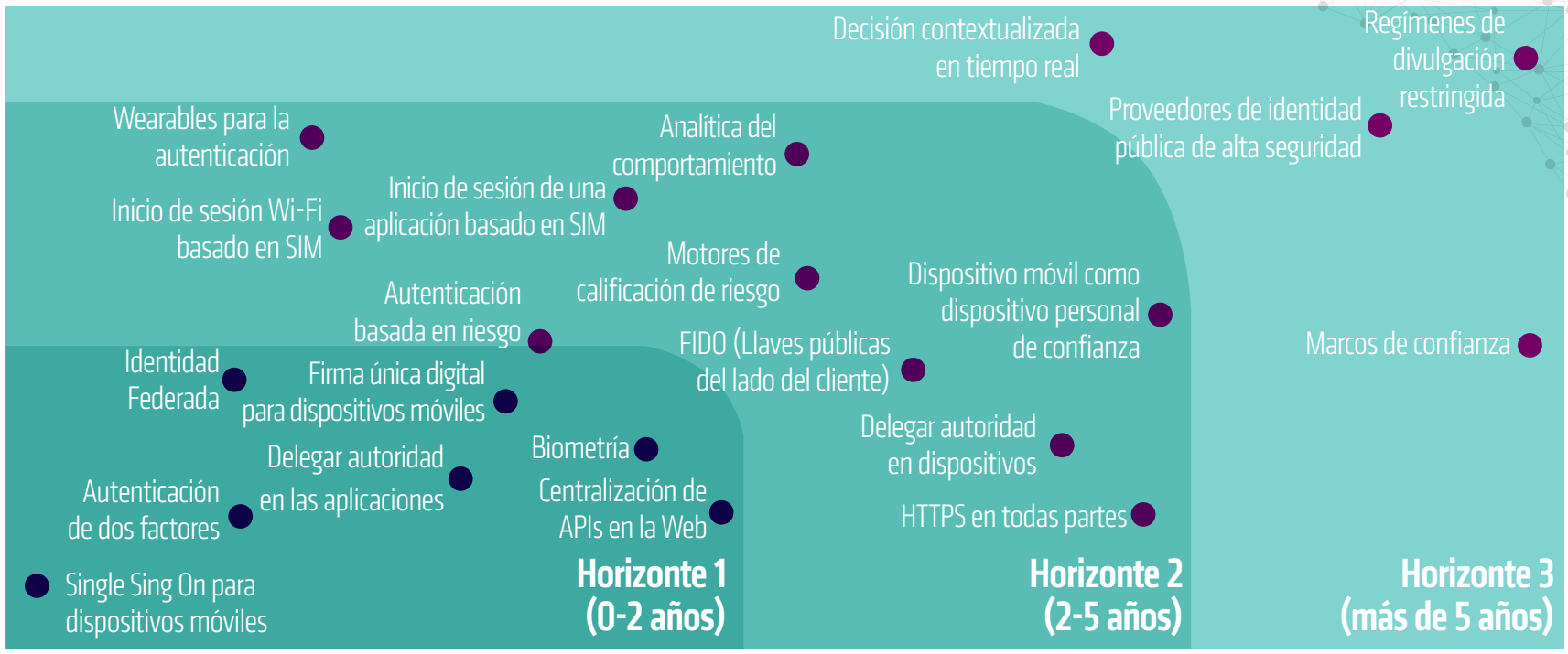
- **Mejorar la detección de vida:** Las huellas, el iris y el rostro son únicos a cada usuario, pero eso no quiere decir que no se pueden copiar. Por eso, es importante avanzar en la sofisticación de la tecnología de tal manera que permita diferenciar una biometría falsa de una verdadera. Que utilice algoritmos avanzados de *machine learning* (inteligencia artificial) y se actualice frente a nuevas amenazas.
- **Usar sistemas de autenticación multi-modal y de múltiples factores:** En la medida que sea práctico, las instituciones deben considerar el uso de más de un factor de autenticación para darle mayor seguridad y mejor probabilidad de reconocimiento a sus sistemas.
- **Robustecer las plantillas biométricas:** Al tener una plantilla biométrica combinada con otra información, como una clave dinámica (OTP en inglés), permitiría a los sistemas reconocer y rechazar una plantilla fraudulenta. La idea en sí es fortalecer las plantillas frente a fraudes electrónicos.
- **Hacer la identidad más resistente:** La cadena de confianza es tan fuerte como su eslabón más débil. Todos los elementos involucrados en la captura y el uso de datos biométricos deben poder encriptarse y volverse resistentes a técnicas fraudulentas. Es importante proteger la integridad de la comunicación entre el usuario y el sensor que captura su información.

importante desarrollar mecanismos de seguridad complementarios en la red para seguir avanzando en la protección de la identidad de todos los usuarios.

Según Telstra, los mecanismos a implementar que veremos en los próximos años son los que se presentan en la figura 5.:

Una consideración final sería que a medida que la globalización y la prestación de servicios en la red se sobreponen a los límites de las fronteras geográficas, la regulación de cada país deberá encontrar un punto medio (una estandarización) para que el flujo de información, incluyendo la identidad digital de las personas, no presente trabas y a la vez cumpla con las normas legales de cada territorio. Es lógico pensar que cuando un cliente usa una autentica-

Figura 5. Hoja de ruta tecnológica para la gestión de identidad[67]



Fuente: Traducido de Telstra Research, 2015.
Nota: La explicación detallada de los componentes puede encontrarse en el blog "Ruta tecnológica para la gestión de identidad" dentro del portal www.fintechgracion.com.

ción biométrica para abordar su vuelo de ida a Japón, debería poder identificarse así cuando esté de regreso para mejorar la experiencia del usuario. Sin embargo, todavía hay un largo debate a resolver en cuanto a ¿quién es dueño de la información y quién puede usarla? O podría reformularse así: ¿quién es efectivamente el dueño de la identidad digital de una persona?

En últimas, el sector financiero tiene la gran oportunidad de ser líderes en el almacenamiento de la información debido a sus niveles de seguridad y adaptación constante frente a nuevas amenazas. Las personas y los gobiernos confían en ellos para guardar su dinero y más importante aún para guardar su información sensible. Sin embargo, para seguir construyendo su reputación en privacidad de datos y seguridad robusta, deben subir el nivel en distintas dimensiones:

- Alinear las prácticas de captura y protección de datos con las expectativas de los consumidores.
- Encontrar formas innovadoras de proporcionar seguridad no intrusiva a los consumidores.
- Desarrollar las capacidades necesarias para monitorear y adaptarse a los riesgos cibernéticos en tiempo real.
- Revisar el modelo de gobernanza de datos.

Abordar las consideraciones en privacidad y seguridad digital, les ofrecerá a los bancos una ventaja comercial estratégica que impulsará una mayor adopción de canales digitales de menor costo operacional y atraerá a nuevos clientes.[68]

NOTAS

1. MasterCard, 2015. Press Releases: MasterCard Identity Check to Simplify and Strengthen Online Shopping. Disponible en https://newsroom.mastercard.com/press-releases/mastercard-identity-check-to-simplify-and-strengthen-online-shopping/

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

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

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

5. IJARCSSE, 2014. Comparative Analysis of Biometric Modalities. Disponible en http://ijarcsse.com/Before_August_2017/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf

6. Goode Intelligence, 2015. Biometrics – An important tool for the customer-first bank. Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-an-important-tool-for-the-customer-first-bank.pdf

7. CNBC, 2017. Alibaba launches 'smile to pay' facial recognition system at KFC in China. Disponible en https://www.cnbc.com/2017/09/04/alibaba-launches-smile-to-pay-facial-recognition-system-at-kfc-china.html

8. Apple, 2018. iOS Security. Disponible en https://www.apple.com/business/docs/iOS_Security_Guide.pdf

9. Goode Intelligence, 2015. Biometrics – An important tool for the customer-first bank. Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-an-important-tool-for-the-customer-first-bank.pdf

10. Goode Intelligence, 2015. "Biometrics – The must-have tool for payment security". Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-

Intelligence-White-Paper-Biometrics-the-must-have-tool-for-payment-security.pdf

11. Barclays, 2018. Infographic: How much time can you save using contactless payments?. Disponible en https://www.home.barclaycard/insights/contactless/How-much-time-can-you-save-using-contactless-payment.html

12. FingerprintsTM, 2017. Biometric Technologies.

13. Ibíd.

14. Andacol, 2017. Bancolombia tendrá cajeros con reconocimiento facial a inicios de 2019. Disponible en https://www.andacol.com/index.php/empresas/2711-bancolombia-tendra-cajeros-con-reconocimiento-facial-a-inicios-de-2019

15. Nuance, 2014. Adiós to PINs, passwords, and security questions. Disponible en https://www.nuance.com/content/dam/nuance/en_au/collateral/enterprise/case-study/cs-banco-santander-mexico-en-us.pdf

16. Goode Intelligence, 2015. Biometrics – An important tool for the customer-first bank. Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-an-important-tool-for-the-customer-first-bank.pdf

17. Goode Intelligence, 2015. "Biometrics – The must-have tool for payment security". Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-the-must-have-tool-for-payment-security.pdf

18. BioCatch, 2017. Invisible Challenges. Disponible en https://www.biocatch.com/hubfs/BioCatch_Invisible_Challenges_%20FINAL-FINAL%20(23.4.17).pdf?hsCtaTracking=e91c8dfb-2419-478e-9cce-9355e404d449%7Cdec5cb3f-c6a3-46f4-9b50-c3f3a4fff5f1

19. Gelb, A. & Clark, J., 2013. Identification for Development: The Biometrics Revolution (CGD Working Paper 315. Washington, DC: Center for Global Development). Disponible en http://www.cgdev.org/content/publications/detail/1426862

20. 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/

21. Redeye, 2016. Fingerprint Cards: China in your hand. Disponible en https://www.redeye.se/company/fingerprint-cards/481400/fingerprint-cards-china-your-hand

22. IJARCSSE, 2014. Comparative Analysis of Biometric Modalities. Disponible en http://ijarcsse.com/Before_August_2017/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf

23. Bain & Company, 2014. Customer Loyalty in Retail Banking: Global Edition. Disponible en http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2014-global.aspx

24. Juniper, 2018. Futureproofing digital banking.

25. Bain & Company, 2016. Customer Loyalty in Retail Banking. Disponible en http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2016.aspx

26. IBM, 2014. Omnichannel Banking. Disponible en https://www-935.ibm.com/services/multimedia/Omnichannel_banking.pdf

27. BBC, 2017. South Africa's Vodacom To Buy 35% Of Kenya's Safaricom From Parent Vodafone. Disponible en https://www.forbes.com/sites/tobyshapshak/2017/05/15/south-africas-vodacom-to-buy-35-of-kenyas-safaricom-from-parent-vodafone/#7e3461452a63

28. Nilson, 2017. Credit card fraud: what you need to know. Disponible en https://nilsonreport.com/upload/pdf/Credit_card_fraud_what_you_need_to_know.pdf

29. Bain & Company, 2016. Customer Loyalty in Retail Banking. Disponible en http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2016.aspx

30. IBM Security, 2018. Future of Identity Study. Disponible en https://www.ibm.com/account/reg/us-en/signup?formid=urx-30345

31. Biometrics Research Group, Inc., 2016. Biometrics & Banking.

32. Have I been pwned. Ultima vez accedido el 20 de marzo de 2018. https://haveibeenpwned.com/

33. Biometrics Research Group, Inc., 2016. Biometrics & Banking.

34. Barclays, 2018. Infographic: How much time can you save using contactless payments?. Disponible en https://www.home.barclaycard/insights/contactless/How-much-time-can-you-save-using-contactless-payment.html

35. Kantar TNS, 2017. Connected Life Report. Disponible en http://connectedlife.tnsglobal.com/

36. MEF, 2017. Mobile Money Report. Disponible en https://mobileecosystemforum.com/mobile-money-report/

37. ElPaís, 2016. Con identidad biométrica entregarán subsidios a víctimas en Mocoa. Disponible en http://www.elpais.com.co/colombia/con-identidad-biometrica-entregaran-subsidios-a-victimas-en-mocoa.html

38. BFNA, 2017. The No Collar Economy. Disponible en http://www.bfna.org/project/the-no-collar-economy/

39. Bloomberg, 2018. UIDAI To Allow Face Recognition For Aadhaar Authentication. Disponible en https://www.bloombergquint.com/aadhaar/2018/01/15/uidai-to-allow-face-recognition-for-aadhaar-authentication

40. IBM Security, 2018. Future of Identity Study. Disponible en https://www.ibm.com/account/reg/us-en/signup?formid=urx-30345

41. Bain & Company, 2017. Evolving the Customer Experience in Banking: 'Alexa, Move My Bank

Accounts to ...'. Disponible en http://www.bain.com/publications/articles/evolving-the-customer-experience-in-banking.aspx

42. Bain & Company, 2016. Customer Loyalty in Retail Banking. Disponible en http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2016.aspx

43. Deloitte, 2017. Predicciones sobre tecnología, medios y telecomunicaciones. Disponible en https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/technology-media-telecommunications/TMT%20Predictions%202017%20Spanish-Americas%20Region.pdf

44. Microsoft, 2017. What's the solution to the growing problem of passwords? You, says Microsoft Disponible en https://news.microsoft.com/features/whats-solution-growing-problem-passwords-says-microsoft/

45. Goode Intelligence, 2015. Biometrics – An important tool for the customer-first bank. Disponible en http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-an-important-tool-for-the-customer-first-bank.pdf

46. Biometrics Research Group, Inc., 2016. Biometrics & Banking.

47. Telesign, 2015. TeleSign Consumer Account Security Report. Disponible en http://info.telesign.com/rs/911-SFQ-678/images/Report%20-%20TeleSign%20Consumer%20Account%20Security%20Report%20-%20EN.pdf

48. Microsoft, 2017. What's the solution to the growing problem of passwords? You, says Microsoft Disponible en https://news.microsoft.com/features/whats-solution-growing-problem-passwords-says-microsoft/

49. Microsoft, 2017. What's the solution to the growing problem of passwords? You, says Microsoft Disponible en https://news.microsoft.com/features/whats-solution-growing-problem-passwords-says-microsoft/

50. Telesign, 2016. Beyond the Password: The Future of Account Security. Disponible en http://info.telesign.com/rs/911-SFQ-678/images/Report-The%20Future%20of%20Account%20Security-EN.pdf

51. Juniper, 2017. Mobile Biometrics – Thumbs up?

52. Daon, 2016. NEQUI AIMS TO BUILD A NEW WAY OF ACCESSING MONEY. Disponible en https://www.daon.com/newsroom/press-releases/340-nequi-aims-to-build-a-new-way-of-accessing-money

53. Enter, 2017. SOLUCIÓN BIOMÉTRICA COLOMBIANA MEJORA SEGURIDAD EN BANCOS. Disponible en http://www.enter.co/especiales/colombia-bringiton/empresa-colombiana-desarrolla-solucion-que-mejora-seguridad-en-bancos/

54. Dinero, 2017. Adiós al efectivo y tarjetas convencionales gracias a estos novedosos sistemas de pago. Disponible en http://www.dinero.com/empresas/articulo/redeban-multicolor-estrena-sistemas-de-pago-en-colombia/246808

55. Forbes, 2017. EMV Chips On Debit And Credit Cards Have Pushed Fraud To E-Commerce.

Disponible en https://www.forbes.com/sites/tomgroenfeldt/2017/12/12/emv-chips-on-debit-and-credit-cards-have-pushed-fraud-to-e-commerce/#40db179812e8

56. Asobancaria, 2017. Discurso de instalación - XI Congreso de Prevención del Fraude y Seguridad: Anticipar para Prevenir. Disponible en https://marketing.asobancaria.com/hubfs/Asobancaria%20Eventos/Asobancaria%20-%20Semanas-Economicas/1113.pdf

57. Acuity Market Intelligence, 2017. The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy

58. TheEconomist, 2017. What machines can tell from your face. Disponible en https://www.economist.com/news/leaders/21728617-life-age-facial-recognition-what-machines-can-tell-your-face

59. Capgemini, 2017. The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure. Disponible en https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/

60. Tomado de la presentación de Edgar Helou. "10 X Thinking, 10 veces más, 10 veces más rápido". Disponible en https://www.youtube.com/watch?v=zZPdg0--IEE (minuto 34).

61. TheGuardian, 2016. KFC China is using facial recognition tech to serve customers - but are they buying it?. Disponible en https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition

62. Gartner, 2011. Gartner Customer 360 Summit 2011. Disponible en https://www.gartner.com/imagesrv/summits/docs/na/customer-360/C360_2011_brochure_FINAL.pdf

63. SingularityHub, 2017. Is Quantum Computing an Existential Threat to Blockchain Technology?. Disponible en https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/#sm.00001qz7us8twhdp2r70d702ehck3

64. Biometrics Research Group, Inc., 2016. Biometrics & Banking.

65. The Washington Post, 2015. OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought. Disponible en https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.6bd0612756fe

66. Gemalto. Ultima vez accedido el 20 de marzo de 2018. https://safenet.gemalto.es/multi-factor-authentication

67. Telstra, 2015. Mobile Identity: The Fusion of Financial Services, Mobility and Identity.

68. Capgemini, 2017. The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure. Disponible en https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/

“La disrupción del sistema financiero no va a suceder: **¡está sucediendo!”.**

www.fintechgracion.com