

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**CIBERATAQUE AL BANCO SANTANDER  
REVELA LA FRÁGIL CADENA DE SEGURIDAD  
DE LOS PROVEEDORES**

14 / 05 / 2024

## CONTENIDO

|                           |   |
|---------------------------|---|
| INTRODUCCIÓN.....         | 3 |
| RESUMEN.....              | 5 |
| NOTICIA COMPLETA.....     | 6 |
| CONTACTOS DE SOPORTE..... | 7 |

## INTRODUCCIÓN

En un incidente que destaca la vulnerabilidad inherente en la era digital, el Banco Santander ha sido objeto de un ciberataque masivo, sacudiendo los cimientos de la confianza en la seguridad de los datos bancarios. Sin embargo, lo que hace que este evento sea aún más impactante es el hecho de que el ataque no se produjo directamente en las entrañas del banco, sino a través de un proveedor externo. Este evento subraya la necesidad crítica de que las empresas reconsideren sus estrategias de seguridad no solo dentro de sus propias infraestructuras, sino también en todo el ecosistema de proveedores con los que trabajan.

## RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

|                                     |                        |
|-------------------------------------|------------------------|
| ID de alerta:                       | DSOC-CERT_2024_05_14_1 |
| Clasificación de alerta:            | Noticia                |
| Tipo de Impacto:                    | Alta                   |
| TLP (Clasificación de información): | <b>CLEAR</b>           |
| Fecha de publicación:               | 14/05/2024             |
| Es día cero (0 day):                | No                     |

## RESUMEN

### El Ataque

El Banco Santander ha revelado que su base de datos, alojada en un proveedor externo, fue comprometida, permitiendo a los hackers acceder de manera no autorizada a información sensible de clientes en España, Chile y Uruguay. Esta infracción no solo afectó a los clientes activos, sino también a los empleados actuales y anteriores del banco, exacerbando la magnitud del incidente.



### La Respuesta del Banco

El Banco Santander ha emitido un comunicado asegurando a sus clientes que, a pesar del acceso no autorizado, no se vieron comprometidas credenciales de acceso o contraseñas de banca por internet que permitieran operaciones financieras. A pesar de esta afirmación tranquilizadora, la entidad ha expresado su pesar por la situación y ha iniciado una campaña proactiva de informar a los afectados directamente.



Abre tu cuenta

Ingresar



## Comunicación Importante

Hemos tomado conocimiento de un acceso no autorizado a una base de datos de Grupo Santander alojada en un proveedor. Ha afectado a clientes de Santander Chile, España y Uruguay y a trabajadores de la institución.

Santander ha activado sus protocolos para gestionar estos casos, bloqueando el acceso a la información a la que se tuvo acceso de manera irregular.

Es importante destacar que **no existe información de contraseñas y claves comprometidas, por lo cual los fondos de clientes están seguros.**

La operación y sistemas del banco, en tanto, no han sido afectados y funcionan con total normalidad.

Igualmente, recordamos a todos los clientes nuestros habituales consejos de seguridad para evitar cualquier tipo de fraude:

- Estemos alerta de esquemas de "phishing" en los que los cibercriminales intentan obtener información sensible, como credenciales de acceso a cuentas y aplicaciones.
- Piense antes de hacer clic. Nunca haga clic en un enlace que haya recibido hasta asegurarse de que es auténtico.
- Nunca comparta sus contraseñas con nadie. El banco nunca le preguntará por sus contraseñas por e-mail ni por teléfono.
- Si sospecha, repórtelo. Ante cualquier actividad sospechosa póngase en contacto con el banco reportándolo a [fraudesinformaticos@santander.cl](mailto:fraudesinformaticos@santander.cl).

Reiterando que no existe información transaccional comprometida, le pedimos disculpas por la preocupación que esta situación pueda ocasionarle y quedamos a su disposición para cualquier pregunta en nuestros canales habituales y oficinas.

Le mantendremos informado ante cualquier novedad relevante que se produzca en relación con este asunto.

### Lecciones Aprendidas

Este ciberataque deja al descubierto una verdad inquietante: las organizaciones no pueden depender únicamente de sus propias medidas de seguridad interna para proteger sus datos críticos. La interconexión digital en el mundo empresarial moderno significa que las debilidades de los proveedores pueden convertirse rápidamente en debilidades propias. Es imperativo que las empresas implementen medidas rigurosas de evaluación y monitoreo de proveedores para salvaguardar sus datos y la confianza de sus clientes.

### **Próximos Pasos**

En respuesta a este incidente, el Banco Santander ha instado a sus clientes a mantener la vigilancia y a no proporcionar información confidencial a ninguna entidad que se identifique como representante del banco, recordando que nunca solicitarán códigos o claves bancarias por teléfono. Además, han establecido un canal de comunicación dedicado para reportar actividades sospechosas relacionadas con el phishing.

### **Conclusión**

El ciberataque al Banco Santander sirve como un llamado de atención para todas las empresas sobre la importancia crítica de proteger no solo sus propios sistemas, sino también los de sus proveedores. En un mundo cada vez más interconectado, la seguridad de los datos es una responsabilidad compartida que requiere una vigilancia constante y una acción proactiva. Este incidente debe ser un catalizador para que todas las organizaciones revisen y refuercen sus estrategias de ciberseguridad, reconociendo que la cadena de seguridad es tan fuerte como su eslabón más débil.

## **NOTICIA COMPLETA**

<https://devel.group/blog/ciberataque-al-banco-santander-revela-la-fragil-cadena-de-seguridad-de-los-proveedores/>

## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto:cert@develsecurity.com)

### Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>