



## Claves de acceso: un paso más cerca de un futuro sin contraseñas

Ante el significativo aumento de ciberataques respaldados por los Estados y la creciente presencia de agentes malintencionados, nos esforzamos más que nunca por **proteger** a las personas, las empresas y los gobiernos. Para lograr este objetivo y contribuir a crear un mundo más seguro para todos, compartimos nuestra experiencia, **capacitamos** a la sociedad y **avanzamos** constantemente en el ámbito de la ciberseguridad.

Hoy en día las contraseñas son fundamentales para la seguridad online, pero resultan insuficientes frente a amenazas como la suplantación de identidad, que se conoce como "phishing". Hace tiempo que en Google somos conscientes de estos desafíos y, por eso, promovemos el uso de herramientas de autenticación como la verificación en dos pasos (2SV), el Gestor de contraseñas de Google, las llaves de seguridad y, ahora, las llaves de acceso.

### El reto

A lo largo de más de 60 años, las contraseñas han sido una herramienta clave en informática. Sin embargo, en la actualidad, ya no son suficientes para garantizar la seguridad de los datos de usuarios y organizaciones. Los ataques de phishing siguen aumentando en escala y complejidad aprovechando las vulnerabilidades inherentes a las contraseñas. Por ejemplo:

- ✓ Más del **60 % de las filtraciones de datos** en 2021 estaban relacionadas con robos de credenciales o suplantación de identidad.<sup>1</sup>
- ✓ En 2022, las filtraciones de datos causadas por ataques de phishing costaron a las organizaciones un promedio de **4,91 millones de dólares**.<sup>2</sup>
- ✓ Los ataques de phishing aumentaron un **61 %** en 2022, alcanzando la cifra de 255 millones en un periodo de seis meses.<sup>3</sup>

La verificación en dos pasos/autenticación de dos factores (2SV/2FA) es muy útil, pero también complica el proceso para los usuarios. Además, no proporciona una protección completa contra ataques de phishing y técnicas selectivas, como los "duplicados de SIM" utilizados para la verificación por SMS.

### La solución

En colaboración con FIDO Alliance, hemos habilitado la compatibilidad con las llaves de acceso, una alternativa más sencilla y segura a las contraseñas que pone al alcance de miles de millones de personas de todo el mundo una tecnología a prueba de phishing. Con las llaves de acceso, puedes prescindir de tu contraseña y disfrutar de una experiencia de inicio de sesión más fácil y segura utilizando tu huella dactilar, el reconocimiento facial o el bloqueo de pantalla.

Las llaves de acceso están disponibles para las cuentas personales de Google y para los usuarios de más de 9 millones de clientes de Google Workspace, así como para sitios y aplicaciones de terceros en Chrome y Android desde principios de 2023.



#### La forma más rápida y sencilla de iniciar sesión

Las llaves de acceso son **4 veces más fáciles** de usar porque no necesitas recordar ni escribir nada. Solo tienes que utilizar tu huella dactilar, el reconocimiento facial o el bloqueo de pantalla para iniciar sesión en todos tus dispositivos y plataformas.<sup>4</sup>

#### Seguridad de cuenta de última generación

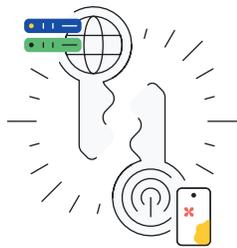
Las llaves de acceso ofrecen la máxima protección contra amenazas como el phishing. Al estar almacenadas en tu dispositivo local, resulta imposible adivinarlas o reutilizarlas, lo que permite mantener tu información a salvo de los atacantes.

#### Privacidad exclusivamente tuya

Tu llave de acceso permanece de forma privada en tu dispositivo personal y nunca se comparte con Google ni con terceros. Solo tendrás que usar tu huella dactilar, el reconocimiento facial o el bloqueo de pantalla para verificar que eres tú quien intenta acceder a tu clave privada.



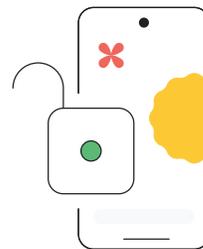
## Cómo funciona



Una llave de acceso consta de dos partes: una clave pública en el servidor web donde inicias sesión y la correspondiente clave privada en tus dispositivos.



Al iniciar sesión, el sitio web comprueba si tu clave pública corresponde con tu clave privada.



Para esta verificación, lo único que tienes que hacer es desbloquear tu dispositivo.



Podrás iniciar sesión en tu cuenta, sabiendo que tu clave privada y tus datos biométricos están a salvo en tu dispositivo y nunca se comparten con terceros.

## Un ecosistema más seguro

### Llaves de acceso para empresas y administraciones públicas

Las llaves de acceso ofrecen importantes ventajas de seguridad y facilidades de uso. Estamos encantados de ser el primer gran proveedor de nube pública en ofrecer esta tecnología a nuestros clientes, desde pequeñas y grandes empresas hasta instituciones educativas y administraciones públicas.

### Juntos, para un inicio de sesión en la red más seguro y sin contraseñas

Colaboramos con las empresas para permitir el uso de llaves de acceso en las plataformas de Chrome y Android y proporcionar a sus usuarios un acceso más sencillo y seguro. Contamos con numerosos colaboradores de sectores como el comercio electrónico, la tecnología financiera y los viajes, entre otros, que ya se han unido a nosotros en este camino hacia un futuro sin contraseñas: 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal y Yahoo! Japón.

## Nuestro camino hacia un futuro sin contraseñas

Las llaves de acceso nos acercan mucho más al futuro sin contraseñas que llevamos más de una década proyectando.

2008	2011	2012	2013	2014	2017	2019	2023
Lanzamos el Gestor de contraseñas de Google para facilitar y proteger los inicios de sesión.	Habilitamos la verificación en dos pasos (2SV) en las cuentas de Google.	Introducimos una clave de seguridad a prueba de phishing para los empleados de Google.	Nos incorporamos a la FIDO Alliance para impulsar estándares abiertos para un mundo sin contraseñas.	Ampliamos el acceso a las claves de seguridad a prueba de phishing a todos los usuarios.	Presentamos el Programa de Protección Avanzada para usuarios de alto riesgo.	Ampliamos la compatibilidad con FIDO en Android para la reautenticación sin contraseña en sitios web.	Habilitamos las llaves de acceso para las cuentas de Google, los clientes de Workspace y los colaboradores externos en Chrome y Android.

Aunque las contraseñas seguirán formando parte de nuestras vidas durante la transición a las llaves de acceso, nos comprometemos a ayudar a los usuarios, y a otros miembros del sector, a dar el siguiente paso para lograr un inicio de sesión más sencillo y seguro con Google.

Fuentes: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023 | 3 - CNBC's Cyber Report | 4 - Google Security Blog, May 2023