eBook

# Más allá de las contraseñas: Una guía de la autenticación biométrica

¿Cuál es el estado actual de la biometría y cómo evaluar la solución adecuada para proporcionar a los clientes de confianza acceso a sus cuentas?

Mitek

# Las contraseñas son una reliquia del pasado

Las contraseñas son una solución de acceso para clientes de confianza que entraña dificultades y resulta altamente imperfecta. Por un lado, pedir a los clientes que confirmen su identidad en cada interacción solo provoca frustración y abandono, y, por otro, las contraseñas dejan a los clientes vulnerables al robo de identidades y a los ataques de apropiación de cuentas.

Tanto para las firmas de servicios financieros como para sus clientes, los riesgos y los costes asociados a las contraseñas superan de lejos las ventajas.

La tecnología biométrica combinada con dispositivos del consumidor disponibles de forma generalizada es una forma más segura y práctica de autenticar la identidad de los clientes. Pero no todos los métodos son iguales. En este ebook, te explicamos por qué y analizamos opciones que debes considerar en el camino hacia un futuro en el que desaparecerán las contraseñas a favor de la autenticación biométrica mediamente dispositivos.

## CONTENIDOS

# El problema de las contraseñas

Las contraseñas han sido los cimientos del acceso digital y la autenticación de identidades durante décadas. Sin embargo, las contraseñas sencillas (incluso las reforzadas con factores adicionales como los códigos de acceso de un solo uso) ya no son suficientes para defendernos contra determinados agentes maliciosos. A continuación, exponemos algunos de los principales motivos por los que tantas organizaciones están buscando alternativas a las contraseñas:

## VULNERABLES A LOS ATAQUES

Para los piratas informáticos, las contraseñas son escandalosamente fáciles de robar, interceptar o adivinar. Las organizaciones pueden combatir estas vulnerabilidades con factores adicionales como las contraseñas de un solo uso o los tokens, pero también estas estrategias tienen debilidades bien documentadas que los piratas informáticos pueden aprovechar.

## INCREMENTO DE LOS COSTES

Una de las principales razones por las que los clientes contactan con un centro de atención telefónica es para restablecer contraseñas. Los restablecimientos de contraseñas y los bloqueos de cuentas requieren todos los años cantidades ingentes de recursos en el servicio de atención telefónica y el servicio informático, además de un tiempo que se podría dedicar a proyectos más estratégicos. Según Forrester, el coste medio en mano de obra de restablecer una sola contraseña es de unos 70 $.

## DEFICIENCIAS EN LA EXPERIENCIA DEL CLIENTE

Cada vez se tienen más cuentas en internet y más contraseñas que recordar. Los clientes están cansados de las contraseñas, eligen muchas veces contraseñas débiles y las utilizan para varias cuentas, lo que los hace aún más vulnerables a los ataq

**Más del 80 % de los accesos no autorizados a aplicaciones web se pueden atribuir a credenciales robadas.**

Informe de investigación de filtración de datos de 2021, Verizon.

**El coste medio en mano de obra de los servicios de asistencia al cliente de restablecer una sola contraseña es de unos 70 $.**

Investigación de Forrester

**El usuario medio tiene unas 100 contraseñas.**

Estudio de NordPass, 2020



[1] The top 12 password-cracking techniques used by hackers, IT Pro, February 2022.

# Hacia un futuro sin contraseñas

Ante estas dificultades, no sorprende que la autenticación sin contraseñas sea un tema candente..

**“El 91% de las organizaciones afirman que detener los ataques basados en las credenciales es su prioridad nº 1 cuando buscan formas de implementar la autenticación sin contraseñas.”**

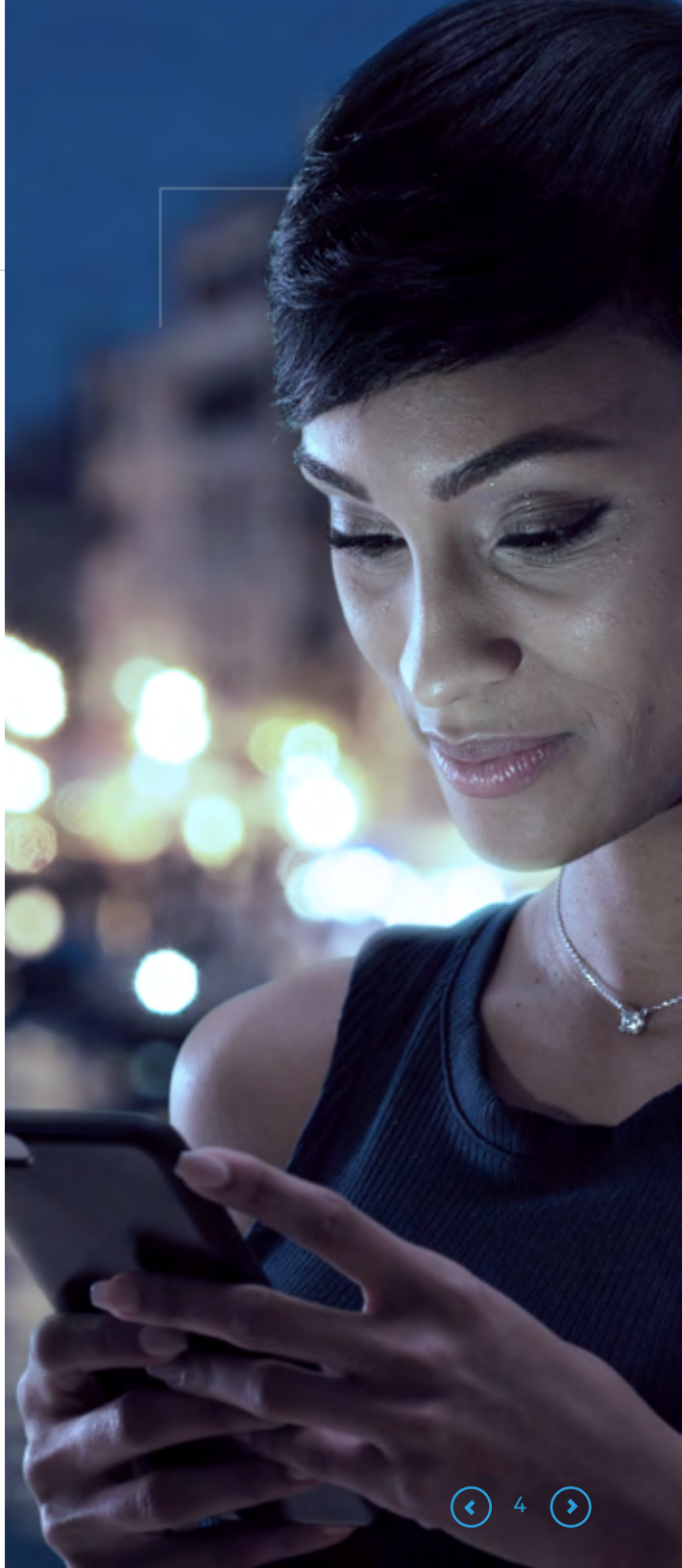
2021 State of Passwordless Security, by Cybersecurity Insiders

Reducir la necesidad de contraseñas es, obviamente, el primer paso para un futuro sin contraseñas. Para ello, muchas organizaciones han puesto la mirada en la autenticación biométrica mediante dispositivos. En lugar de introducir una contraseña, ¿por qué no permitir a los clientes el acceso a sus cuentas con un selfie o una huella?

La proliferación de dispositivos inteligentes nos ha acercado esta meta. Las interfaces biométricas son estándar en prácticamente todos los smartphones y portátiles. Los dispositivos más recientes, como el iPhone X y el Microsoft Surface Pro 8, incluyen funciones de reconocimiento facial. La generalización de dispositivos equipados con potentes cámaras, micrófonos y lectores de huellas hacen que resulte más fácil capturar datos biométricos con precisión y a escala. Y los clientes actuales, que se sienten cómodos con la biometría en su vida

**“El 64% de los clientes confían en la biometría frente a las contraseñas tradicionales y las preguntas basadas en conocimiento.”**

Javelin 2021 Identity Fraud Study



# La biometría como alternativa a las contraseñas

Para comprender cómo la biometría puede abordar las vulnerabilidades de las contraseñas, comenzaremos viendo los métodos de autenticación en la práctica.

La autenticación es el proceso que utilizan las organizaciones para comprobar la identidad digital del cliente. ¿Es la persona que está intentando acceder a nuestros sistemas realmente el cliente de confianza que dice ser? Los métodos actuales emplean uno o más factores: algo que la persona sabe, algo que la persona tiene o algo que la persona es. Cuantos más factores se empleen, más difícil será para los atacantes conseguir acceder a la cuenta de sus clientes.

Para proteger contra el robo de identidad y cumplir con la normativa (SCA), muchas instituciones financieras han implementado la autenticación de dos factores (2FA) o la autenticación multifactorial (MFA) para proteger con confianza el acceso de los clientes a sus cuentas de internet.

Aunque la autenticación 2FA y MFA son avances importantes hacia una mejor gestión de la identidad y del acceso, los factores adicionales pueden añadir fricción a la experiencia del cliente. Y el mero hecho de sumar factores puede no ser suficiente. Por ejemplo, las preguntas y respuestas basadas en conocimientos pueden conseguirse fácilmente con ingeniería social; los tokens se pueden robar; las notificaciones push se pueden aceptar erroneamente por rutina, y los códigos de un solo uso enviados por SMS o texto se pueden frustrar fácilmente cambiando la tarjeta SIM.

Muchas organizaciones ven la autenticación biométrica mediante dispositivos como un factor de autenticación más seguro y práctico que los métodos basados solo en contraseñas o en contraseñas y 2FA.


## Algo que la persona sabe

Una contraseña o respuestas a preguntas de seguridad.

## Algo que la persona tiene

Un teléfono móvil o token.

## Algo que la persona es

Una característica biométrica inherente, como la cara, huella o voz.

# Evaluación de los métodos biométricos de autenticación mediante dispositivos

Ofrecer a los clientes la opción de acceder a sus cuentas utilizando funciones de biometría de sus dispositivos en lugar de contraseñas suele consistir en uno de dos métodos, y cada uno de ellos tiene sus implicaciones en lo que respecta a comodidad y segurida

**La autenticación biométrica en el dispositivo** | Cloud-based biometric authentication

Apple, Google, Microsoft y otros han unido fuerzas con la FIDO Alliance para habilitar la autenticación sin contraseñas en dispositivos de consumidor de uso común. Las organizaciones de servicios financieros que emplean los protocolos FIDO permiten a sus clientes usar sus dispositivos móviles para iniciar sesión en cuentas online automáticamente usando la detección facial o el reconocimiento de huellas digitales para verificar su identidad.

Pero, ¿qué ocurre si falla la biometría? El dispositivo suele volver de manera predeterminada a un código de acceso (normalmente un código muy sencillo de cuatro dígitos) o pide al usuario las credenciales de inicio de sesión y una contraseña, lo que añade fricción y resulta relativamente fácil de frustrar. Como la mayoría de los ataques basados en credenciales, el eslabón más débil es el humano. Es bien sabido que la gente registra las caras y huellas de sus amigos y familiares en sus dispositivos, y los sensores de los dispositivos no son a prueba de esto.

Las organizaciones de servicios financieros con estrictos requisitos de conocimiento del cliente (KYC, como se conoce por sus siglas en inglés) y baja tolerancia al riesgo, la autenticación biométrica en dispositivos puede no ser suficiente. El mero hecho de que una persona pueda desbloquear un dispositivo con su cara o huella no demuestra que sea el propietario legítimo de la cuenta.

## ¿Qué es FIDO2?

El propósito del estándar FIDO2 es eliminar las contraseñas utilizando tokens criptográficos multifactoriales.

FIDO2 utiliza WebAuthn en segundo plano, un estándar abierto que permite a la criptografía de claves públicas fuertes garantizar la presencia del usuario en el punto de autenticación.

Los dispositivos compatibles con FIDO2 utilizan claves digitales únicas que son fáciles de usar e inexpugnables para los ladrones. Son claves que no se pueden compartir y se almacenan en el dispositivo del cliente. Los usuarios acceden a sus credenciales de inicio de sesión en FIDO desbloqueando su dispositivo con su cara o huella.



[2] Can fingerprint authentication on smartphones be fooled with 3D printing? Researchers find out, ZDnet, April 2020.

# Evaluación de los métodos biométricos de autenticación mediante dispositivos

Ofrecer a los clientes la opción de acceder a sus cuentas utilizando funciones de biometría de sus dispositivos en lugar de contraseñas suele consistir en uno de dos métodos, y cada uno de ellos tiene sus implicaciones en lo que respecta a comodidad y segurida

La autenticación biométrica en el dispositivo | Autenticación biométrica basada en la nube

Las empresas que desean una solución compatible con todas las plataformas implementan la autenticación biométrica directamente en su experiencia de cliente online o aplicaciones móviles. En este caso, la biometría permite un factor de autenticación independiente del dispositivo, un auténtico segundo factor. Utilizando cualquier smartphone u ordenador con capacidades biométricas, los clientes inician sesión en sus cuentas de forma segura comparando su cara o voz con una plantilla de datos biométricos verificados que se tiene registrada. No se requiere ningún PIN ni contraseña. Y, si el dispositivo se pierde o roba, nadie que consiga desbloquear el dispositivo conseguirá acceder a las cuentas online del propietario.

Con este método, las organizaciones pueden usar de forma fácil y segura la comparación de datos biométricos del lado del servidor basada en la nube, y no depender del dispositivo único del cliente. Soluciones de otros fabricantes pueden proporcionar a las organizaciones más control sobre el registro del cliente y la configuración, incluyendo, por ejemplo, la elección de las modalidades biométricas (cara, voz o ambas cosas) según la tolerancia al riesgo y las necesidades empresariales.

## INDEPENDIENTE DEL DISPOSITIVO

Accesible desde cualquier dispositivo con capacidades biométricas

## REFORZADA CON IA

Algoritmos entrenados con IA garantizan una autenticación precisa y sin sesgos

## MULTIMODAL

Capas de comprobaciones de cara, voz y vida para protección adicional

## Comparación de métodos de autenticación biométrica

| | La autenticación biométrica en el dispositivo | La autenticación biométrica basada en la nube |
|---|---|---|
| **Experiencia de usuario Sencilla** | Sencilla | Sencilla |
| **Método de verificación biométrica** | Face ID, Touch ID, Windows Hello, etc. | Cara y voz, incluida la detección de vida, incluidos en la UX |
| **Fortaleza del factor de autenticación** | Una sola señal biométrica | Señales biométricas única, multimodal o dinámica según el caso práctico |
| **Umbrales de aprobación** | No personalizable | Totalmente personalizable |
| **Niveles de seguridad** | Varían según la implementación | Capas de verificación alta e incremento gradual, según la necesidad |
| **Precisión para bloquear a los estafadores** | El acceso a los dispositivos se puede hackear o compartir | Los algoritmos de comparación de datos biométricos pueden evolucionar más rápido, al ritmo de las nuevas amenazas |
| **Independiente de los dispositivos** | Todavía no | Sí |
| **Antisesgo** | Las cámaras de los smartphone presentan debilidades bien conocidas[3] | Algoritmos formados y probados contra datos equilibrados y representativos ayudan a eliminar el sesgo en la biometría |



[3] Can better tech really fix darker-skin bias in smartphone cameras? Google thinks so, CBC, February 2022.

# Consideraciones adicionales

Aunque es posible brindar a los clientes acceso a sus cuentas con solo un detector de caras o una huella en su smartphone, las empresas pueden incrementar la protección utilizando la biometría como factor de autenticación independiente del dispositivo.

**¿Qué debe tener en cuenta a la hora de evaluar la biometría como una alternativa a las contraseñas?**

## 1 COSTE DE IMPLEMENTACIÓN

Utilizar los dispositivos que los clientes ya tienen es el primer paso para reducir el coste de implementación de la autenticación biométrica. Busca soluciones que puedan implementarse de forma rápida en la nube o soluciones nativas en plataformas iOS y Android, que no requieran inversión en servidores nuevos y dedicados o que no requieran costes adicionales de almacenamiento y administración de plantillas biométricas que cumplan con las leyes internacionales y nacionales.

## 2 MÚLTIPLES MODALIDADES BIOMÉTRICASS

Cada caso práctico requerirá una combinación de comodidad y seguridad en diferentes proporciones. Ten en cuenta si la solución permite añadir capas de modalidades biométricas, añadir la prueba de vida para una protección aún más fuerte o implementar medidas de incremento progresivo cuando esté justificado. Sumar capas de modalidades biométricas (la combinación de detección de cara y voz) es 100 veces más efectivo para detener a los estafadores que usar solo la detección de la cara o solo la voz.[4]

## 3 PRECISIÓN

La precisión de la autenticación biométrica depende de dos errores: la tasa de aceptación errónea (FAR, por sus siglas en inglés), que calcula el acceso concedido a personas no autorizadas, y la tasa de denegación errónea (FRR), que mide el acceso denegado a clientes autorizados. Las tasas de error se pueden producir a causa de factores ambientales (las condiciones en las que se captura la imagen de la cara o el patrón de voz), cuando la gente envejece o, incluso, si cambia de género. Busca soluciones con algoritmos de comparación sofisticados y que se actualicen constantemente para garantizar mejor el acceso a los buenos clientes, pero bloquear el acceso a los estafadores.

## 4 ALMACENAMIENTO DE DATOS BIOMÉTRICOS

La elección entre almacenar datos biométricos en el dispositivo del cliente o en servidores independientes requiere un detenido estudio. Las soluciones de otros fabricantes mantienen los datos biométricos guardados de forma segura en un lugar aparte del dispositivo y vinculados al usuario, en lugar de al dispositivo, lo que proporciona una seguridad mucho mayor sin añadir fricción adicional. Los usuarios pueden cambiar de dispositivo sin tener que volver a registrar sus datos biométricos. Busca proveedores de soluciones que garanticen que tu empresa cumple en todo momento con las cambiantes prácticas recomendadas de seguridad de datos y los complejos requisitos reguladores.



[4] ID R&D internal analysis

# Consideraciones adicionales

## 5 DEFENSA CONTRA EL FRAUDE SINTÉTICO Y EL SESGO

Las tecnologías basadas en inteligencia artificial (IA) específicas para la detección de cara y voz son más seguras y sofisticadas en la defensa contra los ataques de apropiación de cuentas. Soluciones de otros fabricantes también ofrecen la posibilidad de comprobar si los nuevos usuarios están incluidos en listas de estafadores reincidentes, mientras que la biometría para consumidores, no. Busca soluciones que permitan la detección activa o pasiva de vida, que puedan detectar trampas (máscaras, fotos o vídeos de caras) y que hayan superado las pruebas de laboratorios independientes de la norma ISO 30107- 3 para detección de ataques de presentación. Los algoritmos entrenado y probados constantemente en este tipo de escenarios, usando conjuntos de datos grandes y representativos, son más capaces de ofrecer autenticación a prueba de trampas y resultados precisos independientemente de la raza, grupo étnico, edad o género.

## 6 EXPERIENCIA DEL USUARIO

Asegúrate de que tus flujos de autenticación capturan los datos biométricos del cliente en una experiencia segura, sin contratiempos ni molestias, fundada en la confianza y la velocidad. Capturar la información biométrica de forma precisa y rápida es fundamental, así como evitar la fricción adicional, ya sea añadiendo una capa más a la experiencia o, lo que es peor, pidiendo al cliente que contacte con el equipo de asistencia técnica. Busca soluciones que proporcionen un proceso de registro, autenticación o recuperación sencillo para todos los grupos de usuarios, tipos de dispositivos y plataformas de software.

# Casos prácticos comunes en los servicios financieros

Ve cómo están sustituyendo las organizaciones de servicios financieros las contraseñas con datos biométricos para empresas en una gran variedad de casos prácticos.

## Ofrece un inicio de sesión más seguro y sencillo

**Ofrece a los clientes de confianza la opción de registrar sus datos biométricos como una forma más segura y sencilla de acceder a sus cuentas.**

**Cómo funciona:**

Cuando va a iniciar sesión, Jessica recibe instrucciones sobre cómo hacerse un selfie y grabar una frase para registrar su plantilla biométrica. La siguiente vez que Jessica inicie sesión, podrá hacerlo con un selfie o un patrón de voz que se compara de forma rápida y fiable con la plantilla que se tiene archivada.

**Ventajas:**

Las contraseñas son una molestia para los clientes y, además, son susceptibles de ataques. Los datos biométricos son únicos para cada persona, y a los estafadores les resultan extremadamente difíciles de imitar.

## Evita los fraudes de robo de cuentas

**Captura y registra una plantilla biométrica durante el proceso de onboarding que se utilizará durante todo el ciclo de vida del cliente.**

**Cómo funciona:**

Durante el proceso inicial de onboarding, la identidad de Susan se verifica usando una combinación de la captura de su documento de identidad (¿es el documento legítimo?) y los datos biométricos faciales en directo (¿es la propietaria genuina del documento?). Los datos biométricos capturados se almacenan de forma segura como una plantilla. Cuando Susan acceda a su cuenta en el futuro, o se presente a nuevas ofertas, un nuevo selfie o patrón de voz se comparará con la plantilla almacenada. Si coincide, Susan obtendrá la autenticación.

**Ventajas:**

La información biométrica se almacena en un lugar independiente del dispositivo, lo que elimina problemas como los cambios de tarjeta SIM que permiten a usuarios no autorizados a obtener acceso a cuentas con tan solo desbloquear el dispositivo.

## Reducir el tráfico del centro de atención telefónica

**Empoderar a los clientes con un acceso seguro de autoservicio para el restablecimiento de contraseñas y los cambios en las cuentas.**

**Cómo funciona:**

Jeff es un cliente de confianza del banco y tiene una plantilla biométrica guardada. Recientemente, se ha divorciado, por lo que necesita quitar a su exmujer de sus cuentas. Lo que antes habría exigido la ayuda de un agente del servicio de atención al cliente, ahora se puede hacer fácilmente utilizando un nuevo selfie o patrón de voz, que se contrasta con la plantilla que tiene guardada, para acceder a su perfil y realizar los cambios en su cuenta.

**Ventajas:**

La información biométrica proporciona una capa de protección que es mucho más efectiva que las contraseñas a la hora de aportar los niveles de seguridad que requieren los bancos para las actividades de los clientes que entrañan más riesgo.

# Resumen

## Una autenticación biométrica segura y sin fricción para la empresa

Las organizaciones de servicios financieros se encuentran con la difícil tarea de reforzar la seguridad sin que ello afecte a la experiencia de usuario global. La tecnología biométrica puede ofrecer una forma fiable de autenticar a los clientes sin necesidad de contraseñas. Es importante evaluar soluciones que no solo puedan ofrecer una experiencia sin fricción para buenos clientes, sino, además, ofrecer la seguridad, el control y la flexibilidad que las firmas de servicios financieros necesitan.



## Descubre cómo puede Mitek ayudar con MiPass

gracias sus innovadoras funciones biométricas de reconocimiento facial y de voz, a proporcionar una protección mejorada contra las formas más sofisticadas y actuales de robo de identidades y de técnicas de fraude cada vez más peligrosas, como los deepfakes y las identidades sintéticas. Estas tecnologías garantizan el más alto nivel de seguridad contra las nuevas amenazas con una experiencia superior para el consumidor..

Más información en
www.miteksystems.com/es

Saber más

Mitek