# Caso Banco Santander y Banco Estado

En mayo de 2024, Grupo Santander sufrió un acceso no autorizado a una base de datos alojada en un proveedor externo, comprometiendo datos personales de clientes y empleados en España, Chile y Uruguay (santander.com, cincodias.elpais.com). Ese mismo año, BancoEstado descubrió un fraude interno por aproximadamente CLP 6 100 millones realizado por exgerentes de sistemas y un proveedor tecnológico, lo que derivó en detenciones y acciones legales (interferencia.cl). Santander implementó medidas inmediatas y notificó a la CNMV y a la AEPD, mientras que BancoEstado presentó querellas por asociación ilícita y lavado de dinero, reforzando sus controles internos (df.cl).

### Incidente de seguridad en Banco Santander

### Origen y descubrimiento

El 14 de mayo de 2024, el Grupo Santander confirmó un acceso no autorizado a una de sus bases de datos alojada en un proveedor externo (santander.com). La entidad detectó actividad irregular tras alertas de monitoreo y confirmó que no se vulneraron sistemas de autenticación ni credenciales de banca online (cibersafety.com).

### Alcance y datos comprometidos

La intrusión expuso información de clientes en España, Chile y Uruguay, así como registros de empleados y exempleados del grupo (cincodias.elpais.com). Channel Partner precisó que la filtración se limitó a datos de back-end y no incluyó contraseñas ni información transaccional (channelpartner.es). Emol reportó que cerca de 4 millones de clientes en Chile vieron sus datos accedidos durante el incidente (emol.com).

### Respuesta y mitigación

Santander bloqueó de inmediato el acceso a la base de datos comprometida y reforzó sus sistemas de prevención de fraude para proteger a los clientes (santander.com). La entidad informó proactivamente a los usuarios afectados, a la CNMV y a la AEPD, cumpliendo con la legislación vigente (cincodias.elpais.com, santander.com). Según Cibersafety, el banco contrató peritos forenses externos para evaluar el alcance del ataque y asegurar la integridad del resto de sus sistemas (cibersafety.com).

## Consecuencias y lecciones aprendidas

La AEPD, aunque notificada, rechazó revelar públicamente detalles de su investigación interna (elconfidencialdigital.com). El Confidencial señaló que este incidente se enmarcó en una serie de ciberataques a grandes empresas del IBEX 35, evidenciando riesgos en proveedores externos (elconfidencial.com). Un tribunal en Bilbao obligó a Santander a devolver fondos a una cliente afectada por un incidente asociado, subrayando el impacto jurídico de estas violaciones (bitlifemedia.com). Infobae detalló que los campos expuestos incluían nombres, direcciones, correos y números telefónicos, lo que refuerza la necesidad de cifrar datos sensibles en reposo (infobae.com).

## Fraude informático en BancoEstado

### Mecanismo del fraude

Entre 2021 y 2024, exgerentes del área de sistemas de BancoEstado junto a un proveedor manipulaban un software de transferencias masivas para desviar fondos a cuentas propias (interferencia.cl). El esquema permaneció oculto hasta que uno de los implicados se autodenunció, lo que permitió el descubrimiento de la irregularidad (interferencia.cl).

### Cronología de los hechos

En marzo de 2024, BancoEstado registró el pico mensual de fraudes de la industria con 164 871 reclamos pagados, por un total de CLP 71 922 millones (latercera.com). El 22 de octubre de 2024, Emol informó la detención de exfuncionarios y colaboradores acusados del multimillonario fraude (emol.com). Posteriormente, Cooperativa.cl comunicó la formalización de cinco imputados por un desfalco de CLP 6 171 millones (cooperativa.cl).

### Impacto y montos defraudados

La Policía de Investigaciones detuvo a cuatro ciudadanos chilenos y una ciudadana colombiana implicados, revelando la sofisticación del lavado de activos mediante 15 sociedades intermediarias (biobiochile.cl). El monto total estimado en fraude ascendió a CLP 6 100 millones, cifra equivalente a casi el 0,3 % de los depósitos corporativos de la entidad. (df.cl)

**Acciones legales y recomendaciones**

BancoEstado presentó querellas por asociación ilícita y lavado de dinero, y colabora con la Fiscalía para recuperar los activos desviados (df.cl). Además, reforzó sus controles de acceso a sistemas críticos, implementó auditorías continuas y revisó los protocolos de proveedores externos para prevenir nuevos incidentes.

Estos casos ejemplifican que tanto los ataques externos a grandes entidades como el fraude interno demandan políticas de seguridad integrales, que incluyan gestión proactiva de parches, evaluación rigurosa de terceros, monitoreo continuo y controles internos estrictos para proteger la integridad financiera y la confianza de los clientes.