EL MERCURIO

Fecha: 25/02/2026 Audiencia: 320.543 Sección: NACIONAL
Vpe: $6.541.570 Tirada: 126.654 Frecuencia: 0
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 31,8%



Alerta dada por EE.UU., en medio de firma de decreto para cable chino:

# Fiscalía abre investigación penal, luego de que Gobierno entregara antecedentes de supuesto hackeo a empresas de telecomunicaciones chilenas

La indagatoria es instruida por la jurisdicción metropolitana Centro Norte, encabezada por Xavier Armendáriz, y se espera que las diligencias sean encargadas a la PDI.

SOFÍA FARÍAS G.

Mientras ayer seguía la polémica por la firma —y casi inmediata anulación— del decreto que aprueba la concesión de un cable de fibra óptica impulsado por la empresa China Mobile International (CMI), que interconectaría Valparaíso con Hong Kong, el Ministerio Público ya tenía abierta una investigación penal por un eventual hackeo a compañías de telecomunicaciones y una constructora locales, que se habría producido desde el extranjero.

Esa información fue entregada por el Gobierno a la Fiscalía Metropolitana Centro Norte, luego de que Estados Unidos le advirtiera de una supuesta vulneración de seguridad hace un par de semanas. Se trata de una alerta que el propio embajador norteamericano, Brandon Judd, había confirmado en la víspera, durante una conferencia de prensa.

## Eventual ataque contra compañías de telecomunicaciones y constructora locales

"Algunas semanas atrás, compartimos información específica con múltiples funcionarios de gobierno de distintas agencias, sobre incursiones en los sistemas de telecomunicaciones chilenos por parte de actores malignos extranjeros", dijo la autoridad diplomática este lunes. Aunque no especificó públicamente quiénes eran esos "actores malignos".

La indagatoria, que hoy es dirigida por el fiscal regional Xavier Armendáriz y se tramita bajo estricta reserva, fue abierta recientemente y se espera que las diligencias se encarguen a una unidad especializada de la Policía de Investigaciones (PDI), como el Cibercrimen.

Se trata de una intervención, puntualizó Judd, que "estuvo dirigida a múltiples compañías de telecomunicaciones privadas, poniendo la privacidad y la información personal de casi todos los chilenos que usan un teléfono celular en riesgo de que sus datos fueran robados, sus comunicaciones espiadas y sus vidas afectadas".

**RIESGO .—**De acuerdo con los antecedentes entregados por EE.UU. al Gobierno, la información personal de casi todos los chilenos que usan un teléfono celular habría estado en riesgo, dijo el embajador Judd, este lunes. Esa posible vulneración de seguridad es la que pesquisa la fiscalía.

"Igual de preocupante, este actor maligno hackeó una prominente empresa chilena de la construcción, una empresa local que compite directamente con compañías extranjeras por proyectos en Chile", agregó en la conferencia.

Además de informar a la fiscalía, el Gobierno también habría traspasado antecedentes a las agencias gubernamentales —como la Agencia Nacional de Ciberseguridad— y al Estado Mayor Conjunto.

## Protección de datos, "un asunto de seguridad y de confianza pública"

Un posible hackeo a empresas de telecomunicaciones no solo da cuenta de una vulnerabilidad de los sistemas de estas, sino que además pone en entredicho la "seguridad y confianza pública", afirman entre expertos.

Así, Jorge Atton, exsubsecretario de Telecomunicaciones, explica que "cuando un ciberataque proviene de grupos vinculados a potencias extranjeras, el problema va más allá del robo de contraseñas o tarjetas de crédito. El riesgo es mayor y más profundo".

Por eso, advierte, "la protección de datos ya no es solo un tema tecnológico: es un asunto de seguridad y de confianza pública. En un entorno global cada vez más digital y competitivo, fortalecer la ciberseguridad es una condición básica para proteger a las personas y resguardar la estabilidad del país".

Coincide en la importancia de la protección de datos Néstor Strube, CEO ITQ Chile, compañía especialista en ciberseguridad. "Este escenario, originado por el proyecto de cable submarino Chile-China Express (CCE), demuestra que las decisiones tecnológicas hoy son, ante todo, definiciones de seguridad nacional", dice.

"Un intento de hackeo por potencias extranjeras —agrega— busca la interceptación masiva de tráfico para espionaje, perfilamiento de ciudadanos y robo de identidad mediante el acceso a metadatos y comunicaciones no cifradas. Esto compromete la privacidad nacional y permite la exfiltración de información sensible hacia bases de datos externas, fuera del control de la legislación chilena de protección de datos".

**MEDIDAS**

**Expertos plantean necesidad de exigir mayores estándares de seguridad digital a organismos públicos y empresas que manejan información sensible.**

Entre las medidas que pueden adoptarse para evitar este tipo de vulneraciones, enumeran: exigir mayores estándares de seguridad digital a organismos públicos y empresas que manejan información sensible; actualización de sistemas y auditorías periódicas de seguridad. También, consideran que es "imperativo implementar un cifrado de extremo a extremo robusto y tecnologías de distribución de claves cuánticas, para blindar el transporte de datos frente a posibles capturas físicas en la fibra", por ejemplo.