El jueves, Google presentó un nuevo PIN para su Administrador de Contraseñas, que permitirá a los usuarios de Chrome sincronizar sus claves de acceso en dispositivos con Windows, macOS, Linux, ChromeOS y Android.

> *«Este PIN proporciona una capa adicional de seguridad para garantizar que tus claves de acceso estén cifradas de extremo a extremo y no puedan ser accedidas por nadie, ni siquiera por Google»*, explicó Chirag Desai, gerente de producto de Chrome.

De manera predeterminada, el PIN es un código de seis dígitos, pero los usuarios pueden optar por crear un PIN alfanumérico más extenso eligiendo la opción *«Opciones de PIN»*.

Este lanzamiento supone un cambio con respecto a la funcionalidad anterior, donde las claves de acceso solo podían guardarse en el Administrador de Contraseñas de Google en Android.

Aunque era posible utilizar las claves en otras plataformas, se necesitaba escanear un código QR con el dispositivo en el que se generaron.

Con la nueva actualización, ese paso se elimina, lo que hace que sea mucho más sencillo para los usuarios iniciar sesión en servicios en línea utilizando claves de acceso, simplemente escaneando sus datos biométricos. Google también mencionó que próximamente se añadirá soporte para iOS.

Sin embargo, para usar las claves de acceso en un nuevo dispositivo, los usuarios deben conocer el PIN del Administrador de Contraseñas o el bloqueo de pantalla de sus dispositivos Android.

> *«Estos factores de recuperación te permitirán acceder de manera segura a tus claves de acceso guardadas y sincronizar nuevas entre tus computadoras y*

> *dispositivos Android»,* afirmó Desai.

Este avance llega después de que la empresa tecnológica informara que más de 400 millones de cuentas de Google ya utilizaban claves de acceso hasta mayo de 2024. Dos meses después, esta alternativa resistente al phishing se puso a disposición de usuarios de alto riesgo a través de su Programa de Protección Avanzada (APP).