LUN

Fecha: 03/05/2026 Audiencia: 271.020 Sección: ACTUALIDAD
Vpe: $3.164.345 Tirada: 91.144 Frecuencia: 0
Vpe pág: $4.399.200 Difusión: 91.144
Vpe portada: $4.399.200 Ocupación: 71,93%

Kareen Schramm, directora (s) de la Secretaría de Gobierno Digital, reacciona ante sospechas de que la herramienta fue hackeada

"Cambiar la ClaveÚnica con demasiada frecuencia no es recomendable"

Supuesta filtración de datos desató alarma en redes sociales y llevó a miles a plantearse cambiar su contraseña. Autoridades descartan vulneración del sistema.

MAURICIO RUIZ

La alarma se propagó en redes sociales. Bastaron pocas horas para que la supuesta filtración de datos sensibles desde servicios públicos, entre ellos la Tesorería General de la República y el Registro Civil, terminara con un efecto colateral inmediato: la ClaveÚnica se transformó en trending topic en X y miles de usuarios comenzaron a preguntarse si debían cambiarla de forma urgente; incluso, algunos lo hicieron.

El detonante fue la circulación en redes y foros de una base de datos que incluía información personal -direcciones, teléfonos y hasta antecedentes de salud-, lo que instaló la idea de un hackeo importante al Estado y a algunas empresas de telecomunicaciones.

El diagnóstico oficial fue más frío que la alharaca digital. La Agencia Nacional de Ciberseguridad (ANCI), en un documento técnico, informó: "Prácticamente la totalidad de la información publicada corresponde a datos filtrados con anterioridad".

Según la autoridad, solo una fracción menor proviene de un acceso no autorizado reciente, mediante credenciales previamente comprometidas, situación que fue contenida.

"Es difícil que haya sido un hackeo técnico y debe haber sido información que principalmente se filtró hace un tiempo. Por eso la reacción de la ANCI fue muy mesurada. Si hubiese sido un hackeo más importante, la reacción habría sido diferente", dice Giordano Castro, docente del diplomado de Ciberseguridad y Ciberdefensa de la Universidad Autónoma.

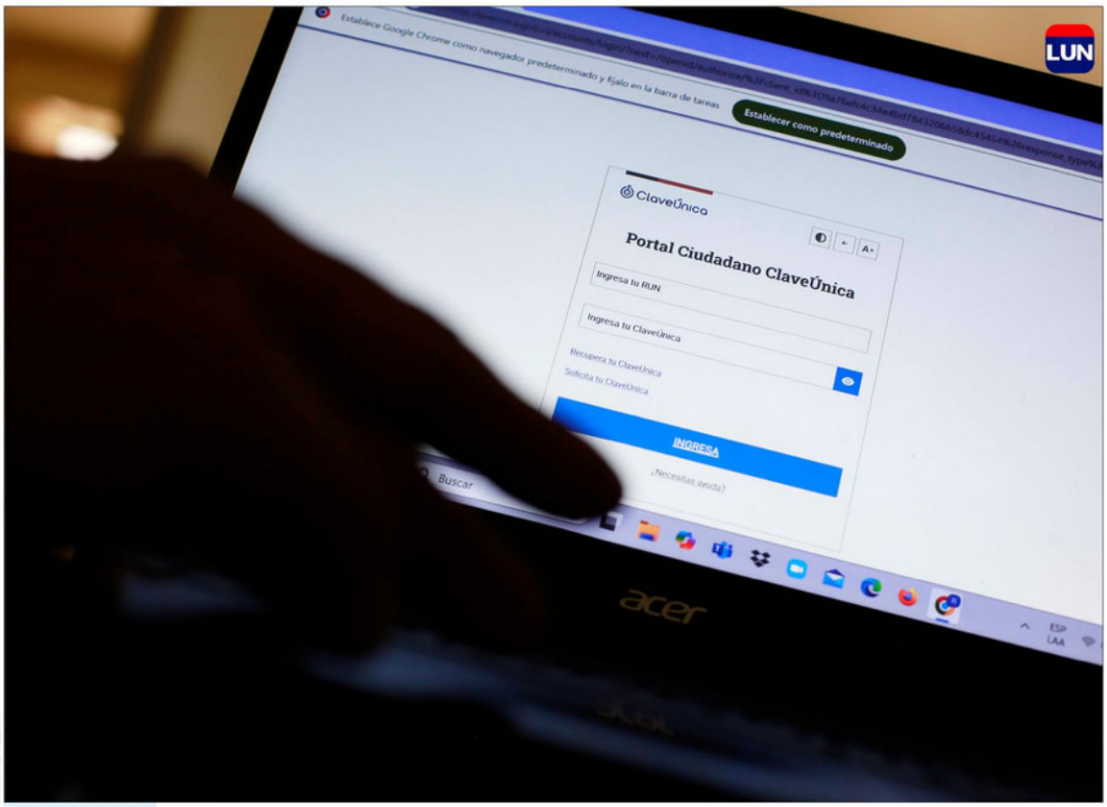
Diego Fuentealba, director del Laboratorio de IA en Contabilidad y Auditoría de la Universidad de Santiago, también duda de la magnitud del supuesto ciberataque. Explica que cuando un hacker expone información en plataformas como Telegram, como ocurrió en este caso, muchas veces busca "validación personal y demostración de capacidades", especialmente en actores menos experimentados.

"Un experimentado no expone esos datos; más bien, los utiliza", plantea.

El foco ciudadano, sin embargo, no estuvo en el origen de los datos, sino en el riesgo percibido: si la ClaveÚnica -la llave maestra para trámites del Estado y usada también en algunos servicios privados- estaba comprometida.

Ahí entró en escena la Secretaría de Gobierno Digital, dependiente del Ministerio de Hacienda y responsable de la plataforma. La entidad fue enfática: no existe evidencia de vulneración de la base de datos de ClaveÚnica ni de su operación, que ha seguido funcionando con normalidad.

Los números ayudan a dimensionar lo que estaba en juego. Al 2 de mayo, más de 16 millones de personas tienen ClaveÚnica activa. En 2024 se registraron más de 474 millones de accesos exitosos; en 2025, más de 482 millones; y en lo que va de 2026, ya se contabilizan más de 174 millones.



RICHARD ULLOA

En 16 años de funcionamiento, nunca se ha vulnerado la base de datos de la ClaveÚnica.

Confusión

La ClaveÚnica fue creada en 2010 y si bien el primer paso para obtenerla se realiza en el Registro Civil, que valida la identidad de las personas, la administración y operación de la plataforma corresponde a la Secretaría de Gobierno Digital, lo que explica parte de la confusión generada en redes en este supuesto hackeo.

"Como ocurre con múltiples plataformas digitales de alta demanda, el sistema de ClaveÚnica enfrenta de manera permanente distintos tipos de intentos de ataque y amenazas de ciberseguridad. No obstante, a la fecha, la operación del servicio se ha mantenido funcionando con normalidad y no se ha registrado una vulneración de la base de datos de ClaveÚnica", señala Kareen Schramm, directora de la Secretaría de Gobierno Digital.

Agrega que el sistema utiliza estándares internacionales de seguridad y que en los últimos años se han incorporado nuevas capas de protección. Entre ellas, mecanismos de doble autenticación, como códigos de verificación enviados al correo electrónico. Y viene más protección.

"Se está desarrollando una aplicación de seguridad que genera claves temporales, similar al sistema de pin pass que se utiliza en la banca", adelanta.

¿Hay que cambiar la ClaveÚnica cada cierto tiempo?, ¿qué lapso es recomendable?

"Contrario a lo que mucha gente piensa, cambiar la contraseña con demasiada frecuencia no es lo más recomendable, ya que esto puede derivar en prácticas inseguras, como anotarlas en cualquier parte o utilizar contraseñas más débiles. Nuestra recomendación es que la ClaveÚnica debe actualizarse principalmente cuando exista sospecha de uso indebido, filtración, compromiso de la cuenta o si se compartió con algún tercero, sea o no un conocido o familiar".

Schramm asegura que la Secretaría de Gobierno Digital, junto a la ANCI, mantiene un monitoreo permanente de filtraciones públicas. Cuando se detectan credenciales expuestas, se activan protocolos preventivos de bloqueo de cuentas y se notifica a los usuarios. Algunos de esos bloqueos coincidieron con la viralización del supuesto ataque o hackeo, lo que pudo reforzar en la ciudadanía la percepción de que la ClaveÚnica había sido vulnerada, algo que no ocurrió, recalca.