WHITE PAPER

El futuro de la identidad

Demostrar quiénes somos en el mundo físico y en el digital

Steve Ritter, Director de Tecnología (CTO), Mitek

«¿Quién eres?» siempre ha sido una pregunta de vital importancia tanto en el ámbito empresarial como en el social. Pero la respuesta nunca había implicado algo tan trascendental como lo que actualmente supone para el posible futuro y el día a día de tantas personas y empresas.

Hoy en día, nuestra capacidad para demostrar quiénes somos en el mundo físico y en el digital es un factor fundamental para explicar el nivel de acceso que tenemos a la gran cantidad de información y servicios móviles y online, siempre en constante expansión. En nuestros negocios, la manera en la que solicitamos y verificamos la acreditación de identidad de nuestros consumidores y de los consumidores potenciales es un factor fundamental que determina el éxito que alcanzaremos.

Estamos en un momento crucial. En los próximos años la identidad será muy diferente a lo que ha sido durante siglos, tanto a nivel conceptual como práctico.

¿Qué está cambiando? ¿Es para mejor? ¿O para peor? En este documento compartimos nuestro punto de vista sobre el estado actual de la identidad y la manera en la que podemos dirigirnos hacia un futuro de la identidad con muchas más ventajas para todos.

Mitek

La identidad en un mundo «en el que todo el mundo sabe cómo te llamas» y nadie puede guardar un secreto

Durante siglos, el concepto de identidad ha estado fuertemente arraigado en el mundo físico, sobre todo por el importante papel que jugaba en las transacciones locales.

No cabe duda de que el concepto ha evolucionado mucho desde la época en que la identidad de una persona dependía de si era miembro de un grupo nómada de cazadores-recolectores o si era el hijo o la hija de alguien. A medida que la sociedad ha ido avanzando, el concepto de la identidad se ha ampliado hasta incluir nociones como la residencia o la ciudadanía en un pueblo, una ciudad o una nación.

Sin embargo, durante todo ese período de tiempo y hasta hace muy poco, la ratificación y validación de la identidad se llevaba a cabo principalmente mediante interacciones en persona. El dueño del bar o de la tienda del barrio fiaba al cliente porque lo conocía de vista. Uno acudía a las oficinas de la Administración pública para que le expidieran el pasaporte o el permiso de conducir. Para abrir una cuenta o pedir un préstamo, la mayoría íbamos al banco a hablar con el director de la sucursal.

Todo esto ha cambiado, claro está, porque gracias a internet podemos adquirir bienes o servicios e interactuar con gente en todo el mundo. Para algunas de estas transacciones e interacciones, necesitamos crear una cuenta y aportar algún tipo de acreditación que confirme quiénes somos.

«A veces quieres ir a donde todo el mundo sabe tu nombre».

Al escuchar la canción de la serie ochentera *Cheers* nos invade la nostalgia recordando su famoso bar de barrio y aquella época en la que los vecindarios eran nuestra esfera de interacción principal. En la actualidad las conexiones digitales expanden esa esfera por todo el mundo. Aunque estén a miles de kilómetros, las personas y las organizaciones se dirigen a nosotros por nuestro nombre, ¿pero cómo saben quiénes somos?

Al comienzo de la conectividad global, los métodos basados en el conocimiento que dependían de secretos, como las contraseñas y los grupos de pregunta-respuesta, funcionaban bastante bien para verificar la identidad. Sin embargo, debido a la piratería, al tratamiento de grandes volúmenes de datos y a las herramientas de inteligencia artificial que actualmente están al alcance tanto de estafadores que actúan por su cuenta como de redes criminales organizadas, los almacenes «seguros» de información personal de identificación (PII, por sus siglas en inglés) sufren ataques y filtraciones constantemente. Ya no existen los secretos.

Y esto tiene implicaciones trascendentales para los consumidores, las empresas y los gobiernos. Analicemos el estado de la identidad en el mundo conectado de hoy día.

CÓMO ERA ANTES

CÓMO ES AHORA

Los mejores y los peores momentos

A Charles Dickens, novelista del siglo XIX, le gustaba observar la sociedad en etapas de cambios tumultuosos. Si ahora estuviera aquí, se decantaría por escribir tragicomedias sobre el robo, el mal uso o la confusión de las identidades. Aun así, las historias de Dickens solían tener un lado bueno, con personajes que iban siempre más allá de los límites de su vida en busca de fortuna y mejores oportunidades. El mundo conectado en el que vivimos hoy podría compararse con una caja en la que se mezclan los «mejores momentos» con los «peores momentos».

En realidad, el lado bueno es extraordinario tanto para los consumidores como para las empresas. Tal como dijo Chris Skinner, consultor y comentarista de servicios financieros globales, en su libro *Digital Human* (2018):

«Esta digitalización del planeta está provocando una gran transformación. Cualquier persona del mundo formará parte de la red y tendrá la oportunidad de hablar, intercambiar y negociar en tiempo real con cualquier otra persona del mundo, esté donde esté. A diferencia de la Revolución Industrial, en la que solo un número limitado de personas tenía acceso a la riqueza y a los negocios, esta revolución digital brindará una oportunidad a todo el mundo».

Sin embargo, los consumidores y las empresas ahora se enfrentan a muchos más riesgos de los que tenían antes, dado que el método tradicional de verificación de la identidad en persona ya no es práctico y el método basado en el conocimiento, relativamente reciente, ya no es fiable.

No se trata simplemente de que los hackers tienen acceso a nuestra información de identificación personal...

Actualmente, los consumidores y las empresas también se enfrentan a nuevos riesgos porque muchas de las organizaciones con las que hacen transacciones online no usan métodos fiables para verificar la identidad del usuario.

Por si quedaban dudas al respecto, en mayo de 2019 la Oficina Pública de Contabilidad de los Estados Unidos (GAO, por sus siglas en inglés) emitió un informe en el que señalaba su preocupación ante el hecho de que seis agencias federales todavía se basaban en la información que contenían los archivos de varias agencias de informes de crédito del consumidor para llevar a cabo de forma remota la verificación de la identidad basada en el conocimiento. El informe instaba a un cambio urgente tras considerar que cada vez era mayor el riesgo de que un atacante pudiera obtener y utilizar la PII de una persona para responder preguntas de verificación, tal como sucedió en 2017 con la filtración masiva de datos en Equifax.

Dado que la transición hacia las transacciones digitales va cogiendo cada día más velocidad, las empresas deben adoptar urgentemente nuevas estrategias de verificación de la identidad, propias de un mundo sin secretos. En el sector de los servicios financieros, por ejemplo, el porcentaje de productos bancarios a los que pueden acceder los consumidores a través de canales digitales ha incrementado del 43 % al 76 % en los últimos dos años, y un 90 % de esos productos permite el acceso desde dispositivos móviles.

Sin embargo, mientras que los consumidores parecen cada vez más dispuestos a confiar en los proveedores de servicios y productos digitales, cabe preguntarnos lo siguiente: ¿esa confianza está plenamente justificada?

«La GAO recomienda a seis agencias que refuercen sus procesos de verificación de la identidad digital...

«...hasta que estas agencias no tomen medidas para acabar con el uso de la verificación basada en el conocimiento, las personas a las que atienden seguirán estando en riesgo de sufrir un fraude de identidad».

Oficina Pública de Contabilidad de los Estados Unidos
GAO-19-288, mayo de 2019

[1] 2019 State of Digital Sales in Banking (Estado de las ventas digitales en la banca 2019), FinTech Futures, abril de 2019

«La identidad es la base de la confianza».

Filip Verley,
Identity Innovator

Y la confianza es la base de:

los servicios financieros globales, como la banca móvil, los pagos y transferencias de dinero de autoservicio, y los cambios de moneda virtuales;

los mercados online;

las plataformas de intercambio y servicios entre iguales;

el sector del transporte, del turismo y de la hostelería;

las criptomonedas;

el almacenamiento y la gestión de datos basados en la nube;

simplemente, cualquier nuevo negocio digital que puedas imaginar.

Apuesta por el lado positivo: lo que ahora funciona

Para darnos cuenta realmente de lo positivo de vivir en un mundo conectado, tenemos que ser capaces de confiar. ¿Las organizaciones con las que interactuamos digitalmente como consumidores se merecen nuestra confianza? ¿Nuestros consumidores pueden confiar en nosotros? No tanto como nos gustaría creer.

Tal como sucedía con las agencias gubernamentales cuyos arriesgados métodos de verificación de la identidad fueron señalados por la GAO, algunas empresas todavía confían en la autenticación basada en el conocimiento. En el sector de los servicios financieros, las empresas que usan estos métodos tan arcaicos se arriesgan a incumplir las normativas de conocimiento de la clientela (know your customer, KYC) y de prevención del blanqueo de capitales (anti-money-laundering, AML). Si bien es cierto que quizás otros sectores no estén sujetos a un control normativo tan estricto, las organizaciones que simplemente se fían de la palabra del usuario para confirmar su identidad, sin tomar las medidas de seguridad necesarias ni requerir la confirmación de terceros (que probablemente también utilicen un método de verificación ineficaz) participan en un negocio arriesgado.

Evidentemente, la precisión que se necesita para la verificación de la identidad varía según el contexto. Está claro que queremos que las organizaciones tengan especial cuidado cuando tratan nuestra información confidencial o nuestros asuntos económicos, laborales, sanitarios o legales. Pero seguramente nos importa menos cuando se trata de alquilar un coche o reservar una habitación para las vacaciones.

Aun así, cada vez está más extendida la idea de que el proceso de registro para cualquier servicio o para la compra de un producto debe ser seguro, rápido y fácil. Incluso algunos prestamistas para empresas prometen actualmente una decisión «en menos de tres minutos».

Los proveedores digitales se ven constantemente en la tesitura de tener que encontrar el punto intermedio entre la necesidad de ofrecer rapidez y comodidad y la obligación de minimizar el riesgo. Según la experiencia de Mitek en el trabajo a escala global con miles de empresas de sectores muy diversos, las organizaciones que realmente consiguen ese equilibrio siguen unos principios similares.

«El proceso de verificación de la identidad concierne a casi todos los sectores, por lo que la identidad se convierte en un elemento esencial en cada transacción».

Foro Económico Mundial, enero de 2018

«En 2022, las empresas digitales cuyos consumidores tengan un nivel de satisfacción muy alto durante la corroboración de la identidad obtendrán un 20 % más de ingresos en comparación con aquellas empresas que tengan un nivel de satisfacción deficiente».

Don't Treat Your Customers Like a Criminal, Gartner, abril de 2017

Muchos de los proveedores digitales que consiguen satisfacer las expectativas de sus consumidores en lo que respecta a la velocidad, la comodidad y la seguridad, tienen varias características en común. Entre ellas, se incluyen:

1. Hacer hincapié en los dos puntos fuertes de la tríada de verificación

Tradicionalmente, los procesos de identificación de la identidad (IDV, pos sus siglas en inglés) siempre han buscado indicios combinando «algo que tienes», «algo que sabes» y «algo que eres». De hecho, las contraseñas basadas en «algo que sabes» y los grupos de pregunta-respuesta se convirtieron en los métodos predominantes porque eran los más fáciles de implementar con los consumidores. Sin embargo, como en la actualidad es imposible mantener esta información en la más estricta confidencialidad, se ha hecho más hincapié en los otros dos puntos de la tríada de verificación.

Algo que tienes

Algo que muchísima gente tiene (se estima que el 79 % de la población mundial) es un documento de identidad expedido por el gobierno, como por ejemplo, el permiso de conducir o el pasaporte. Con la tecnología IDV actual, podemos utilizar este método predominante de acreditación de la identidad en el mundo físico para crear una identidad fiable. Los consumidores simplemente utilizan otro objeto que la mayoría de ellos tiene, es decir, el teléfono móvil, para hacer y enviar una foto de su documento de identidad que se analiza mediante software para determinar si es auténtica.

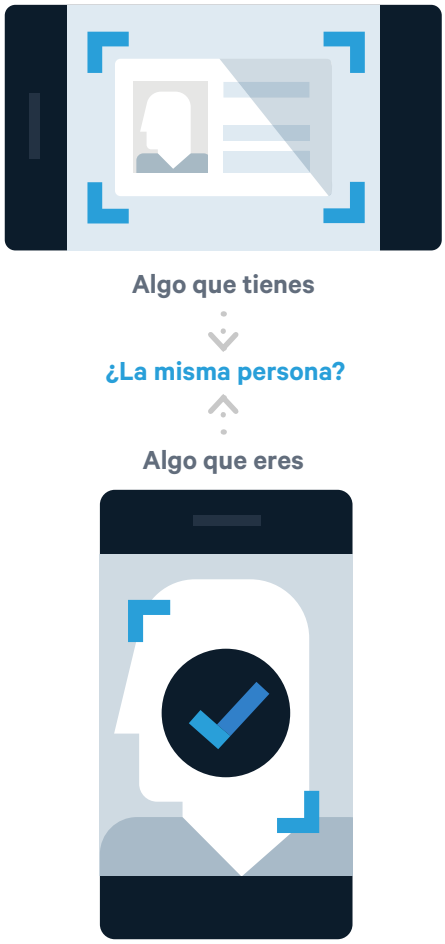
Algo que eres

Si los consumidores envían también un selfie, la tecnología IDV es capaz de compararlo con la imagen del documento de identidad para ver si se corresponden. De esta manera, se verifica si la persona del selfie es el propietario legítimo del documento de identidad. Esta comparación se basa en el reconocimiento facial, una forma de biometría física que compara pequeñas mediciones de la geometría facial para identificar la combinación de características que distinguen a un individuo concreto.

Se están incorporando de manera generalizada otras formas de biometría física (principalmente el reconocimiento de la huella dactilar, pero también el del iris y de la voz) en los dispositivos móviles. A menudo se combinan con una contraseña sencilla para que el usuario final acceda al dispositivo y a las aplicaciones instaladas. Pero el reconocimiento biométrico realmente no certifica que la persona que configura el perfil biométrico sea quien dice ser. Por esta razón, se necesita añadir un paso más, como por ejemplo, la asociación de un documento de identidad emitido por el gobierno al escáner biométrico inicial.

Aunque la biometría física es popular porque mejora la seguridad y reduce la fricción para el usuario final, también es motivo de preocupación por razones de privacidad y puede volverse menos segura a medida que evolucione la tecnología. A los hackers y las redes criminales les atraen los grandes sobornos, y cuanto más se extienda el uso de la biometría, mayor será el botín que puedan conseguir con la piratería. Algunos investigadores ya han demostrado que, aunque requiera de gran habilidad y esfuerzo, la biometría basada en la huella dactilar, el iris y la voz no es invulnerable y puede verse comprometida.

Las herramientas de inteligencia artificial, fácilmente accesibles, permitirán reducir aún más los obstáculos. Por ejemplo, un investigador de la Universidad de Nueva York[2], utilizó hace poco el aprendizaje automático para crear una huella dactilar que funcionara como una especie de "llave maestra", con la que pudo acceder a diferentes dispositivos móviles e incluso a sistemas de seguridad del hogar.



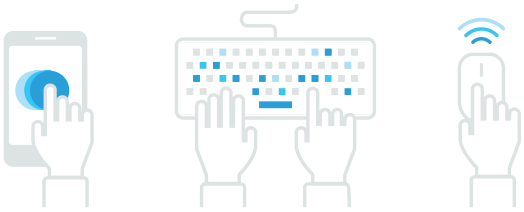
[2] Machine Learning Masters the Fingerprint to Fool Biometric System, NYU Tandon School of Engineering, noviembre de 2018

Todavía no se ha producido ninguna filtración de datos biométricos almacenados, pero si esto sucediera, las consecuencias serían (o serán, cuando suceda) mucho peores que con anteriores filtraciones de PII. Si bien a los consumidores se les notifica periódicamente si su información está en peligro y se les advierte de que deben cambiar las contraseñas, las características físicas no se pueden modificar.

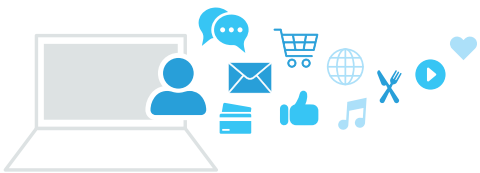
La filtración de datos biométricos podría ponernos en riesgo de maneras tan impredecibles e insólitas que podríamos vernos afectados de por vida. Por lo tanto, las organizaciones que no logran proteger su información biométrica están expuestas a un enorme riesgo legal.

El análisis conductual es otra forma de tecnología biométrica y, aunque ofrece una seguridad potencialmente mayor que las medidas de biometría física, también es motivo de preocupación por razones de privacidad. El análisis conductual nos identifica a través de patrones basados en la manera en que nos movemos en nuestros dispositivos digitales (por ejemplo, presionar teclas, deslizar el dedo, desplazarse, escribir o mover el cursor) o lo que hacemos (como visitar algunas páginas web de forma habitual o hacer periódicamente ciertas transacciones online). En su mayoría, tanto los sensores de los teléfonos como el código de los sitios web recogen toda esta información sin que lo sepamos. Esto es algo positivo, ya que es un método de IDV completamente pasivo y discreto, es decir, no implica ninguna fricción para el usuario final. La parte menos positiva, quizás, es que no sabemos qué dicen de nosotros los perfiles de biometría conductual o cualquier otro tipo de información, ni tampoco para qué otros propósitos se utilizan además de para la IDV.

La biometría conductual te identifica por:



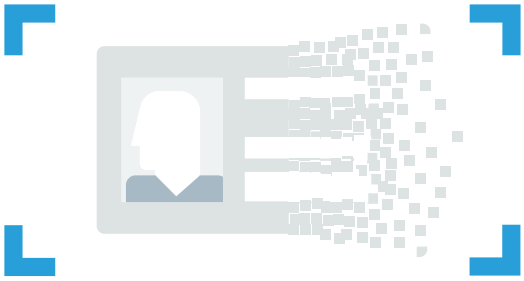
Tus gestos característicos en Internet



Tus lugares y actividades habituales en Internet

Los bots de IA buscan errores en el doc. de identidad

O para reconstruir instantáneamente una identidad digital a partir de fragmentos de datos de un origen activo



2. Movilizar un ejército de bots de inteligencia artificial en un instante

Para satisfacer las expectativas del consumidor en cuanto a seguridad, comodidad y velocidad, los proveedores digitales prefieren las soluciones de IDV que incorporan IA. Es la única manera de llevar a cabo en un instante tareas de verificación complejas, de manera masiva e invisible, en segundo plano.

Por ejemplo, la confirmación de que la fotografía que se ha tomado del documento de identidad expedido por el gobierno es realmente una imagen de un documento legítimo, original e inalterado implica una gran cantidad de comprobaciones, comparaciones y medidas pequeñas y detalladas. Mobile Verify® de Mitek lo hace en pocos segundos, liberando cientos de bots de IA que se propagan por la imagen, cada uno ejecutando una tarea distinta. Los algoritmos de visión artificial comprueban el retrato del documento de identidad para verificar que es una cara humana, además de examinar la calidad de la imagen (que sea muy alta o muy baja puede ser algo significativo) y buscar sombras sospechosas que puedan indicar que se trata de una fotocopia o una imagen alterada digitalmente. Los algoritmos de aprendizaje automático examinan la consistencia y el uso de las fuentes. Los algoritmos de aprendizaje profundo buscan problemas casi imperceptibles, como irregularidades leves en o entre algunas letras. Después, en otra fase adicional del aprendizaje automático se recogen los resultados de este ejército de bots de IA, se determina cuánto peso (importancia relativa) se otorga a cada una de las pruebas y se responde a las siguientes preguntas: ¿es genuina esta identidad? ¿pertenece al solicitante?

La biométrica conductual entraña unos niveles de complejidad similares. Por ejemplo, un socio de Mitek recoge continuamente las huellas digitales que deja la actividad online de una persona y utiliza bots de IA para reconstituir esos fragmentos de información obtenidos de un origen activo y recomponer una visión holística y actual de la identidad de esa persona.

Los métodos que utiliza Mitek y su socio analizan la información tanto en el mundo digital como en el físico, y tienen en cuenta que ambos son imperfectos y están siempre en constante cambio. Utilizar la IA para combinar multitud de tipos diferentes de prueba permite realizar ajustes matizados en lo que está (o no) disponible, o lo que está más o menos claro, en cada caso. Además, los bots de IA aprenden a medida que ven nuevas tendencias conductuales y nuevas técnicas de falsificación de documentos. Se pueden añadir también bots adicionales para que ejecuten nuevas tareas, incrementando así la concentración de inteligencia que trabaja en segundo plano de forma imperceptible mientras se lleva a cabo la verificación de la identidad.

3. Abarcar toda la diversidad mundial

Actualmente, la verificación de la identidad debe tener un alcance global. No solo nuestras esferas de interacción crecen, sino que también una parte cada vez más extensa de las transacciones llevadas a cabo por empresas y consumidores se está trasladando a mercados y plataformas globales que admiten envíos, pagos y operaciones de gestión de contratos, seguros y finanzas transfronterizos.

Por supuesto, el problema reside en que actualmente no hay ninguna normativa internacional que regule los documentos de identidad, ni físicos ni digitales (en la siguiente sección se analiza con más detalle este tema). Hasta que esto no suceda, los proveedores de soluciones IDV cuyo alcance sea global son fundamentales en la verificación de la identidad transfronteriza.

Por ejemplo, para confirmar que el permiso de conducir que has fotografiado y enviado desde tu teléfono es un documento legítimo expedido por el gobierno, Mobile Verify® de Mitek compara la fotografía con miles de plantillas de documentos de todo el mundo que se encuentran almacenadas en su repositorio. A continuación, compara con la plantilla tanto la estructura general como los pequeños detalles de la imagen fotografiada, para asegurarse de que las distintas secciones (la información biográfica, el área de la firma, la parte de la imagen, la zona legible automáticamente (MRZ) o el código de barras) están exactamente donde tendrían que estar. Al extraer la información de estos elementos, el software también comprueba que la información del documento de identidad tenga una consistencia interna; por ejemplo, verifica si la información cifrada en la zona MRZ y en el código de barras concuerdan con la información biográfica.

4. Combinar métodos de forma flexible e innovadora

Dado que los mundos físico y digital son imperfectos a la par que cambiantes, es necesario implementar de manera flexible una IDV de múltiples factores que se adapte a diferentes situaciones.

Por ejemplo, para diseñar la secuencia de pasos de manera específica, es posible que quieras utilizar un método de verificación gradual, que reduce el índice de abandono en el proceso de incorporación del cliente. De manera similar, un proceso en cascada debería seguir tus reglas de escalamiento para desencadenar peticiones automatizadas de información adicional o ejecutar procesos de enrutamiento a un experto en verificación.

También desearás tener flexibilidad para adaptar lo que sucede con cada componente de tu proceso de IDV. Por ejemplo, puede que en determinados casos estés dispuesto a aceptar fotografías en blanco y negro del documento de identidad, mientras que, en otros casos, es posible que prefieras analizar el color para poder evaluar la fidelidad del documento. En determinados usos, quizás solo importa la información que aparece en el reverso del documento de identidad, pero en otros usos es fundamental comparar el reverso y el anverso del documento. La IDV debería permitirte enfatizar y señalar componentes específicos del proceso según sea necesario.

Además, la IDV debe tener en cuenta las diferencias culturales que se dan en los distintos mercados globales. Un buen ejemplo al respecto: MoneyGram ha descubierto que, en algunas partes del mundo, a muchos consumidores les encanta empezar el proceso de incorporación fotografiando su documento de identidad físico. Al ahorrarles tener que utilizar el teclado, ven el proceso como una forma de ahorrar tiempo, ya que el formulario de solicitud online rellena automáticamente los datos extraídos de la imagen escaneada. Sin embargo, en otras partes del mundo, los consumidores prefieren empezar el proceso de incorporación mediante un código de verificación que reciben por SMS. MoneyGram utiliza las instantáneas del documento de identidad para reforzar la comprobación al final

del proceso. A muchos de los consumidores a los que se les solicita una foto de su documento de identidad les gusta la idea de que se tomen medidas adicionales para protegerlos.

«Al ser pioneros en la IDV, creo que podemos coger un proceso lleno de fricción y "darle la vuelta" para que, en lugar de un obstáculo, esta experiencia sea agradable para el consumidor».

Nash Ali, Jefe de Riesgos y Pagos, MoneyGram International

Hacia un futuro de la identidad mejor: ¿qué debe cambiar?

Las soluciones que funcionan hoy para la verificación de la identidad no tienen por qué ser suficientes en el futuro. En 2020, la mitad de la población del mundo tendrá acceso a Internet, mientras que la otra mitad lo hará para 2025.[3] Cada una de estas personas se verá afectada por problemas complejos derivados de la identidad digital.

Tal y como ha señalado el Foro Económico Mundial (FEC): «Nuestras identidades digitales tienen una implicación cada vez mayor en todo lo que hacemos en nuestro día a día... Si ampliamos el ámbito de actuación, las identidades digitales en la actualidad pueden ayudar a transformar el futuro de millones de personas en todo el mundo, permitiéndoles que accedan a nuevas oportunidades económicas, políticas y sociales, a la vez tienen garantizada la privacidad y seguridad digital, así como otros derechos humanos».[4]

¿Cómo llegamos a ese futuro? ¿Cómo llegamos al futuro de la identidad que deseamos la mayoría? Esta es la opinión de Mitek acerca de lo que nos depara el futuro:

Todo el mundo tendrá una identidad digital que le proporcionará un nivel de seguridad alto.

Hay dos grandes grupos de problemas que se deben resolver antes de que todo el mundo disponga de una identidad digital con un nivel de seguridad alto.

El primer grupo gira en torno a la privación de los derechos humanos y se centra en las economías de bajos o medianos ingresos de los países en vías de desarrollo, donde se estima que alrededor de mil millones de personas no disponen de ninguna acreditación formal, ni digital ni física, de su identidad. Históricamente, muchos países no han contado con los medios necesarios para registrar los nacimientos o identificar unívocamente a las personas que viven dentro de sus fronteras. Existen distintas iniciativas globales, como la Identidad para el Desarrollo (ID4D) del Banco Mundial, que pretenden cambiar esta situación, y no cabe duda que la tecnología les será de gran ayuda. De manera similar a cómo los teléfonos móviles hacen posible que las regiones sin líneas de teléfono puedan dar un salto hacia la edad moderna, los smartphones asequibles, el procesamiento de imágenes y la biometría deberían permitirles superar la falta de sistemas de distribución física de credenciales y acceder directamente a los documentos de identidad digitales.

El segundo grupo se centra en la fiabilidad, un gran reto incluso para las economías más avanzadas. Se incluyen en este grupo aquellas economías con programas universales del gobierno para la tramitación del documento de identidad digital (como Estonia) y aquellas que han dejado el asunto en manos del sector privado (como Estados Unidos). En ambos extremos de este espectro, y en todos los demás puntos que hay entremedio, se plantean ciertas cuestiones sobre si los consumidores, las empresas y los organismos gubernamentales pueden confiar en la seguridad de los procesos que se utilizan para expedir, almacenar y verificar los documentos de identidad digitales.

Incluso la Smart-ID de Estonia fue vulnerada por medio de ataques de suplantación de identidad en 2019. Esta app comercial, que irrumpió en 2014 tras el descubrimiento de las vulnerabilidades que presentaba el chip incorporado al documento nacional de identidad del país, está teniendo una gran acogida en los países bálticos. Mientras tanto, otras iniciativas nacionales, tales como el proyecto Aadhaar de India, suscitan motivos de preocupación, ya que se fundamentan en una base de datos central y en una sola pila tecnológica, es decir, en un único punto de error potencial. Además de los problemas de seguridad, la fiabilidad de un documento de identidad digital se ve afectada por el número de personas que lo utilizan y la finalidad con la que lo utilizan.

[3] La Comisión de la Banda Ancha de la ONU fija objetivos de banda ancha a nivel mundial para que los 3800 mill. de personas no conectadas accedan a Internet, UIT, enero de 2018

[4] *Identidad en un mundo digital,* Foro Económico Mundial, 2019

La empresa de consultoría internacional McKinsey&Company ha sugerido que el índice de adopción relativamente bajo del documento de identidad digital en el Reino Unido, Alemania y Austria puede deberse a «la falta de funcionalidad avanzada del intercambio de datos», necesaria para admitir una gran cantidad de casos de uso.[5] Incluso en India, donde la adopción de Aadhaar se encuentra por encima del 90 %, los habitantes no pueden disponer del documento de identidad digital para la totalidad de las transacciones que necesitan realizar en la vida digital, ya que la variedad de casos de uso aplicables todavía es limitada.

Estados Unidos es, sin lugar a dudas, un batiburrillo, ya que los consumidores tienen que configurar sus identidades múltiples veces y de múltiples maneras con casi cada producto o servicio digital con el que interaccionan. La fiabilidad de estos documentos de identidad digital varía en función de lo bien que cada una de estas entidades gubernamentales y comerciales gestione la seguridad y de lo dispuestas que estén para permitir que las credenciales de identidad que emiten sean utilizadas por otras entidades.

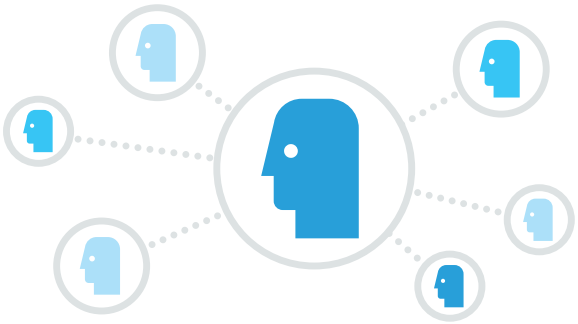
Algunas empresas cooperativas, como Mastercard y Microsoft, han aunado fuerzas para desarrollar «una identidad digital única y reutilizable» con la que pretenden liderar el camino hacia una mayor unificación y simplicidad. Algunas plataformas, como Apple Pay, Amazon PayPal y Facebook Libra, también están compitiendo para convertirse en una autoridad de confianza con respecto a la solución de identidad como servicio basada en la nube. Sin embargo, las crecientes preocupaciones sobre la confianza de las grandes tecnologías hacen que sea menos probable que se les permita asumir esta crucial responsabilidad. Es posible que iniciativas público-privadas, como la Alianza ID2020, cuenten con una mayor aceptación. Incluso es posible que veamos un esfuerzo de múltiples sectores en cooperación con el relativamente apolítico Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de EE. UU.

La normativa global hace viable el uso transfronterizo de las identidades digitales

La creación de una normativa internacional para el intercambio y la verificación de la información de la identidad supondrá un gran paso para subsanar las diferencias entre las distintas credenciales de identidad y los requisitos de cada país. La idea es permitir la interoperabilidad y la transferencia de confianza por medio de la creación de un conjunto de normativas que sirvan de referencia o se puedan aplicar a los propios requisitos de las distintas normativas nacionales.

A nivel global, algunas organizaciones internacionales, como la Fundación para la Identidad Descentralizada (DIF, por sus siglas en inglés) han adoptado una serie de medidas destinadas a cumplir con este objetivo. También existe un grupo de trabajo conjunto de la Organización Internacional para la Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC). Incluso Estados Unidos, un país muy fragmentado donde cada estado expide su propio permiso de conducir, ha dado un paso hacia la normalización recientemente. En la actualidad, muchos de los permisos expedidos por el estado cumplen con los requisitos de la Ley REAL ID, necesarios para embarcar en aviones comerciales sujetos a la normativa federal.

Creemos que es muy probable que la normativa internacional, similar a las que subyacen en Internet, será adoptada finalmente por la inmensa mayoría de identidades digitales. Con el tiempo, y a medida que los países lleven a cabo sus propios experimentos basados en distintas estrategias de verificación de la identidad, se producirá una convergencia en torno a un conjunto de prácticas recomendadas. En Estados Unidos también es probable que aumente la cooperación y el desarrollo de soluciones conjuntas, especialmente porque las empresas estadounidenses se han dado cuenta de que sus empresas homólogas de otras partes del mundo están cosechando beneficios económicos derivados de los programas uniformes de identidad digital.



Las personas tendrán a su disposición la visibilidad y el control sobre cómo son reconocidos en Internet

Una crítica frecuente que suscitan los sistemas centralizados de identidad nacional es que los ciudadanos no tienen ningún tipo de visibilidad de la información recopilada sobre ellos y del uso que se le da. Se puede decir lo mismo de los planteamientos ultradescentralizados.

Por ejemplo, en Estados Unidos la identidad tecnológica se está insertando en las capas de aplicaciones, programas y dispositivos, y hay escasas o inexistentes restricciones normativas acerca de cómo utilizan nuestra información los proveedores de estos componentes (un proveedor de una aplicación de bloqueo de llamadas no deseadas reutilizó los datos personales de sus usuarios en una empresa de verificación de la identidad que dirigía a modo de negocio adicional). A menudo se solicita

[5] Digital Identification: A Key to Inclusive Growth, McKinsey Global Institute, enero de 2019

permiso para indicar nuestros contactos, nuestra ubicación y otros datos, aunque esta información no sea necesaria para la función en cuestión. Sin embargo, si optamos por excluir la divulgación de esta información, es posible que no podamos usar dicha función.

También existe el problema en torno a la propagación de la biometría conductual, ya que el propio concepto de identidad podría estar evolucionando más allá de lo que logramos comprender o controlar. Las empresas están recogiendo nuestras huellas digitales para sintetizar perfiles de alta densidad que representan quiénes somos (una empresa de IDV sostiene que se puede verificar al 70-80 % de los consumidores únicamente a partir de su número de teléfono, lo cual «da acceso a una información valiosísima que se puede vincular de manera probabilística» a otras formas de datos personales).

«Las identidades digitales han evolucionado. Ya no se trata de fragmentos de información simples y remotos, sino de complejas redes que viajan por Internet..., de la suma de toda la información que hay sobre nosotros, que crece y evoluciona constantemente, de nuestros perfiles y del historial de nuestra actividad en la red... [y] de lo que se deduce de nosotros según este conjunto de información, que a su vez se convierte en nuevos puntos de información.

«El resultado para la población es una disminución del conocimiento y del control sobre su representación en Internet. Estos cambios se suman a una reescritura del contrato social, dado que la representación digital determina en gran medida la manera en la que vivimos nuestras vidas, y apenas somos conscientes de ello».

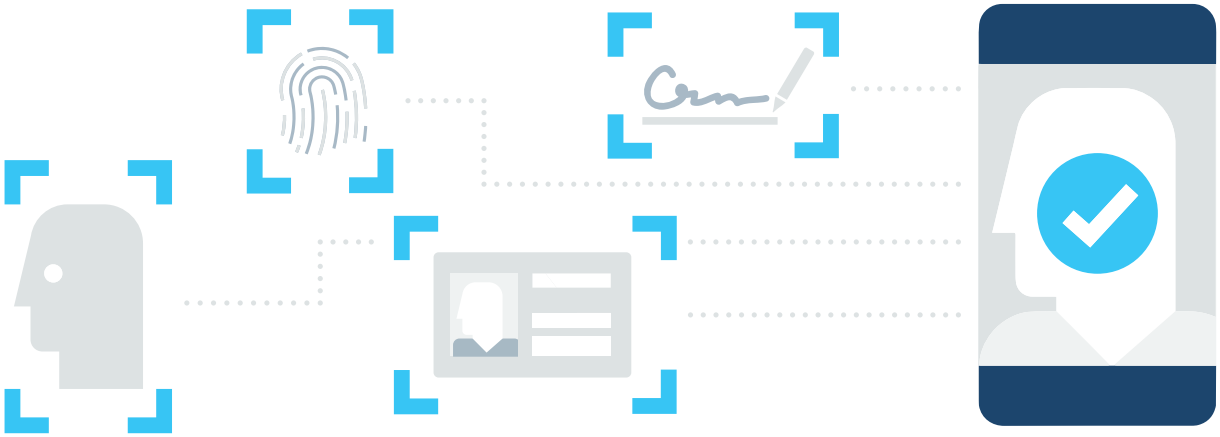
Identity in a Digital World, Foro Económico Mundial, 2019

Muchas empresas analizan datos similares para extraer conclusiones sobre nosotros. A partir de similitudes estadísticas con otras personas, los análisis avanzados pueden llegar incluso a predecir comportamientos que no hayamos mostrado nunca pero que es probable que desarrollemos. Tales conclusiones y predicciones también forman parte de nuestra identidad digital. Otras empresas están desarrollando procesos «continuados de verificación de la identidad» a partir de la transmisión ininterrumpida de datos procedentes de nuestra actividad digital. La ventaja es que estas identidades siempre están actualizadas. La desventaja es que nuestras identidades cambian constantemente sin que nosotros lo sepamos, y este proceso podría abrir la puerta a la vigilancia inapropiada de nuestra actividad.

La creciente preocupación en todo el mundo para conseguir una mayor transparencia en los datos y en los procesos de identidad digital está dando lugar a una mayor regulación. Algunos ejemplos los encontramos en el Reglamento General de Protección de Datos (RGPD) y en la Ley de Privacidad del Consumidor de California (que, cuando entre en vigor en 2020, será la primera ley en solicitar información sobre la biometría conductual). Asimismo, dicha preocupación también está impulsando innovaciones tecnológicas que facilitan la verificación de la identidad y que, a su vez, limitan la divulgación de la información personal que no está relacionada con la transacción en cuestión.

En términos generales, estamos asistiendo al surgimiento del movimiento de la identidad soberana, que pretende proporcionar a los consumidores las herramientas online necesarias para gestionar sus propios documentos de identidad digitales permanentes y verificables. Los consumidores podrán administrar su documento de identidad como lo deseen, además de controlar el flujo de información relacionada con la identidad que aportan a los proveedores de productos y servicios. Algunas de estas iniciativas se desarrollan en torno a la tecnología hyper-ledger, similar a blockchain.

En nuestra opinión, no cabe duda de que se necesitan estrategias más trasparentes para el tratamiento de las identidades digitales, puesto que estas son el futuro.



Hemos conseguido un mejor equilibrio entre la comodidad y el riesgo

Los consumidores serán los que determinen en última instancia si esta afirmación es cierta. No obstante, no hay duda de que estamos empezando a apreciar un cambio que va de una actitud en la que se prioriza la comodidad por encima de todo hacia un enfoque más comedido y equilibrado.

Se pueden apreciar ciertos indicios que demuestran el cambio de tendencia en el Experian 2019 Global Identity and Fraud Report (Informe global sobre identidad y fraude, publicado por Experian en 2019). Se pidió a los consumidores que dieran su opinión al respecto.

En definitiva, los consumidores quieren ambas cosas, pero parecen estar dispuestos a aguantar un poco de fricción y tener una mejor protección, especialmente en las transacciones financieras de alto riesgo o las que implican la divulgación de la PII.

Desde Mitek también hemos percibido la misma tendencia con las empresas de distintos sectores con las que trabajamos en todo el mundo. A medida que los consumidores adquieran más experiencia en las transacciones digitales y sean conscientes de lo que está en riesgo, el equilibrio adecuado entre seguridad y facilidad de uso se encontrará de manera natural.

Demostraciones de seguridad durante las operaciones de banca online

32% declaró que eran **sumamente importantes**

34% declaró que eran **muy importantes**

Acceso fluido a sus cuentas bancarias digitales

29% declaró que eran **sumamente importantes**

37% declaró que eran **muy importantes**

Ahora todos juntos...

A pesar de que todavía quedan muchos problemas por resolver, **creemos que el futuro de la identidad es prometedor.**

Ahora mismo, todos debemos pensar qué es lo que queremos para trabajar codo a codo para que nuestros propósitos se hagan realidad. Porque una cosa está clara: En adelante, la identidad afectará a casi todo lo que sucede tanto en nuestros negocios como en nuestras vidas.

Queremos saber tu opinión.
Comparte aquí tus observaciones, ideas y preocupaciones.

Mitek