

Clave Única reforzará su seguridad con nuevo sistema de doble verificación



El nuevo sistema añadirá un código temporal de verificación similar al de aplicaciones bancarias y buscará prevenir accesos indebidos a cuentas de usuarios.

Nicole Villanueva

La Secretaría de Gobierno Digital confirmó que durante este mes comenzará a operar un nuevo sistema de protección para la Clave Única, incorporando una verificación adicional mediante códigos temporales al momento de acceder a trámites en línea.

La iniciativa busca fortalecer la seguridad de las cuentas y disminuir el riesgo de accesos no autorizados, especialmente considerando el alto número de personas que utilizan la plataforma para realizar gestiones estatales.

El nuevo mecanismo llevará por nombre "pinpass" y funcionará como un segundo factor de autenticación, similar a los sistemas utilizados por aplicaciones bancarias o servicios financieros digitales. De esta manera, además de ingresar el RUT y la contraseña habitual, algunos usuarios podrán validar su identidad mediante un código dinámico generado desde una aplicación móvil.

La directora subrogante de la Secretaría de Gobierno Digital, Kareen Schramm, explicó que la herramienta operará a través de una app de autenticación. "Se trata de una aplicación de seguridad para generar un código temporal o pinpass, similar al que se utiliza en servicios como los bancos", indicó en conversación con El Mercurio.

Pese a la incorporación de esta nueva medida, desde el organismo aclararon que su uso no será obligatorio. Cada usuario podrá decidir si habi-



"Se trata de una aplicación de seguridad para generar un código temporal o pinpass, similar al que se utiliza en servicios como los bancos".

KAREEN SCHRAMM
 Directora subrogante de la Secretaría de Gobierno Digital

lita o no esta capa adicional de protección para su cuenta.

En caso de activarla, el sistema solicitará el código temporal cada vez que la persona quiera ingresar a cualquier plataforma estatal asociada a Clave Única, sin importar el sitio web o servicio público que utilice.

Según detallaron desde la

Secretaría de Gobierno Digital, el objetivo principal es reforzar la seguridad digital de millones de usuarios y reducir posibles vulneraciones relacionadas con robo de contraseñas o fraudes informáticos.

"Protege la cuenta incluso si la contraseña ha sido vulnerada, previene accesos no autorizados y refuerza la confianza en el uso de servicios digitales del Estado", sostuvo Schramm.

Actualmente, cerca de 16 millones de personas poseen Clave Única activa en Chile. Además, durante 2025 se registraron más de 482 millones de accesos exitosos a distintas plataformas estatales mediante este sistema, el cual permite ingresar a aproximadamente 1.700 portales y servicios públicos.

Respecto al proceso de activación, quienes quieran habilitar el "pinpass" deberán ingresar a su cuenta de Clave Única y dirigirse al apartado "Seguridad". Posteriormente tendrán que seleccionar la opción "Configurar Aplicación", escanear un código QR con una app de autenticación e ingresar el código temporal generado por la aplicación.

Tras completar esos pasos, la cuenta quedará protegida con esta verificación adicional.

Finalmente, las autoridades reiteraron el llamado a no compartir la contraseña personal con terceros. "Ningún funcionario público, entidad estatal o empresa autorizada debe solicitar la clave", enfatizó Schramm.

La implementación de este nuevo sistema se da semanas después de que surgieran reportes sobre una presunta filtración de datos en plataformas estatales. No obstante, la Agencia Nacional de Ciberseguridad descartó recientemente la existencia de una filtración masiva o accesos ilícitos relacionados con Clave Única.