

Expertos recomiendan mayores medidas para proteger a los ciudadanos, además de avanzar en la legislación:

# Masiva obtención de datos del Servel alerta sobre vulnerabilidad de barreras de seguridad

El organismo electoral descarta que se hayan atacado sus sistemas y afirma que la información de 14,3 millones de personas que se publicó ya había estado disponible, pues la ley así los mandaba.

MANUEL HERNÁNDEZ G.

El nombre, la dirección y el RUT de todos los votantes que hubo para las elecciones de 2017 se publicaron ayer masivamente. Así lo informaron dos portales de Estados Unidos —Wizcase y ZDNet— que señalan que los datos de 14,3 millones de personas habían quedado expuestos en un servidor de internet tras una filtración (de origen desconocido) del padrón electoral del Servel. Las páginas web incluso mostraban que estaban disponibles los datos del Presidente Sebastián Piñera y de la exmandataria Michelle Bachelet.

Frente a esto, el ente encargado de los comicios emitió un comunicado en el que se “descarta cualquier vulneración a sus sistemas”, tras la difusión de datos que alcanza a casi el 80% de la población del país.

El Servel confirmó que los datos a los cuales se hace referencia son los del padrón electoral de 2017, utilizados para la última elección presidencial, y enfatizó que son públicos, tal como lo establece la Ley 18.556, que crea el Servicio Electoral y los obliga a publicar la información “en su sitio web con al menos sesenta días de anticipación a la fecha en que deba verificarse una elección”.



**INFORMACIÓN PERSONAL.**— La obtención de datos que evidenciaron medios estadounidenses obedece al padrón electoral del año 2017 y corresponde a nombres, direcciones y RUT de 14,3 millones de personas, lo que representa el 80% de la población chilena.

## Mejorar el resguardo

El abogado de la organización Derechos Digitales, Pablo Viollier, afirmó que la filtración es “grave”, pero recaló que “también es grave que el Servel haya publicado esos datos. Eso impli-

ca que el problema ya existía, porque la ley establece la publicación del padrón electoral, y ese es un problema de cómo el Estado disponibiliza innecesariamente los datos personales de los chilenos”.

Viollier sostuvo que esa infor-

mación no puede modificarse frente a una filtración, y eso solo sería posible si existiera un hackeo de datos.

Agregó que para evitar que esta situación se repita, el Servel debería establecer mecanismos de autenticación para que los datos

solo pueda consultarlos el titular y no un tercero. Además, para garantizar la transparencia de la información, sugirió “que los partidos políticos u otros entes fiscalizadores puedan revisar el padrón sin que se publiquen los datos de todos los chilenos en internet”.

Coincidió el especialista en seguridad informática de ESET Latinoamérica Miguel Angel Mendoza, quien explicó que la página web del Servel utilizaba una configuración “por defecto”, o predeterminada, que permite acceder fácilmente a la información. “Esa configuración predeterminada está pensada para cuando se utiliza en una red interna”, criticó.

Mendoza recomendó aplicar más medidas de protección a la información, como generar cuentas de usuario a quienes soliciten la información, para así limitar el acceso.

El director general de Pallavicini Consultores, César Pallavicini, atribuyó las filtraciones de datos a una falla de políticas públicas y tildó de “obsoleta” la legislación actual.

“La Ley 19.628 sobre privacidad de datos de personas lleva cinco años en el Congreso y los parlamentarios se han dado vuelta tratando de reformarla, pero a la fecha no se ha promulgado y estamos muy atrasados respecto a países desarrollados”.

Agregó que jugó en contra la salida del asesor presidencial de ciberseguridad Jorge Atton, quien asumió como intendente de La Araucanía. “Ese cargo quedó vacío varios meses y eso fue una señal positiva para los ciberdelincuentes (...). Es necesario que el Estado asigne recursos para protegerse mejor, con tecnología, políticas públicas y capacitación del personal”.