

Fecha: 18-02-2026
Medio: Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Supl.: Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Tipo: Noticia general
Título: 5 Claves del alarmante aumento de la filtración de datos en Chile durante 2025

Pág.: 126
Cm2: 769,4

Tiraje:
Lectoría:
Favorabilidad: ☐ Sin Datos
☐ Sin Datos
☐ No Definida

5 Claves del alarmante aumento de la filtración de datos en Chile durante 2025



La filtración de datos en Chile aumentó un 188% durante 2025, según el Reporte de Ciberseguridad 2026 del Centro de Ciberinteligencia de Entel Digital. Este fuerte incremento marca un punto de inflexión tras la baja registrada en 2024 y confirma que el país enfrenta una nueva etapa del cibercrimen, caracterizada por mayor organización, sofisticación y profesionalización de los ataques.

El informe identifica como principal causa el uso masivo de infostealers, programas maliciosos diseñados para robar credenciales, contraseñas, cookies y otra información sensible sin generar alertas inmediatas. A esto se suma la venta de accesos iniciales a sistemas comprometidos, lo que permite que distintos grupos criminales compren “puertas de entrada” para ejecutar ataques posteriores como ransomware, fraude corporativo o extorsión. En este contexto, la fil-

Fecha: 18-02-2026

Medio: Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa

Supl. : Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa

Tipo: Noticia general

Título: 5 Claves del alarmante aumento de la filtración de datos en Chile durante 2025

Pág. : 127

Cm2: 776,8

Tiraje:

Lectoría:

Favorabilidad:

Sin Datos

Sin Datos

☐ No Definida

tración de datos deja de ser un hecho aislado y pasa a formar parte de una cadena delictiva más amplia.

Los sectores más impactados en Chile han sido banca, gobierno, retail y educación, principalmente por debilidades en autenticación multifactor, monitoreo de credenciales y gestión de identidades digitales. Esto ha llevado a que la filtración de datos sea considerada un riesgo estratégico para la continuidad operacional y la reputación de las organizaciones.

Aunque la actividad de ransomware en Chile se mantuvo relativamente estable en 2025, a nivel global aumentó cerca de un 20% el número de grupos activos, impulsados por modelos de Ransomware-as-a-Service y esquemas de doble y triple extorsión. Además, se observó un incremento en amenazas avanzadas persistentes (APT), muchas vinculadas a intereses estatales, con foco en sectores críticos como telecomunicaciones, energía, transporte, minería y organismos públicos.

El reporte también advierte que la inteligencia artificial está amplificando el riesgo. Durante 2025, los ataques a entornos cloud crecieron un 136%, gracias al uso de machine learning y herramientas generativas para automatizar ofensivas digitales. Si bien estas

tecnologías también fortalecen la defensa, su adopción sin adecuada gobernanza puede aumentar la exposición.

Finalmente, el informe destaca avances regulatorios en Chile, como la creación de la Agencia Nacional de Ciberseguridad y la nueva Ley de Protección de Datos. Sin embargo, advierte que el desafío principal sigue siendo fortalecer la madurez operativa y la resiliencia digital de las organizaciones frente a un escenario de amenazas cada vez más complejo.

Además, el reporte subraya que el impacto de la filtración de datos no solo se mide en términos tecnológicos, sino también económicos, legales y reputacionales. Las organizaciones afectadas enfrentan costos por interrupciones operativas, recuperación de sistemas, pérdida de clientes y eventuales sanciones regulatorias, especialmente en un contexto de mayores exigencias en protección de datos.

Ante este escenario, los expertos recomiendan fortalecer la cultura de ciberseguridad interna, capacitar constantemente a los equipos e implementar autenticación multifactor y una gestión más estricta de credenciales. También es clave el monitoreo continuo de datos filtrados y el uso de inteligencia de amenazas para anticipar ataques y reducir el tiempo de exposición ante incidentes.