

Biometría: conveniente y segura

- Las instituciones financieras han implementado tecnologías biométricas en una amplia gama de canales bancarios, incluyendo cajeros automáticos, sucursales bancarias, banca telefónica, banca en línea y aplicaciones de la banca móvil. Una de las iniciativas más importantes y de mayor impacto en esta materia es liderada por Asobancaria en conjunto con la Registraduría Nacional del Estado Civil.

- El proyecto de autenticación biométrica dactilar se realiza con la base de datos de la Registraduría, considerada la base de datos biométricos y biográficos más completa y confiable que existe en nuestro país y cuenta con los mayores estándares de seguridad a nivel mundial. Hoy el 60% de las entidades bancarias hacen uso de la biometría dactilar en sucursales bancarias y en la actualidad se realizan 1,1 y 1,3 millones de transacciones por mes. Este proyecto se ha convertido en un referente a nivel regional en materia de seguridad en el sector bancario y en la punta de lanza de los procesos de transformación digital en los servicios financieros.

- Desde una perspectiva global, los bancos son las organizaciones en las que las personas más confían para proteger su información biométrica. Por lo tanto, deben emplear esa confianza para que se consoliden como líderes en los servicios de autenticación y como facilitadores de medios de pago.

- 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. Con los ataques cibernéticos cada vez más sofisticados, las medidas de seguridad también deben ser más inteligentes. Así, abordar aspectos como la privacidad y seguridad digital le ofrecerá a los bancos una ventaja estratégica que promoverá la adopción de canales digitales de menor costo operacional y, al tiempo, atraerá a nuevos clientes. Desarrollar el enorme potencial en materia de seguridad y confiabilidad con estas herramientas es y seguirá siendo un imperativo para la banca y el sistema financiero.

28 de mayo de 2018

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Jonathan Malagón González
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

Para suscribirse a Semana Económica, por favor envíe un correo electrónico a semanaeconomica@asobancaria.com

Visite nuestros portales:
www.asobancaria.com
www.yodecidomibanco.com
www.sabermassermas.com

Biometría: conveniente y segura

La identificación y la autenticación de información de las personas son mecanismos fundamentales para la sociedad moderna, pues permiten interacciones seguras y previenen el fraude y la criminalidad. Actualmente, nuevas técnicas para la verificación de usuarios están siendo exploradas y acondicionadas en el entorno digital. La biometría, por ejemplo, verifica la identidad de un individuo en función de sus características físicas y de comportamiento, lo que ofrece ventajas de seguridad, conveniencia y eficiencia en la autenticación de las transacciones.

Con la implementación de estos mecanismos no solo las instituciones financieras se benefician, sino también el consumidor, ya que obtiene protección y tranquilidad. Estos beneficios son cada vez más importantes en un mundo en el que la movilidad digital y el comercio electrónico son crecientes. Mantener un sistema de seguridad basado únicamente en usuarios y contraseñas representa un riesgo a las instituciones y expone a los usuarios a prácticas vulnerables para proteger su información.

En este contexto, esta Semana Económica hace una caracterización de la biometría, explorando los principales identificadores biométricos utilizados a nivel mundial por la industria financiera, de igual manera, analiza los riesgos a los que la industria financiera se enfrenta debido al actual proceso de digitalización, explicando cómo deben estar preparados los bancos para afrontar estos desafíos; además, se indica cómo abordar aspectos como la privacidad y la seguridad digital para que las entidades bancarias cuenten con una alternativa importante para disminuir sus costos operacionales y atraer a nuevos clientes. Por último, se describen los resultados de una de las iniciativas de autenticación biométrica de mayor impacto en el sector liderada por Asobancaria.

Reconocimiento: de lo análogo a lo digital

La necesidad de un sistema formal que mida los rasgos de identidad de las personas ha existido por bastante tiempo. El primer avance en la materia fue la antropometría, donde se recopilaba información en tarjetas sobre la dimensión de varias partes del cuerpo. Este sistema fue aplicado durante gran parte del siglo XIX, siendo reemplazado por la identificación a partir de huellas dactilares, que actualmente prevalece.

Años después se comenzó a investigar sobre otras modalidades de identificación biométrica como el iris y el reconocimiento facial. Al coincidir con el surgimiento de

Editor

Germán Montoya Moreno
Director Económico

Participaron en esta edición:

Paola Gutiérrez Domínguez
Ángela Vaca Bernal



31
HOTEL HILTON
CARTAGENA

18°

CONGRESO PANAMERICANO
DE RIESGO DE LAVADO DE ACTIVOS
Y FINANCIACIÓN DEL TERRORISMO

Visión multidimensional
del crimen organizado

MÁS INFORMACIÓN
AQUÍ



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, ha sido posible el reconocimiento bajo un esquema digital.

Así las cosas, la identificación biométrica consiste en capturar una imagen o las métricas de un individuo en un dispositivo (por ejemplo, una cámara o un sensor) y, con un algoritmo, apoyado en *hardware* y *software*, se extrae, codifica, almacena y comparan esas características.

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 gran variedad de aplicaciones para distintas industrias. De hecho, se espera que para 2020 la biometría sea el método predominante de identificación para acceder a servicios bancarios¹.

Las instituciones financieras vienen implementando tecnologías biométricas en una amplia gama de canales bancarios, incluyendo cajeros automáticos, sucursales bancarias, banca telefónica, banca en línea y aplicaciones de la banca móvil, empleando distintos identificadores biométricos (Cuadro 1). Por otra parte, han comenzado a trabajar en pilotos y pruebas de conceptos con proveedores de tecnologías biométricas innovadoras sobre dispositivos portátiles².

Cuadro 1. Clases de identificadores biométricos

Identificador	Visión general	Tendencias de uso y ejemplos
 Huellas dactilares	<p>Las crestas epidérmicas en las puntas de los dedos forman un patrón único de huella para cada persona. 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 2020³.</p>	<p>Tarjetas de pago biométricas: mientras que los consumidores tienen un medio de pago conveniente y ágil gracias a las tarjetas <i>contactless</i>, al incluirle biometría se mantiene la seguridad sin necesidad de un PIN. Esto no solo promueve la confianza, sino que también ahorra tiempo. <i>Barclaycard</i> estima un ahorro mayor a siete segundos por cada compra <i>contactless</i> en vez de usar "Chip & PIN"; y, de 15 segundos, en comparación con el efectivo⁴.</p>
 Ojos	<p>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 la esclerótica (<i>eyeprint</i>). Recientemente, el reconocimiento ocular ha comenzado a abrirse paso en la autenticación biométrica móvil.</p>	<p>Acceso simple a la cuenta bancaria: bancos como Wells Fargo comenzaron a utilizar la biometría <i>eyeprint</i> para la autenticación rápida de sus clientes. A diferencia del iris y la retina, <i>eyeprint</i> no necesita de hardware especializado, sino que con una cámara de al menos un megapixel de resolución es suficiente⁵.</p>
 Cara	<p>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, analizándolas a través de grupos denominados puntos nodales⁶.</p>	<p>Reconocimiento facial en cajeros automáticos: ahora las personas no necesitan tener su tarjeta para sacar plata del cajero automático. Hoy se han habilitado cajeros que al acercarse generan un código legible por un celular y este último ayude a verificar el rostro de la persona dándole acceso a la cuenta. Bancolombia traerá esta tecnología a Colombia a inicios del año 2019⁷.</p>

¹ Goode Intelligence (2015). "Biometrics: An Important Tool for the Customer-first Bank" [en línea], consultado en mayo de 2018, 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>

² Íbid.

³ Goode Intelligence (2015). "Biometrics – The must-have tool for payment security". [en línea], consultado en mayo de 2018, disponible en: <http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-the-must-have-tool-for-payment-security.pdf>

⁴ Barclays (2018). Infographic: How much time can you save using contactless payments? [en línea], consultado en mayo de 2018, disponible en: <https://www.home.barclaycard/insights/contactless/How-much-time-can-you-save-using-contactless-payment.html>

⁵ Fingerprints TM (2017). Biometric Technologies.

⁶ Íbid.



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. Como su implementación es relativamente costo-eficiente, 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 dólares⁸.

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)⁹. Aquellos que defienden esta tecnología aseguran que es muy difícil de falsificar.

Wearables para proteger 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 financieras¹⁰.

Conductuales



La biometría conductual identifica patrones de comportamiento de las personas, incluyendo la forma de escribir y 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, rapidez 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 (posinicio 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)¹¹.

Fuente: Elaboración Asobancaria.

Cada vez con mayor frecuencia las instituciones intensifican el uso de la biometría multimodal, donde varios identificadores biométricos son utilizados en el proceso de verificación. Esto no solo permite abarcar una mayor parte de la población, sino que también ofrece más eficiencia. Por otro lado, su uso simultáneo logra aumentar la resistencia al fraude.

su identidad por medio de lo que saben o tienen (contraseñas o documento de identidad), sino que son reconocidos por lo que son.

Autenticación: desbloqueando el potencial bancario en un mundo hiperconectado

En últimas, la biometría es la única tecnología que asegura la identidad de la persona en un alto grado de confianza. Con ella, las personas no necesitan corroborar

Con la banca electrónica, las instituciones financieras pudieron llegar a nuevos consumidores y realizar negocios transnacionales. Desde entonces, el protagonismo de las

⁷ Andacol (2017). Bancolombia tendrá cajeros con reconocimiento facial a inicios de 2019 [en línea]. Disponible en <https://www.andacol.com/index.php/empresas/2711-bancolombia-tendra-cajeros-con-reconocimiento-facial-a-inicios-de-2019>

⁸ Nuance (2014). "Adiós to PINs, passwords, and security questions" [en línea]. Disponible en https://www.nuance.com/content/dam/nuance/en_au/collateral/enterprise/case-study/cs-banco-santander-mexico-en-us.pdf

⁹ Goode Intelligence (2015). "Biometrics: An Important Tool for the Customer-first Bank" [en línea], consultado en mayo de 2018, 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" [en línea], consultado en mayo de 2018, 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 BioCatch (2017). Invisible Challenges. [en línea], consultado en mayo de 2018, disponible en: [https://www.biocatch.com/hubfs/BioCatch_Invisible_Challenges_%20FINAL-FINAL%20\(23.4.17\).pdf?hsCtaTracking=e91c8dfb-2419-478e-9cce-9355e40d449%7Cdec5cb3f-c6a3-46f4-9b50-c3f3a4fff5f1](https://www.biocatch.com/hubfs/BioCatch_Invisible_Challenges_%20FINAL-FINAL%20(23.4.17).pdf?hsCtaTracking=e91c8dfb-2419-478e-9cce-9355e40d449%7Cdec5cb3f-c6a3-46f4-9b50-c3f3a4fff5f1)

Edición 1138

interacciones digitales ha crecido, en especial con el uso de dispositivos móviles.

Hoy en día los usuarios realizan más de la mitad de sus interacciones bancarias por medio de canales digitales¹² y se estima que, en el transcurso de 2018, el mundo llegará a 2.000 millones de usuarios de banca móvil (alrededor del 40% de la población adulta del mundo)¹³.

De esta manera, en el proceso de digitalización, las instituciones financieras tienen la oportunidad de ser más eficientes a la hora de prestar servicios y ofrecer nuevos productos, debido a una menor dependencia de las sucursales virtuales. Sin embargo, a medida que los usuarios se acostumbran a la tecnología, la industria financiera experimenta nuevos desafíos, algunos de estos asociados a:

- ✓ **Omnicanalidad:** a diferencia de la multicanalidad, donde los clientes pueden realizar diferentes transacciones a través de ciertos canales, la omnicanalidad se refiere a la posibilidad de interactuar de manera fluida y consistente a través de cualquier canal¹⁴. 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-Pesa¹⁵. En Europa, siete de cada ocho compras se hicieron de forma electrónica en el año 2015¹⁶.

- ✓ **Legitimidad de las interacciones:** verificar que el acceso, el intercambio de mensajes, las transacciones y la identidad pertenezcan al usuario genuino 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.

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. En los últimos seis años se han perdido USD 112.000 millones en el mundo por robos de identidad, lo que equivale a una pérdida de USD 35.600 cada minuto¹⁷. Por ello, las medidas de seguridad deben fortalecerse y estar acordes al panorama digital.

Actualmente, los esfuerzos de los bancos y demás instituciones para reducir la fricción, la suplantación y el fraude a través de sus canales se manifiestan en un cambio de actitud frente a los mecanismos de identificación. Al enfocar sus esfuerzos hacia los sistemas biométricos automatizados tienen la oportunidad de enfrentar varios de los retos digitales y aprovechar los beneficios de esta tecnología, tales como trazabilidad, dinamismo y conveniencia.

Hasta ahora, la implementación de los sistemas biométricos no se ha dado en su totalidad debido a los costos en que deben incurrir las entidades bancarias para utilizar estos métodos de verificación y por las preocupaciones que todavía tienen los consumidores sobre la protección de su información. No obstante, los bancos deberían aprovechar su posición como las instituciones más confiables en la protección de los datos biométricos de los usuarios (Gráfico 1), de tal manera que se consoliden como líderes en los servicios de autenticación de identidades y como los facilitadores de medios de pago.

¹² Bain & Company (2014). "Customer Loyalty in Retail Banking: Global Edition" [en línea], consultado en mayo de 2018, disponible en: <http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2014-global.aspx>

¹³ Juniper (2018). "Futureproofing Digital Banking".

¹⁴ IBM (2014). Omnichannel Banking [en línea], consultado en mayo de 2018, disponible en: https://www-935.ibm.com/services/multimedia/Omnichannel_banking.pdf

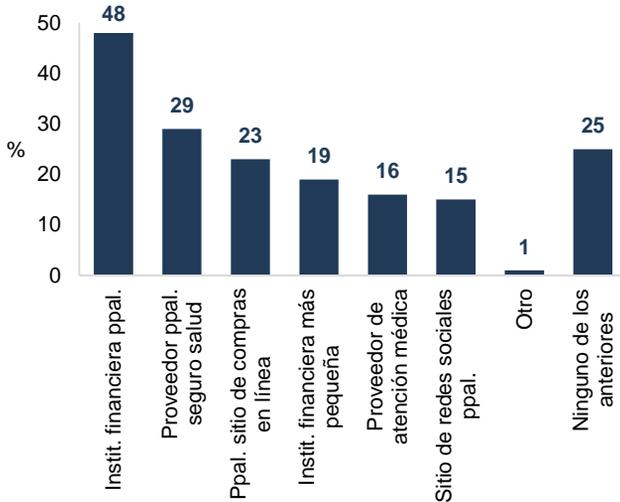
¹⁵ BBC (2017). South Africa's Vodacom to Buy 35% Of Kenya's Safaricom From Parent Vodafone. Disponible en <https://www.forbes.com/sites/tobyshapshak/2017/05/15/south-africas-vodacom-to-buy-35-of-kenyas-safaricom-from-parent-vodafone/#7e3461452a63>

¹⁶ Nilson (2017). Credit card fraud: what you need to know. [en línea], consultado en mayo de 2018, disponible en: https://nilsonreport.com/upload/pdf/Credit_card_fraud_what_you_need_to_know.pdf

¹⁷ IBM (2018). "Future of Identity Study" [en línea], consultado en mayo de 2018, disponible en: <https://www.ibm.com/account/reg/us-en/signup?formid=urx-30345>, IBM Security.

Edición 1138

Gráfico 1. Organizaciones en las que más se confía para proteger información biométrica (perspectiva global)



Fuente: IBM, 2018.

Adicionalmente, es importante reconocer que la entrada de gigantes digitales como *Amazon*, *Apple* y *Alibaba* en el ámbito financiero traerá un nivel de competencia mucho más alto. De acuerdo con 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 diarias¹⁸. Según predicciones de *Goode Intelligence*, para 2020 el papel que tomará la biometría dentro del sistema financiero será de gran importancia (Gráfico 2).

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 creciente, los bancos deben enfocarse principalmente en el relacionamiento con sus clientes y en bajar significativamente sus costos.

Ciberespacio: identidad más allá de las contraseñas

Las maneras como las personas logran corroborar su identidad se pueden 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 (Gráfico 3).

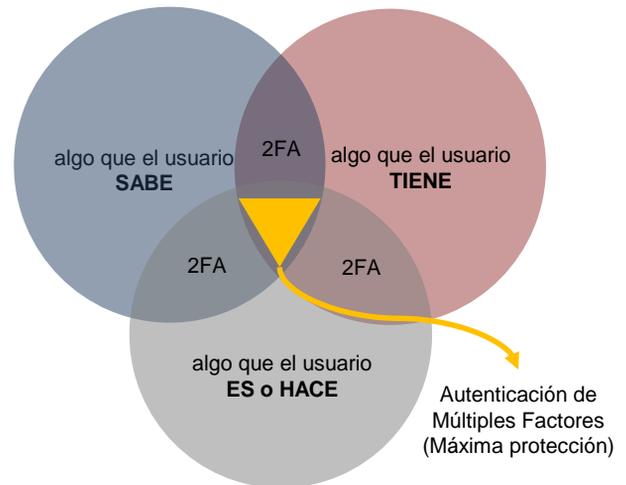
Gráfico 2. La biometría a 2020 en los servicios financieros

La biometría como el método predominante de identificación.



Fuente: Biometrics Research Group. (2016). Biometrics and Banking.

Gráfico 3. Tres factores de autenticación



Nota: 2FA hace referencia al término en inglés *Two-Factor Authentication*.

Fuente: Biometrics Research Group. (2016). Biometrics and Banking.

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, entre otros. Como se

¹⁸Bain & Company (2017). "Evolving the Customer Experience in Banking: 'Alexa, Move My Bank Accounts to ...'", [en línea], consultado en mayo de 2018, disponible en: <http://www.bain.com/publications/articles/evolving-the-customer-experience-in-banking.aspx>

Edición 1138

ha mencionado, 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.

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. En 2004, Bill Gates ya establecía la necesidad de migrar a otros sistemas de autenticación¹⁹. Pero fue en 2013 cuando el mundo empezó a adoptar masivamente los mecanismos de autenticación de 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.

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.

Tal es el caso de Nequi, una empresa que ofrece servicios bancarios móviles, al ser 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 adicional²⁰. Asimismo, a principios de 2017, el Banco Colpatria ya tenía en operación una plataforma multibiométrica en sus oficinas. Esta plataforma, llamada ReconoSer, valida en tiempo real la identidad del

ciudadano logrando mitigar la suplantación o robo de identidad²¹. Otro ejemplo es Redeban MultiColor, entidad que 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 sus rasgos faciales²².

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.

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 con puntajes que describen la probabilidad de coincidencia. De esta manera, se tiene en cuenta qué tan parecidos son los datos biométricos de un usuario con aquellos registrados en una plantilla digital. No obstante, los resultados pueden terminar en falsos positivos, identificando incorrectamente a alguien como el genuino usuario, o en falsos negativos, señalando incorrectamente que el legítimo usuario no es el verdadero.

La biometría funciona mejor si se vincula con un segundo factor de autenticación, como un teléfono celular o una contraseña, entre otros. 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, para aprobar una transacción internacional multimillonaria harían falta métodos complementarios para garantizar su seguridad. Seguramente, el proceso de autenticación que podría ser más pertinente es aquel que incorpore un sistema biométrico multimodal atado a una

¹⁹ Telesign (2016). "Beyond the Password: The Future of Account Security" [en línea], consultado en mayo de 2018, disponible en: <http://info.telesign.com/rs/911-SFQ-678/images/Report-The%20Future%20of%20Account%20Security-EN.pdf>

²⁰ Daon (2016). "Nequi Aims to Build a New Way of Accessing Money" [en línea], consultado en mayo de 2018, disponible en: <https://www.daon.com/newsroom/press-releases/340-nequi-aims-to-build-a-new-way-of-accessing-money>

²¹ Luzardo, A. M. (2017). "solución biométrica colombiana mejora seguridad en bancos" [en línea], consultado en mayo de 2018, disponible en: <http://www.enter.co/especiales/colombia-bringiton/empresa-colombiana-desarrolla-solucion-que-mejora-seguridad-en-bancos/>

²² Dinero (2017). "Adiós al efectivo y tarjetas convencionales gracias a estos novedosos sistemas de pago" [en línea], consultado en mayo de 2018, disponible en: <http://www.dinero.com/empresas/articulo/redeban-multicolor-estrena-sistemas-de-pago-en-colombia/246808>

sucursal bancaria con fuertes protocolos de seguridad.

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 inquietud 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 asegurada 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 de biométrica en el mercado, los usuarios podrán escoger este mecanismo de autenticación con mayor facilidad.

Sin embargo, los usuarios son cada vez más conscientes de que lo normal de los rasgos biométricos es la exposición, a diferencia de las contraseñas, que permanecen secretas. Esto podría facilitar que las personas puedan ser identificadas fácilmente con o sin su permiso. 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, tener garantías de que están bien protegidos. Un estudio de Capgemini²³ encontró que las preocupaciones de seguridad impiden que casi la mitad de los consumidores (47%) usen canales digitales y también concluyó que el 74% 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. 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.

Hay que considerar que ninguna tecnología ha probado ser inquebrantable. 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 se debe 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; 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 su sofisticación, estandarización y confiabilidad.

Avances: Proyecto de autenticación biométrica dactilar liderado por Aso Bancaria

Con el fin de apoyar los procesos de cambio anteriormente descritos, Aso Bancaria junto con la Registraduría Nacional del Estado Civil y Certicámara S.A puso en marcha uno de los proyectos de autenticación biométrica más importante para el sector financiero, una iniciativa que ha permitido la autenticación dactilar de los clientes en toda la red de oficinas y a través de dispositivos móviles, en tiempo real y con los mayores estándares de seguridad.

El proceso de validación biométrica inicia con la captura de las minucias dactilares de los usuarios a través de un captor de huellas que coteja la información contra la base de datos biométricos y biográficos más completa que existe en nuestro país, recopilada por la Registraduría Nacional del Estado Civil y genera una respuesta afirmativa o negativa sobre la identidad de la persona que surte el proceso en cuestión de segundos.

²³ Capgemini Consulting (2017). "The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure" [en línea], consultado en mayo de 2018, disponible en: <https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/>

²⁴ Gemalto (s. f.). "Autenticación de factores múltiples" [en línea], consultado el 20 de marzo de 2018, disponible en: <https://safenet.gemalto.es/multi-factor-authentication/>

Edición 1138

Con menos de dos años desde su lanzamiento, hoy el 60% de las entidades bancarias realizan autenticación biométrica y mensualmente se realizan entre 1,1 y 1,3 millones de validaciones en sus oficinas. El uso de la biometría dactilar ha cambiado y mejorado la experiencia de los clientes en cuanto el tiempo de una transacción pasa de minutos a segundos. Para las entidades financieras la biometría dactilar ha permitido avanzar en la mitigación del riesgo de suplantación, en la ejecución de las políticas de “cero papel” y se ha convertido en la punta de lanza de los procesos de transformación digital de los servicios financieros.

Esta iniciativa ha sido nominada por la Asociación Latinoamericana de Seguridad (ALAS) como uno de los proyectos de seguridad más importantes e innovadores de la región y un referente a nivel regional en materia de seguridad en el sector bancario. En la actualidad, se busca hacer uso de la biometría facial como complemento de la biometría dactilar manteniendo los mismos niveles de seguridad y eficiencia para el usuario financiero.

Conclusiones y consideraciones finales

En un horizonte de tiempo cercano, la autenticación de múltiples factores, siempre y cuando involucre la biometría, será el método más robusto para acceder a distintos servicios²⁴. Sin embargo, es importante desarrollar mecanismos de seguridad complementarios en la red para seguir avanzando en la protección de la identidad de todos los usuarios.

Una de las iniciativas más importantes y de mayor impacto en el uso de la biometría en el acceso a servicios financieros liderada por Asobancaria en conjunto con la Registraduría Nacional del Estado Civil permite la autenticación por medio de la huella dactilar de los clientes en toda la red de oficinas y a través de dispositivos móviles, en tiempo real y con los mayores estándares de seguridad. Por sus resultados se ha constituido como un referente regional en materia de seguridad y eficiencia.

El sector financiero tiene la gran oportunidad de ser líder en el almacenamiento de la información debido a sus niveles de seguridad y adaptación constante frente a nuevas amenazas. La gente y los gobiernos confían en él para guardar su dinero y, más importante aún, para guardar su información sensible.

Para seguir construyendo su reputación en privacidad

de datos y seguridad robusta, deben 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 y desarrollar las capacidades necesarias para monitorear y adaptarse a los riesgos cibernéticos en tiempo real.

Así, abordar aspectos como la privacidad y seguridad digital les ofrece a los bancos una ventaja estratégica que promueve la adopción de canales digitales de menor costo operacional y, al tiempo, atrae a nuevos clientes. Desarrollar el enorme potencial en materia de seguridad y confiabilidad con estas herramientas es y seguirá siendo un imperativo para la banca y el sistema financiero.

Edición 1137

Colombia Principales Indicadores Macroeconómicos

	2015					2016					2017					2018*	
	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Producto Interno Bruto**																	
PIB Nominal (COP Billones)	804,7	199,6	211,0	213,7	239,6	863,9	213,4	224,7	232,4	257,5	928,1	228,5	232,4	257,5	928,1	228,5	985,6
PIB Nominal (USD Billones)	255,5	63,8	70,4	73,1	79,6	287,0	72,6	74,0	79,1	86,3	311,0	82,2	86,3	91,1	311,0	82,2	344,6
PIB Real (COP Billones)	804,7	192,8	201,1	203,1	223,5	820,5	195,3	204,4	208,1	227,4	835,2	199,6	208,1	227,4	835,2	199,6	856,9
PIB Real (% Var. interanual)	3,1	2,5	2,4	1,5	1,8	2,0	1,5	1,7	2,3	1,6	1,8	2,2	2,3	1,6	1,8	2,2	2,6
Precios																	
Inflación (IPC, % Var. interanual)	6,8	8,0	8,6	7,3	5,7	5,7	4,7	4,0	4,0	4,1	4,1	3,1	4,0	4,1	4,1	3,1	3,1
Inflación sin alimentos (% Var. interanual)	5,2	6,2	6,3	5,9	5,1	5,1	5,1	5,1	4,7	5,0	5,0	4,1	5,0	5,0	5,0	4,1	3,5
Tipo de cambio (COP/USD fin de periodo)	3149	3129	2995	2924	3010	3010	2941	3038	2937	2984	2984	2780	2984	2984	2984	2780	2860
Tipo de cambio (Var. % interanual)	31,6	21,5	15,8	-6,3	-4,4	-4,4	-6,0	1,5	0,4	-0,9	-0,9	-5,5	-0,9	-0,9	-0,9	-5,5	-4,2
Sector Externo (% del PIB)																	
Cuenta corriente	-7,4	-5,1	-3,8	-4,8	-3,4	-4,3	-4,1	-3,6	-3,3	-2,4	-3,4	...	-3,6	-3,3	-3,4	...	-3,0
Cuenta corriente (USD Billones)	-18,7	-3,6	-2,8	-3,6	-2,6	-12,5	-3,2	-2,7	-2,6	-1,9	-10,4	...	-2,7	-2,6	-10,4	...	-11,4
Balanza comercial	-7,3	-5,4	-3,9	-4,7	-4,2	-4,6	-3,4	-3,9	-3,1	-1,9	-3,1	...	-3,9	-3,1	-3,1	...	-3,2
Exportaciones F.O.B.	17,9	12,9	13,9	14,0	14,9	13,9	14,0	14,8	15,3	16,6	15,2	...	15,3	16,6	15,2
Importaciones F.O.B.	25,1	18,4	17,8	18,7	19,1	18,5	17,5	18,7	18,6	18,4	18,3	...	18,6	18,4	18,3
Renta de los factores	-2,2	-1,6	-1,8	-1,9	-1,4	-1,7	-2,5	-1,9	-2,3	-2,9	-2,4	...	-2,3	-2,9	-2,4	...	-2,3
Transferencias corrientes	2,1	1,9	1,9	1,8	2,2	1,9	1,8	2,2	2,2	2,4	2,1	...	2,2	2,4	2,1	...	1,8
Inversión extranjera directa	4,6	6,8	5,0	2,9	4,1	4,7	3,3	3,6	6,3	4,9	4,5	...	3,6	4,9	4,5
Sector Público (acumulado, % del PIB)																	
Bal. primario del Gobierno Central	-0,5	-0,2	0,3	0,1	-1,1	-1,1	-0,7	0,0	0,6	-0,8	-0,8	...	0,6	-0,8	-0,8	...	0,4
Bal. del Gobierno Central	-3,0	-0,9	-1,0	-2,6	-4,0	-4,0	-1,2	-1,4	-2,0	-3,6	-3,6	...	-1,4	-3,6	-3,6	...	-3,1
Bal. estructural del Gobierno Central	-2,2	-2,2	-2,0	-2,0	...	-1,9
Bal. primario del SPNF	-0,6	1,0	2,1	1,8	0,9	0,9	-0,1	1,2	0,0	...	1,2	...	0,0	...	0,5
Bal. del SPNF	-3,4	0,6	0,5	-0,1	-2,3	-2,4	-0,8	-0,1	-3,2	...	-0,1	...	-3,2	...	-2,7
Indicadores de Deuda (% del PIB)																	
Deuda externa bruta*	37,9	40,4	41,2	41,1	42,5	42,5	39,0	39,1	40,2	40,2	40,2	...	40,2	40,2	40,2
Pública	22,7	24,2	24,8	24,8	25,2	25,2	23,3	22,8	23,4	23,2	23,2	...	23,4	23,2	23,2
Privada	15,2	16,2	16,3	16,3	17,2	17,2	15,7	16,2	16,8	17,0	17,0	...	16,8	17,0	17,0
Deuda bruta del Gobierno Central	45,1	43,2	44,0	44,6	46,1	46,0	44,3	44,9	46,4	47,4	45,8	...	44,9	47,4	45,8

* Proyecciones para el cierre de 2018. ** Series originales del DANE, base 2015.

Fuente: PIB y Crecimiento Real – DANE, proyecciones Asobancaria. Sector Externo – Banco de la República, proyecciones MHCP y Asobancaria. Sector Público – MHCP. Indicadores de deuda – Banco de la República, Departamento Nacional de Planeación y MHCP.

Edición 1137

Colombia Estados Financieros*

	feb-18 (a)	ene-18	feb-17 (b)	Variación real anual entre (a) y (b)
Activo	580.720	579.011	553.737	1,5%
Disponible	40.699	37.494	37.013	6,4%
Inversiones y operaciones con derivados	116.850	107.005	99.309	13,8%
Cartera de crédito	419.656	416.734	396.435	2,4%
Consumo	116.541	116.043	107.320	5,0%
Comercial	235.699	233.605	227.623	0,2%
Vivienda	55.521	55.257	50.418	6,5%
Microcrédito	11.896	11.829	11.074	3,9%
Provisiones	24.731	24.395	19.558	22,3%
Consumo	9.093	9.007	7.279	20,8%
Comercial	12.850	12.629	9.867	26,0%
Vivienda	1.913	1.893	1.602	15,5%
Microcrédito	863	854	797	4,7%
Pasivo	503.814	502.657	480.341	1,5%
Instrumentos financieros a costo amortizado	442.531	441.714	420.424	1,8%
Cuentas de ahorro	165.953	166.445	157.802	1,7%
CDT	150.513	144.308	141.571	2,8%
Cuentas Corrientes	52.203	53.145	49.511	2,0%
Otros pasivos	3.794	3.201	2.604	40,9%
Patrimonio	76.906	76.354	73.396	1,4%
Ganancia / Pérdida del ejercicio (Acumulada)	1.142	529	1.342	-17,7%
Ingresos financieros de cartera	7.552	3.656	7.413	-1,4%
Gastos por intereses	2.784	1.354	3.302	-18,4%
Margen neto de Intereses	4.951	2.354	4.339	10,4%
Indicadores				Variación (a) - (b)
Indicador de calidad de cartera	4,76	4,52	3,72	1,03
Consumo	6,04	5,92	5,25	0,79
Comercial	4,33	3,99	3,11	1,23
Vivienda	3,14	3,12	2,40	0,74
Microcrédito	8,07	8,04	7,69	0,38
Cubrimiento**	123,9	129,4	132,5	8,56
Consumo	129,2	131,1	129,2	-0,03
Comercial	125,8	135,6	139,5	-13,76
Vivienda	109,7	109,9	132,6	-22,87
Microcrédito	89,8	89,8	93,6	-3,75
ROA	1,19%	1,10%	1,46%	-0,3
ROE	9,25%	8,63%	11,49%	-2,2
Solvencia	15,40%	15,55%	15,11%	0,3

* Cifras en miles de millones de pesos.

** No se incluyen otras provisiones.