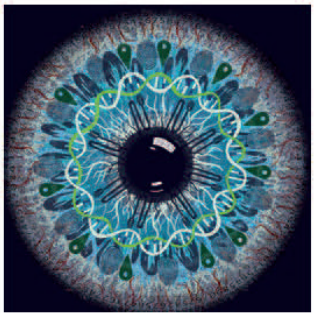
# Deloitte Review

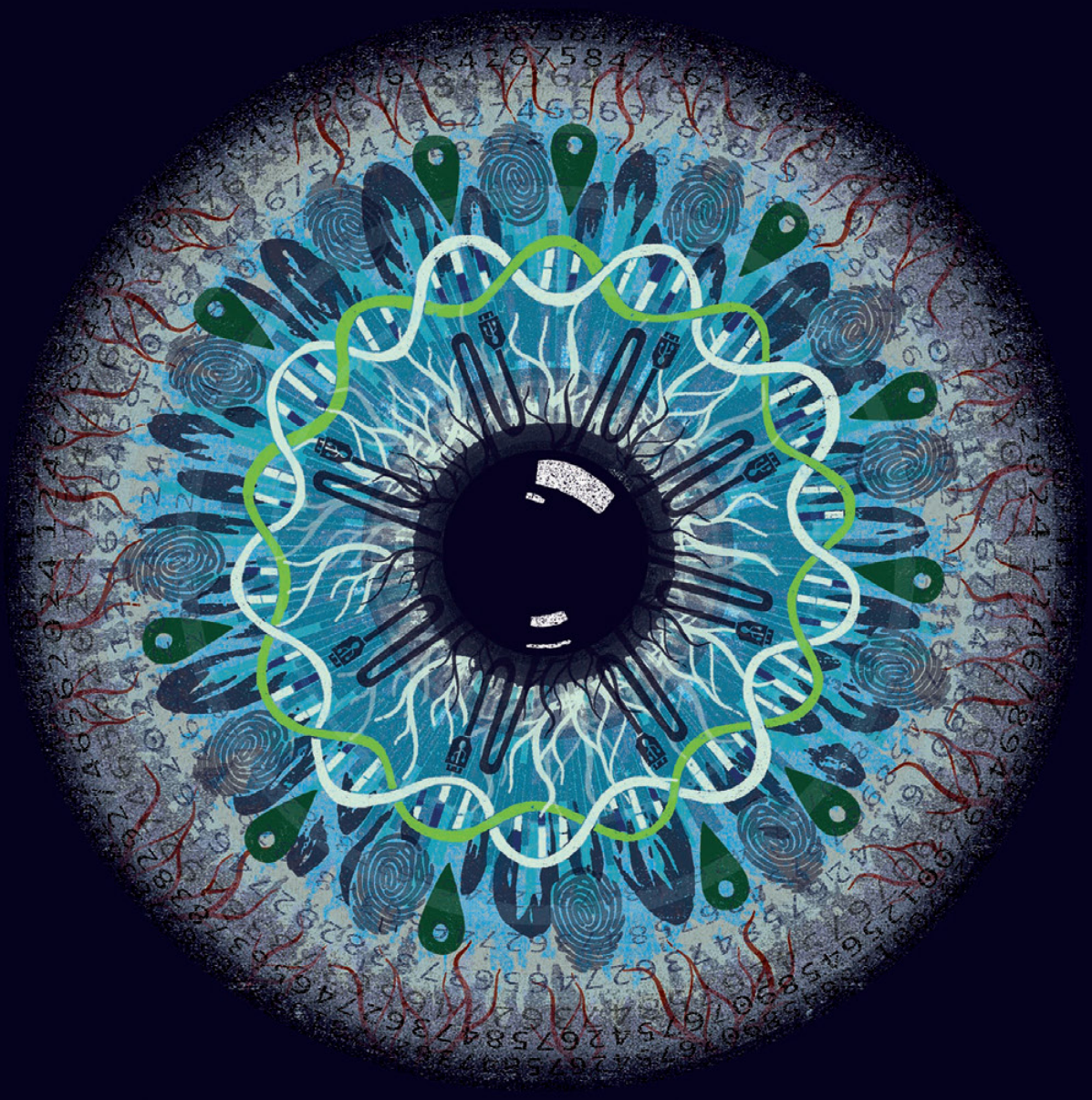
2016



# Un mundo más allá de las contraseñas

## Mejorando la seguridad, la eficiencia y la experiencia del usuario en la transformación digital

**Por** Mike Wyatt, Irfan Saif, **y** David Mapgaonkar



# Un mundo más allá de las contraseñas♦

## Mejorando la seguridad, la eficiencia y la experiencia del usuario en la transformación digital

**Por Mike Wyatt, Irfan Saif, David Mapgaonkar**
**Ilustración por Lucy Rose**

La próxima vez que usted esté en su computador a punto de acceder a información financiera sensible acerca de, dígase, una adquisición, imagine si usted no tendría que empezar por recordar la contraseña que usted generó hace algunas semanas para este sitio particular: mayúsculas, minúsculas, numerales, caracteres especiales, y similares. En lugar de exigir que usted teclee el usuario y la contraseña, el sitio le pregunte dónde almorzó ayer; y al mismo tiempo, su reloj inteligente valide la firma de su frecuencia cardíaca única. El proceso no solo proporciona una mejor experiencia de usuario – es más seguro. Usando información única acerca de usted, este enfoque es más capaz y robusto que el sistema de contraseñas que discierne qué tan probable es que usted sea quien esté reclamando que es.

♦ Documento original: "A world beyond passwords: Improving security, efficiency, and user experience in digital transformation", Deloitte Review Issue 19, July 25, 2016. Written by Irfan Saif, Mike Wyatt, & David Mapgaonkar. Illustration by Lucy Rose. http://dupress.com/articles/moving-beyond-passwords-cybersecurity/?id=us:2sm:3tw:4dup3362:5eng:6DUPress:20160810:cyberrisk:du_press&linkId=27439431
Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

La transformación digital es la piedra angular de la mayoría de las estrategias empresariales hoy, estando la experiencia de usuario en el corazón del diseño de la filosofía que orienta esa transformación. Pero la mayoría de las experiencias de usuario – para clientes, socios de negocio, empleados de primera línea, y ejecutivos – comienza con una transacción que es tanto molesta y, en términos de seguridad, uno de los eslabones más débiles. De hecho, las contraseñas débiles o robadas son la causa raíz de más de tres cuartos de los ataques cibernéticos corporativos,[1] y como cualquier lector probablemente sabe, las violaciones cibernéticas corporativas a menudo cuestan muchos millones de dólares en gastos de tecnología, legal, y relaciones públicas – y mucho más luego de los golpes menos tangibles pero más dañinos a reputación o calificaciones de crédito, pérdida de contratos, y otros costos.[2] Apuntalar la vulnerabilidad de la contraseña probablemente significaría menor riesgo cibernético corporativo – para no mencionar el aumento de la productividad del usuario, y la plusvalía de clientes agradecidos, y la reducción de gastos de administración del sistema de administrar de manera rutinaria las contraseñas olvidadas y bloqueadas de los empleados.

Las buenas noticias, para los CIO así como también para quienes se cansan de memorizar contraseñas cada vez más largas, es que las nuevas tecnologías – biometría, analíticas del usuario, aplicaciones del Internet de las cosas, y más – les ofrecen a las compañías la oportunidad para diseñar un paradigma fresco basada en confianza bilateral, experiencia del usuario, y seguridad mejorada del sistema. La ejecución exitosa puede ayudar tanto a acelerar el negocio como a diferenciarlo en el mercado.

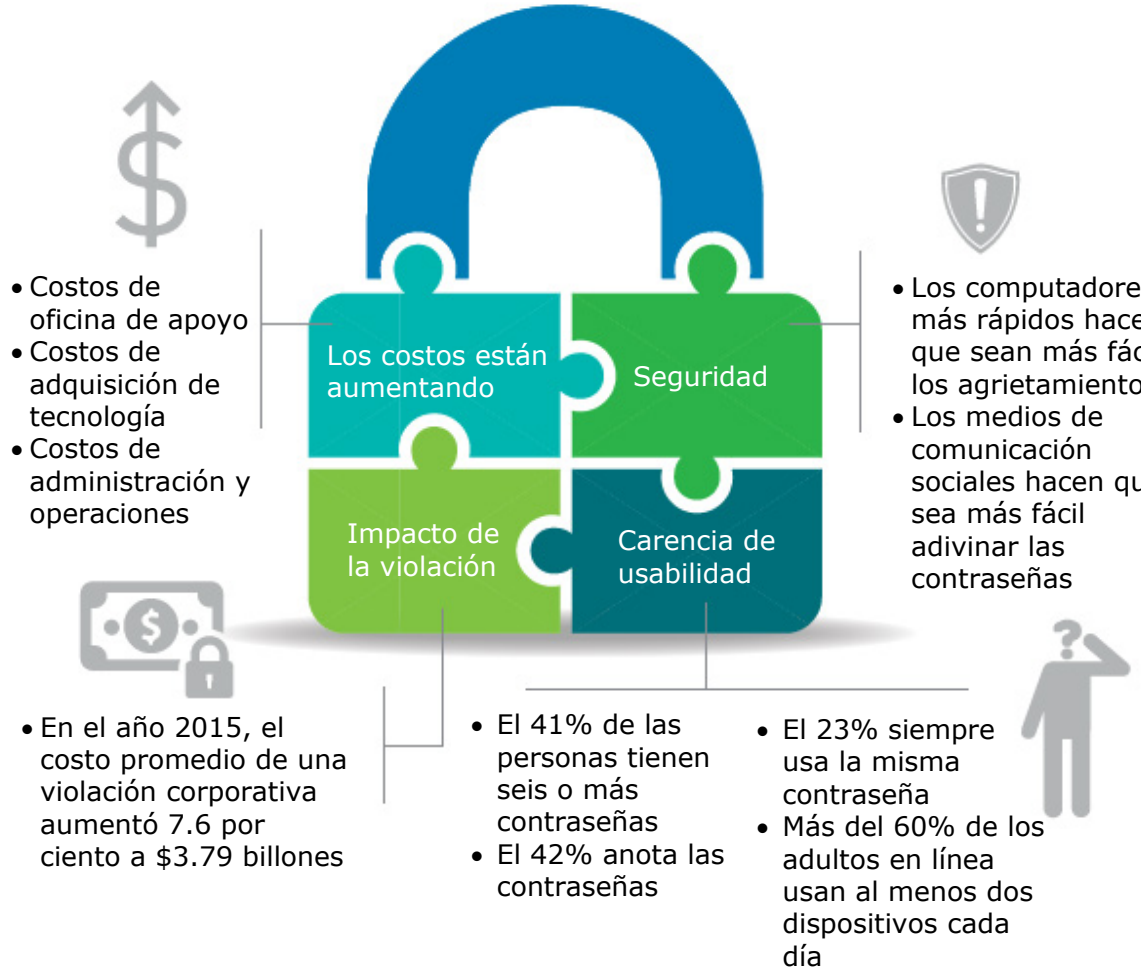
De hecho, la capacidad para tener acceso a información digital seguramente sin la necesidad de usuario y contraseña representa una actualización largamente esperada para el trabajo y la vida. Las contraseñas carecen de la escalabilidad requerida para ofrecer a los usuarios toda la experiencia digital que esperan. De manera específica, carecen de la escalabilidad para respaldar la miríada de aplicaciones en línea que están siendo usadas hoy, y no ofrecen la fluidez de la experiencia que los usuarios de manera creciente han llegado a esperar y demandar. Inevitablemente, los usuarios asediados ignoran las recomendaciones[3] y usan la misma contraseña una y otra vez, agravando la vulnerabilidad de cada sistema al cual ingresan. Quizás aún más importante, las contraseñas carecen de la escalabilidad para proporcionar una respuesta de autenticación que esté ajustada al valor de la transacción; en otras palabras, los sistemas fuertes de contraseñas que requieren políticas complicadas sobre uso de caracteres y extensión de la contraseña hacen que los administradores del sistema sean incapaces de tener acceso a la fortaleza de cualquier contraseña dada. Sin tal conocimiento, las empresas se esfuerzan por tomar decisiones informadas basadas-en-el-riesgo sobre cómo tener capas de contraseñas junto con otros factores de autenticación.

## EL SIGLO 21 CUMPLE CON LOS LÍMITES HUMANOS

Hace veinte años, el consumidor típico solo tenía una contraseña, para el correo electrónico, y probablemente era el mismo número de cuatro dígitos del PIN de su cuenta bancaria. Hoy, los usuarios en línea crean una nueva cuenta cada pocos días, eso parece, cada una requiriendo una contraseña compleja: para tener acceso a información corporativa, compra de calcetines, pago de facturas de servicios públicos, verificación de inversiones, registro para operar un 10K, o simplemente iniciar sesión en el sistema de correo electrónico del trabajo. Para el 2020, algunos predicen, cada usuario tendrá 200 cuentas en línea, cada una requiriendo una contraseña única.[4] De acuerdo con una encuesta reciente, el 46 por ciento de quienes respondieron tienen 10 o más contraseñas.[5]

Y las demandas por seguridad de las contraseñas están llegando a los límites de las capacidades humanas, tal y como se muestra en la figura 1. De acuerdo con el sicólogo George Miller, los humanos son mejores recordando números de siete dígitos, más o menos dos.[6] En una era donde una contraseña de ocho caracteres le llevaría a un atacante de alta potencia 77 días para agrietarla, la política que requiere el cambio de contraseña cada 90 días significaría que una contraseña de nueve caracteres sería suficientemente segura.[7]

Figura 1. Por qué las contraseñas son problemáticas




*Fuentes*: RoboForm, "Password security survey results—part 1," http://www.roboform.com/blog/password-security-survey-results, accessed April 21, 2016; Philip Inglesant and M. Angela Sasse, "The true cost of unusable password policies: Password use in the wild," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010): pp. 383–392; PortalGuard, *Top 10 real costs associated with requiring multiple passwords*, 2011; Tom Rizzo, "The hidden costs of passwords," *ScorpionSoft*, August 20, 2015, http://insights.scorpionsoft.com/the-hidden-costs-of-passwords; Victoria Woollaston, "Think you have a strong password? Hackers crack 16-character passwords in less than an HOUR," *Daily Mail*, May 28, 2013; Matt Smith, "The 5 most common tactics used to hack passwords," *makeuseof*, December 20, 2011, http://www.makeuseof.com/tag/5-common-tactics-hack-passwords/; Ponemon Institute, *2015 cost of data breach study: Global analysis*, May 2015; Olly Robinson, "Finding simplicity in a multi-device world," *GfK Insights Blog*, March 6, 2014, http://blog.gfk.com/2014/03/finding-simplicity-in-a-multi-device-world/.

**Gráfica: Deloitte University Press | DUPress.com**

Pero tal contraseña larga – especialmente cuando es una de muchas y cambia de manera regular – comienza a forzar la memoria de las personas. El resultado inevitable: las personas vuelven a usar las mismas contraseñas débiles para múltiples cuentas, colocan notas adhesivas a los monitores de sus computadores, comparten las contraseñas, y frecuentemente se apoyan en la función de contraseña olvidada que tienen los sitios web. En una encuesta reciente realizada a usuarios de los Estados Unidos y del Reino Unido, el 23 por ciento admitió que siempre usa la misma contraseña, con el 42 por ciento anotando las contraseñas. Si bien el 74 por ciento inicia sesión en seis o más sitios web o aplicaciones durante un día, solo el 41 por ciento usa seis o más contraseñas únicas.[8] De acuerdo con otra encuesta, más del 20 por ciento de los usuarios de manera rutinaria comparten las contraseñas, y el 56 por ciento vuelve a usar contraseñas a través de las cuentas personales y corporativas.[9] El software de administración de contraseñas parcialmente alivia este problema particular, pero en últimas todavía está atado a la construcción de la contraseña.[10]

Incluso si un empleado sigue todas las regulaciones y tiene seis contraseñas fuertes distintas que recuerde, todavía puede ser vulnerable. Los humanos todavía están incentivados o son engañados para revelar sus contraseñas. Hay malware, o software malicioso instalado en los computadores; hay phishing, en el cual los ladrones cibernéticos se apropian de los datos de inicio de sesión, tarjetas de crédito, y otros datos bajo la apariencia de sitios web o aplicaciones aparentemente legítimos; e incluso hay ataques de "día cero," en el cual los hackers explotan las vulnerabilidades del software sobrecargado.[11] Y por supuesto, persisten los ataques humanos de vieja data, incluyendo la navegación a través del hombro para observar a los usuarios escribiendo sus contraseñas, saltando para encontrar la información de la contraseña, suplantando las figuras de autoridad para extraer contraseñas de los subordinados, discerniendo información acerca de las personas proveniente de medios de comunicación social para cambiar su contraseña, y empleados que venden contraseñas corporativas.

No extrañan los costos operacionales de mantener contraseñas, incluyendo gastos de oficinas de apoyo para quienes hayan olvidado las contraseñas, y pérdidas de productividad a causa de que están aumentando demasiados intentos de bloqueo y otros problemas. Incluso más inquietante, el cada vez más creciente poder de computación está facilitando nuevos ataques de fuerzas brutas para simplemente adivinar contraseñas. El futuro de la contraseña es tanto costoso como lleno de tensión.

- El 74 por ciento inicia sesión en seis o más sitios web o aplicaciones durante un día.[12]
- El 20 por ciento de los usuarios de manera rutinaria comparten las contraseñas.[13]
- El 56 por ciento vuelve a usar contraseñas a través de las cuentas personales y corporativas.[14]

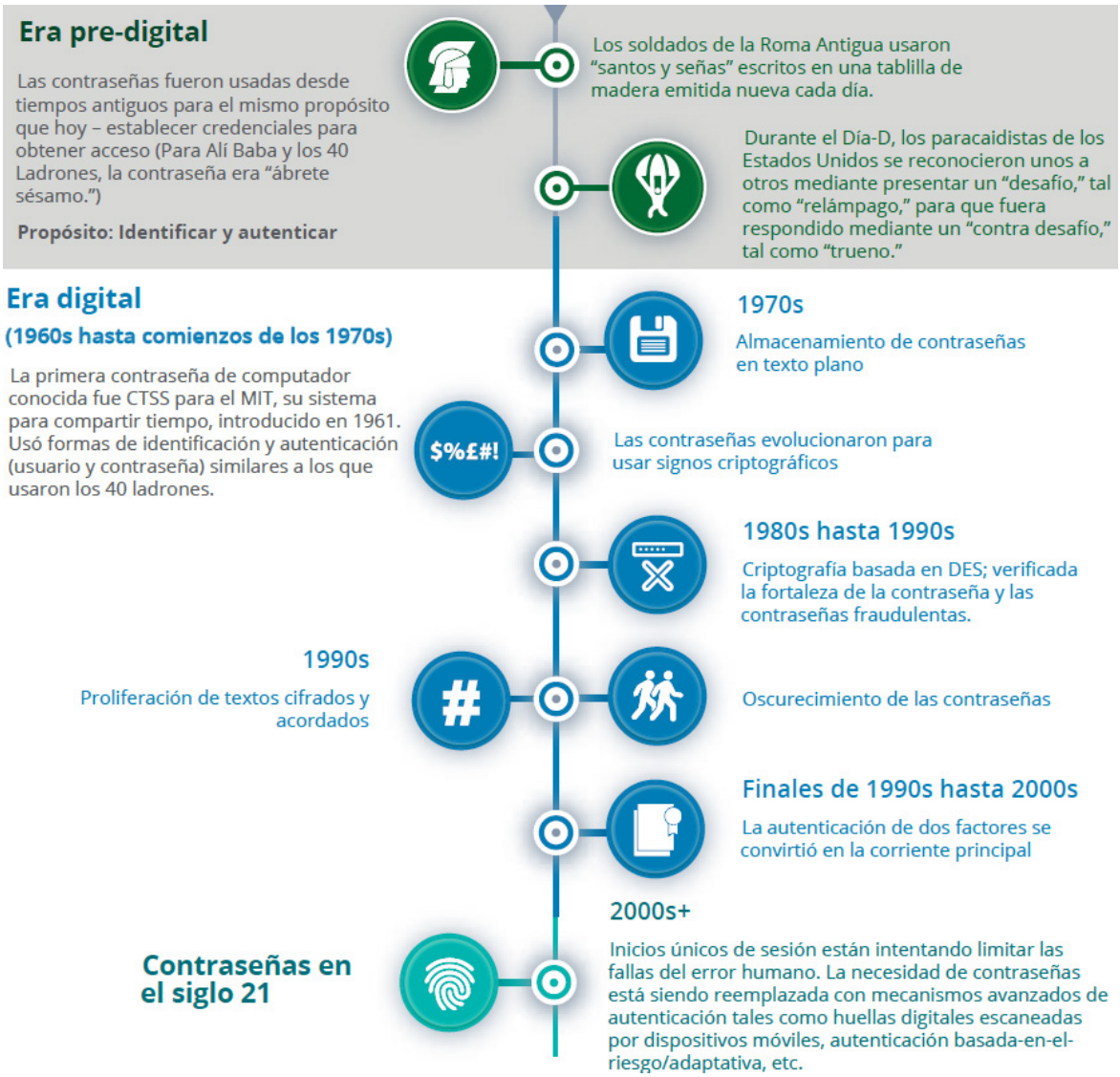
## DE LA GEOLOCALIZACIÓN HACIA LA BIOMÉTRICA

Los líderes corporativos son bien conscientes de que la estrategia de información y acceso están en el corazón de casi todos los negocios hoy. Es el momento para reconocer también que la contraseña – el mecanismo históricamente usado para implementar esta estrategia – está fundamentalmente fracturada. Dadas sus responsabilidades fiduciarias y de gobierno, las juntas de directores y los ejecutivos directores tienen la deuda frente a los *stakeholders* de proteger el tesoro corporativo – la información digital – mediante proporcionar protecciones más robustas ante el acceso en línea. A su vez, inversionistas, clientes, empleados, socios, proveedores, y otros se beneficiarán de la protección más fuerte de los datos corporativos unida a acceso más fácil para los usuarios legítimos, reforzando así la confianza bilateral que está en el corazón de cualquier relación de negocios saludable.

## DESDE LA GRECIA ANTIGUA HACIA LA ERA DIGITAL

Las contraseñas han estado en uso desde tiempos antiguos para el mismo propósito que hoy: establecer las credenciales de uno para el acceso a los activos protegidos. El establecimiento de la autoridad de esta manera depende de presentar "algo que usted conoce" – la contraseña – para que sea "autenticado" contra el valor registrado. Tal y como lo muestra la figura 2, las contraseñas han sido la piedra angular de nuestra historia, incluyendo servir como la clave digital durante los últimos 50 años. Además, las contraseñas digitales usadas poseían ventajas: eran simples, fáciles de usar, y relativamente convenientes. Podrían ser cambiadas, si llegaran a estar comprometidas. De manera conveniente, podrían ser compartidas, si bien esta práctica compromete la seguridad. Dado que las contraseñas son el estándar que prevalece, las políticas corporativas que las gobiernan están bien establecidas, así como los sistemas de administración de la identidad y del acceso que las respaldan.

Figura 2. La contraseña a través de la historia




Fuentes: Black, "The language of espionage: Signs, countersigns, and recognition," Imminent Threat Solutions, August 11, 2015; David Walden and Tom Van Vleck, eds., *The Compatible Time Sharing System (1961–1973): Fiftieth anniversary commemorative overview*, IEEE Computer Society, 2011; "Password security: Past, present, future," Openwall, 2012.

**Gráfica: Deloitte University Press | DUPress.com**

De manera creciente, consumidores, empleados, y socios, todos ellos esperan interacciones digitales perfectamente integradas, conduciendo a un cambio fundamental del paradigma de la manera como las compañías ayudan a concebir, usar, y administrar las identidades. Apoyando el cambio de imagen, las nuevas credenciales de inicio se sesión pueden incluir no solo "lo que usted conoce" o una contraseña específica sino también "quién es usted" y "qué tiene usted," junto con "dónde está usted" y "qué está haciendo usted." Pueden incluir detección de patrones personales para tener acceso a cierta información según la hora del día y el día de la semana, otras evaluaciones dinámicas y contextuales de las características comportamentales de los usuarios, geolocalizaciones de los individuos, biométricas, y símbolos. Los sistemas que confían en la autenticación están evolucionando para volverse adaptativos y pueden generar una alerta ante un intento de autenticación que sea demasiado riesgoso si no se satisface el uso típico de los patrones – incluso aunque las credenciales básicas puedan parecer correctas – y el sistema puede entonces aumentar la autenticación, desafiando al usuario para que proporcione prueba adicional para verificar su identidad. A causa de su ubicuidad, el teléfono móvil es el dispositivo más obvio en el cual ocurre la autenticación, pero los capitalistas de riesgo también están financiando compañías que creen otros dispositivos conectados, tales como pulseras que identifiquen el latido del corazón que es único de uno y dijes de USB que realización máquina-a-máquina sin requerir que un humano escriba un código de acceso.[15]

Las fuerzas están convergiendo para una revisión. "Desde la perspectiva de la tecnología, tenemos increíbles modalidades nuevas de autenticación además de las contraseñas, y la capacidad de computación para hacer el análisis para tomar decisiones informadas," dice Ian Glazer, vicepresidente del consejo de administración de Identity Ecosystem Steering Group, un grupo liderado por el sector privado que trabaja con el gobierno federal para promover la autenticación digital más segura. "También nos estamos sobreponiendo a uno de los mayores desafíos: nosotros ponemos la plataforma de autenticación en las manos de cada uno en la forma de un teléfono inteligente."[16]

Para las compañías, navegar el cambio desde lo heredado hacia nuevos sistemas nunca es fácil. Pero mediante seguir un enfoque basado-en-el-riesgo, pueden crear una hoja de ruta bien considerar para hacer el cambio mediante focalizar la inversión y la implementación en las operaciones de negocio de prioridad más alta. Comenzando con un piloto para probar las opciones seleccionadas, las compañías pueden entonces ampliar las soluciones exitosas donde más se necesiten. Por encima de todo, es crucial establecer pronto la ruta del cambio. Después de todo, los negocios están operando en un tiempo donde la innovación y el crecimiento continuados dependen más que nunca de la integridad de la información.

## LOS NUEVOS PORTEROS

Con los costos de protección de la contraseña aumentando – en tiempo, riesgo, y dólares – las empresas están mirando implementar enfoques flexibles basados-en-el-riesgo: requerir la autenticación del usuario con una fortaleza que sea proporcional con el valor de la transacción que esté siendo solicitada. Afortunadamente, tal y como se muestra en la figura 3, están surgiendo varias tecnologías que pueden ser combinadas de una manera que satisfaga al mismo tiempo la tolerancia de la empresa ante el riesgo y la flexibilidad del usuario. Tecnologías emergentes tales como la cadena de bloques[17] están posicionadas para reemplazar con múltiples factores la vulnerabilidad de la contraseña única.

Tener múltiples porteros, en cascada, fortifica la seguridad mediante requerir puntos de chequeo adicionales. A más diferentes pruebas de identidad requeridas a través de rutas separadas, más difícil es para el ladrón robar su identidad o suplantar la suya. De igual manera, las plataformas del consumidor están pavimentando la manera para proporcionar experiencia mejorada del usuario mediante empoderar a los consumidores para que escojan cómo tener acceso a la información digital.

Figura 3. Un nuevo mundo con muchos porteros


**Gráfica: Deloitte University Press | DUPress.com**

La economía del enviar mensajes de texto, del compartir, y de las aplicaciones móviles, ha hecho que ñas comunicaciones inmediatas, en línea, y suaves, sean ubicuas. En una reversa a una era anterior, los consumidores son ahora quienes adoptan primero, seguidos por las empresas. Por consiguiente, en la medida en que el teléfono inteligente se convierte en centro de actividad digital de los consumidores, en su persona casi en todo momento, está bien posicionado para desempeñar una función central. Ya, la mayoría de quienes tienen entre 16 y 24 años perciben la seguridad como un paso molesto extra antes de hacer un pago en línea y consideran que la seguridad biométrica sería más rápida y más fácil que las contraseñas.[18] En función de esas tendencias, compañías líderes de tecnología fundaron en el año 2012 la Fast IDentity Online Alliance para avanzar nuevos estándares técnicos para nuevos sistemas de autenticación en línea abiertos, inter-operables, y escalables, sin contraseñas.[19]

Para mantener la seguridad y proporcionar mayor conveniencia para el usuario, un precepto clave en los recientes sistemas de inicio de sesión que están evolucionando es la *autenticación de múltiples factores*. Gmail y Twitter, entre otros, hoy despliegan esta solución en una forma sencilla: les proporcionan a los usuarios el envío a sus teléfonos móviles de un código por una vez, además de la tradicional contraseña que se ingresa en la pantalla del computador portátil del usuario. La seguridad mejorada que viene de la autenticación ocurre en dos dispositivos de propiedad del usuario. Un ladrón cibernético tendría que tener acceso al teléfono del usuario, además de su contraseña en línea, para tener acceso a la cuenta protegida.

Para otro nivel de protección, además de la entrega en diferentes dispositivos, los factores requeridos para autenticación pueden variar según el tipo. En un proceso de autenticación de dos factores, por ejemplo, el usuario podría escanear su retina vía la cámara en su computador portátil o en su teléfono inteligente, usando información biométrica como un primer paso para obtener acceso a su cuenta bancaria en línea. En un segundo paso, el banco podría enviar al teléfono móvil del usuario un desafío vía mensaje de texto, requiriendo que el usuario replique el mensaje de texto para finalizar la autenticación.

Uno de los factores nuevos más populares para la autenticación son las *tecnologías biométricas*, las cuales no requieren memorización de combinaciones complejas de letras, números, y símbolos, mucho menos con la combinación que usted usó como recurso.[20] Simplemente es parte de usted – de su huella dactilar, voz, rostro, ritmo cardíaco, e incluso movimientos característicos. Las biométricas que puedan ser capturadas mediante las cámaras de los teléfonos inteligentes y grabadoras de voz probablemente se convertirán en las que prevalezcan primero, incluyendo huellas dactilares, iris, voz, y reconocimiento de voz. Chequear sus datos biométricos contra un dispositivo de confianza que solo usted posee – en oposición a un depósito central – está surgiendo como el enfoque preferido. Por ejemplo, usted podría usar sus huellas dactilares para tener acceso a un recurso particular en su propio teléfono inteligente, el cual a su vez envía su propia firma única de dispositivo a un mecanismo de autenticación que le otorga a usted acceso.[21] Esta es la base para la escalabilidad de la autenticación a través de múltiples servicios en línea, y es el modelo que adoptó la Fast IDentity Online Alliance.

## AUTORIZACIÓN BASADA-EN-EL-RIESGO, EN ACCIÓN

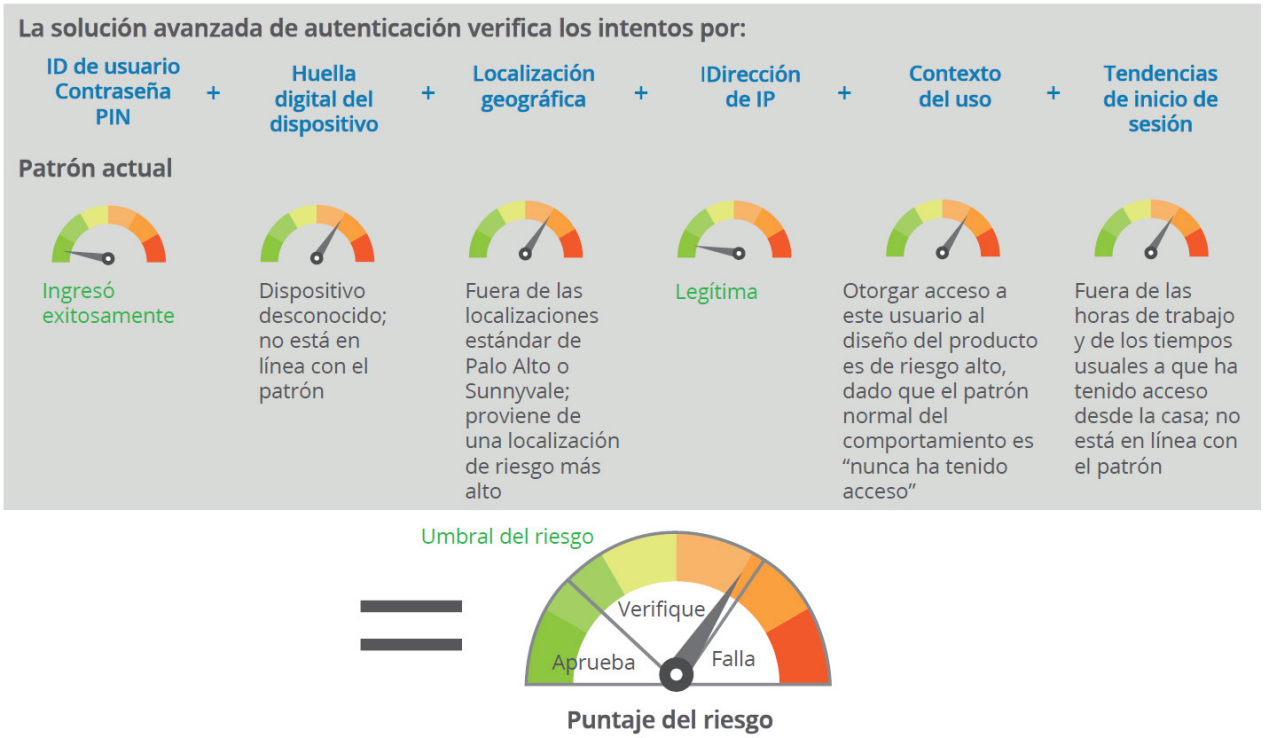
En un ejemplo hipotético (figura 4), un usuario corporativo usualmente inicia sesión alrededor de las 8:30 am. PTS, inicia sesión a las 6 p.m., e inicia sesión de nuevo alrededor de las 9:30 p.m. Típicamente, inicia sesión en las oficinas corporativas en Palo Alto o Sunnyvale, teniendo acceso a los sistemas de su compañía durante el día vía un computador portátil o un computador de escritorio de la compañía.

El lunes, el usuario intenta iniciar sesión desde su oficina de Sunnyvale a las 11 a.m., usando un computador de trabajo para tener acceso al sistema financiero corporativo. El usuario está iniciando sesión en un computador de la compañía desde su oficina durante sus horas regulares por información a la cual típicamente accede. El sistema le otorga acceso.

Al día siguiente, el usuario intenta iniciar sesión desde el Aeropuerto Internacional de Los Ángeles a las 7 p.m., usando un computador portátil de la compañía para tener acceso a la lista de festivos de la compañía en el sistema de beneficios internos. Si bien esta localización y hora son inusuales, los otros factores son típicos para él, y la información no es sensible. El sistema le otorga acceso.

El día siguiente, un hacker intenta iniciar sesión desde Belaurus a las 3 a.m., con el usuario y la contraseña para tener acceso a los diseños de un producto todavía no lanzado, en un servidor interno de desarrollo. El usuario, la contraseña, y la dirección de IP son legítimos, pero los otros factores – tales como localización, hora, y la información solicitada – son altamente atípicos para este usuario. El sistema implementa controles que inician técnicas de autenticación para verificar la identidad del usuario – por ejemplo, enviando al teléfono del usuario un código de autenticación por una vez. Dado que el hacker en este escenario no tiene el teléfono del usuario, es incapaz de ingresar el código de autenticación, y el sistema niega el acceso.

Figura 4. Autenticación del usuario basada-en-el-riesgo




**Gráfica: Deloitte University Press | DUPress.com**

El conjunto separado de factores de autenticación llega bajo la rúbrica de "qué tiene usted" – no solo teléfonos inteligentes sino quizás símbolos de seguridad transportados por individuos, símbolos facilitados por software, o incluso una adaptación de las bases de datos de las cadenas de bloques usadas por bitcoin. Las claves del hardware de USB les permiten a los trabajadores iniciar sesión mediante ingresar su usuario y contraseña, seguidos por un código de acceso generado por el llavero en intervalos de tiempo establecidos. Los símbolos del software operan de manera similar, con una aplicación del teléfono inteligente, por ejemplo, generando los códigos. Más lejos, el uso potencial de la tecnología distribuida de las cadenas de bloques podría ayudar a proporcionar un sistema más seguro y descentralizado para la autenticación.

Una de las posibilidades más intrigantes en los nuevos controles de acceso está en la *autorización basada-en-el-riesgo*, un sistema dinámico que otorga acceso dependiendo de la confiabilidad de la solicitud de admisión del usuario y de la sensibilidad de la información protegida. Con el Project Abacus, el Advanced Technology and Projects de Google está desarrollando aprendizaje de máquina para autenticar a los usuarios con base en múltiples valoraciones de su comportamiento.[22] Usando sensores tales como la cámara, el acelerómetro, y las funciones de GPS, los teléfonos inteligentes pueden obtener un rango amplio de información acerca de los usuarios, incluyendo expresiones faciales típicas, sus geolocalizaciones habituales, y cómo escriben, caminan y hablan. Juntos, esos factores son 10 veces más seguros que las huellas dactilares y 100 veces más seguros que los PIN de cuatro dígitos.[23] Con tales capacidades, el teléfono del usuario, u otro dispositivo, puede constantemente calcular un puntaje de verdad – el nivel de confianza – de que el usuario es quien reclama ser. Si el sistema tiene duda, solicitaría más credenciales mediante el aumento de la autenticación para verificar la identidad del usuario o para negar el acceso.

Tal puntaje de verdad es útil para diseñar protecciones para la información, dependiendo de su sensibilidad. Las aplicaciones de la banca, por ejemplo, requerirían puntajes de verdad muy altos; el acceso a sitios generales de noticias podría requerir menos. Para la adopción generalizada de este enfoque, las compañías tienen que tener en cuenta los problemas de la privacidad del consumidor.

## LA MEJOR DEFENSA

Para ilustrar cómo una compañía puede adoptar el nuevo sistema, asuma el escenario hipotético de una cadena minorista que descubre el robo de información de la tarjeta de crédito del cliente. Para fortificarse contra ataques futuros, la cadena realiza una valoración a nivel de toda la compañía respecto de sus potenciales vulnerabilidades y descubre tres debilidades que habrían podido llevar al ataque: Primero, el equipo de administración del servidor conserva los nombres del usuario y las contraseñas en un archivo de texto no encriptado en un directorio compartido. Para conveniencia, los administradores del almacén comparten sus contraseñas de los sistemas de registro de efectivo en el punto de venta [point-of-sale (POS)], dándoles a los asociados del almacén mayores privilegios para emitir devoluciones, hacer cambios, y similares. Por último, para simplificar la integración, las contraseñas de proveedores terceros se establece que nunca expiren.

El minorista considera varias opciones nuevas de autenticación para fortalecer la seguridad en los puntos de venta, que el análisis sugiere eran probablemente los más culpables para la violación. A causa del inconveniente los administradores están en contra de requerir de nuevo que los empleados ingresen una contraseña por una vez entregada por teléfono inteligente cada vez que desean tener acceso al sistema. En lugar de ello, optan por probar – en una división de los almacenes – una combinación de huellas dactilares y reconocimiento facial para autenticar en los sistemas POS los inicios de sesión de los asociados del almacén. No solo es más conveniente para los usuarios, esta opción aprovecha la infraestructura existente. Usando cámaras ya en funcionamiento para monitorear la actividad del POS, combinada con una aplicación de escaneo de huellas adicionada al inicio de sesión del hardware de tacto de la pantalla de POS, la compañía

lanzó el piloto sin hardware adicional, gastando principalmente en los costos de desarrollo del software de un tercero. Los resultados: los asociados del almacén aprecian los inicios de sesión más fáciles y más rápidos; la compañía hace forzosos los derechos apropiados para un usuario dado; y el recuerdo constante de la cámara del POS ayuda a reducir el robo entre los asociados.

Con el éxito del piloto, el minorista implementa la solución a través de todos los 1,500 almacenes, actualizando las políticas para adicionalmente asegurar la seguridad para el nuevo sistema, incluyendo la aplicación de las huellas dactilares y la autenticación facial para operaciones de seguridad más alta con mayor impacto y mecanismos seguros de recuperación para los factores de autenticación comprometidas.

La compañía también se compromete en actividades educativas para los asociados del almacén. Los entrenadores del almacén local enfatizan la facilidad de uso del nuevo sistema, su efectividad contra las vulnerabilidades detrás del robo cibernético original, y la disposición de la compañía para invertir en las últimas tecnologías para beneficio de empleados y clientes.

Además, los entrenadores comparten documentos que explican cómo funciona la solución, con aseguramientos fuertes de que la información biométrica capturada no será usada para propósitos diferentes a la autenticación del POS.

## NO SOLO SEGURIDAD – TRANSFORMACIÓN DIGITAL

Moverse más allá de las contraseñas no es solo una ola del futuro – hoy tiene sentido económico. Una encuesta reciente realizada a compañías de los Estados Unidos encontró que cada empleado pierde, en promedio, $420 anualmente lidiando con contraseñas.[24] Con el 37 por ciento de los encuestados reseteando sus contraseñas más de 50 veces por año, las solas pérdidas en productividad pueden ser asombrosas.[25] Cuando se tiene en cuenta el costo del personal de apoyo y de las oficinas de ayuda requeridos, los ahorros provenientes de solo eliminar las contraseñas – dejando aparte las ventajas de seguridad – pueden comenzar a justificar rápidamente la transición. Además, facilitar las tareas diarias de los empleados puede mejorar la felicidad y la productividad del empleado: la investigación realizada en los departamentos de reclamos en el Reino Unido encontró una correlación entre el mejoramiento del proceso y la actitud y retención del empleado, e incluso variables tan lejanas como el desempeño financiero de la organización.[26]

Es verdad, abandonar el sistema heredado de contraseñas – familiar, aunque sin embargo irritante – y adoptar nuevos métodos de inicio de sesión puede parecer de enormes proporciones para administradores, usuarios, y clientes. Cualquiera de esas migraciones requiere una inversión y un plan de implementación, de visión clara, animado a sobreponerse a desafíos muy reales. Primero, desde la perspectiva técnica, ningún sistema es hermético. Si los teléfonos inteligentes o los símbolos son el eje, los dispositivos perdidos o robados podrían introducir riesgo: tal y como es el caso de la pérdida de la tarjeta de crédito, el usuario tendría que contactar al emisor del dispositivo o a la autoridad de autenticación para reportar la pérdida y conseguir el reemplazo. Los delincuentes algunas veces usan la cuenta de recuperación de los factores de autenticación de pérdida para secuestrar cuentas.[27] Y los teléfonos móviles pueden ser un vínculo débiles, dado que las comunicaciones inalámbricas a menudo no están encriptadas y pueden ser robadas estando en tránsito.[28]

Incluso las tecnologías biométricas no son seguras ante la falla – muchas son difíciles de engañar pero no son a prueba de engaño. Las huellas dactilares, por ejemplo, pueden ser falsificadas utilizando plastilina.[29] Los diseñadores del sistema pueden abordar esas vulnerabilidades potenciales mediante implementar la detección de la vitalidad [*liveliness detection*] en los sensores y almacenar la información biométrica de una manera específica para la aplicación, pero estas técnicas no están listas para ser implementadas plenamente. Tampoco lo son la mayoría de sistemas basados-en-analíticas, los cuales no entregarían la lista completa de beneficios sin cambios a los procesos de

negocio. Por ejemplo, considere el sistema de seguridad basado-en-la-reputación que se discute en el recuadro "Autenticación del usuario basada-en-el-riesgo." Allí, las defensas examinan no solo el intento del ID del usuario para tener acceso al sistema sino también su localización, hora, patrones de comportamiento, y los datos a los cuales desea tener acceso; en los casos en que esos marcadores fueran inusuales, el sistema niega el acceso a datos sensibles del negocio. Este es un excelente enfoque de seguridad pero es predicado en una organización que conoce y controla todos sus datos: usted puede ser consciente si alguien está intentando tener acceso a datos sensibles solo si usted ha clasificado esa información como sensible y ha determinado sus protocolos para el acceso.

Concedido, moverse más allá de las contraseñas puede sonar abrumador, requiriendo actualizaciones importantes de tecnología así como también cambios a la administración interna del conocimiento y a otros procesos de negocio. Pero las organizaciones pueden dar pasos incrementales (figura 5) en el camino hacia una transición suave. Lo que sigue ofrece una hoja de ruta:

- **Priorice**. Valore las prioridades estratégicas del negocio contra el panorama de las amenazas e identifique las debilidades en los sistemas de autenticación para las operaciones clave de negocios clasificadas según su importancia.

- **Investigue**. Examine las posibles soluciones para autenticación más fuerte, evaluando las ventajas y desventajas en la protección contra las principales amenazas y la capacidad para proporcionar una respuesta práctica, costo-efectiva, y escalable para el entorno específico de trabajo. Las soluciones del software de autenticación basada-en-estándares ayudan a evitar los costos de infraestructura nueva y también sientan las bases para la integración de las soluciones de la siguiente generación.

- **Pruebe**. Luego de seleccionar una(s) solución(es) prometedora(s), realice el piloto en una o en unas pocas operaciones de negocio de prioridad alta. En esos ensayos, recaude los datos y la retroalimentación a partir de la experiencia de los usuarios. ¿Los usuarios son capaces de adoptar la solución fácil e intuitivamente? ¿El más fácil acceso en línea hace que su trabajo sea más eficiente? ¿El acceso en línea está siendo usado correctamente más a menudo de una manera que proporciona mayor seguridad? ¿Los usuarios plantean preocupaciones de seguridad u otras acerca de cualesquiera soluciones dinámicas, biométricas o adaptivas, con base en sus normas comportamentales? Desde la perspectiva del administrador en línea, ¿cuál es la experiencia en los costos de mantenimiento del nuevo sistema, comparado con el viejo sistema de contraseñas?

- **Amplíe**. Aprovechando las lecciones derivadas del piloto, aplique la solución a un conjunto más amplio de operaciones clave, haciéndolo por fases con base en la priorización.

- **Modernice y eduque**. Actualice las políticas de acceso. Reemplace las políticas sobre la seguridad de la contraseña con políticas basadas-en-el-riesgo para la autenticación basada en la sensibilidad de la información solicitada. Enseñe a los usuarios cómo funciona el nuevo sistema, centrándose en sus ventajas sobre la tecnología vieja.

Figura 5. Cinco cosas que los ejecutivos pueden hacer ahora


**Gráfica: Deloitte University Press | DUPress.com**

Los avances tecnológicos les están dando a las organizaciones la oportunidad para comenzar a moverse más allá de las contraseñas – y deben considerar seriamente darse esa oportunidad, especialmente en la media en que las amenazas cibernéticas se amplían. Dados la pobre experiencia que el usuario tiene con los mecanismos de contraseñas, los costos en aumento, y las debilidades de la seguridad, las compañías deben considerar migrar hacia los nuevos sistemas de autenticación digital que cumplen con los dos objetivos de fortalecer la protección y mejorar la experiencia del usuario.

Las organizaciones pueden iniciar su camino mediante comenzar a invertir en soluciones de autenticación no-basadas-en-contraseñas, haciéndolo como parte de sus esfuerzos de transformación digital, tal como la adopción rápida de plataformas de software-como-un-servicio e iniciativas omnicanal♦ para el compromiso del cliente. Esas nuevas áreas de solución pueden servir como el fundamento para iniciativas de autenticación más amplias para la empresa, lo cual puede llevar tiempo. Si bien durante algún tiempo podemos tener que vivir con las contraseñas dadas las restricciones de las plataforma heredada y dadas las limitaciones de tecnología, no hay razón para demorar la integración de iniciativas de autenticación que no sean contraseñas. **DR**.

♦ En el original: 'omnichannel' = omnicanal = múltiples canales transversales (N del t).

***Mike Wyatt*** *es el director administrativo de la práctica Cyber Risk Services de Deloitte & Touche LLP, donde lidera los servicios de solución digital e identidad de la empresa para la práctica Advisory de Deloitte.*

***Irfan Saif*** *es director en la práctica Cyber Risk Services de Deloitte & Touche LLP'. Sirve como el líder del sector de US Advisory Technology y también es líder del programa CIO de Deloitte y de la práctica Cyber Risk.*

***David Mapgaonkar*** *es director en la práctica Cyber Risk Services de Deloitte & Touche LLP, especializado en administración de identidad y acceso.*

*Los autores desean darles las gracias a* ***Abhi Goel****,* ***Colin Soutar****, y* ***Ian Glazer*** *por sus importantes contribuciones a este artículo.*

**NOTAS FINALES**

[1] LaunchKey, *The decentralized authentication and authorization platform for the post-password era*, May 2015, https://launchkey.com/white-paper.
[2] Para más sobre los costos ocultos de los ataques cibernéticos, particularmente en relación con propiedad intelectual, vea Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 2016, http://dupress.com/articles/loss-of-intellectual-property-ip-breach.
[3] Brian X. Chen, "Apps to manage passwords so they are harder to crack than 'password,'" *New York Times*, January 20, 2016, www.nytimes.com/2016/01/21/technology/personaltech/apps-to-manage-passwords-so-they-are-harder-to-crack-than-password.html.
[4] Guillaume Desnoës, "How will we manage 200 passwords in 2020?," *ITProPortal*, September 13, 2015, www.itproportal.com/2015/09/13/how-will-we-manage-200-passwords-in-2020/; Steve Cook, "Could biometric give us a world without passwords?," LinkedIn Pulse, September 17, 2015, www.linkedin.com/pulse/could-biometrics-give-us-world-without-passwords-steve-cook.
[5] Ian Barker, "84 percent of people support eliminating passwords," *BetaNews*, October 2015, http://betanews.com/2015/08/27/84-percent-of-people-support-eliminating-passwords/.
[6] Hossein Bidgolli, editor, *Handbook of Information Security* (Hoboken, NJ: John Wiley & Sons, 2006), p. 434.
[7] Ibid, p. 433.
[8] RoboForm, "Password security survey results," www.roboform.com/blog/password-security-survey-results, accessed April 5, 2016.
[9] Rob Waugh, "What are the alternatives to passwords?," *WeLiveSecurity*, February 5, 2015, www.welivesecurity.com/2015/02/05/alternatives-passwords/.
[10] Chris Hoffman, "Why you should use a password manager and how to get started," *How-To Geek*, September 9, 2015, www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/.
[11] Kim Zetter, "Hacking team's leak helped researchers hunt down a zero-day," *Wired*, January 13, 2016, www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/.
[12] RoboForm, "Password security survey results—part 1," http://www.roboform.com/blog/password-security-survey-results, accessed April 21, 2016.
[13] Kevin Cunningham, "Password management problems: Employees significantly increasing risk of security breaches," SailPoint, January 29, 2015, http://www.sailpoint.com/blog/2015/01/survey-password-management/.
[14] Ibid.
[15] Jeremy Quittner, "Why the 'Internet of Things' nabbed $1 billion in VC in 2013," *Inc.*, March 20, 2014, www.inc.com/jeremy-quittner/venture-capital-flows-to-gadget-and-hardware.html; Chris Quintero, "Who invests in hardware startups?," *TechCrunch*, September 12, 2015, http://techcrunch.com/2015/09/12/who-invests-in-hardware-startups/.
[16] Ian Glazer, interview with Mike Wyatt, February 10, 2016, in Austin, TX.
[17] See David Schatsky and Craig Muraskin, *Beyond bitcoin: Blockchain is coming to disrupt your industry*, Deloitte University Press, December 7, 2015, http://dupress.com/articles/trends-blockchain-bitcoin-security-transparency/.
[18] Visa Europe, "Generation Z ready for biometric security to replace passwords," January 12, 2015, www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords.
[19] FIDO Alliance, "About the FIDO Alliance," https://fidoalliance.org/about/overview/, accessed April 5, 2016.
[20] PYMNTS.com, "Is it time to cash in PINs for biometrics?," January 28, 2016, www.pymnts.com/news/biometrics/2016/is-it-time-to-cash-in-pins-for-biometrics/.
[21] Mark Hachman, "Microsoft's Windows Hello will let you log in to Windows 10 with your face, finger, or eye," *PCWorld*, March 17, 2015, www.pcworld.com/article/2898092/microsofts-windows-hello-will-let-you-log-in-to-windows-10-with-your-face-finger-or-eye.html; Hachman, "Hands on: Without apps, Intel's RealSense camera is a puzzle," *PCWorld*, March 5, 2015, www.pcworld.com/article/2893270/hands-on-without-apps-intels-realsense-camera-is-a-puzzle.html.
[22] Beverly Zena Janelinao, "Project Abacus: Google's plan to get rid of the password," *Travelers Today*, January 25, 2016, www.travelerstoday.com/articles/21353/20160125/project-abacus-google-s-plan-to-get-rid-of-the-password.htm.
[23] Tom Maxwell, "Smart Lock Passwords is cool, but Google Project Abacus puts us closer to a password-free world," 9to5Google, May 29, 2015, http://9to5google.com/2015/05/29/smart-lock-passwords-is-cool-but-google-project-abacus-wants-to-eliminate-password-authentication/.
[24] Centrify, "U.S. businesses lose more than $200,000 annually from employees struggling with passwords," October 14, 2014, www.centrify.com/about-us/news/press-releases/2014/us-businesses-lose-more-than-200-000-annually-from-employees-struggling-with-passwords/.
[25] Ibid.
[26] Robert Johnston, "Linking complaint management to profit." *International Journal of Service Industry Management* 12, no. 1 (2001): pp. 60–69 (2001).

[27] Maya Kamath, "Hackers are using password recovery scam to trick victims into handing over their email account access," *TechWorm*, June 21, 2015, www.techworm.net/2015/06/hackers-are-using-password-recovery-scam-to-trick-victims-into-handing-over-their-email-account-access.html.
[28] IBM MaaS60, *Mobile: The new hackers' playground, Data Breach Today,* February 6, 2016, www.databreachtoday.com/whitepapers/mobile-new-hackers-playground-w-2243.
[29] Archibald Preuschat, "Watch out, your fingerprint can be spoofed, too," *Wall Street Journal*, February 24, 2016, http://blogs.wsj.com/digits/2016/02/24/watch-out-your-fingerprint-can-be-spoofed-too/?mod=ST1.