LITORALPRESS

Fecha: 01-04-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Editorial
Título: Editorial: SEGURIDAD DIGITAL DEL ESTADO

Pág. : 13
Cm2: 221,0
VPE: $ 1.958.266

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

EDITORIAL

SEGURIDAD DIGITAL DEL ESTADO

El reciente acceso no autorizado a las cuentas personales del Presidente José Antonio Kast, desde donde se difundió un mensaje falso con implicancias en política exterior, puso en evidencia que el resguardo de la identidad digital de las autoridades del Estado permanece aún subestimado en el país. El episodio, ocurrido el pasado jueves -y que pasó prácticamente inadvertido en medio de una nutrida agenda pública-, dejó al descubierto un riesgo sistémico, que lejos de tratarse como una anécdota, debe abordarse como un fallo de seguridad en infraestructura crítica, con impactos potenciales en reputación y estabilidad.

Durante la madrugada del 26 de marzo, terceros intervinieron las cuentas del mandatario y emitieron mensajes que aludían al Presidente de EEUU, Donald Trump, en un contexto internacional sensible. Durante el lapso en que el contenido circuló, operó como una señal potencialmente atribuible al jefe de Estado chileno, lo que expuso la ausencia de controles. Y aunque hubo una aclaración oficial posterior, esto no eliminó el hecho de que en entornos digitales los efectos se producen en tiempo real.

La identidad digital de las autoridades del país es un activo estratégico y, como tal, cuando una cuenta oficial es capturada el mayor daño, por lo general, no es comunicacional. En este caso, lo que se puso en juego fue la certeza jurídica y la coherencia de la política exterior, factores que los mercados y los inversores monitorean con atención. Pero también pueden generarse señales económicas falsas, afectarse decisiones de mercado o inducirse errores en organismos públicos o privados. Y, en estos términos, la credibilidad de una alta autoridad -y más aún la de un jefe de Estado- es un componente central del valor de la "marca país".

El incidente expuso así, al menos, tres debilidades que el sector público debe cerrar. La primera se relaciona con la gobernanza de accesos, pues aunque el país ha avanzado en digitalización de servicios públicos, interoperabilidad y gobierno electrónico, esto no ha sido acompañado por un desarrollo equivalente en estándares de ciberseguridad en gestión de la identidad digital de autoridades. Aún faltan estándares de grado estratégico y hardware de autenticación física como normas de cumplimiento obligatorio para la alta magistratura.

A ello se suma que la identidad digital de las autoridades no ha sido formalmente incorporada entre las categorías de infraestructura crítica, pese a que su vulneración puede afectar la continuidad operativa del Estado. Es imperativo que la arquitectura legal de ciberseguridad las clasifique en ese rango, lo que permitiría asignar recursos, definir protocolos y establecer responsabilidades administrativas acordes al riesgo que representa su vulneración para el orden público.

El resguardo de la identidad digital de las autoridades permanece aún subestimado, pese a sus costos en reputación y estabilidad.

Las limitaciones de la capacidad de respuesta en tiempo real son el tercer flanco. La brecha temporal entre el ataque y la recuperación del control refleja que los protocolos aún son reactivos. De acuerdo con los estándares internacionales, lo que se requiere es un Centro de Operaciones de Seguridad dedicado a la integridad de las comunicaciones oficiales, capaz de neutralizar amenazas antes de que escalen al terreno diplomático o financiero.

Chile aspira a ser un polo de servicios tecnológicos y economía digital, marco en el que la seguridad de sus autoridades forma parte de su carta de presentación. Sin embargo, el país, aún no blinda su soberanía en este ámbito. Avanzar en este camino es una inversión en resiliencia institucional.