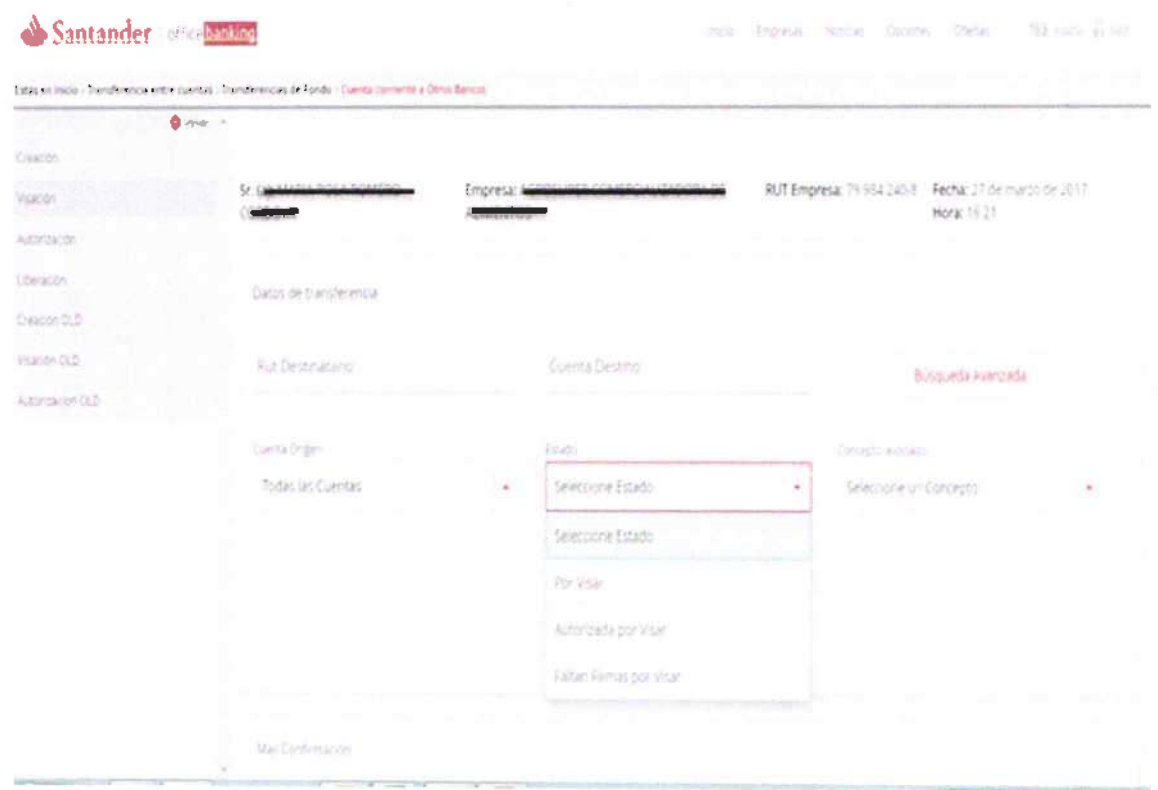
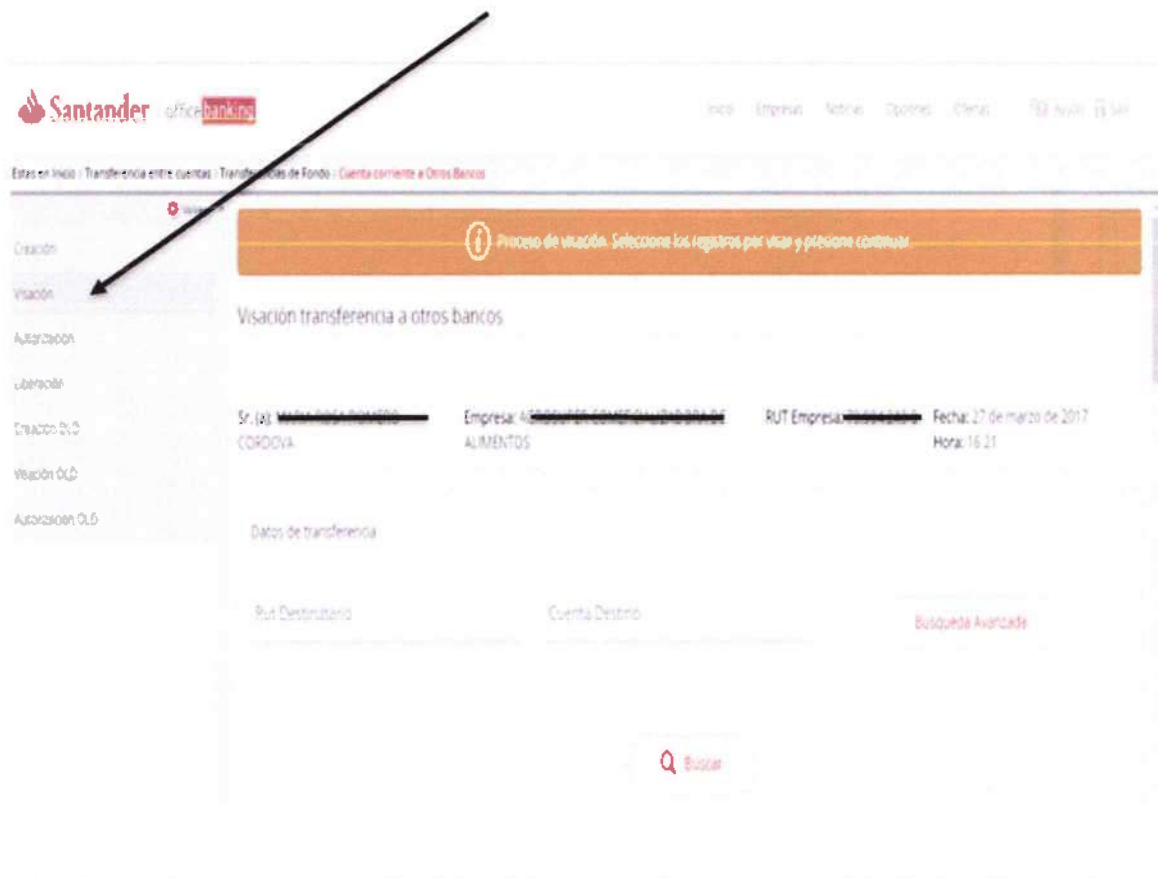


**Paso 7:** El usuario debe marcar el o las transferencias electrónicas que desea autorizar de acuerdo a lo que aparece en la siguiente pantalla, y esto corresponde al flujo de la visación de las TEF.

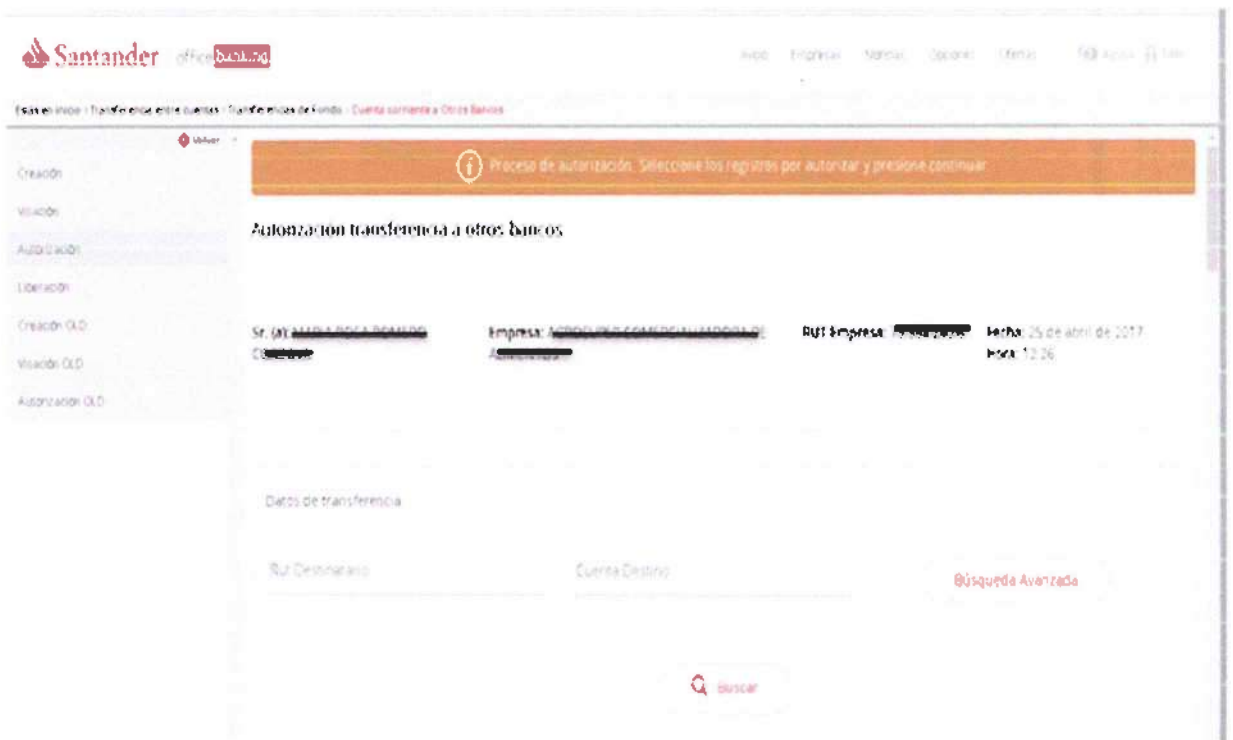
**Visación,** corresponde a una validación de datos del beneficiario ingresado para la creación de las transferencias electrónicas.



**Paso 8:** Cuando ya tenemos seleccionada la transferencia electrónica que queremos realizar, nos va a indicar que la operación que se encuentra realizada, donde aparecerán los datos del destinatario, por lo que el proceso de visación está listo.



**Paso 9:** Posteriormente debemos ingresar al módulo de Autorización, para continuar con el flujo.



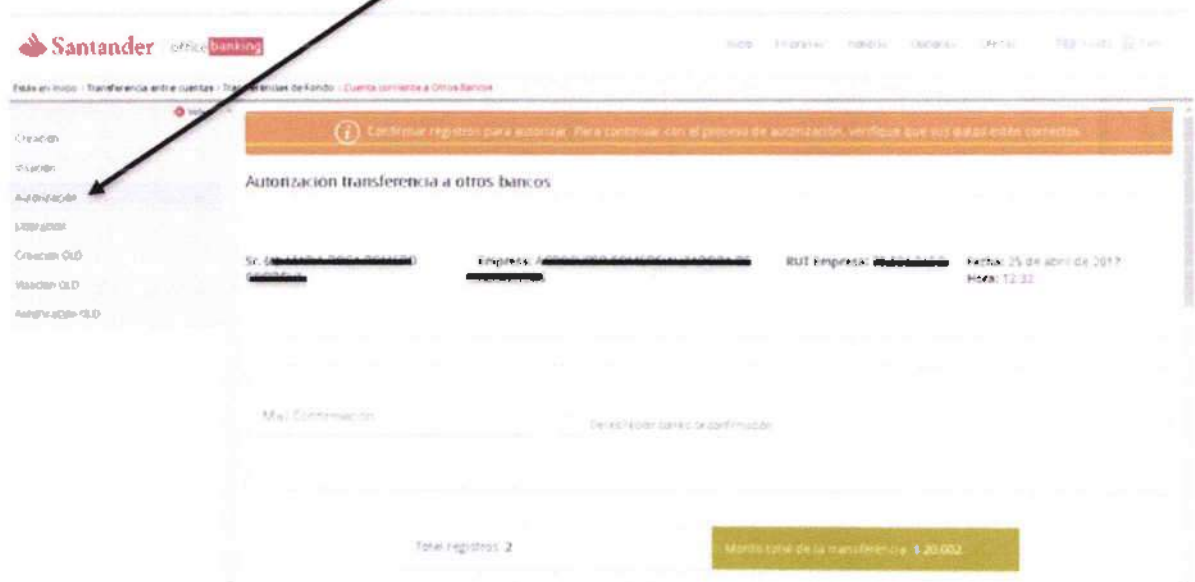
doscientos ochenta y tres

293

**Paso 10:** Para continuar debemos ingresar el Rut del destinatario donde irán los fondos, para buscar sus datos en la lista de creadas.



**Paso 11:** Una vez que tenemos los datos del destinatario debemos realizar una confirmación para la autorización.



documentos monte ) fecho 294

**Paso 12:** Cuando ya tenemos la confirmación pasamos a la autorización, donde ingresamos las coordenadas de la superclave asignada al cliente.

**Santander office banking**

Inicio | Empresa | Noticias | Servicios | Ofertas | Ayuda | Perfil

Estás en Inicio > Transferencia entre cuentas > Transferencias de Fondo > Cuenta corriente > Otros Bancos

Operación	Cuenta de origen	Cuenta de destino	Identificación de destino	Monto	Detalle	Medio	Fecha de emisión
Visión	0-000-0000000000	000-00000000	BANCO CHILE / EDWARDS (CI)	10.000	Pago de Remuneraciones	En línea	20/03/2017 13:34:00
Autorización	0-000-0000000000	000-00000000	BANCO CHILE / EDWARDS (CI)	10.000	Pago de Remuneraciones	Oficina 24h	17/02/2017 11:47:00

**Confirmar transferencia**

Ingresa que el número de serie de tu Tarjeta Super Clave es 463

Si es así, ingresa el valor de las siguientes coordenadas:

A1 0 0

**Paso 13:** Y por último debemos ingresar la clave 3.0 de acuerdo a los códigos enviados (SMS) al celular del cliente registrado en office Banking, donde finalmente la transferencia electrónica queda aprobada.

**Santander office banking**

Inicio | Empresa | Noticias | Servicios | Ofertas | Ayuda | Perfil

Estás en Inicio > Transferencia entre cuentas > Transferencias de Fondo > Cuenta corriente > Otros Bancos

**Clave 3.0**

Hemos enviado una Clave 3.0 a tu teléfono celular 99\*\*\*\*367 registrado en el Banco.

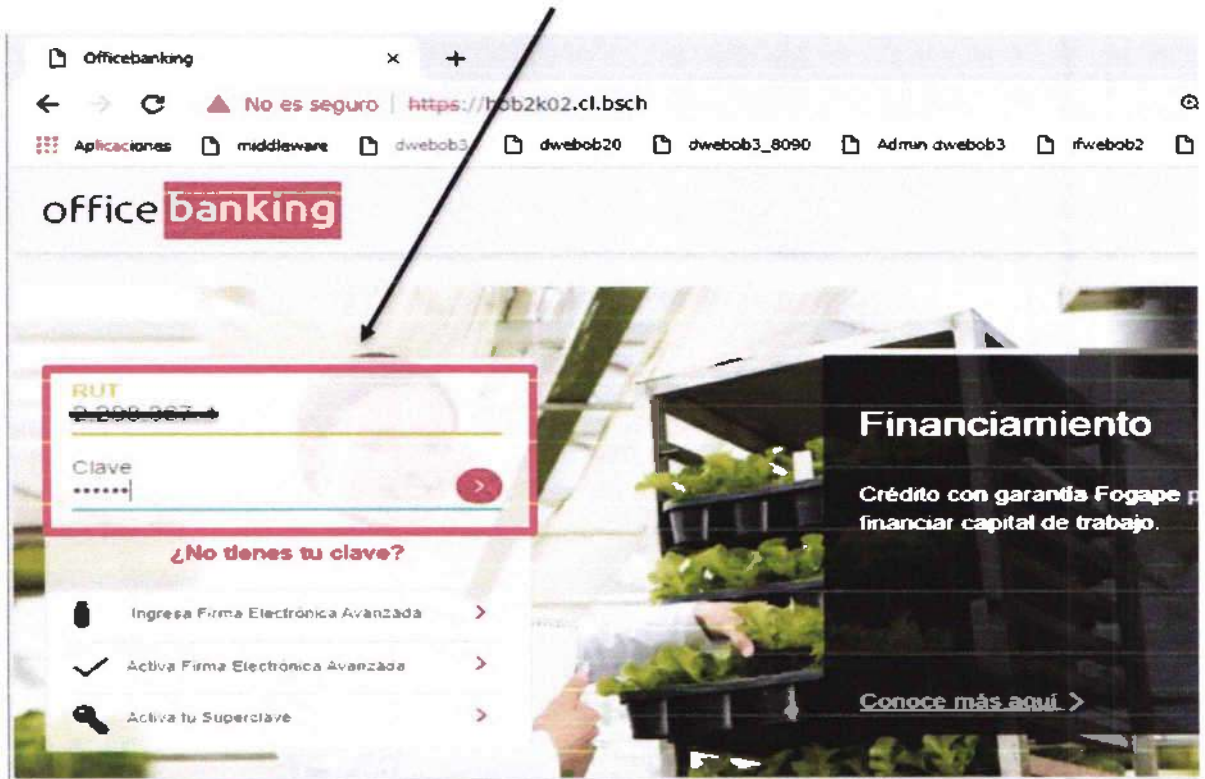
Esta clave es válida sólo para esta operación y debe ser ingresada en los próximos minutos.

< Volver Continuar

\* Información sobre la garantía en Chile de los depósitos en el Banco por www.bcb.cl. Política de privacidad y uso de Office Banking

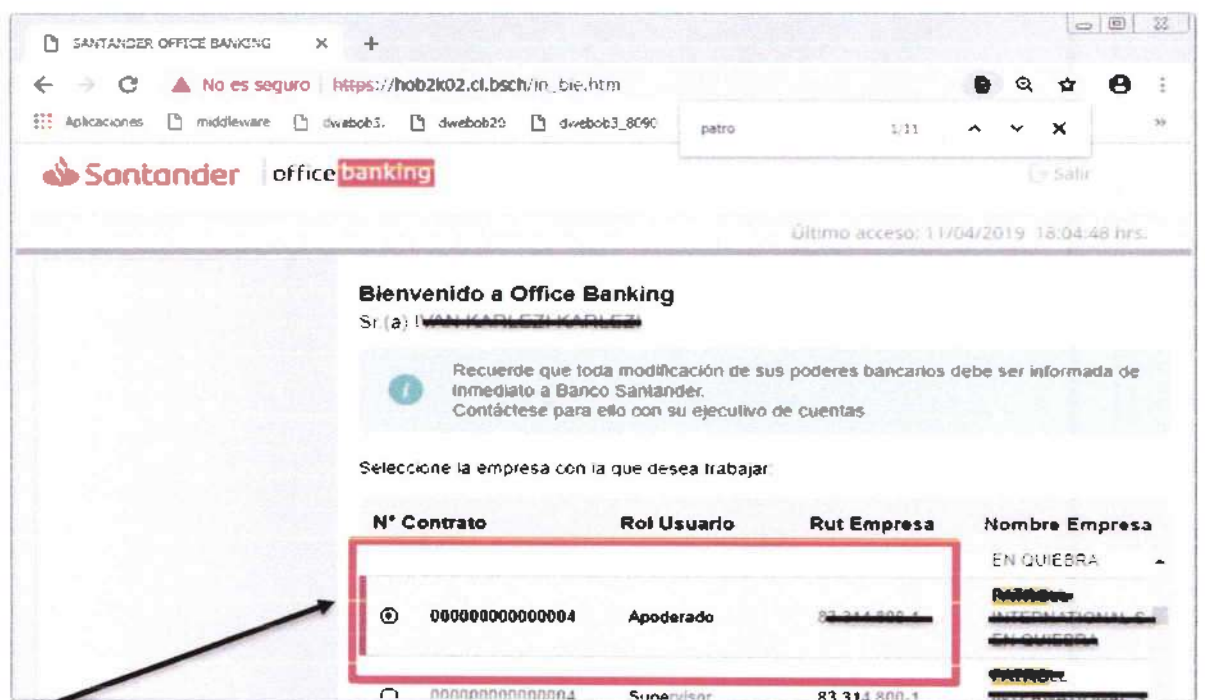
o **Creación y autorización de Vale Vista Electrónico Office Banking (Flujo).**

**Paso 1:** El usuario por medio de esta pantalla puede ingresar a la plataforma donde se encuentran sus productos del Banco , desde donde puede realizar la generación de Vale Vista (Acceso a sitio [www.officebanking.cl](http://www.officebanking.cl)), posteriormente digita su Rut y clave de acceso en la página.



**Paso 2:** El usuario debe seleccionar la Empresa donde necesita operar. Esto debido a que un Apoderado de Office Banking puede tener 1 o más Empresas asociadas.

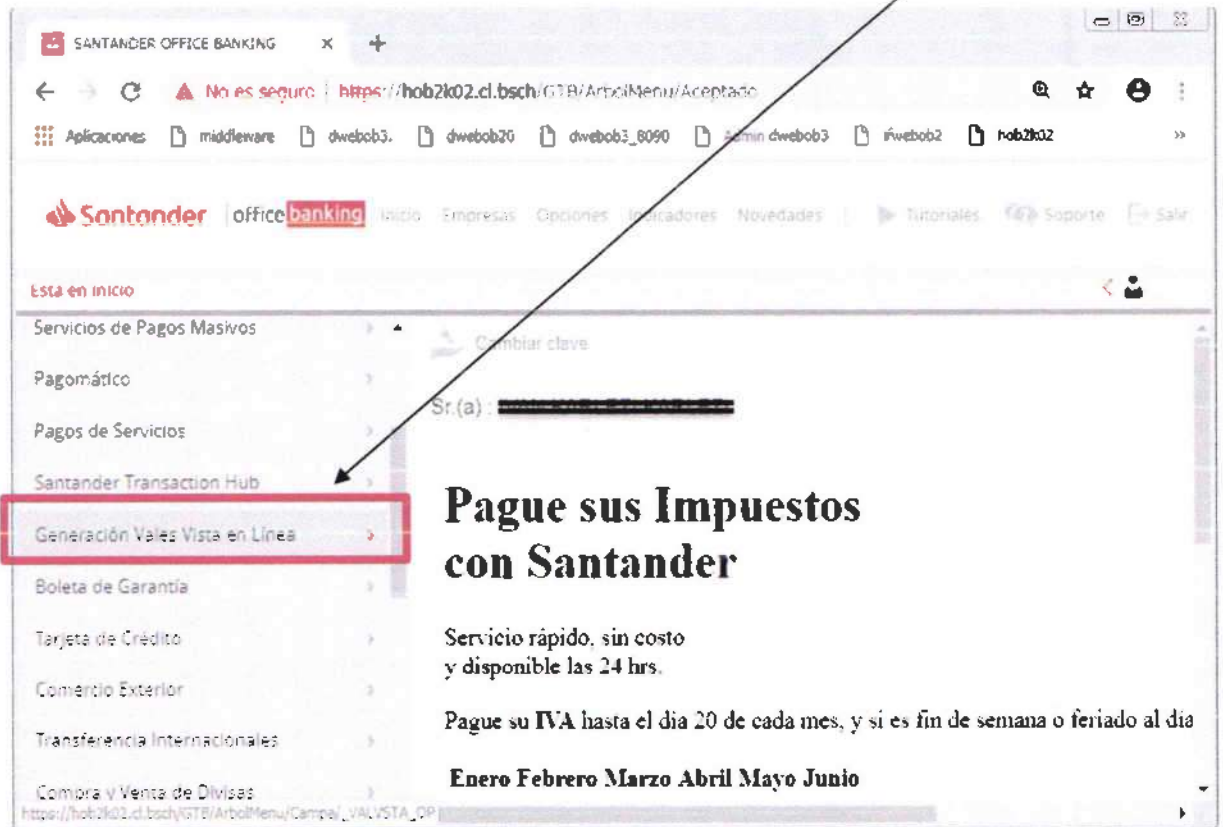
**Importante que esté creado,** puesto que sólo este Rol puede visar las nóminas. Si no está creado en Office Banking, las operaciones no se podrán concretar.



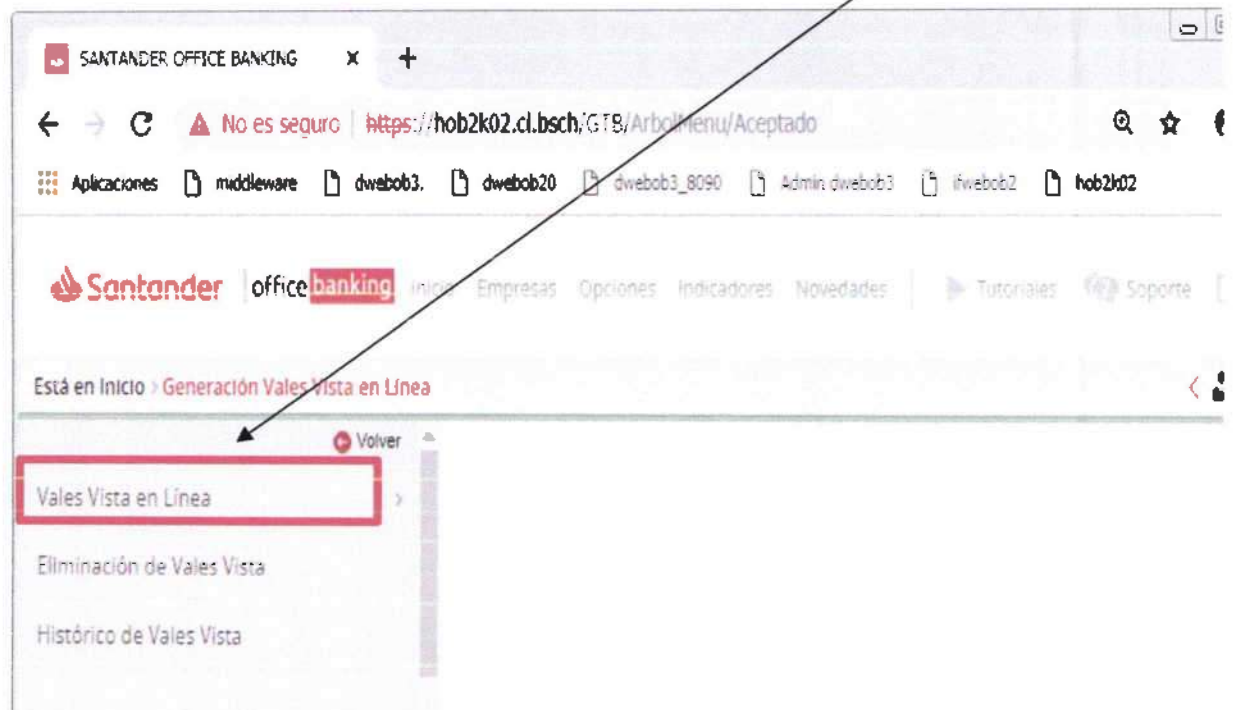
descuento monte 7 ptes

296

**Paso 3:** El usuario debe presionar la opción que indica Generación Vale Vista (cuadro seleccionado en color rojo) que permite continuar con la creación.



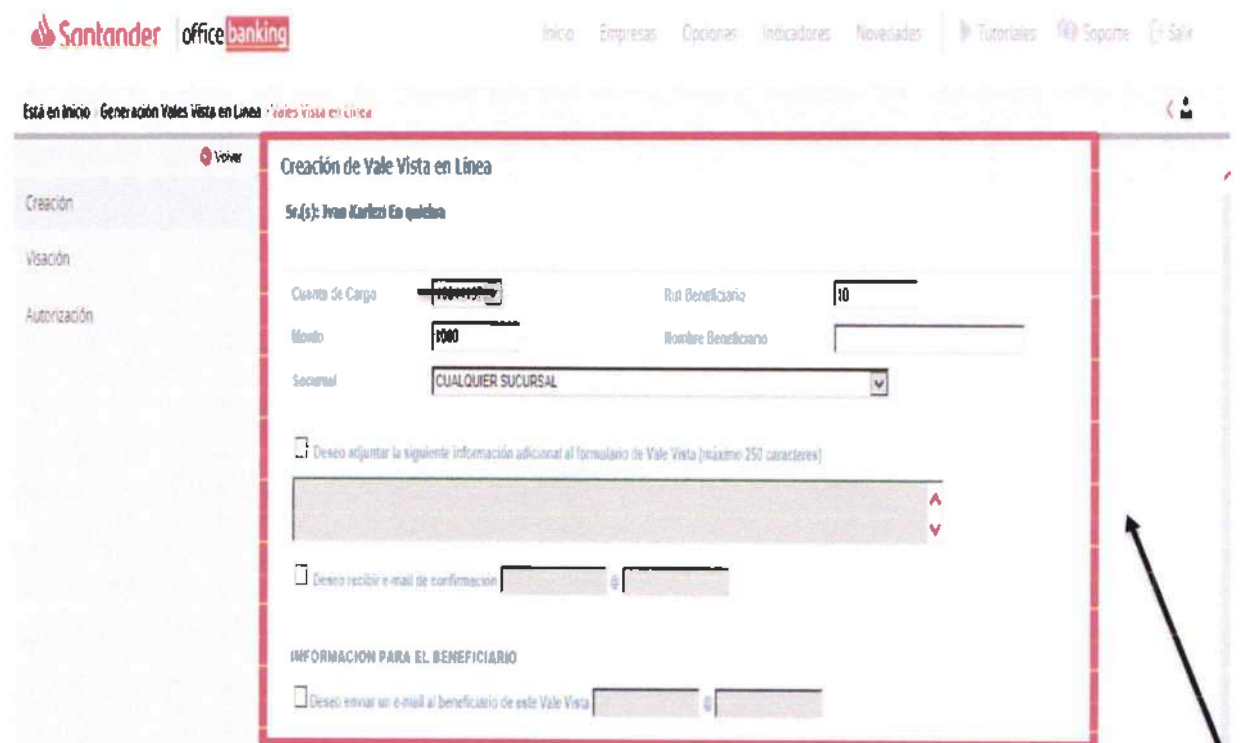
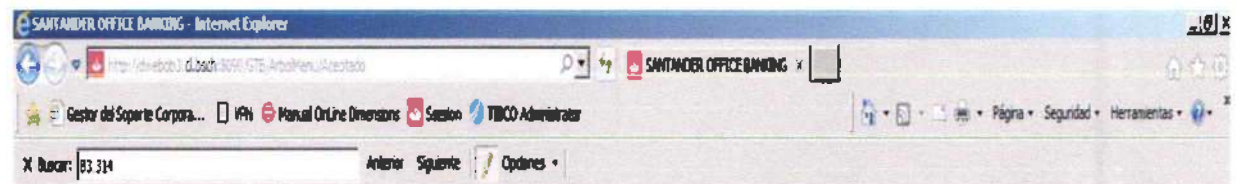
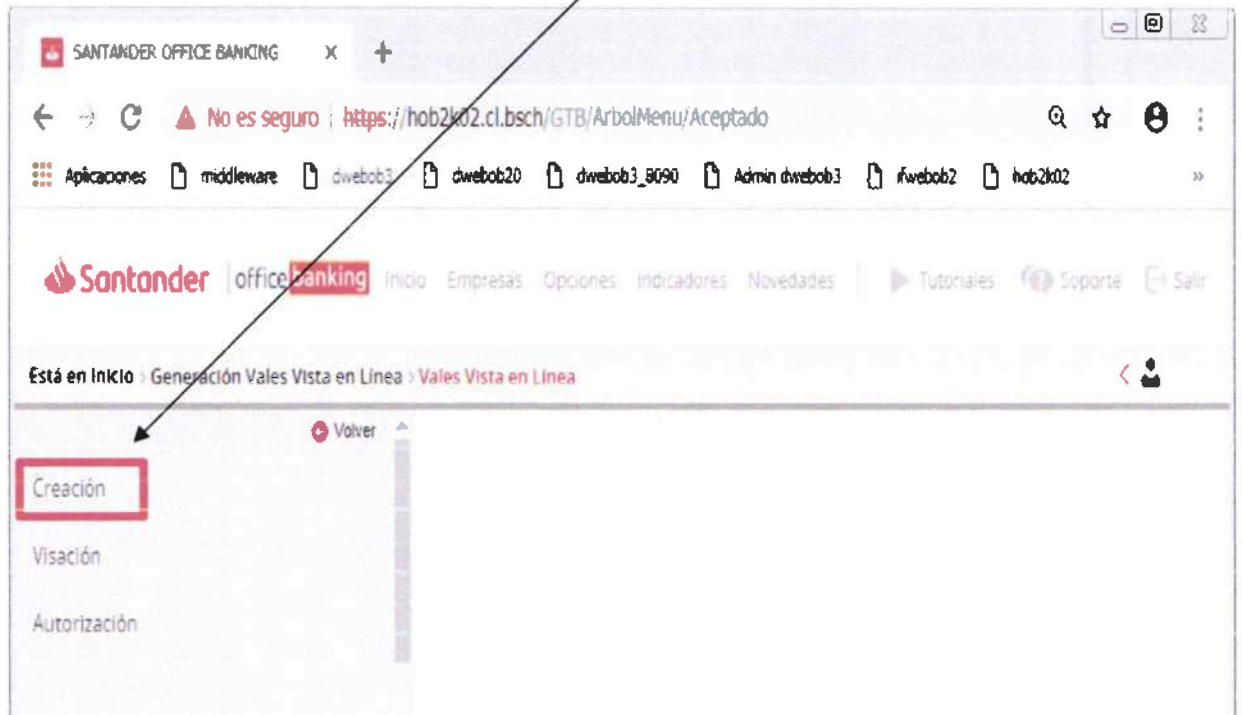
**Paso 4:** El usuario selecciona la opción donde dice Vale Vista en Línea, el que permite crear un vale vista electrónico nuevo.



documentos monedas y piete 28/9

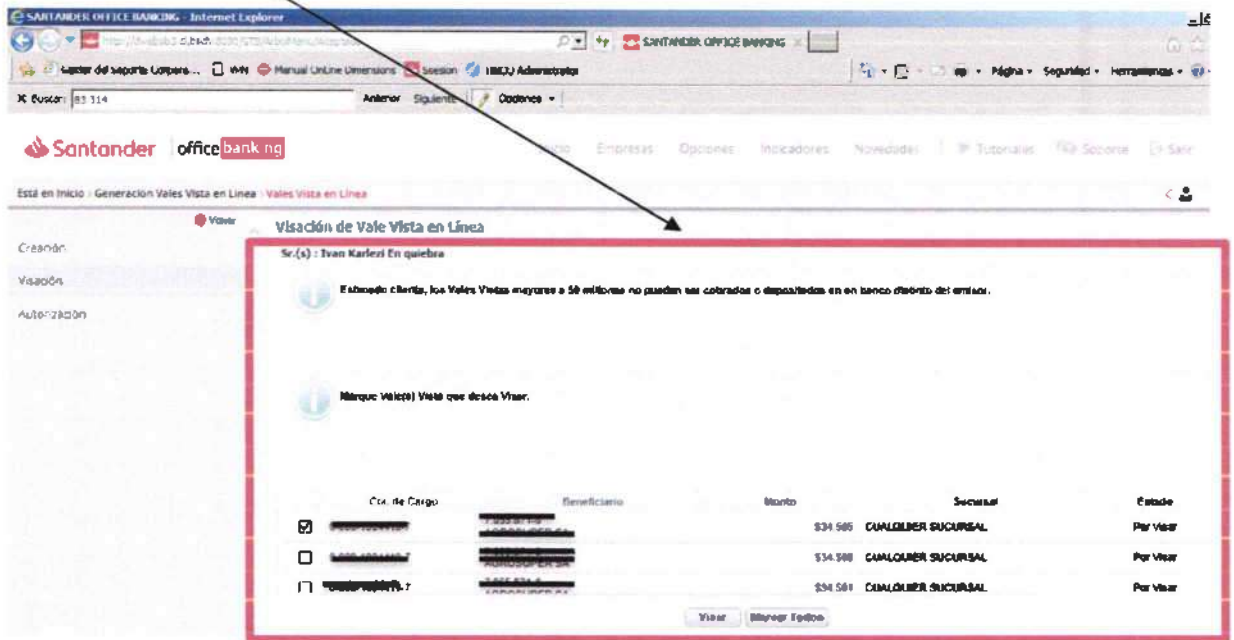
**Paso 5:** El usuario debe seleccionar la opción Creación, para posteriormente ingresar los datos del beneficiario (Rut y nombre, además del monto), luego debe pinchar botón continuar.

El beneficiario corresponde a la persona que realizará cobro del Vale Vista.

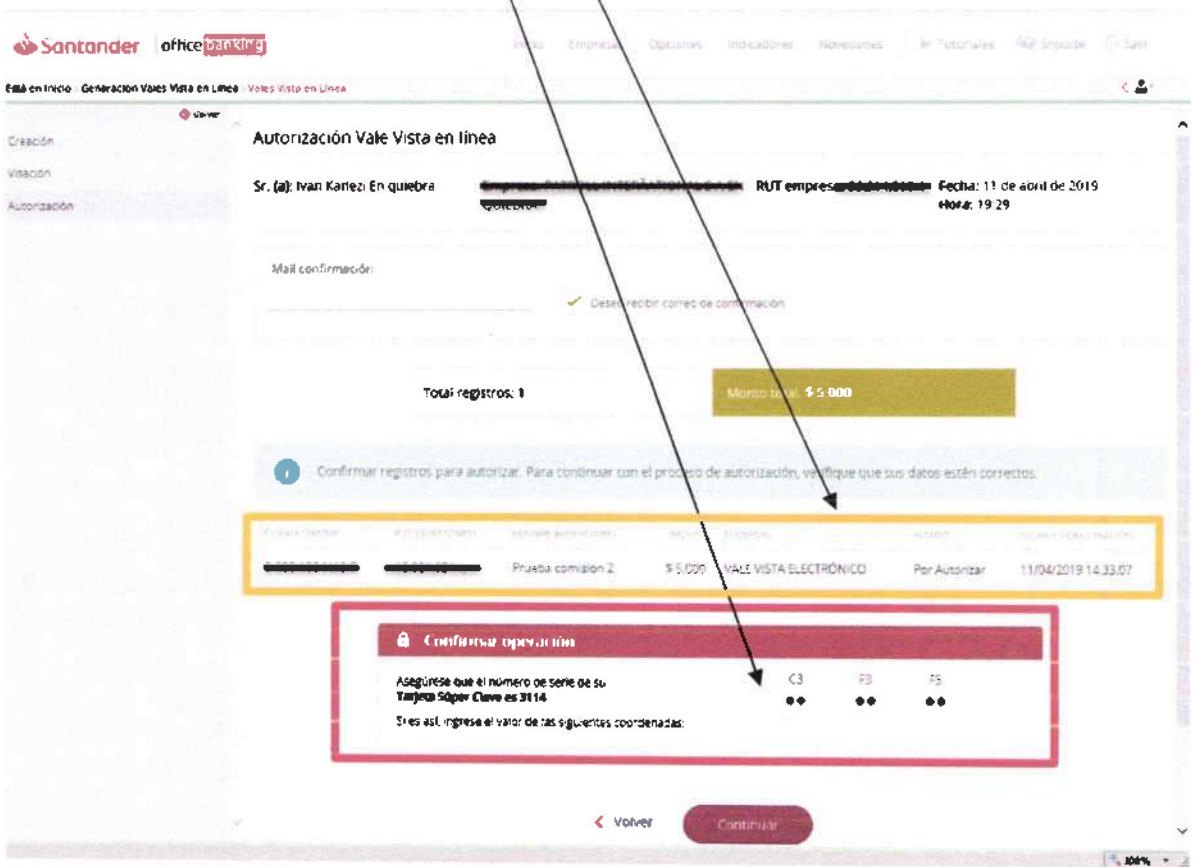


**Paso 6:** El usuario debe marcar el o los Vale Vista que desea autorizar de acuerdo a lo que aparece en la siguiente pantalla, y esto corresponde al flujo de la visación del vale vista.

**Visación** corresponde a una validación de datos del beneficiario ingresado para la creación del Vale Vista.

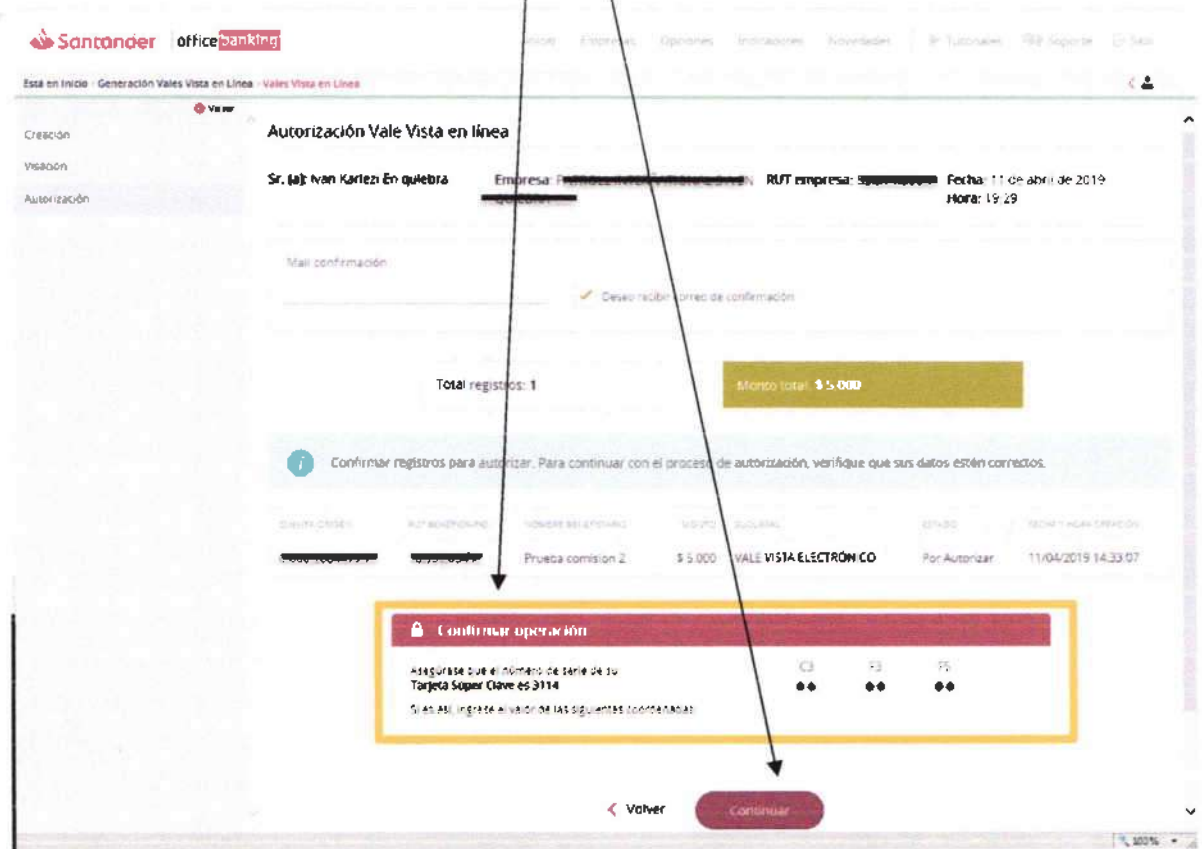


**Paso 7:** Luego de confirmar el registro del beneficiario, la página solicita la autorización para el Vale Vista electrónico, donde el sistema del Banco pide ingresar 3 coordenadas de la Superclave.

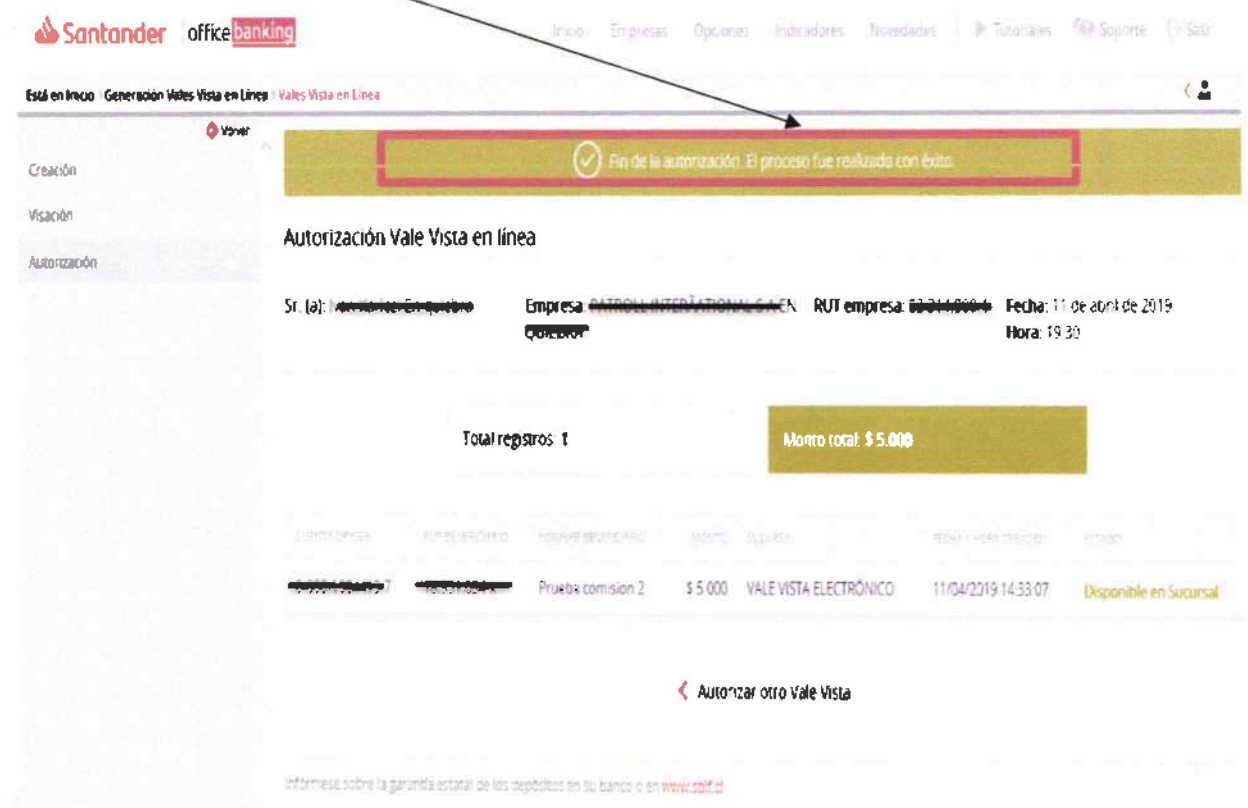




**Paso 8:** El usuario ingresa las 3 coordenadas solicitadas para la autorización del Vale Vista. Debe presionar el botón continuar.



**Paso 9:** Finalmente en la pantalla de la página va aparecer un mensaje que indica, Fin de la autorización, donde confirma que el proceso fue realizado con éxito.



Adicionalmente el portal de Office Banking presenta varias Atribuciones de perfiles que se detallan a continuación:



	Contrato	RUT Empresa	Razón Social	RUT Usuario	Nombre Usuario	Rol
<input checked="" type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-500-402-1	RODRIGO PEREZ	Apoderado
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-500-402-1	LUIS CRISTO PEREZ	Supervisor
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-447-557-2	MARIA ISABEL DIAZ BECERRA	Usuario
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-447-557-2	MARIA ISABEL DIAZ BECERRA	Controller
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-447-557-2	MARIA ISABEL DIAZ BECERRA	Apoderado
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-447-557-2	MARIA ISABEL DIAZ BECERRA	Supervisor
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	9-447-557-2	MARIA ISABEL DIAZ BECERRA	Apoderado
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.	40-562-500-6	MARCIO GARRIGOSO DEL PINO	Supervisor
<input type="radio"/>	500050001524300	89-009-200-R	OFFICE BANKING S.A.			Usuario

**Apoderado:** Persona natural que en la mayoría de los casos corresponde al representante legal de la empresa. Tiene facultades únicas por la empresa, las cuales van inscritas en las escrituras de la misma. Es el único perfil facultado para autorizar movimientos de transferencias y traspasos de dinero de una cuenta de la empresa a cualquier destino. Este nombre del perfil se presenta sólo en la modalidad de Office Banking no Modelado.

**Transaccional:** Cumple con el mismo perfil del Apoderado, pero en la modalidad de Office Banking Modelado (donde la Visación de los movimientos es automática).

**Supervisor:** Es un perfil dentro del portal online [www.officebanking.cl](http://www.officebanking.cl), que no es consultivo ni tampoco sirve para realizar movimientos de fondos de ningún tipo. El uso es netamente la Perfilación de las personas creadas en la empresa (Perfilación de servicios, asignación de cuentas a los servicios perfilados, crear dependencias, etc.). También puede Crear, Eliminar o Perfilar a Controller, Apoderados y Usuarios. Se presenta en Office Banking Modelado y no modelado.

**Controller:** Es un perfil dentro de la plataforma web Office Banking que puede, consultar, crear, subir y visar nominas o transferencias. Solo existe en el Office Banking no modelado, y es muy importante que esté creado, puesto que sólo este Rol puede visar las nóminas, si no está creado en Office Banking, las operaciones no se pueden concretar.

**Usuario:** Es un perfil dentro de la plataforma web Office Banking que puede, consultar, crear y subir nóminas o transferencias. Existe en Office Banking modelado y no modelado.

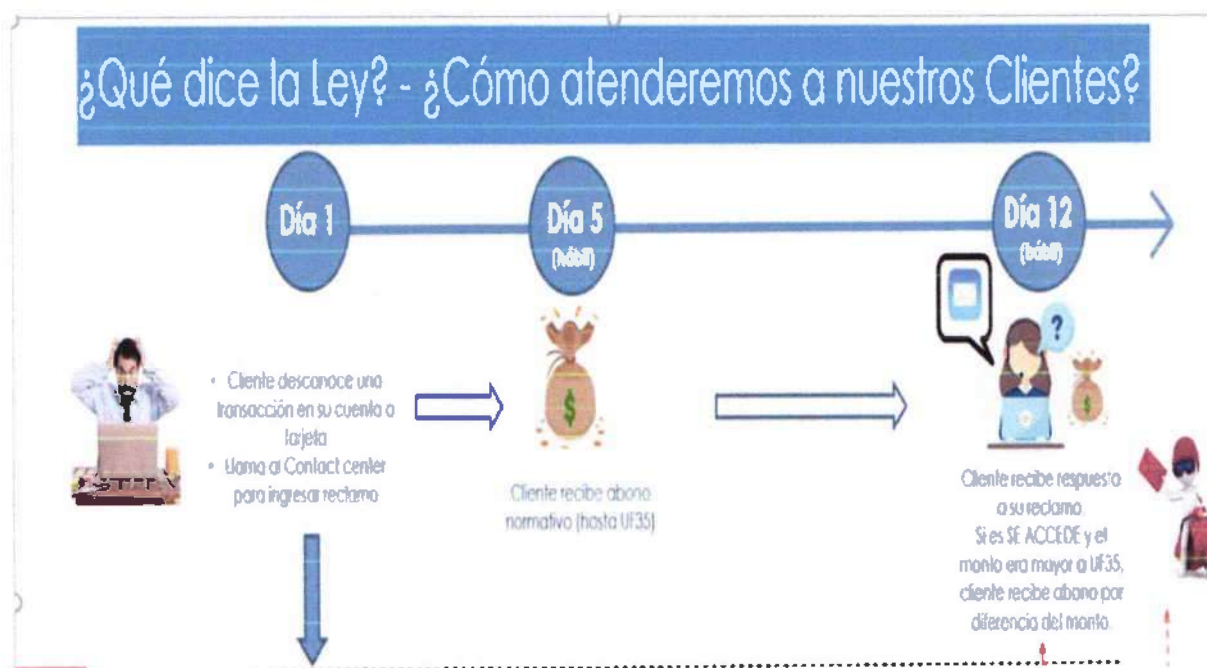
o **Medidas de alerta por parte de los clientes afectados.**

Conforme lo exige la normativa vigente, los cliente disponen de diversos mecanismos y canales de comunicación expeditos, los que operan durante las 24 horas del día para urgencias, sea este hábil o inhábil y plataformas de ingresos de reclamos.

Frente a cualquier evento los clientes deben llamar al Call Center (600) 320 3000 24 HRS, si registran transacciones desconocidas.

Ingresado el reclamo a través del Call Center, VOX ingresa un reclamo en el workflow (interno), SAC (servicio de atención a clientes), asignándole un número y fecha de compromiso para la respuesta.

**Flujo actual, luego de entrada en vigencia de la nueva Ley de Fraudes (Modificación de Ley N°20.009) en fecha 28 de Mayo 2020:**



**Las llamadas son registradas y almacenadas en Aplicativo Banco, el cual permite realizar trazabilidad y análisis a través de un identificador de la llamada ( Código ID)**

Adicionalmente frente a registro de transacciones desconocidas se procede al bloqueo de productos.

**Nota:** Los seguros de fraudes ya no operan para este tipo de fraudes en razón de la nueva Ley.

o **Medidas de Seguridad Plataforma Bancaria Santander.**

El Banco Santander Chile, posee una plataforma tecnológica segura, confiable que cumple con políticas y normativas de seguridad, estándares de seguridad de la información y ciberseguridad nacional e internacional y la cual es constantemente auditada.

Su plataforma digital transaccional online (Persona-Empresa), provee un conjunto de elementos y mecanismos que entregan seguridad y confiabilidad a los sistemas y las operaciones de sus clientes, con el fin de prevenir y evitar la ocurrencia de fraudes.

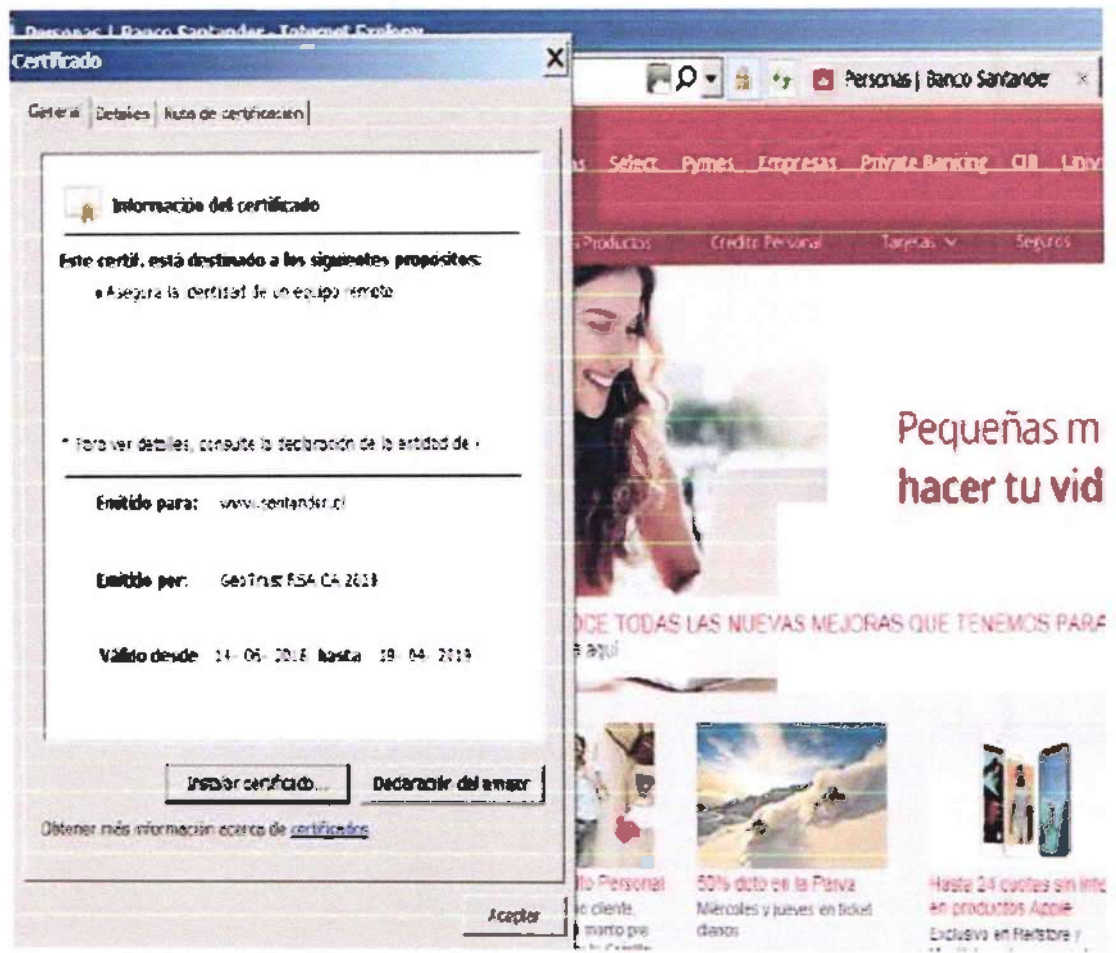
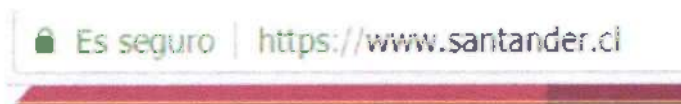
El siguiente cuadro muestra las medidas de protección que se toman en cada una de las etapas (Antes, Durante y Después) de un Fraude.

Antes	Durante	Después
1.- Protección y Confidencialidad de la información.	1.-Monitoreo de transaccionales inusuales con patrón de Fraudes de clientes.	1.-Investigación del Evento o reclamo de Fraude.
2.-Factores de autenticación de Seguridad robustos "autenticación y autorización de transacciones online".	2.-Bloqueo de cuentas (origen-destino) y claves de acceso ante la detección de un fraude o posibles fraudes.	2.-Recuperación de fondos en bancos destinos. (en caso de existir fondos retenidos)
3.-Políticas de accesos y contraseñas.	3.-Bloqueo y Marcado de cuentas receptoras de fraude.	3.-Gestiones Legales y denuncias.
4.-Montos Limites de transacciones por día.	4.-Monitoreo y Bloqueo de direcciones IPs de fraudadoras.	4.-Contacto con unidades de prevención de Fraudes de otras instituciones bancarias.
5.-Monitoreo y baja de sitios phishing en internet.	5.-Notificación via correo y push App 2.0. al cliente por movimientos en cuentas.	
6.-Monitoreo de seguridad 7x24. ante ataques a la plataforma Bancaria (SOC)	6.-Reporte de fraude y solicitud de retención de fondos a Bancos destino.	
7.-Equipamiento de seguridad perimetral y de protección a la infraestructura y sistemas Banco.		
8.-Campañas informativas de prevención de fraudes y concientización a clientes.		

• **Medidas de Seguridad: (Antes).**

**1. Protección y Confidencialidad de la información: Encriptado de la información y Navegación Segura.**

Encriptado de la Información: Protocolo seguro <https://www.santander.cl>. Como primera medida de seguridad en los sistemas transaccionales online que el Banco Santander disponibiliza a sus clientes, se encuentra el uso del protocolo seguro "https" y certificados digitales de firma con algoritmo **SHA256**, el cual tiene como objetivo más importantes la **encriptación de la información que viaja desde el equipo del cliente hasta los servidores del banco**, otorgando confidencialidad e integridad de la información y previniendo cualquier tipo de ataque de interceptación de la comunicación y robo de datos. Referencia también en la página 5 (navegación por la web de manera segura).



**2. Factores de autenticación de seguridad robustos "autenticación y autorización de transacciones online".**

El Banco a través de su plataforma transaccional online, coloca a disposición de sus clientes las siguientes medidas de seguridad y factores de autenticación de

flujo y empleabilidad secuencial, aplicados en distintas fases del flujo del proceso de pago, para mayor seguridad de los clientes:

**a) Clave de login de acceso a cuenta en el portal.**

Es el primer factor de autenticación de seguridad del sistema donde se autentifica al cliente. Consiste en la autenticación del cliente por su nro. De RUT y clave de cuatro dígitos, la que es creada por el mismo cliente, es de carácter personal e intransferible y es solo conocida por el cliente.



En consecuencia, si no se cuenta con la clave de ingreso al portal, no se puede operar en la plataforma digital. Si existe un error en el ingreso de claves por más de 3 intentos fallidos, ésta automáticamente es bloqueada por el sistema.

**b) Claves de Tarjeta de Coordenadas. (Super Clave).**

Es el segundo mecanismo de seguridad a validar por el sistema al cliente. Es un sistema de seguridad que consta de 50 claves de combinación única por tarjeta de cliente, y es utilizada para autorizar transacciones de pagos y transferencias remotas en los portales de atención online. Cada vez que el cliente registre una transferencia de fondos o realice pagos desde cualquiera de sus productos, el Banco le pedirá una combinación aleatoria de 3 claves de coordenadas diferentes, ubicadas en la tarjeta 'Super Clave' única, asignada cada cliente.

El cliente deberá ingresar de acuerdo a la combinatoria única de su tarjeta de coordenadas. Cabe señalar, que esta tarjeta de coordenadas, es un medio físico, el que es asociado al rut del cliente y entregado de forma presencial al cliente, luego de ser autenticado con carnet y validación de huella dactilar en la sucursal Bancaria. Este mecanismo es obligatorio para realizar cualquier transferencia a terceros o pago de servicios.

**Claves Tarjeta de Coordenadas o Super Clave.**



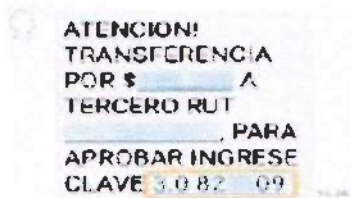
Si no se cuenta con el ingreso de las coordenadas correctas, la operación es rechazada. Si existe un error en el ingreso de claves por más de 3 intentos fallidos, al igual que se explica en el punto anterior, ésta automáticamente es bloqueada por el sistema.

Adicionalmente se utiliza el cálculo de las combinatorias únicas de la TC de 10 columnas y 5 fila, lo que da 50 elementos de los cuales el banco elige 3 en cada desafío, con una duración de tiempo, por lo que genera 19.600 combinatorias únicas para realizar las autorizaciones de las transacciones.

**c) Clave dinámica de un solo uso enviada vía SMS al cliente (Clave 3.0)**

**Clave 3.0. (OTP):** Es el tercer mecanismo de seguridad en el orden a validar por el sistema al cliente. Banco Santander envía y valida con una 3era. clave de seguridad dinámica y de un sólo uso, para todas aquellas transacciones electrónicas que cumplan con ciertos criterios y condiciones de riesgo.

La clave 3.0, es enviada vía SMS al nro. de teléfono móvil del cliente, el cual se encuentra registrado en la base de clientes del Banco, cada vez que se realice una transferencia electrónica.



Si el cliente no ingresa la Clave 3.0 cuando ésta es requerida por el Banco, la operación no será realizada. Si existe un error en el ingreso de claves por más de 3 intentos fallidos, esta automáticamente es bloqueada por el sistema.

**d) Clave Santander Pass: Permite autorizar las transacciones desde el celular, previamente enrolando la aplicación con las credenciales del cliente.**

**Video tutorial:**

[https://www.youtube.com/watch?v=nseegd6QqzU&feature=emb\\_logo](https://www.youtube.com/watch?v=nseegd6QqzU&feature=emb_logo)

### Mecanismos de Seguridad por Tipo de Transacción.

#### Transferencia electrónica de fondos (TEF) a terceros del mismo Banco u otro banco:

- Clave de login de acceso al portal.
- Autorización con clave de tarjeta de coordenadas. (Super Clave).
- Validación con tercera clave vía SMS al número de Teléfono del cliente. (Clave 3.0).
- El cliente es Notificado del pago o transferencia, a su correo y aplicación push en app Santander 2.0.

#### A Continuación, las acciones que podrían realizar los clientes.

#### Transferencia entre productos del mismo cliente (Avance de Línea de crédito, Avance de Tarjeta de crédito a cuenta corriente del mismo cliente):

- Clave de login de acceso al portal.
- El cliente es Notificado del pago o transferencia, a su correo y notificación PUSH en app Santander 2.0.

#### Pago en línea de servicios a través del Portal Santander:

- Clave de login de acceso al portal.
- Autorización con clave de tarjeta de coordenadas. (Super Clave).
- Notificación vía correo y PUSH acerca de los pagos realizados en app Santander 2.0.

### 3. Políticas de accesos y contraseñas.

Los portales transaccionales online Persona-Empresa del Banco Santander, cuentan con políticas de accesos, bloqueos y contraseñas, los cuales dan seguridad, confidencialidad y robustez a los procesos de autenticación de los clientes en el sistema, se mencionan a continuación:

- a) Política de robustez de contraseña en flujos de creación y cambio de clave login de acceso a cuenta en el portal.

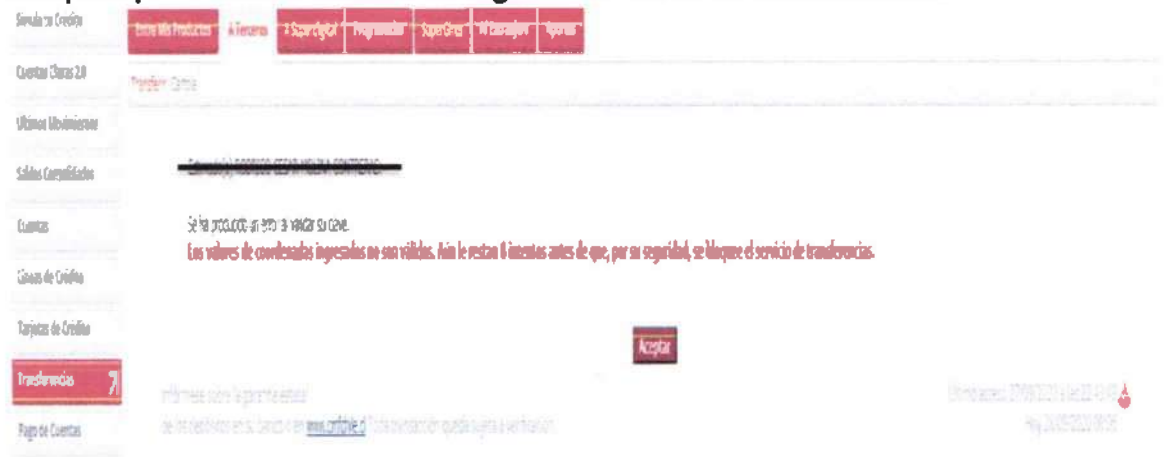




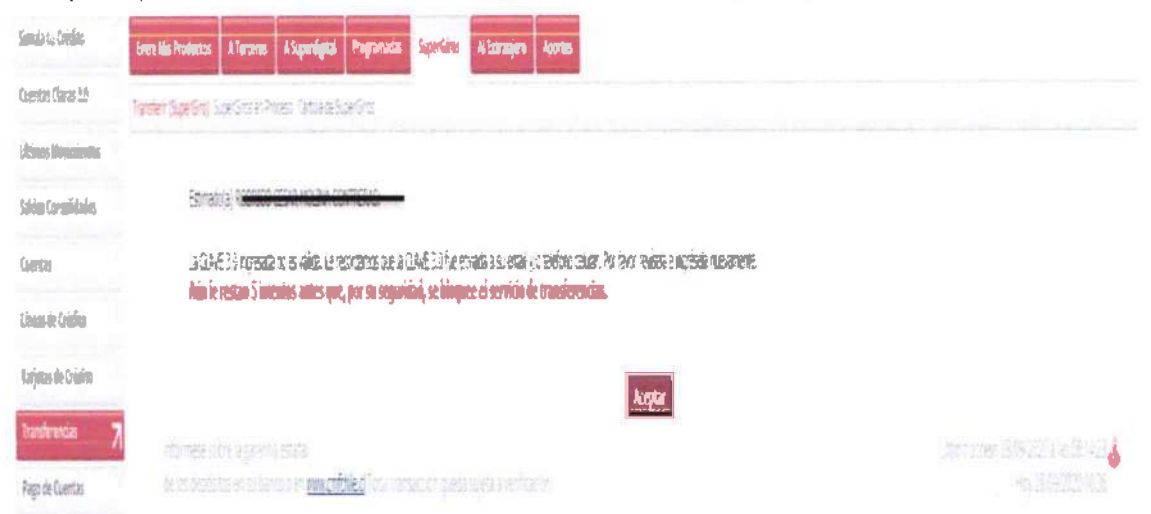
b) Bloqueo por intentos fallidos de ingreso de clave login portal.



c) Bloqueo por intentos fallidos de ingreso de clave de coordenadas.



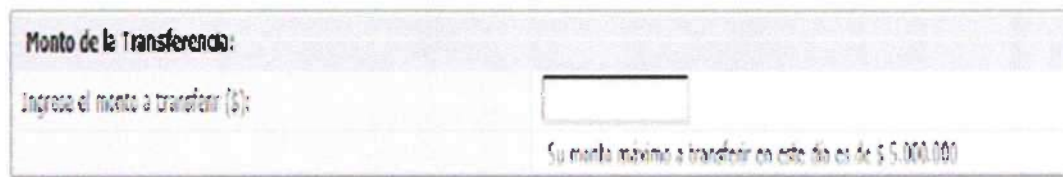
d) Bloqueo por intentos fallidos de ingreso clave 3.0. (OTP).



#### 4. Control de Monto Limite de transacción por día.

Actualmente Banco Santander, en sus portales transaccionales persona-Empresa online, establece y maneja controles de montos limites diarios por transferencia.

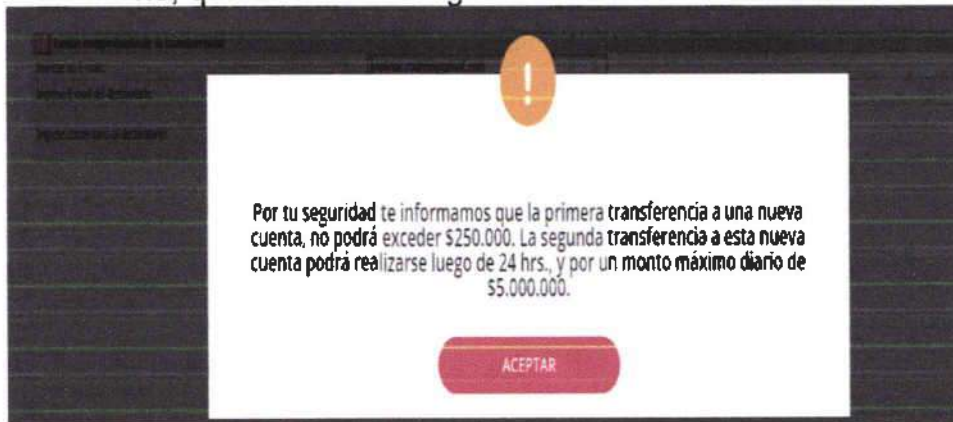
a) Portal Persona: Monto límite máximo transferencia por día 5M.



b) Portal Empresa: Monto máximo transacción 7M.

#### 5. Nuevo límite para primeras transacciones permitido por Banco Santander.

Portal Persona: Monto limite (\$250.000) 1ra transferencia electrónica a nuevo beneficiario, que comenzó a regir desde Noviembre 2018.



#### 6. Monitoreo y baja de sitios phishing en internet.

Banco Santander, posee un proceso de Monitoreo y baja de sitios phishing (ver página 3, "Tipos de fraudes electrónicos detectados en la actualidad"); que tiene como objetivo detectar y dar de baja los sitios phishing o sitios maliciosos que simulan ser sitios legítimos del Banco Santander, alojados en el internet.

#### 7. Monitoreo de seguridad 7x24 (SOC), ante ciber ataques.

Banco Santander, cuenta con una unidad especializada de monitoreo 7 x 24, de detección, prevención y respuesta ante eventos de amenazas de ciberseguridad o ciber ataques, dirigidos a la plataforma Bancaria.

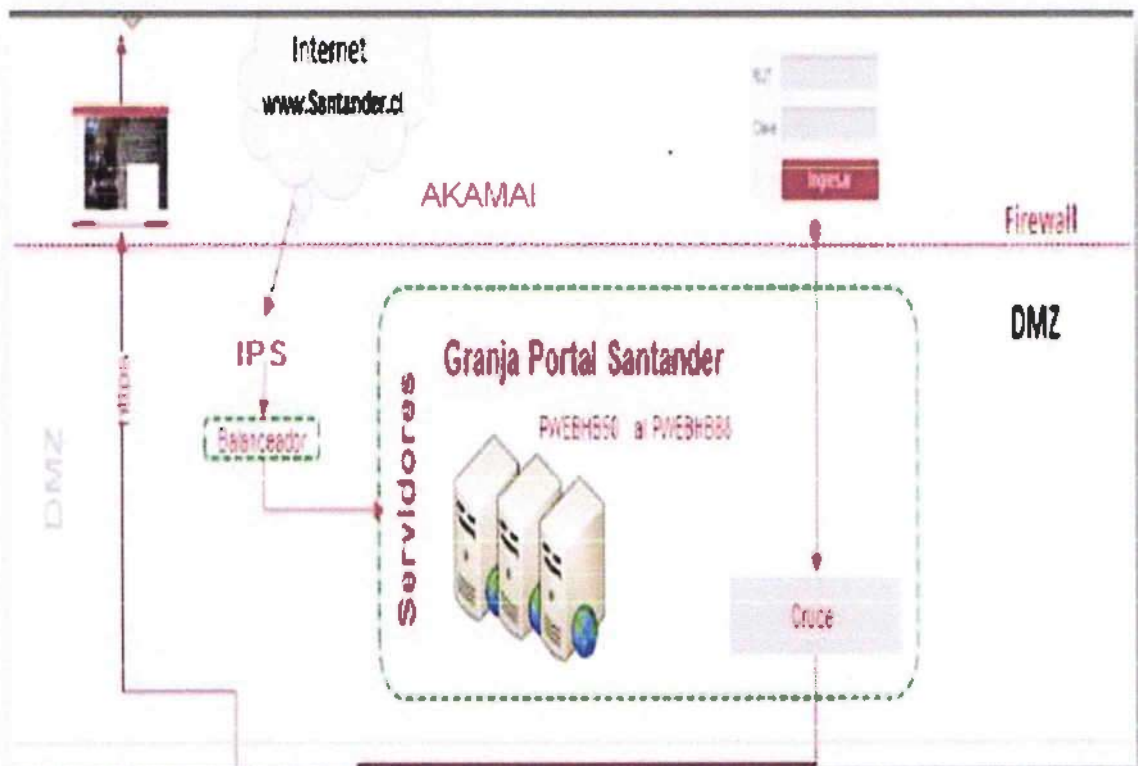
#### 8. Equipamiento de seguridad y protección perimetral a la infraestructura y sistemas del Banco.

El Banco Santander, cuenta con sistemas de protección de seguridad de sistemas y perimetral de última generación, que previenen las amenazas de ciberseguridad, también con un equipo especializado en el área de ciberseguridad, los cuales se encargan de garantizar la confidencialidad, integridad y disponibilidad de la información, servicios y sistemas del Banco.

Dentro de protección de equipos se pueden mencionar:

- a) Firewall y Web Application Firewall (Cortafuegos).
- b) Sistemas de detección y Prevención de Intrusos IPS-IDS.
- c) Sistemas de prevención de ataques volumétricos de denegación de servicio.
- d) Sistemas de prevención de ataques de día cero.
- e) Sistema de cargas y Balanceo.
- f) Otros.

**Topología de Seguridad, Banco Santander.**



DMZ: Zona desmilitarizada (en inglés, demilitarized zone).

**9. Campañas de comunicación de prevención de fraude y concienciación:**

Banco Santander permanentemente difunde campañas de prevención del fraude y concienciación a sus clientes a través de diversos canales y medios de información, para prevenir y evitar que sus clientes sean víctimas del fraude, generar conciencia, y entregar recomendaciones de seguridad y prevención de los tipos de fraudes de la actualidad.

Los medios utilizados para informar las campañas preventivas, se realizan a través del sitio público del Banco Santander (www.santander.cl), sitio privado (cliente dentro de su cuenta), a través de correos electrónicos, redes sociales y diario digitales de información (Diario, La Tercera).

Actualmente el Banco Santander tiene disponibles las siguientes Campañas de prevención:

Sitio público: Santander.cl



no dudes en llamarnos al 600 320 3000.

**Protege tus Tarjetas de Crédito**

- Recuerda que debes cuidar siempre tu Código CVV (Card Verification Value). Este código lo solicitan en la mayoría de los comercios cuando realizas compras online para verificar tu Tarjeta.

**En comercios Online:**

- Siempre lee atentamente lo Términos y Condiciones que tiene el comercio.
- Siempre verifica que se efectúen correctamente los cargos a tu Tarjeta.
- Siempre mantén deshabilitada la modalidad de suscripción automática en caso de no requerirla.
- Sé cuidadoso: no almacenes los datos de tus tarjetas en dispositivos que no son de tu uso personal. Terceros podrían hacer mal uso de ellas y efectuar compras sin tu autorización en comercios como iTunes, Uber, PayPal, Google, Netflix, entre otros.

**Te recomendamos:** Descargar la App Santander y activar las notificaciones, para estar siempre al tanto de los cobros que se realizan en tu Tarjeta.

luego realizar compras en el comercio.

**Sigue siempre estos consejos:**

- Digita directamente **www.santander.cl** y verifica que siempre la URL comience por **HTTPS://** (en vez de HTTP).
- Cambia periódicamente tu clave, idealmente cada 3 meses. Puedes realizarlo en Santander.cl o al 600 320 3000.
- Protégete de virus y malware descargando un antivirus en cada uno de tus dispositivos.
- En caso de extravío o hurto de tu teléfono registrado para recibir tu clave 3.0 te recomendamos llamarnos para bloquear tu Tarjeta de coordenadas y pedir el cambio de Clave de Acceso al Call Center (600) 320 3000.

### Sitio privado del cliente.

Santander.cl

Sitio privado - Santander.cl

**INFÓRMATE Y PROTÉGETE DE POSIBLES FRAUDES**

**Protege tus tarjetas** Si necesitas más protección, puedes bloquear o desactivar tus tarjetas en el momento que quieras por SMS.

**Protege tus pagos** Podrás hacer clic en cualquier momento en el sitio de nuestra App.

**Protege tus pagos** Siempre que recibas un correo de cualquier banco o tienda.

<p><b>Digita directamente www.santander.cl</b></p> <p>Almacena siempre la clave de URL directamente por HTTPS:// en vez de HTTP://</p>	<p><b>Protégete de virus y malware</b></p> <p>Descarga un antivirus en cada uno de tus dispositivos y actualízalo regularmente.</p>	<p><b>En caso de extravío o hurto de tu celular</b></p> <p>Te recomendamos llamarnos al 600 320 3000 para bloquear tu tarjeta de crédito y pedir el cambio de clave de acceso a tu tarjeta.</p>	<p><b>En caso de pérdida de servicio en tu celular</b></p> <p>Te recomendamos llamar a tu compañía telefónica para solicitar el cambio de clave de acceso a tu tarjeta.</p>
--	---	---	---

Protege tus productos también contra fraude y clonación. [Controla aquí >](#)

**INFÓRMATE Y PROTÉGETE DE POSIBLES FRAUDES.**

**INFÓRMATE Y PROTÉGETE DE POSIBLES FRAUDES.**

- Nunca, jamás, te haremos pagar por tu clave de acceso ni tu contraseña ni los términos que estás...
- Nunca, jamás, enviaremos correo electrónico sin tu consentimiento...
- Nunca, jamás, descargaremos archivos o datos de tus dispositivos sin tu consentimiento...

Te recomendamos además seguir estos consejos:

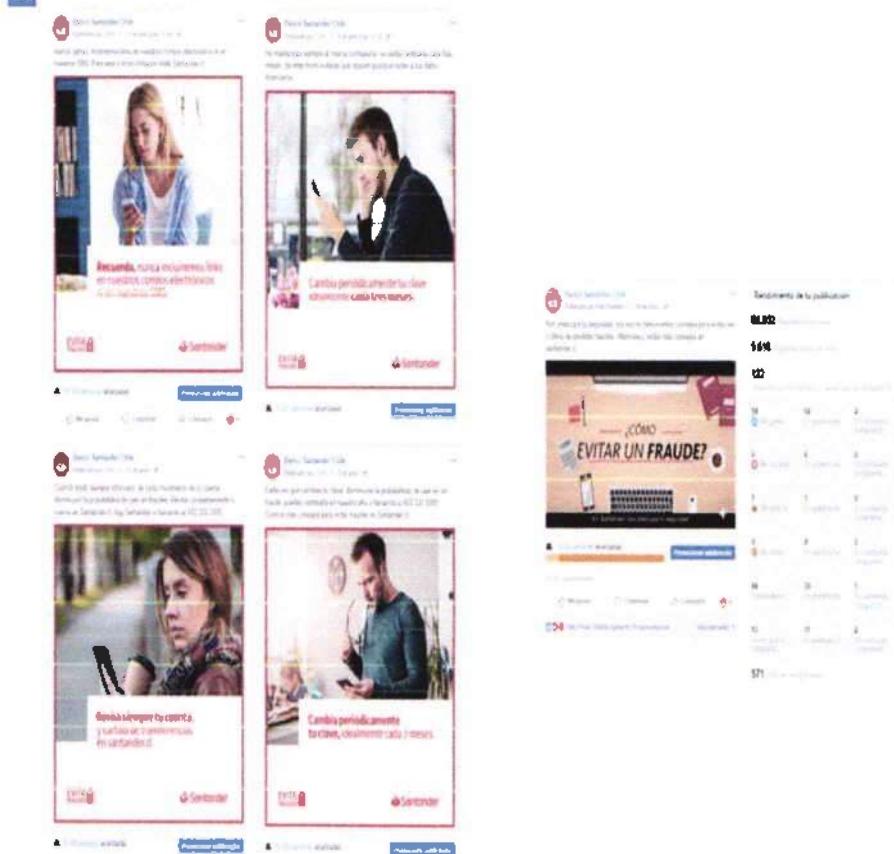
- Protégete de virus y malware descargando un antivirus en cada uno de tus dispositivos.
- En caso de extravío o hurto de tu teléfono registrado para recibir tu clave 3.0 te recomendamos llamarnos para bloquear tu tarjeta de coordenadas y pedir el cambio de clave de acceso al Call Center (600) 320 3000.
- En caso de pérdida de servicio en tu celular te recomendamos llamar a tu compañía telefónica para solicitar el cambio de clave de acceso a tu tarjeta.

Mensaje enviado al correo electrónico personal de cliente registrado en Banco Santander.



Publicaciones semanales con patrocinio en Facebook Santander Chile.

Publicaciones semanales con patrocinio en Facebook Santander Chile



### Campañas de prevención en sucursales.

En la actualidad, en las Sucursales de Banco Santander, se presentan 4 tutoriales activos en las pantallas de las Sucursales, los cuales entregan consejos y tips para prevenir fraudes.



En el siguiente link de YouTube se encuentran estos tutoriales disponibles.

[https://www.youtube.com/playlist?list=PLpEgeFOKf72PmAIjHRkcZjCLUXm\\_M2YB4](https://www.youtube.com/playlist?list=PLpEgeFOKf72PmAIjHRkcZjCLUXm_M2YB4)



Nota: Las campañas van rotando y cambiando periódicamente (por mes).

• **Medidas de Seguridad: (Durante).**

**1. Monitoreo de transaccionales inusuales con patrón de Fraudes de clientes.**

El Banco Santander, cuenta con sistemas de detección y mitigación de fraudes, también con un equipo de analistas Monitoreo y especialistas de Gestión de fraudes, quienes tienen como objetivo detectar los comportamientos transaccionales de posibles fraude en clientes y prevenir o mitigar el desarrollo y materialización del fraude en los clientes, gestionar el fraude y aplicar las acciones de seguridad que correspondan ante un evento de fraude, con el fin de reducir el impacto y la continuidad de un evento de fraude en los clientes. Se adjunta consola de Monitoreo de Eventos.

Date ID	Date	Business Unit	Total Amount	Issue	Issue	Sec	Party Code	Party Key	TID
81302703	01/20/11 11:32	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302703000	00000001
81302702	01/20/11 0:34	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302702000	00000001
81302701	01/20/11 0:32	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302701000	00000001
81302700	01/20/11 0:31	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302700000	00000001
81302699	01/20/11 0:30	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302699000	00000001
81302698	01/20/11 0:29	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302698000	00000001
81302697	01/20/11 0:28	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302697000	00000001
81302696	01/20/11 0:27	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302696000	00000001
81302695	01/20/11 0:26	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302695000	00000001
81302694	01/20/11 0:25	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302694000	00000001
81302693	01/20/11 0:24	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302693000	00000001
81302692	01/20/11 0:23	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302692000	00000001
81302691	01/20/11 0:22	Cuadras	1,000.00	No_Sol.		Banco Interamericano: NIBOR10000000	157049630000	81302691000	00000001

**2. Bloqueo de cuentas (origen-destino) y claves de acceso del cliente afectado.**

Luego de detectado y confirmado un fraude o en vías, en un cliente, el analista de Monitoreo y gestión de fraude (en Banco Santander), procede de manera inmediata con los bloqueos de las cuentas origen (para evitar que continúe la fuga de fondos) y cuentas destinos para bloquear y retener los fondos defraudados.

Adicionalmente, se bloquean las claves de accesos del cliente afectado al sistema, se marca en base Negative File el RUT del beneficiario destino defraudador y se marca en lista negra la cuenta receptora de los fondos defraudados.



### **3. Contacto con el cliente y recomendaciones de seguridad que debe seguir el cliente para el desbloqueo de las cuentas.**

Posteriormente de aplicar los bloqueos de seguridad, se contacta al cliente a través del ejecutivo, para indicar las acciones de seguridad que debe seguir el cliente y recomendaciones de seguridad que debe cumplir, para posteriormente, proceder a realizar el desbloqueo de la cuenta.

Entre las recomendaciones de seguridad se encuentran:

**"Cliente registra movimientos no habituales, que pueden permitir la ocurrencia de un eventual fraude, por lo cual necesitamos que puedas contactarlo e indicarle lo siguiente:**

**Se ha realizado un bloqueo preventivo de la cuenta del cliente, se solicita proceder con las siguientes acciones:**

- **Es necesario que el cliente realice una limpieza a su computador y a todos los equipos con los cuales opera regularmente con el Banco (celular, tablet, pc oficina, pc casa, etc.), luego debe instalar Antivirus.**
- **Nunca debe entrar en la web del Banco haciendo clic en links incluidos en correos electrónicos o eventualmente desde algún buscador (Google). Muchos correos fraudulentos utilizan nombres e imágenes corporativas de empresas, sin embargo, al hacer ingresar a los links, son re-direccionados a webs fraudulentas.**
- **Finalmente, cabe destacar que en los Portales del Banco Santander o a través de correos electrónicos, nunca se le solicitará información de la SUPERCLAVE (Tarjeta de Coordenadas) para desbloquear su cuenta o actualizar algún aplicativo.**

**Nota: Favor informar cuando cliente haya realizado cambio de claves y se le entregue nueva superclave, para dejar su cuenta desbloqueada."**

### **4. Bloqueo de direcciones IPs defraudadoras.**

Una vez detectada una dirección IP de origen fraudulenta, y tomadas las acciones de seguridad con los clientes afectados, la dirección IP es bloqueada para su ingreso en los portales del Banco.

### **5. Notificación vía correo y push App 2.0, al cliente por movimientos en cuentas.**

El Banco Santander, notifica a través de correo y mensaje PUSH por la APP móvil 2.0, los movimientos realizados en la cuenta del cliente. El cliente es notificado de toda transacción ejecutada dentro del Portal Santander, esto puede ser a través de correo electrónico registrado por el cliente y en caso que cliente tenga instalada la APP de Banco Santander en su equipo celular es notificado por medio de mensajería Push.

El Banco cuenta con este servicio de notificaciones de forma gratuita, la cual puede ser administrada y configurada por el Titular de la cuenta.



• **Medidas de Seguridad: (Después del Fraude).**

**1. Investigación del Evento o reclamo de Fraude.**

El equipo de especialistas de gestión de fraudes del Banco Santander, realizan un análisis e investigación exhaustiva, de las distintas fuentes de información tecnológicas y antecedentes para determinar la causa u origen del fraude y tomar las acciones correspondientes.

**2. Recuperación de fondos en Bancos destinos. (en caso de existir fondos retenidos).**

En caso de que las unidades de gestión de fraudes de los Bancos destinos (receptores de los fondos reportados) informen que los fondos lograron ser retenidos, se inician las acciones legales para proceder con la gestión de recuperación o devolución de fondos a su cuenta origen del cliente Banco Santander.

**En relación a las medidas de Prevención y Detección de Fraudes en Medios de Pagos (Tarjetas de Débito y Crédito):**

- I. Banco Santander Chile cuenta con todo el Parque de Tarjetas migrado a tecnología Chip, por lo que el comercio que tenga esta tecnología sólo permitirá la transacción con CHIP, asegurando que es la tarjeta física la que está operando.

**Respecto de la Tecnología Chip, se indica lo siguiente:**

La tecnología EMV define un conjunto de estándares de seguridad para las transacciones con tarjeta de débito y crédito, que también pueden usarse para los pagos móviles NFC. Comúnmente llamadas "tarjetas EMV" o "tarjetas de crédito EMV", estas tarjetas usan un chip inteligente en lugar de una banda magnética para alojar los datos requeridos para procesar una transacción, generando un código único que es validado para cada transacción y el cuál no puede reutilizarse. Un estafador no podría hacer una transacción usando una tarjeta falsa con datos robados en un terminal EMV porque no podría generar el código correcto.

La seguridad EMV se basa en una criptografía robusta que se utiliza para generar los códigos de transacción únicos que permiten a la terminal autenticar la tarjeta. Esta criptografía se basa en infraestructura de clave privada, lo que significa que solo una tarjeta con chip personalizada con la clave privada del tarjetahabiente durante la fabricación puede generar una transacción válida.

- II. A la fecha, Banco Santander Chile cuenta con 3D Secure™ (o 3DS), un sistema de seguridad en el cual se autentican las transacciones por internet Internacional para MasterCard, de los comercios que están asociados a los protocolos de Comercio seguro. Actualmente, a estas compras se les pide clave de portal más la clave de coordenadas.
- III. Por otra parte, Banco Santander cuenta con Webpay Plus, sistema de seguridad en el cual se autentican transacciones por Internet Nacional para todas las marcas, de los comercios que están asociados a los protocolos de

comercio seguro. A estas compras se les pide clave de portal más la clave de coordenadas o Santander Pass.

- IV. Notificaciones a clientes con diversos tipos de mensajería, esto dependerá de las reglas que se encuentren configuradas en el Sistema de Prevención de Fraudes para Medios de Pagos, por ejemplo: transacciones de alto riesgo, restricciones por Canales, bloqueos preventivos o definitivos, etc. Si el cliente tiene instalado en su teléfono móvil la App del Banco, se genera la mensajería a través de Notificaciones PUSH, de lo contrario el envío se realiza mediante SMS (Short Message Service) al número de teléfono registrado en el sistema del Banco.
- V. Campañas de comunicación de prevención de fraude a través del sitio público y privado de los clientes Santander, correos electrónicos, redes sociales y en las sucursales.

(\*) Actualmente, Banco Santander Chile cuenta con un Sistema autónomo de Prevención de Fraudes para Medios de Pagos, permitiendo realizar Monitoreo online de las transacciones de tarjetas de débito y crédito. Este monitoreo se ejecuta de las siguientes formas:

**Real Time:** Monitoreo online, es decir se puede detener el fraude desde la primera transacción. El sistema antes de autorizar, solicita la confirmación del sistema de monitoreo anti fraude.

**Near Real Time:** La transacción después de ser autorizada, llega al sistema de monitoreo para su análisis, esto es un complemento ya que permite realizar análisis con más información.

### 3. Gestiones Legales y denuncias.

Banco Santander, activa las acciones legales contra los responsables de los hechos, siempre y cuando exista un perjuicio a la organización. Banco Santander se encuentra en disposición de apoyar y aportar la información requerida en procesos legales de sus clientes.

#### • Medidas de seguridad para proveedores (medios de pagos).

##### 1. Servicio de Monitoreo 24\*7.

Servicio que monitorea en línea las alertas que se generan por transacciones con comportamientos riesgosos, con el objetivo de validar estos movimientos con el cliente.



## 2. Sistema Neural de Prevención de fraudes Near Real Time.

Sistema que se alimenta de reglas y condiciones para alertar transacciones riesgosas de los clientes, con el objetivo de tomar acciones preventivas ante un posible fraude.



## 3. Secure Code:

Las Compras internacionales a través de internet que se realicen en comercios adheridos a 3DS, poseen doble factor de autenticación para realizar el pago de la compra (Clave HB + coordenadas), datos adicionales de los datos de la tarjeta.



# 3D Secure

Verified by  
**VISA**

**MasterCard**  
SecureCode

El sistema 3D Secure, permite garantizar la identidad del titular de la tarjeta durante una compra en una tienda online.



## 4. CHIP:

Las tarjetas cuentan con la tecnología EMV, tecnología la cual es más segura y hasta la fecha no se ha sido posible clonar el CHIP.



**5. 100% Fallback:**

Los terminales que están con tecnología CHIP y la tarjeta tiene la misma tecnología, solo permita lectura de chip (operar / transaccional), lo que genera seguridad, pues no es necesario deslizar la banda, la cual frente a una clonación es la más vulnerable.



**6. VGP.** Servicio que permite la restricción de transaccionar a las tarjetas de débito de acuerdo a una zona geográfica determinada, ejemplo: por Regiones y/o Países. Cliente puede configurar su tarjeta a través del sitio privado del Banco.

**7. Bloqueo/Desbloqueo.**

Servicio de Bloqueo y desbloqueo de las tarjetas en línea, el cual el cliente lo puede realizar a través de la app o el sitio privado.

COMO BLOQUEO Y DESBLOQUEO MIS TARJETAS DESDE LA APLICACION SANTANDER CHILE



## 8. Notificaciones.

Envío de mensajes en línea a través de la app notificando cada movimiento de las tarjetas.



## 9. Alertas SMS:

Envío de mensaje de texto a los clientes notificando transacciones riesgosas.



Envío de mensaje de texto a los clientes notificando bloqueos preventivos y definitivos.

- **Flujo de autorización de una compra (medios de pago)**

El Banco Santander ofrece diversos productos y/ o servicios, entre los que se encuentra el otorgamiento de tarjeta de crédito.

La tarjeta de crédito **es un medio de pago** y un instrumento de crédito o financiamiento personal e intransferible, que permite al cliente adquirir bienes y servicios en cualquier establecimiento comercial del país y el extranjero.

El banco, previa evaluación del cliente (rentas e informes comerciales) le otorga montos en dinero (pesos y/o dólares) a la tarjeta, los cuales el cliente puede utilizar para comprar, pagar y girar, tanto nacionalmente como internacionalmente.

Son llamadas tarjetas "de crédito" porque cuando se paga a través de ellas, el banco que la otorgó está concediendo un préstamo que se debe pagar de acuerdo al periodo que se elija, según los plazos negociados con la entidad. Si se paga con tarjeta de crédito un producto el valor se debe al banco que expidió la tarjeta.



Las operaciones bancarias que se pueden realizar con tarjeta de crédito son:

- Medio de pago abierto y válido en cualquier comercio que acepte Tarjeta de Crédito en Chile o el extranjero.
- Habilitada para realizar avances en efectivo desde cajeros automáticos, en Chile y el extranjero.
- Acceso al servicio de Pago Automático de Cuentas de Servicios con Tarjeta de Crédito (PAT).
- El cliente puede utilizar las tarjetas de crédito para compra, tanto nacionalmente como internacionalmente. Ello por cuanto se le otorga al cliente montos en dinero en pesos y/o dólares a la tarjeta.
- Banco Santander utiliza un modelo de autorizaciones primero se debe distinguir entre una compra presencial y una compra a través de las plataformas on-line.

▪ **Compra Presencial.**

**Clave PinPass.**

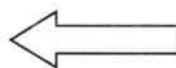
Consiste en la clave secreta de Tarjeta de Crédito para utilizar los cajeros automáticos y efectuar compras en comercios.



**Tecnología Chip.**

La tecnología chip crea datos dinámicos, lo que hace que cada transacción sea única y virtualmente imposible de replicar

CHIP





Para efectuar una compra a través de tarjeta de crédito con chip, si se cuenta frente a un terminal habilitado efectuado los siguientes pasos:

**PASO 1.**

Debe insertarse la tarjeta en el lector.



**PASO 2.**

Se deja la tarjeta en la terminal y siguen las instrucciones que aparecen en pantalla para luego ingresar PinPass (clave personal).



**PASO 3**

Se debe retirar la tarjeta cuando la terminal indique que se ha finalizado la transacción.



▪ **Compra a través de los comercios on-line.**

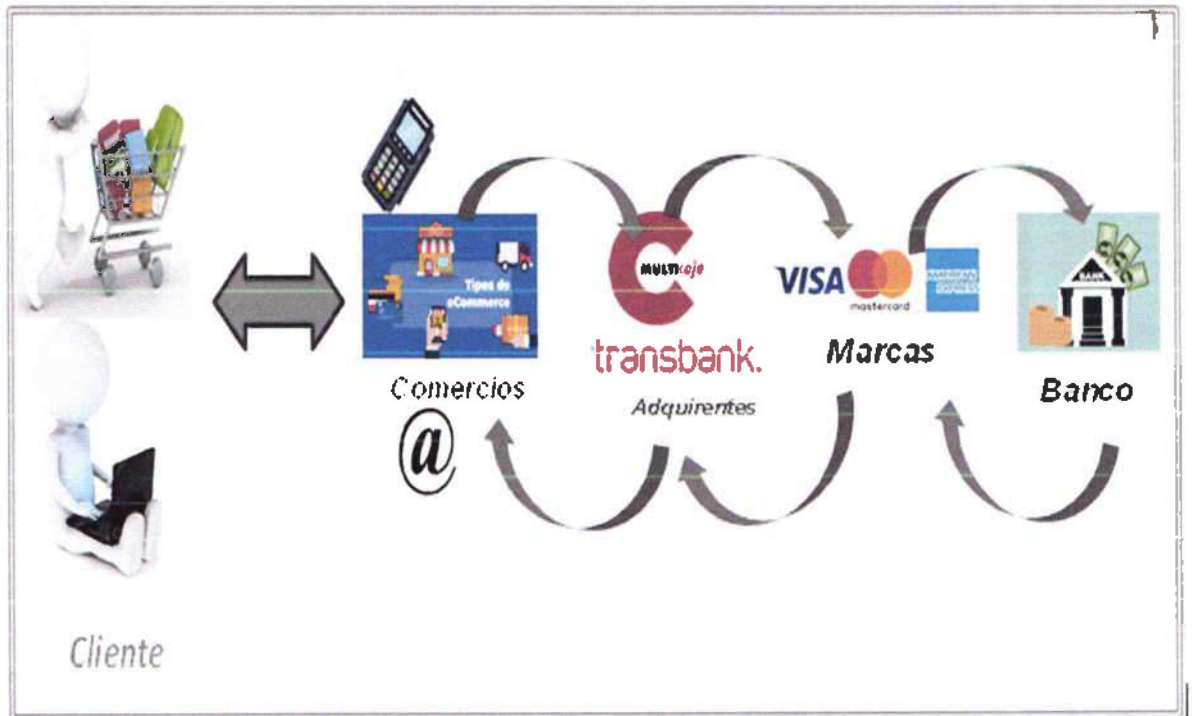
Para proceder a la autorización de las transacciones efectuadas a través de tarjeta de crédito, se distingue entre las transacciones nacionales e internacionales, operando distintas figuras.

Para las **transacciones nacionales**, interviene la figura de **Transbank**.

Para las **transacciones internacionales**, la autorización la otorgan directamente las marcas (**Visa, Mastercard y American Express**).

▪ **Gráfico de flujo de Transacciones Nacionales e Internacionales.**

Se explica en forma gráfica el proceso de autorización.



- Cliente realiza compra en Comercio Físico /ATM o Web y para realizar el pago de ese bien o servicio, debe acercar o ingresar el plástico en el POS/ATM y para el caso no presencial, debe digitar la información de la tarjeta en la página web del Adquirente (Redbanc; Transbank; Multicaja; etc.).
- Una vez que cliente confirma la transacción en POS/ATM o página web para solicitar la Autorización de la transacción, comercio/ATM a través de su Adquirente envía la información de la transacción a la Marca (Visa, AMEX o MasterCard).
- Las Marcas reciben esta mensajería en línea y efectúan validaciones del punto de vista del riesgo de fraude, que puede significar rechazar o no la transacción por este motivo, si ello no ocurre, se envía a emisor/Banco Santander para la Autorización de la compra.
- Emisor/Banco Santander, recibe la mensajería y valida principalmente:
  - o Seguridad de la tarjeta, criptografía de la tarjeta (Datos del plástico).
  - o Riesgos del punto de vista de Fraude.
  - o Situación y/o condición del plástico para operar.
- Realizada la evaluación de la transacción por el emisor/Banco Santander quien Aprueba o Rechaza la solicitud de Autorización de la Compra e informa a la Marca para continuar flujo de respuesta.

- Marca recibe la respuesta del Emisor/Banco Santander (Aprobada o Rechazada) e informa al Adquirente para que este visualice la respuesta en el front utilizado por el cliente, es decir, POS/ATM o Sistema WEB.
- Cabe mencionar, cuando el cliente realiza una compra por canal no presencial en un comercio seguro, el Adquirente solicita previamente a la Autorización de la compra, la autenticación del cliente por medio de los sistemas del Banco (seguridad), si esta es correcta, la transacción se envía a la marca y sigue flujo mencionado anteriormente para Autorizar la compra.

### Transacciones Presenciales y no presenciales.

Las transacciones presenciales son validadas con lectura de CHIP, ya que todos los plásticos cuentan con esta tecnología.

### Las transacciones no presenciales (Internet)

- Transacciones Nacionales

Se realizan utilizando una plataforma de compra (webpay plus), para esto el comercio debe estar adherido a esta modalidad de comercio seguro. Para efectuar las transacciones se ingresan los datos de seguridad de la tarjeta:

- Número de la Tarjeta
- Fecha de Vencimiento
- CVV2 (Card Verification Value).

Adicionalmente de validar los datos de la tarjeta, se autentica con la clave del portal del cliente y las coordenadas solicitadas de la tarjeta Súper Clave.

Paso a Paso:

1. Se elige producto y/o servicio que se desea comprar.
2. Se selecciona método de pago, para pagar con Tarjetas se realiza bajo la plataforma de Webpay Plus.



3. Se debe seleccionar tipo de tarjeta (crédito o débito)





4. La plataforma de Webpay Plus solicitará las claves para validar transacción. Dirigiéndolo automáticamente al sitio privado del Banco, donde el cliente para ingresar al portal Santander personas debe contar con una clave de cuatro dígitos "clave login de acceso a cuenta en el portal".

La clave login, consiste en el primer factor de autenticación de seguridad del sistema con el cual se autentica al cliente, esta clave es creada por el mismo cliente, es de carácter personal e intransferible, sólo conocida por el cliente y dinámica en cuanto éste puede cambiarla cuando lo desee.



5. Una vez ingresada la clave login, se solicitará la super clave, que es la clave contenida en la tarjeta de coordenadas asignada al cliente, la que contiene multi-combinaciones. Luego, se solicitará una combinación única que no se repite nunca, para realizar las operaciones por Internet.



6. Con este último paso se finaliza la compra, y se pasan a realizar las validaciones correspondientes.

• Transacciones Internacionales

Para las transacciones realizadas con tarjetas de crédito Mastercard o tarjetas de débito Masterdebit en comercios adheridos a Mastercard Secure Code se realizan utilizando una plataforma de compra segura.

Para efectuar las transacciones se ingresan los datos de seguridad de la tarjeta:

- Número de la Tarjeta
- Fecha de Vencimiento
- CVV2 (Card Verification Value).

Adicionalmente de validar los datos de la tarjeta, se autentica con la clave del portal del cliente y las coordenadas solicitadas de la tarjeta Súper Clave.

Paso a Paso:

1. Se elige producto y/o servicio que se desea comprar.
2. Se selecciona método de pago.

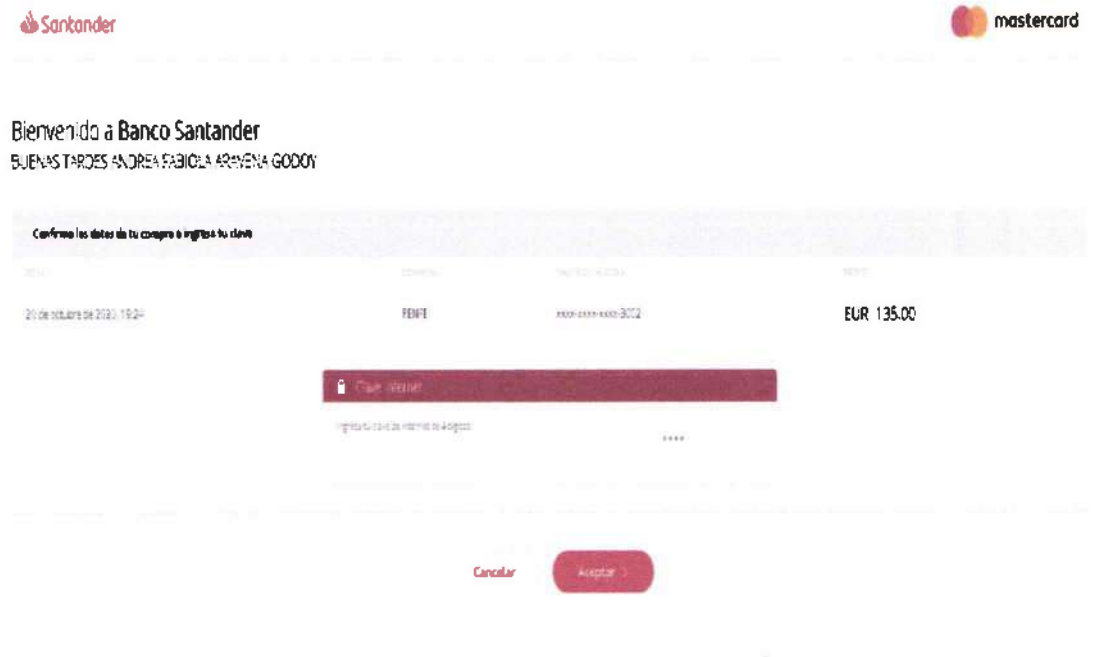


3. Se ingresan los datos de la tarjeta

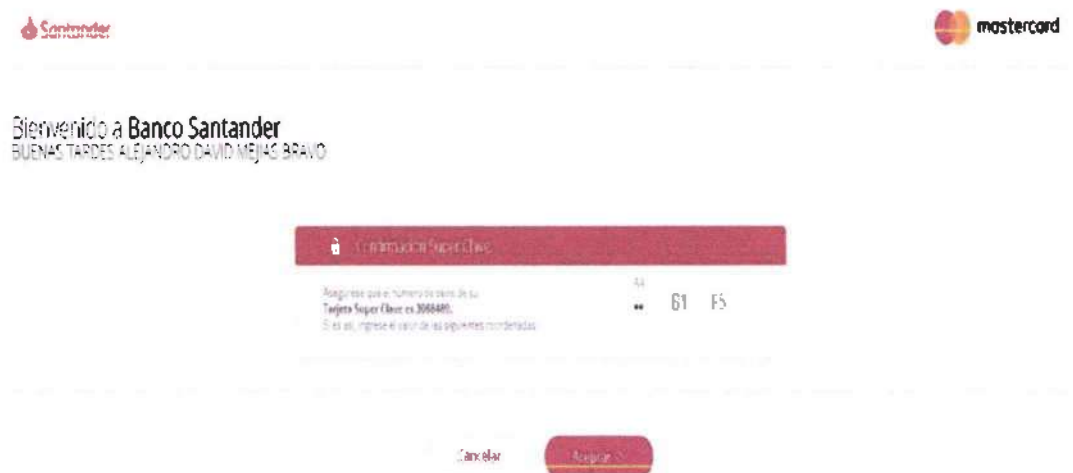


- La plataforma solicitará las claves para validar transacción. Dirigiéndolo automáticamente al sitio privado del Banco, donde el cliente para ingresar al portal Santander personas debe contar con una clave de cuatro dígitos "clave login de acceso a cuenta en el portal".

La clave login, consiste en el primer factor de autenticación de seguridad del sistema con el cual se autentica al cliente, esta clave es creada por el mismo cliente, es de carácter personal e intransferible, sólo conocida por el cliente y dinámica en cuanto éste puede cambiarla cuando lo desee.



- Una vez ingresada la clave login, se solicitará la super clave, que es la clave contenida en la tarjeta de coordenadas asignada al cliente, la que contiene multi-combinaciones. Luego, se solicitará una combinación única que no se repite nunca, para realizar las operaciones por Internet.



- Con este último paso se finaliza la compra, y se pasan a realizar las validaciones correspondientes.

- **Políticas de seguridad y control sobre proveedores Banco.**

Banco Santander, posee un Marco Metodológico de Control y Gestión sobre sus Proveedores, en el cual se establecen las directrices acerca del control, gestión y seguimiento de los proveedores del banco en el ámbito de la gestión del riesgo

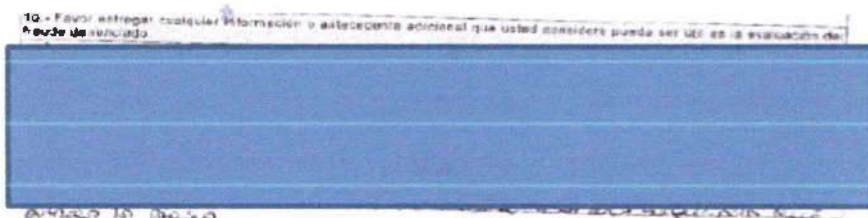
**CONTROLES RELACIONADOS CON PROVEEDORES.**

*El Modelo de acuerdos con terceros y control de proveedores, establece mecanismos de gobierno para gestionar el Riesgo Tecnológico y Operacional en la relación con los prestadores de servicios externos de los que dependen operaciones del Banco y sus filiales, cuyo objetivo es lograr un alto rendimiento y el reconocimiento de esos riesgos en la gestión de servicios externalizados. Para alcanzar el cumplimiento de lo anterior, el modelo cuenta con una figura estratégica: el Gestor de Servicio, quien debe ser un nexo entre el Banco (su Unidad) y el proveedor y, su Unidad con la Gerencia de Riesgos No Financieros, la Gerencia de Riesgo Tecnológico y Operacional, y la Gerencia de Administración, garantizando la existencia y ejecución de mecanismos de control y seguimiento.*

*Dentro de las principales funciones del Gestor de Servicio, están (a) tener plenamente identificados a los proveedores asociados a servicios críticos de su responsabilidad. (b) mantener actualizados los datos del proveedor, datos de contacto, información legal, nómina del personal del proveedor que trabaja directamente o en instalaciones del Grupo Santander, e informar a la Gerencia de Administración y la Gerencia de Riesgo Tecnológico y Operacional cuando éstos se modifiquen (c) verificar, al menos anualmente, que el contrato se encuentra actualizado con los servicios recibidos, las cláusulas mínimas de Riesgo Tecnológico y Operacional, y de corresponder, que la boleta de garantía se encuentre vigente y por un monto adecuado al servicio; (d) realizar anualmente la evaluación de los riesgos del proveedor, realizar seguimiento y mitigar el riesgo identificado; (e) Asegurar al menos anualmente que las cláusulas de Riesgo Tecnológico y operacional están actualizadas y se cumplen, obteniendo las evidencias de ello; (f) Al menos anualmente adquirir, conocer y difundir entre los integrantes de su equipo y de la Gerencia de Riesgo Tecnológico y Operacional, los Planes de Continuidad de Negocio del proveedor, el calendario de actualización de éstos, como también el plan anual de pruebas La Gerencia de Riesgo Tecnológico y Operativo, llevará un control sobre el cumplimiento de estas funciones informando en las instancias que corresponda los resultados. La herramienta a utilizar es el "Cuadro de Mando". Controles existentes en Unidad de Fraude y Seguridad de la Información de Banco Santander.*

- **Se indica breve reseña de ejemplo de caso investigado.**

**IMAGEN DENUNCIA**



**OBS. Analizar y ver si existen vestigios de acceso del cliente en el sistema Banco en la fecha y hora reportada por el cliente en su denuncia escrita.**

- **Se adjuntan evidencias de registros.**

Se puede constatar que conforme registros del Banco, existe solicitud de creación de clave para el cliente de uso del portal de Banco Santander el:

CHA	USUARIO	EVENTO	ESTADO
20/01/2017 10:02:47	<del>XXXXXX</del>	Crear solicitud de clave	Solicitada

La clave personal para la utilización del portal, fue creada por su titular el:

10/02/2017 23:40:04	<del>12.888.457.X</del>	Cambiar clave	Activa
---------------------	-------------------------	---------------	--------

- **Se debe analizar y adjuntar Contrato con Cláusulas (a modo de ejemplo).**

pasen a denominarse toda conjuntamente el Plan. g) Las políticas de seguridad de acceso a sistemas y plataformas de transmisiones electrónicas de datos y de los procedimientos, condiciones, modalidades y formas de operar que tiene el Banco para tales servicios, se encuentran publicadas y fácilmente accesibles y en versión imprimible en [www.santander.cl](http://www.santander.cl) bajo denominación "Políticas de Seguridad de Uso del Portal".


**Santander**

En 20/01/2017 a las 10:02:47 horas en el Portal de Banco Santander

Ciente 1: [Redacted]  
 RUT: [Redacted]  
 Domicilio: [Redacted]  
 Ciudad: [Redacted]

Ciente 2: \_\_\_\_\_  
 RUT: \_\_\_\_\_  
 Domicilio: \_\_\_\_\_ Comuna: \_\_\_\_\_  
 Ciudad: \_\_\_\_\_

ROMINA CARRELLI MOLINA  
Ejecutiva de Atención al Cliente  
BANCO SANTANDER CHILE

Firma Cliente 1  Firma Cliente 2



En cuanto a las claves de seguridad, el contrato celebrado por el cliente señala.

9.4. Clave Secreta y Medidas de Seguridad: La clave para el uso de la Tarjeta de Crédito es secreta, personal e intransferible, por lo que el Cliente debe mantener la debida diligencia, sigilo y cuidado en su utilización. En caso que el Cliente tomare conocimiento que su(s) Tarjeta(s) de Crédito hubiere(n) sido falsificada(s) o adulterada(s), como asimismo, en caso de extravío, hurto o robo de la(s) Tarjeta(s) de Crédito y/o claves secretas (PIN), el Cliente queda

10.4. Firma electrónica: El Cliente ha sido informado, entiende y acepta asimilar jurídicamente las claves secretas o firmas electrónicas que el Banco le proporcione (incluida su PIN de Tarjeta de Débito) a su firma manuscrita. El Cliente se obliga a mantener el debido cuidado en la utilización de su clave secreta, asumiendo la responsabilidad por los perjuicios que su mal uso o la utilización errónea pueda ocasionarle al mismo Cliente, al Banco y/o a terceros, cuando dicha mal utilización le sea imputable a él. El Cliente acepta que, en la primera oportunidad

Analizar si se vulneración a las medidas de seguridad de Banco Santander.

Para efectuar las operaciones de pago de servicios, necesariamente debe existir clave de acceso y Super-Clave, ambas en poder del titular.

- Se deben analizar las Transacciones no reconocidas.

- **Conclusiones.**

En la actualidad existen diversos mecanismos por los cuales los ciber-delincuentes pueden capturar la clave de acceso de un cliente Bancarizado, esto es a través de sitios web maliciosos o correos phishing, malwares / troyanos, usando técnicas de Ingeniería social, etc.

Realizados los análisis técnicos a las plataformas y el funcionamiento de los sistemas, no existe evidencia de que los estándares de seguridad del banco hayan sido vulnerados. Esto porque se concluye que todos los controles, medidas de seguridad y de autenticación operaron de forma efectiva y satisfactoria, por lo cual todas las claves utilizadas fueron validadas por el sistema de forma "exitosa" corresponden a las claves o credenciales del cliente las cuales son sólo del conocimiento y uso único del cliente:

- Clave de acceso al portal (Empresa, persona).
- Claves tarjeta de coordenadas.
- Clave 3.0 (OTP).

Se incorpora a este informe el actual mecanismo de autorización Santander Pass y la explicación de cómo activarlo.

Fueron incorporadas las evidencias de las políticas de bloqueos vigentes actuales con que cuenta el Banco Sander: intentos fallidos de clave de acceso, tarjeta de coordenadas y clave 3,0.

El Banco Santander cuenta con la unidad de Servicios de Atención al Cliente (SAC), para que el cliente frente a cualquier evento deba llamar al Call Center (600) 320 3000 24 HRS, si registra entre sus transacciones compras que desconoce ejecutar, donde el requerimiento del cliente se ingresa al sistema SAC, y puede realizar el bloqueo de inmediato de sus productos.

Se actualizó con un flujograma de gestión de reclamos a raíz de la entrada en vigencia de la Nueva Ley de Fraudes.

Se actualiza funcionamiento y proceso de autorización de operación de WEB PAY PLUS y 3ds. La actualización de Medios de Pagos del Banco Santander donde el nuevo flujo no incluye a que las transacciones pasen NEXUS.

En la actualidad, existen diversos mecanismos por los cuales los ciber-delincuentes pueden capturar la clave de acceso de un cliente Bancarizado, esto es a través de sitios web maliciosos o correos phishing, a través de malwares/troyanos, usando técnicas de Ingeniería social, etc.

Este es un informe genérico, por lo que se deben analizar y acompañar antecedentes de los hechos del caso particular.

Finalmente, destacar que el uso, custodia y confidencialidad de los productos y claves de seguridad, son de exclusiva responsabilidad de los clientes, por lo que éstos deben tomar las medidas necesarias para evitar que lleguen a conocimiento o uso de terceros. De igual forma, es responsabilidad de los clientes tener y mantener debidamente actualizada la seguridad tecnológica de sus equipos computacionales y de comunicación, a fin de evitar los fraudes y utilización de sus accesos y autorizaciones de sus transacciones por terceros.

- **Anexos (que se deben adjuntar, según corresponda).**
  - Contratos
  - Diligencia de Reconocimiento.
  - Visita Inspectoral al Banco Santander (Ejemplo).
  - Póliza de Seguro con sus respectivos anexos (si aplica).
  - Informe Liquidación Siniestro (si aplica, seguro).
  - Superintendencia de Bancos
    - Normas Superintendencia de Bancos (Vales Vistas).
    - Normas Superintendencia de Bancos (Tarjetas de Créditos).

**CAPÍTULO 2-6**

**DEPÓSITOS A LA VISTA**

**I. VALES A LA VISTA.**

**1. Emisión de vales a la vista.**

Los vales a la vista o vales vista que emiten los bancos por cuenta de terceros, pueden originarse solamente por la entrega de dinero en efectivo por parte del tomador o contra fondos disponibles que mantenga en cuenta corriente o en otra forma de depósito a la vista. Por consiguiente, si se toma el vale vista contra valores en cobro, el banco queda impedida de entregarlo hasta que se cumpla la gestión de cobro del documento con que fue tomado, salvo que opte por liberar la retención según lo previsto en el Capítulo 3-1 de esta Recopilación.

Los bancos podrán cobrar comisiones por la emisión de vales a la vista. Cuando establezcan este cobro, deberán anunciarlo mediante avisos que colocarán en un lugar visible de sus oficinas, señalando el importe de la comisión que cobrarán por ese servicio.

**2. Devolución al tomador del importe de un Vale Vista emitido a favor de un tercero.**

Los vales a la vista pueden extenderse, fundamentalmente, en dos formas distintas: a) a favor de un beneficiario que es el mismo tomador o un representante legal o mandatario de él; o, b) a favor de un beneficiario que es un tercero, caso en el cual opera la estipulación a favor de otro, tratada en el artículo 1449 del Código Civil.

Esta coincidencia o falta de coincidencia entre tomador y beneficiario reviste gran importancia para la devolución que deba hacer el banco emisor al tomador, de la suma que representa el documento, en caso de que no haya sido cobrado por el beneficiario.

Si la persona del tomador se confunde con la del beneficiario o si éste es un mandatario o representante legal de aquél y así se justifica ante el banco emisor, éste podrá devolver el dinero representado por el documento, sea al tomador, al beneficiario o a su representante.

En cambio, si se trata de personas diferentes que no son mandatarios o representantes legales del beneficiario o tomador, la existencia de una estipulación en favor de otro que no se sabe si ha sido objeto de una aceptación expresa o tácita de la persona a cuyo nombre se extendió el documento, obliga a tener un cuidado adicional antes de efectuar la devolución del dinero al tomador. Este normalmente deberá acreditar que el beneficiario no ha efectuado tal aceptación, mediante una declaración escrita en el documento que el mismo beneficiario deberá hacer bajo su firma, expresando: "Devuélvase al tomador". Esto puede también suplirse por un endoso del documento suscrito por el beneficiario.

### **3. Pérdida o extravío y caducidad de vales a la vista.**

Para los vales a la vista son plenamente aplicables las normas sobre pérdida o deterioro de títulos de crédito de que trata el Capítulo 2-12 de esta Recopilación Actualizada de Normas.

Por otra parte, estos documentos están sujetos a caducidad según las normas del Capítulo 2-13 de esta Recopilación.

## II. CUENTAS DE DEPÓSITO A LA VISTA.

Conforme a las disposiciones del Banco Central de Chile, los bancos pueden mantener cuentas de depósito a la vista bajo la modalidad de "Cuentas de ahorro a la vista" según lo establecido en el Capítulo III.E.2 de su Compendio de Normas Financieras, o bien, en las "Cuentas a la vista" de que trata Capítulo III.B.1.1 del mismo Compendio.

### 1. Cuentas de ahorro a la vista.

Para operar con las "Cuentas de Ahorro a la vista", los bancos deben ceñirse a las instrucciones establecidas por esta Superintendencia en el Capítulo 2-4 de esta Recopilación.

### 2. Otras cuentas de depósito a la vista.

Para abrir y mantener cuentas de depósito a la vista conforme a las normas del Capítulo III.B.1.1 "Cuentas a la vista" del Compendio de Normas Financieras del Banco Central de Chile, los bancos deberán atenerse a las siguientes disposiciones:

#### 2.1. Características de las cuentas.

Las "Cuentas a la vista" tienen las siguientes características básicas:

- a) Son en moneda nacional y no devengan reajustes, pudiendo convenirse el pago de intereses en los términos establecidos por el Banco Central de Chile en el Capítulo III.B.1.1 de su Compendio de Normas Financieras. Los bancos podrán mantener cuentas en moneda extranjera, las que no devengarán intereses ni reajustes, debiendo cumplirse las condiciones que se indican en el numeral 2.10 al tratarse de depositantes residentes en el exterior.
- b) Pueden ser unipersonales o pluripersonales y a nombre de personas naturales o jurídicas.
- c) Los bancos pueden cobrar comisiones por el manejo de las cuentas.

#### 2.2. Apertura de las cuentas.

##### 2.2.1. Condiciones Generales de Apertura y suscripción de contratos.

Para operar con "Cuentas a la vista", los bancos deberán aprobar y protocolizar ante Notario Público las Condiciones Generales de Apertura de Cuentas a la Vista. Estas condiciones generales deberán estar disponibles para consulta del público en el sitio web de la respectiva institución, sin perjuicio de mantener también ejemplares físicos en sus oficinas a disposición de los interesados.

Para abrir una cuenta se deberá suscribir un contrato entre el banco y el cliente, en que se hará referencia expresa al documento protocolizado que contenga las "Condiciones Generales de Apertura de Cuentas a la Vista" que corresponda.

El contenido del contrato, junto con las condiciones generales a las que hace referencia, corresponderá al dispuesto en el Capítulo III.B.1.1 antes mencionado, sin perjuicio de agregar las cláusulas adicionales que sean necesarias para referirse a las características particulares de la cuenta que se contrata.

Copia de contrato deberá entregarse al titular de la cuenta.

#### **2.2.2. Registro y verificación de los antecedentes básicos.**

Para la apertura de las cuentas deben verificarse y registrarse al menos los siguientes antecedentes:

- a) Número asignado a la cuenta;
- b) Nombre completo;
- c) Número de cédula de identidad del titular o, en el caso de personas jurídicas, de los apoderados;
- d) Domicilio;
- e) Profesión u ocupación y edad, al tratarse de personas naturales; y,
- f) Firma del depositante o, si se trata de una persona jurídica, de los apoderados o representantes de ésta, facultados para girar. En las cuentas pluripersonales deberán registrarse las firmas de todos los titulares.

En todo caso, cuando se trate de cuentas abiertas a nombre de personas jurídicas, deben exigirse las escrituras que den fe de la existencia legal de la sociedad y de la calidad de representantes legales de las personas que se registren como tales.

#### **2.2.3. Depósito inicial.**

Simultáneamente con la apertura de la cuenta debe efectuarse el depósito inicial.

#### **2.2.4. Apertura de cuentas mediante firmas electrónicas.**

De acuerdo con lo establecido en el Capítulo III.B.1.1 antes mencionado, la apertura de las cuentas puede realizarse utilizando firmas electrónicas, siempre que el Directorio, bajo su expresa responsabilidad, haya aprobado las políticas, procedimientos y sistemas para gestionar los riesgos legales y operacionales y prevenir la comisión de delitos.

Dichas normas permiten, no obstante lo indicado en los numerales precedentes, operar de inmediato las cuentas bajo ciertas condiciones que, en todo caso, deberán incluir limitaciones en los montos, disponiéndose de un plazo de 30 días a contar de la fecha del primer depósito para realizar la suscripción y las verificaciones necesarias para mantener abierta la cuenta.

El Directorio deberá además adoptar las medidas para mantenerse informado de los riesgos de estas operaciones, especialmente en lo que toca al funcionamiento de los controles para la prevención del lavado de activos de que trata el Capítulo 1-14 de esta Recopilación.

### **2.3. Utilización de sistemas de transferencia electrónica de fondos.**

El uso de sistemas electrónicos de transferencias de fondos para las cuentas de depósito a la vista se sujetará a las disposiciones generales establecidas en el Capítulo 1-7 de esta Recopilación.

En todo caso, los sistemas de cajeros automáticos u otros sistemas electrónicos que permitan depositar o girar automáticamente en las cuentas de depósito a la vista deberán comprender los controles o procedimientos necesarios para que ninguna cuenta se sobregire.

### **2.4. Depósitos.**

Los depósitos podrán efectuarse por ventanilla, mediante comprobantes de depósito o por medios electrónicos según lo indicado en el numeral 2.3 precedente.

En las cuentas pueden depositarse, además de dinero efectivo, cheques u otros valores a la vista y, en general, cualquier tipo de documentos de los que habitualmente se aceptan en depósito en cuenta corriente bancaria en moneda nacional.

Se recomienda, sin embargo, a los bancos que, con el fin de prevenir hechos delictuosos, se abstengan de aceptar depósitos en cuentas a nombre de personas naturales, constituidos por cheques u otros documentos extendidos a la orden de personas diferentes del titular de la cuenta, y en caso alguno aceptar tales depósitos cuando los beneficiarios de los documentos sean personas jurídicas. No obstante lo expuesto, siempre será admisible que el propio girador de un cheque extendido a su nombre, a su orden o al portador, lo endose para depositarlo en alguna cuenta ajena.

Los valores en cobro depositados quedan sujetos a retención conforme a las normas del Capítulo 3-1 de esta Recopilación, debiendo el banco depositario informar al titular de cualquier cargo que se efectúe en su cuenta con motivo del rechazo de un documento depositado en ella.



### 2.5. Giros.

Los giros podrán efectuarse mediante cajeros automáticos u otros dispositivos electrónicos, o por ventanilla, utilizando para ese fin una papeleta de giro que debe proporcionarle el banco.

Cuando los giros se realicen por caja, los bancos deberán comprobar, además de la identidad del girador y la existencia de fondos disponibles, que la firma de la papeleta esté conforme con la del registro de firmas que deberá mantenerse para el efecto.

### 2.6. Comisiones.

Los bancos fijarán la modalidad que aplicarán en el cobro de comisiones por el manejo de las cuentas y el monto que por ese concepto cobrarán a los respectivos titulares, conforme a las siguientes instrucciones:

- a) El plan de cobro de comisiones que se establezca no podrá hacer discriminación alguna entre clientes que se encuentren en igual situación.
- b) Los bancos que cobren comisiones por las cuentas a la vista deberán informar tal condición y la correspondiente tarifa, en los estados de cuenta que periódicamente deben enviar a los titulares de éstas o en un volante anexo a dichos estados. Igualmente, deberán darlas a conocer mediante avisos colocados en sus locales de atención de público, como también en su sitio web.
- c) Las comisiones serán percibidas detrayendo su importe de la cuenta que las origine. En caso de que la comisión que debe cargarse a la cuenta fuera superior a su saldo, la diferencia podrá ser imputada posteriormente si la cuenta llegare a tener saldo.

### 2.7. Información al Público sobre pago de intereses.

Los bancos que acuerden el pago de intereses por los saldos mantenidos en cuentas a la vista en moneda nacional, deberán informar en pizarra la tasa de interés que pagarán por esos saldos, expresada en términos anuales, sobre base de 360 días, como también las condiciones que puedan exigirse para recibir ese beneficio como, por ejemplo, el requisito de mantener un determinado saldo mínimo. Asimismo, deberán informar que el abono de los intereses se hará mensualmente, calculado sobre los saldos mantenidos en el mes precedente.

En el caso que el banco cobre, por otra parte, comisiones por los servicios relacionados con esas cuentas, según lo indicado en el numeral 2.6 del presente título, y esos cobros afecten a las cuentas que devengan intereses, deberá complementarse la información sobre la tasa de interés, con la relativa a las comisiones que las afectan y los conceptos por los cuales se aplicarán (administración de la cuenta; entrega de "cartola"; uso de cajero automático; etc.). En los casos que proceda, deberá informarse la periodicidad que cubre cada cobro, de modo que los interesados puedan tener conocimiento tanto del beneficio que reciben por los intereses que se le abonarán, como de los costos que deban pagar por concepto de las distintas comisiones, sea por la mantención de la cuenta como por las operaciones que se efectúan en relación con ella.

Sin perjuicio de esa información general, las instituciones depositarias deberán informar mediante avisos en sus oficinas, con una anticipación mínima de cinco días a la fecha de su vigencia, cualquier cambio que se haga a las tasas de interés vigentes. Ese aviso podrá omitirse cuando se trate de un aumento de la tasa vigente.

En la publicidad que se haga en medios escritos deberá incluirse la misma información antedicha. Cuando se trate de publicidad en medios audiovisuales se podrá informar la tasa nominal ofrecida adicionada, en los casos que corresponda, de una leyenda que recomiende informarse sobre las comisiones a que están afectas las cuentas a la vista.

Por otra parte, las instituciones que mantengan una página "web", deberán presentar en ella, en un sitio que sea de fácil acceso y ubicación, la información a que se refiere este numeral, incluyendo a modo ilustrativo, uno o más ejemplos que muestren la rentabilidad neta que se obtiene por aplicación de la tasa de interés ofrecida, menos los gastos a que, por concepto de comisiones pudieren estar afectas esas cuentas.

#### **2.8. Desahucio o cierre de una cuenta.**

Las cuentas de depósito a la vista son de plazo indefinido por lo que sus saldos, mientras esté vigente la cuenta, no quedan sujetos a caducidad.

#### **2.9. Envío periódico del estado de movimiento y saldos.**

Conforme a lo dispuesto en el Capítulo III.B.1.1 del Compendio de Normas Financieras del Banco Central de Chile, las instituciones depositarias deberán enviar periódicamente a los titulares, estados numerados correlativamente con los movimientos y saldo de las cuentas.

Para dar cumplimiento a esas disposiciones, los bancos depositarios deberán sujetarse a las siguientes instrucciones específicas:

- a) En caso de que no se pacte con el titular su frecuencia de entrega, los estados de cuentas deberán enviarse a lo menos mensualmente. Sin embargo, no será necesario enviar un nuevo estado para una cuenta que no haya registrado ninguna imputación desde la fecha a que se refiere el último estado remitido.
- b) El estado deberá contener al menos la siguiente información: i) número del estado; ii) nombre completo del titular, dirección y número de cuenta; iii) fecha de cada débito y crédito; iv) importe de cada partida, identificando el concepto por el cual se acreditó o debitó; y v) saldo inicial y final de la cuenta en el periodo informado.
- c) El estado se enviará por carta al domicilio registrado del titular, salvo que se acuerde con el cliente otra dirección o bien su entrega en un documento magnético por correo electrónico.

#### **2.10. Cuentas abiertas a personas residentes en el exterior.**

Los bancos podrán abrir cuentas de depósito a la vista a personas naturales o jurídicas residentes en el exterior, prescindiendo del requisito de exigencia del Rol Unico Tributario (RUT) mencionado en el Capítulo 20-1 de esta Recopilación.

La finalidad fundamental de estas cuentas, será atender pagos que su titular deba efectuar en Chile por diversos conceptos como, por ejemplo, gastos por la exploración de negocios en el país o aquellos previos a la iniciación de actividades.

En todo caso, el banco que proceda a abrir una cuenta de esta naturaleza, deberá reunir y mantener los antecedentes mínimos que permitan identificar al titular de ella, su actividad, las condiciones convenidas bajo las cuales operará la cuenta y el objeto de la misma.

#### **2.11. Aplicación de otras disposiciones.**

Las "Cuentas a la Vista" utilizadas para operar tarjetas de débito, quedan sujetas a las instrucciones complementarias señaladas en el Capítulo 2-15 de esta Recopilación Actualizada de Normas.

Como es natural, a las cuentas de que trata este título les son aplicables todas las instrucciones generales que afectan a depósitos y captaciones, tales como las relativas al encaje, reserva técnica, prohibición de ofrecer otros beneficios apreciables en dinero a los titulares, distintos al pago de intereses en los casos que corresponda, etc.

Por las razones expresadas en el Capítulo 2-4 de esta Recopilación para las cuentas de ahorro, también resulta aplicable para las "Cuentas a la vista" la recomendación de esta Superintendencia en orden a abstenerse de recibir su saldo en garantía, la que, en todo caso, no es válida para los efectos de los límites de crédito del artículo 84 de la Ley General de Bancos.

- o Superintendencia de Bancos (Tarjetas de Créditos).



## CAPÍTULO 8-3

### TARJETAS DE CRÉDITO

#### 1. Emisión de Tarjetas de Crédito.

De conformidad con las disposiciones del Capítulo III.J.1 del Compendio de Normas Financieras, del Banco Central de Chile, las entidades que emitan u operen sistemas de tarjetas de crédito deberán estar inscritas en el Registro de Emisores y Operadores de Tarjetas de Crédito de esta Superintendencia.

Para los efectos de estas instrucciones y de acuerdo con la definición entregada por el Banco Central de Chile, se entiende por "tarjeta de crédito" cualquier instrumento que permita a su titular o usuario disponer de un crédito otorgado por el emisor, utilizable en la adquisición de bienes o en el pago de servicios prestados o vendidos por las entidades afiliadas con el correspondiente emisor u operador, en virtud de convenios celebrados con estas, que importen aceptar el citado instrumento como medio de pago, sin perjuicio de las demás prestaciones complementarias que puedan otorgarse al titular o usuario.

Los bancos quedan inscritos en el Registro de Emisores y Operadores de Tarjetas de Crédito, en calidad de emisores, por el solo hecho de contar con autorización de esta Superintendencia para funcionar, pudiendo operar por sí mismos las tarjetas que emitan o contratar la operación total o parcial de las mismas a una o más entidades que se encuentren inscritas como operadoras.

Los bancos no podrán actuar como operadores de tarjetas emitidas por terceros. Para los efectos de estas normas, se entiende que un banco no actúa en calidad de operador en los siguientes casos en que la responsabilidad de pago recae sobre el emisor: i) cuando paga a los establecimientos comerciales las adquisiciones de bienes o servicios efectuadas mediante tarjetas de la misma marca, pero emitidas por otra entidad emisora del país; o, ii) cuando sea autorizado por esta Superintendencia para actuar como mandatario de un emisor de tarjetas de crédito situado en el extranjero, en los términos previstos en el Título IV del Capítulo III.J.1 antes mencionado.

#### 2. Información de tarjetas que decidan emitir.

Los bancos deberán informar a esta Superintendencia las marcas de las tarjetas de crédito que decidan emitir, con anterioridad a su puesta en circulación, debiendo indicar si ellas podrán ser usadas en el exterior o sólo en el mercado nacional.



### 3. Contratos.

El Banco Central de Chile ha dispuesto los contenidos mínimos de los contratos que deben suscribirse entre el Emisor y los Titulares o Usuarios de tarjetas de crédito. Para los demás contratos, esto es, los que tocan el ámbito de fiscalización de esta Superintendencia y que deben suscribirse entre los Emisores, Operadores y las personas que aceptan las Tarjetas como medio de pago, las entidades fiscalizadas se atenderán a los siguientes criterios generales:

#### 3.1. Contratos con las entidades afiliadas.

Los contratos que celebren los emisores, o los operadores es su caso, con los establecimientos afiliados que se comprometen a vender bienes o a prestar servicios a los titulares de sus tarjetas, deberán especificar debidamente todas las obligaciones y derechos de las partes, debiendo en todo caso estipularse:

- La responsabilidad de pago a las entidades, en los plazos convenidos con arreglo a lo dispuesto en el Capítulo III.J.1, especificando el momento a partir del cual se computan tales plazos, de acuerdo a las diferentes modalidades de pago puestas a disposición del tarjetahabiente.
- Los procedimientos y mecanismos de conciliación y validación de las transacciones y de los montos que deben ser pagados a las entidades afiliadas, así como aquellos para realizar reclamos y solicitar rectificaciones.
- Las medidas de seguridad que las partes deben considerar para precaver el uso indebido de la tarjeta y para cautelar la integridad y certeza de las transacciones efectuadas por medio de dicho instrumento.
- Responsabilidad económica que le cabe a cada parte, ante el uso indebido de las tarjetas o por los eventuales errores que pudiesen existir en la validación de las transacciones.
- La identificación de las redes y sistemas disponibles, para la transmisión electrónica de la autorización y captura de las transacciones efectuadas.
- Las causales para la suspensión de servicios, que tengan su origen en incumplimientos por parte de la entidad afiliada, junto a las condiciones y plazos para la reposición de los mismos.
- La responsabilidad del emisor u operador respecto de la continuidad del servicio, así como los procedimientos de contingencia y eventuales compensaciones a la entidad afiliada, ante una interrupción de los mismos.
- Identificación de las marcas de tarjetas a las que es aplicable el contrato, así como una mención al derecho del establecimiento afiliado de elegir cuáles acepta.
- Estructura tarifaria aplicable a cada uno de los servicios contratados, así como su periodicidad y formas de pago.

### 3.2. Contratos entre Emisores y los Operadores.

Los bancos que encarguen la administración de sus tarjetas a un operador, dejarán claramente establecidos en los contratos los actos que constituyen dicha administración y las obligaciones que emanan de ella y que contraen ambas partes. Entre los aspectos mínimos que deben ser abordados en los contratos están:

- Identificación de los servicios contratados y de los requisitos y estándares de operación requeridos para la prestación de cada uno de ellos.
- La responsabilidad del operador respecto de la continuidad de los servicios contratados, así como los procedimientos de contingencia y eventuales compensaciones, ante una interrupción de los mismos.
- Los servicios que pueden ser externalizados por parte del operador y aquellos que requieran contar con consentimiento particular del emisor.
- Estructura tarifaria aplicable a cada uno de los servicios contratados, así como su periodicidad y formas de pago.
- La responsabilidad de la empresa operadora para cautelar la seguridad y el oportuno procesamiento y validación de las transacciones, así como las obligaciones económicas que se originen ante errores y transacciones indebidas.
- La responsabilidad del operador de mantener un adecuado orden de los archivos con el registro de las operaciones procesadas, así como de los documentos que respaldan esas transacciones.
- Las obligaciones que le caben a cada una de las partes, en relación a la oportuna liquidación de los pagos.

Igualmente, en los contratos deberá especificarse en forma expresa que las bases de datos que se generen, con motivo de los procesos administrativos de las tarjetas de crédito, son de exclusiva responsabilidad de los respectivos emisores u operadores en su caso y, por ende, su uso o la información que de ellas puede obtenerse no puede ser utilizada por terceros.

## 4. Sobre las características y el uso de las tarjetas

### 4.1 Información en las oficinas de atención de público.

Los bancos deberán mantener en su sitio web y en las oficinas en que ofrezcan sus tarjetas de crédito al público, una amplia información acerca de las marcas, tipo de tarjetas ofrecidas, requisitos para optar a ellas, sus principales características y condiciones de uso, así como de las comisiones y/o cargos a que están afectas, tanto en monto o tasa, como los conceptos por los cuales se cobra y la periodicidad de esos cobros.

#### **4.2. Características de las tarjetas**

Las tarjetas de crédito son intransferibles y deben emitirse con observancia de las mejores prácticas existentes en este negocio.

Las tarjetas deberán contener, a lo menos, la información que permita conocer: la marca, el nombre del emisor, su numeración codificada y el nombre del titular o de la persona autorizada para su uso, cuando se trate de tarjetas adicionales.

#### **4.3. Información al usuario para el manejo de las tarjetas.**

Los bancos deben instruir a los usuarios acerca de las precauciones que deben tener en el manejo de sus tarjetas físicas y de los medios en que ellas pueden ser utilizadas, especialmente para mantener en resguardo las claves personales, así como de las principales normas que rigen su uso.

#### **4.4. Pérdida, hurto, robo, falsificación o adulteración de la tarjeta.**

Conforme a lo dispuesto en la Ley N° 20.009, el emisor u operador, según corresponda, deberá mantener los servicios de comunicación que le permitan al titular avisarle en cualquier momento y en forma gratuita, el extravío, hurto, robo, falsificación o adulteración de su tarjeta.

El banco deberá mantener informado a sus clientes, proporcionando al menos información por escrito al momento de contratar el servicio y manteniéndola en un lugar destacado de su sitio web, del procedimiento que un afectado debe seguir y la vía que puede utilizar para dar el correspondiente aviso. En esa información se debe indicar siempre el número telefónico de atención permanente que se haya habilitado para ese servicio y que debe estar disponible todos los días del año, durante las 24 horas, para recibir dichos avisos, como también del uso de los otros medios que haya establecido para ese fin.

El banco o el operador, en su caso, deberá registrar la recepción del aviso tan pronto lo reciba y proporcionar al tarjetahabiente en ese mismo momento y por la misma vía por la que lo recibió, un número o código de recepción y la constancia de la fecha y hora de ingreso.

#### **5. Disposición transitoria.**

La aplicación de las nuevas normas contenidas en el N° 3 de este Capítulo, será obligatoria para los contratos que se celebren a contar del 2 de enero de 2014.

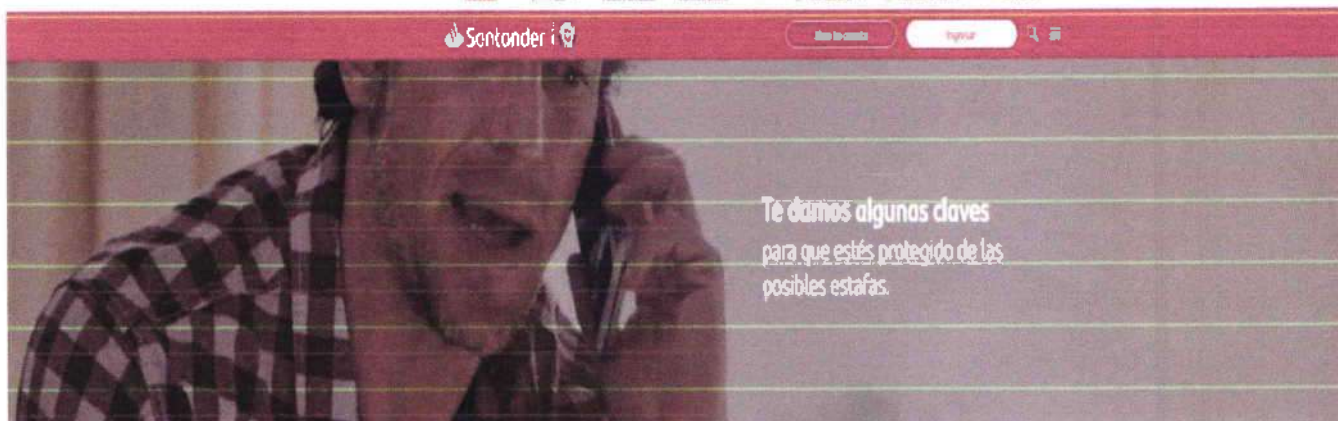


# Banco Santander

## 1. Campañas publicitarias educativas a clientes de Banco Santander : Prevención de fraudes

### 1.1. Campañas seguridad Bancaria, pagina web Banco Santander <sup>1</sup>

← → ↻ 🏠 banco.santander.cl/informacion/seguridad



#### NUNCA, JAMÁS

- Te llamaremos para descargar o configurar una aplicación Santander.
- Te llamaremos para pedir tus claves bancarias o tus coordenadas, ni las pediremos por email ni por SMS.
- Incluiremos links en nuestros correos electrónicos ni en nuestros SMS.
- Descargues archivos adjuntos de remitentes desconocidos.

Revisa nuestros folletos para prevenir estafas

#### NUNCA, JAMÁS

- Te llamaremos para descargar o configurar una aplicación Santander.
- Te llamaremos para pedir tus claves bancarias o tus coordenadas, ni las pediremos por email ni por SMS.
- Incluiremos links en nuestros correos electrónicos ni en nuestros SMS.
- Descargues archivos adjuntos de remitentes desconocidos.





## 1.2 Educación a cliente sobre distintos tipos de estafa e ingeniería social: Smishing, Pishing, Cuento del Tío.

← → ↻ 🏠 banco.santander.cl/informacion/seguridad 🔍

PERSONAS EMPRESAS PRIVATE BANKING NUESTRO BANCO ACCESIBILIDAD SERVICIO AL CLIENTE SUCURSALES

**Santander** Abre tu cuenta Ingresar 🔍 ☰

### Las estafas más comunes

SMISHING	PHISHING	CUENTO DEL TÍO
 <p>Se trata de un método de engaño utilizado por los ciberdelincuentes, que consiste en el envío de un SMS (mensaje de texto), con un link para obtener información personal y así realizar estafas.</p>	 <p>El engaño consiste en enviarte un correo electrónico donde te invita a hacer clic en un link, que aparentemente tiene información importante para ti, pero que busca robarte información personal o financiera. Así es como recogen tus datos para luego estafarte.</p>	 <p>Si te llaman pidiendo dinero porque un familiar ha tenido un accidente, problemas, o se contacta contigo haciéndose pasar por una Institución Financiera o Casa Comercial pidiéndote tus claves o devolución de dinero, ¡Cuidado! Puede ser una estafa.</p>

## 1.3. Prevención de fraudes: Estafas telefónicas

← → ↻ 🏠 banco.santander.cl/informacion/seguridad 🔍 ☆ 🌐

PERSONAS EMPRESAS PRIVATE BANKING NUESTRO BANCO ACCESIBILIDAD SERVICIO AL CLIENTE SUCURSALES

**Santander** Abre tu cuenta Ingresar 🔍 ☰

### ¡Cuidado!

todas estas llamadas pueden ser una estafa!

- Si te llaman pidiendo dinero porque un familiar ha tenido un accidente o está en problemas.
- Si recibes un llamado de un desconocido para comprar un producto que estás vendiendo por internet y te dicen que se equivocaron al transferir el dinero.
- Si alguien llama haciéndose pasar por alguna Institución Financiera o Casa Comercial solicitando tus claves de coordenadas y/o clave SMS para devolverte dinero por comisiones mal cobradas o para decirte que se te hizo una transferencia de dinero errónea y debes devolver el dinero.

¡Cuidado, es una estafa!

Si recibes alguna de estas llamadas o alguna llamada sospechosa no dudes en llamarnos al **600 320 3000**.





## 1.4 .Prevención de fraudes: Compras en comercio Online con tarjetas de crédito

banco.santander.cl/informacion/seguridad

PERSONAS EMPRESAS PRIVATE BANKING NUESTRO BANCO ACCESIBILIDAD SERVICIO AL CLIENTE SUCURSALES

Abre tu cuenta Ingresar

### Protege tus Tarjetas de Crédito

- Recuerda que debes cuidar siempre tu Código CVV (Card Verification Value). Este código lo solicitan en la mayoría de los comercios cuando realizas compras online para verificar tu Tarjeta.
- Actualiza tu Tarjeta a una con Chip, acércate a cualquiera de nuestras Sucursales y WorldCash y combinala.
- Nunca pierdas de vista tu Tarjeta, especialmente al momento de pagar en comercios.

¿Qué hago si me aparece una compra que no reconoczo? Llámanos al 600 328 3000 o comunícame con nosotros vía nuestros canales de atención remota para ayudarte y aclarar dudas.

### En comercios Online:

- Siempre lee atentamente los Términos y Condiciones que tiene el comercio.
- Siempre verifica que se efectúan correctamente los cargos a tu Tarjeta.
- Siempre mantén deshabilitada la modalidad de suscripción automática en caso de no requerirla.
- Se cuidadoso: no almacenes los datos de tus tarjetas en dispositivos que no son de tu uso personal. Terceros podrían hacer mal uso de ellas y efectuar compras sin tu autorización en comercios como iTunes, Uber, PayPal, Google, Netflix, entre otros.
- Te recomendamos descargar la App Santander y activar las notificaciones para estar siempre al tanto de los cobros que se realizan en tu Tarjeta.

Te recomendamos: Descarga la App Santander y activa las notificaciones para estar siempre al tanto de los cobros que se realizan en tu Tarjeta.

## 1.5. Prevención de fraude: Cuidado y resguardo de claves secretas

banco.santander.cl/informacion/seguridad

PERSONAS EMPRESAS PRIVATE BANKING NUESTRO BANCO ACCESIBILIDAD SERVICIO AL CLIENTE SUCURSALES

Abre tu cuenta Ingresar

### Sigue siempre estos consejos:

- Digita directamente en tu navegador [www.santander.cl](http://www.santander.cl) y verifica que siempre la URL empiece con HTTPS // (en vez de HTTP).
- Cambia periódicamente tu clave, idealmente cada 3 meses. Puedes realizarlo [aquí](#).
- Protégete de virus y malwares descargando un antivirus en cada uno de tus dispositivos.
- En caso de extravío o furto de tu teléfono registrado para recibir tu clave 30 te recomendamos llamarnos para bloquear tu Tarjeta de credenciales y pedir el cambio de Clave de Acceso al Servicio de Atención Telefónica 600 328 3000.



## 2.0. Campañas prevención de fraude: Facebook Banco Santander Chile<sup>2</sup>

**Banco Santander Chile** [Contactarnos](#) [Me gusta](#) [Mensaje](#) [Q](#) [...](#)

**Banco Santander Chile** [23 de mayo de 2021](#) [...](#)

¿Qué tan preparado estás contra los fraudes? **NUNCA, NUNCA** ignore los consejos de seguridad. Aquí te compartimos algunos para que **NUNCA, NUNCA** los olvides. 🙌

**NUNCA, NUNCA**  
ignore los consejos de seguridad.

0:09 / 0:23

19 [Comentarios](#) [1 vez compartido](#)

[Me gusta](#) [Comentar](#) [Compartir](#)

<https://www.facebook.com> [Privacidad](#) [Condiciones](#) [Publicidad](#) [Opciones de anuncios](#)  
Cookies Más Facebook © 2021

## 3.0. Campañas prevención fraude: Instagram Banco Santander Chile<sup>3</sup>

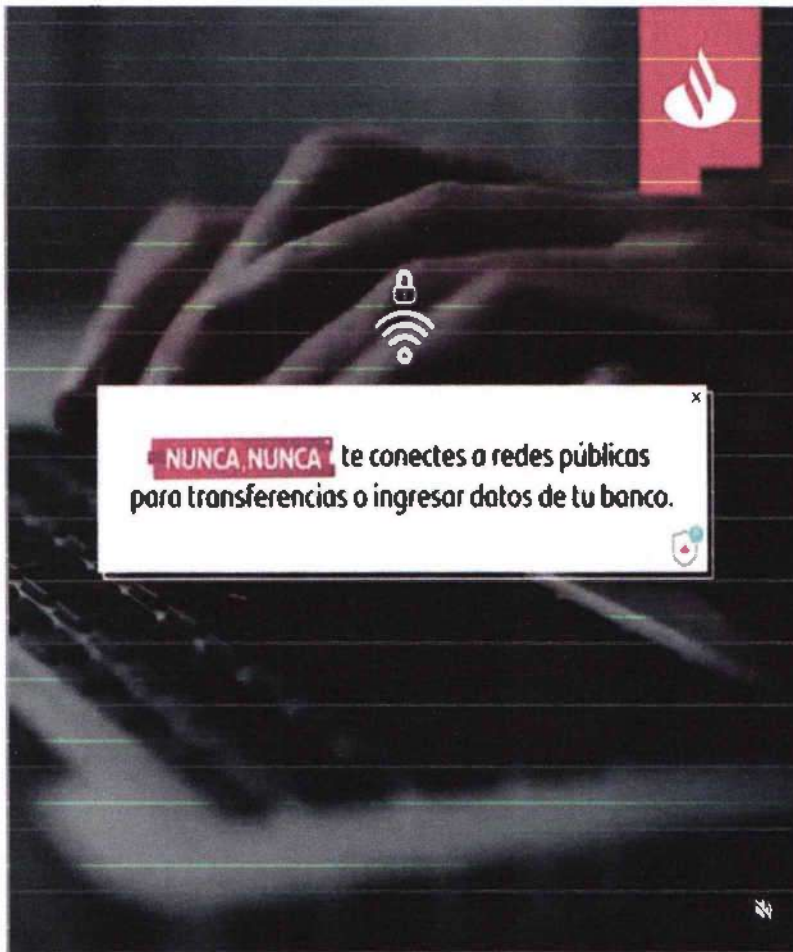
**Instagram** [Buscar](#)

**santanderchile** [...](#)

**santanderchile** [Para que NUNCA, NUNCA pierdas el control de tus tarjetas](#) 📱 te dejamos unos prácticos consejos para que puedas bloquear tus productos desde Santander.cl y desde nuestra App Santander 🙌👤.



### 3.1. Campañas prevención de fraude en Instagram: Consejos de seguridad



santanderchile

santanderchile ¿Qué tan preparado estás contra los fraudes? NUNCA. NUNCA ignores los consejos de seguridad. Aquí te compartimos algunos para que ;NUNCA. NUNCA los olvides!

2 sem

javierasndv1 Gracias por estos consejos

2 sem Responder

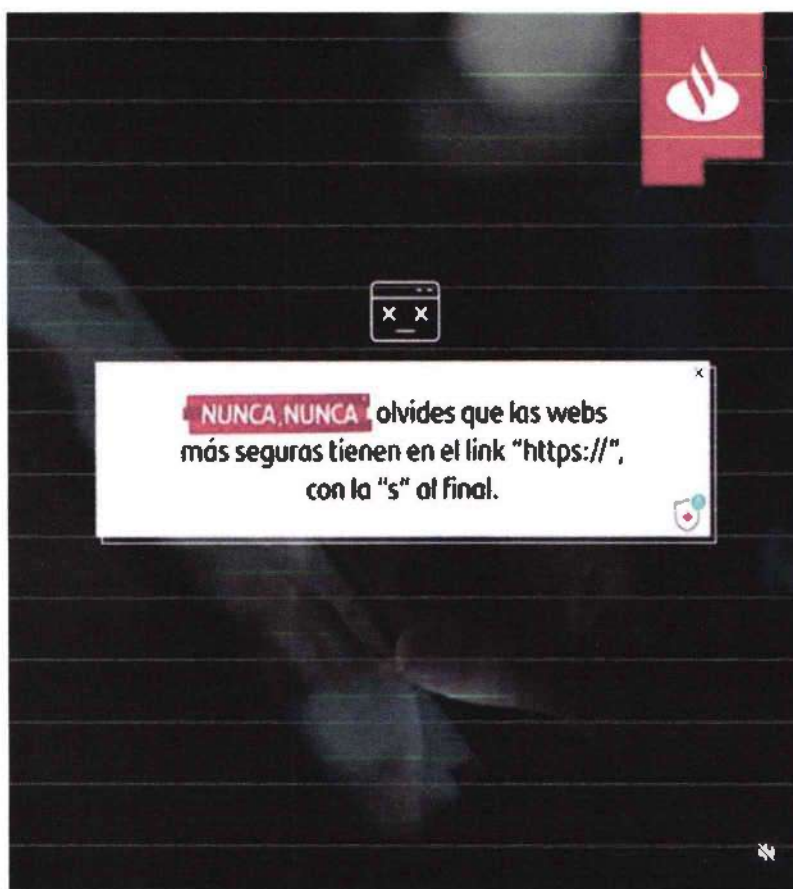
jeronimo\_mendez7 Nunca nunca digas nunca.

1 sem Responder

61.584 reproducciones

28 DE ABRIL

Agrega un comentario...



santanderchile

santanderchile ¿Qué tan preparado estás contra los fraudes? NUNCA. NUNCA ignores los consejos de seguridad. Aquí te compartimos algunos para que ;NUNCA. NUNCA los olvides!

2 sem

javierasndv1 Gracias por estos consejos

2 sem Responder

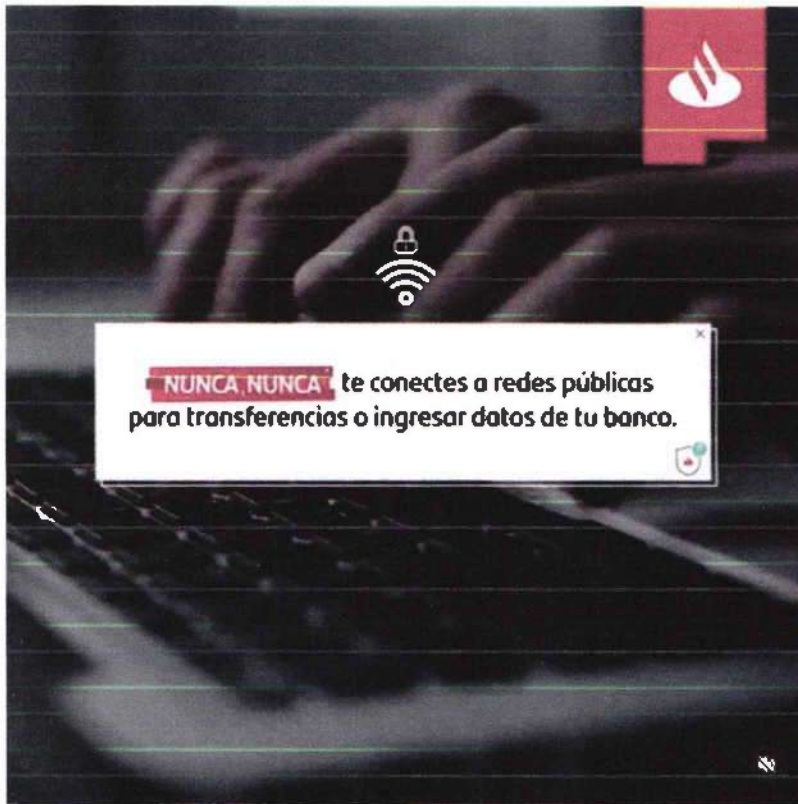
jeronimo\_mendez7 Nunca nunca digas nunca.

1 sem Responder

61.584 reproducciones

28 DE ABRIL

Agrega un comentario...



santanderchile

santanderchile ¿Qué tan preparado estás contra los fraudes? NUNCA, NUNCA ignores los consejos de seguridad. Aquí te compartimos algunos para que ¡NUNCA, NUNCA los olvides!

2 sem

javierasndvl Gracias por estos consejos

2 sem Responder

jeronimo\_mendez7 Nunca nunca digas nunca

1 sem Responder

61.584 reproducciones

28 DE ABRIL

Agrega un comentario...



santanderchile

santanderchile ¿Qué tan preparado estás contra los fraudes? NUNCA, NUNCA ignores los consejos de seguridad. Aquí te compartimos algunos para que ¡NUNCA, NUNCA los olvides!

2 sem

javierasndvl Gracias por estos consejos

2 sem Responder

jeronimo\_mendez7 Nunca nunca digas nunca

1 sem Responder

61.584 reproducciones

28 DE ABRIL

Agrega un comentario...



**santanderchile** • ¿Que tan preparado estás contra los fraudes? **NUNCA, NUNCA** ignores los consejos de seguridad. Aquí te compartimos algunos para que ¡NUNCA, NUNCA los olvides!

3 sem

**javierasndv1** Gracias por estos consejos

2 sem Responder

**jeronimo\_mendez7** Nunca nunca digas nunca

1 sem Responder

61,584 reproducciones

128 de 128%

Agrega un comentario...

### 3.2. Campañas prevención de fraude: Educación claves de seguridad y tarjeta de coordenadas



**santanderchile** • No olvides que tus claves o tarjeta de coordenadas son personales. Nunca, bajo ninguna circunstancia te pediremos estos datos. Evita fraudes y revisa más consejos en Santander.cl #CuidaTusClaves #SantanderInforma #EvitaFraudes

11 sem

**sdcarcamo1** Gracias

11 sem 1 Me gusta Responder

787 reproducciones

2 DE MARZO

Agrega un comentario...



**Sigue estos consejos:**

- ✕ No compartas tus claves secretas.
- 🔄 Cambia frecuentemente tus claves.
- 👤 No incluyas información personal en tus claves.

**santanderchile** No olvides que tus claves o tarjeta de coordenadas son personales. Nunca, bajo ninguna circunstancia te pediremos estos datos. Evita fraudes y revisa más consejos en Santander.cl #CuidaTusClaves #SantanderInforma #EvitaFraudes

11 sem

sdcarcamo1 Gracias

11 sem 1 Me gusta Responder

787 reproducciones

12 DE MARZO

Agrega un comentario...

### 3.3. Campañas prevención fraude: Mensajes de texto fraudulentos

**CUIDADO CON LOS FRAUDES POR SMS**

**santanderchile** ¡Cuidado! Si recibes un SMS que lleva un link hacia un sitio web sospechoso, estás frente a un caso de FRAUDE. Etiqueta a tus amigos y compártelo, para que entre todos estemos alerta.

15 sem

el\_bar\_invita @sebastianpinerae

15 sem Responder

javierasndvl Gracias por la información

15 sem Responder

javierasndvl Gracias por la información

111,841 reproducciones

23 DE ENERO

Agrega un comentario...



**Si recibes SMS con una URL sospechosa, te recomendamos:**

- No abrir URL y eliminar inmediatamente el SMS.
- Jamás compartas tus datos o claves personales.
- Ante cualquier duda, llámanos al 600-320-3000.

111.841 reproducciones  
23 DE ENERO

SANTANDER: Por seguridad bloqueamos tu Tarjeta de Crédito. Verifica tu cuenta para activar acceso <https://santamvalidate-sms.live/sms=santander>.

111.841 reproducciones  
23 DE ENERO





### 3.4. Campañas prevención fraude Instagram: Correo electrónico fraudulento

**SuperClave Suspendida Temporalmente**

La SuperClave es una tarjeta de identificación que ofrece mayor control sobre sus cuentas financieras de tarjetas de crédito y tarjetas de débito.

Usted de forma segura lanzando en cuestión las siguientes consideraciones:

1. El sistema le pedirá una confirmación de sus datos personales que debe ingresar en SuperClave a los 60 segundos siguientes a la recepción.
2. La confirmación de recepción se le indicará en la pantalla de su dispositivo móvil que se muestra una notificación.
3. Si no puede acceder por algún motivo.

233.794 reproducciones

20 DE ENERO

**Recuerda:**

- Nuestros correos electrónicos y SMS NUNCA incluirán links ni botones.
- Nuestros correos SIEMPRE estarán dirigidos a tu nombre.
- JAMÁS compartas tus datos y claves.

233.794 reproducciones



### 3.5. Campañas prevención de fraude: Compas seguras a través de internet

- Hazlo en sitios conocidos.
- No abras URLs de mails o SMS.
- No envíes fotos de tus tarjetas para confirmar compras.
- No compres conectado a una red Wifi pública.

Tu banco

santanderchile

santanderchile Para que compres online sin problemas y de forma segura te recomendamos seguir estos simples consejos y así evitarás fraudes y malos ratos en esta época del año

24 sept

xprishux Gracias por preocuparse. Los mejores tips de la vida

24 sept 1 Me gusta Responder

avolar.cl

24 sept Responder

1.224 reproducciones

24 DE NOVIEMBRE DE 2022

Agrega un comentario...

Santander Chile Hemos bloqueado tu Tarjeta de Crédito. Recibidos

Tu banco

## Te recordamos

- Nuestros correos electrónicos y SMS **NUNCA** incluirán link.
- Nuestros correos siempre estarán dirigidos a su nombre.
- Jamás debes compartir datos y claves.

santanderchile

santanderchile Recuerda que **NUNCA** enviaremos enlaces a otros sitios desde correos electrónicos o SMS. No abras esos mensajes y evita un mal rato

31 sept

\_evelyn\_mz Me llegan todos los días. y yo nisisquiera tengo una cuenta en santander. wtf

13 sept Responder

shinoworkout Como es posible ...si no tengo santander

147.735 reproducciones

9 DE OCTUBRE DE 2022

Agrega un comentario...

Verifica tu cuenta para activarla:  
<https://bcsantander-sms.website/?sms=0>

**Sr.  
Eugenio Labarca Birke.  
Gerente Defensa Procesal Banco Santander Chile.**

**Presente**

**FRANCISCO JAVIER VARAS UNDURRAGA**, Ingeniero, domiciliado en Monroe N° 6582, comuna de Las Condes, Santiago, perito judicial con especialidades en Computación e Informática, Fraude y Delito informático, a solicitud de don **EUGENIO LABARCA BIRKE**, para anexo complementario a informe pericial sobre las medidas de seguridad con que cuenta Banco Santander.


Vengo en evacuar el Anexo complementario de informe pericial sobre IP

**Anexo complementario IP de Informe Pericial**

Este informe, es un anexo complementario al informe pericial sobre las medidas de seguridad con que cuenta Banco Santander.

La metodología del presente informe pericial se basará en las siguientes etapas:

- Objetivo.
- Herramientas del Trabajo Teórico.
- Desarrollo.
- Conclusiones.

  
**Francisco J. Varas Undurraga**  
Rut: 7.014.520 - 0  
Perito en Computación e Informática  
Poder Judicial

- **Objetivo.**

Este informe anexo complementario, consiste en informar sobre el concepto de IP con respecto a la conectividad que tienen los clientes del Banco Santander a su sitio WEB.

- **Herramientas del trabajo teórico.**

Se procede a entregar definición de algunos conceptos técnicos con el propósito de hacer entendible la lectura de este informe.

### **Dirección IP**

Se entiende por IP (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica un dispositivo (computador, Tablet, Smart-phone) conectado a una red que corre el protocolo IP. La IP es un conjunto de cuatro números del 0 al 255, separados por puntos, a modo de ejemplo: 200.36.127.40

Las IP públicas y privadas no son diferentes en sí mismas, como tampoco lo son las IP fijas y dinámicas. Tienen una forma y una función muy parecida, pero se utilizan en casos distintos.

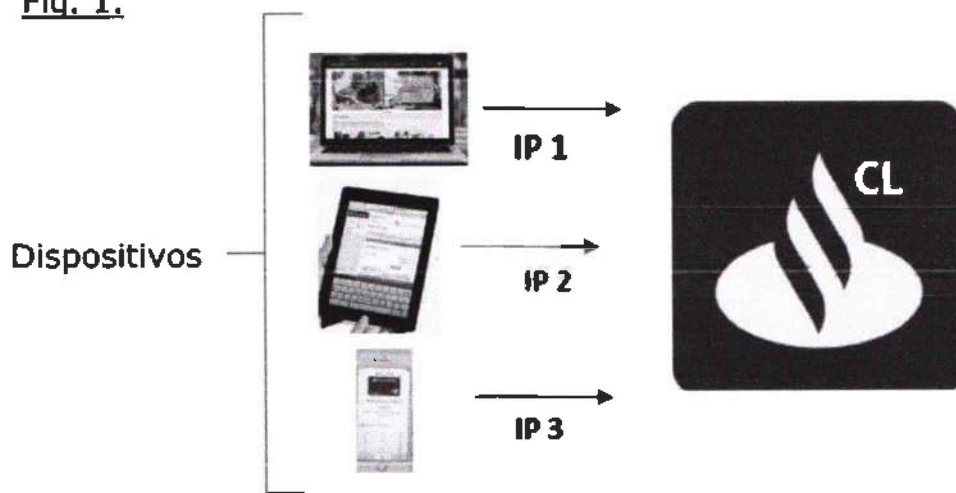
- **IP pública:** Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet.
- **IP privada:** Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo (el mismo "idioma" de comunicación).
- **IP fija:** Es una IP la cual es asignada por el usuario, o bien dada por el proveedor ISP en la primera conexión.
- **IP dinámica:** Los servidores DHCP se encargan de asignar las IP dinámicas a cada equipo que se conecte a Internet u otra red. Según el caso serán IP públicas o privadas.

- **Desarrollo.**

Cada vez que un cliente se conecta al sitio web de Banco Santander, por medio de un dispositivo, ya sea éste un computador; una Tablet o un Smart-phone, para operar sus productos por medio de la red, lo hace con una IP, la que está asociada al equipo con que se está conectando. Este mecanismo es pre-requisito para lograr la conexión al Banco, en otras palabras, si el equipo no cuenta con IP, no podrá establecer conectividad con el sitio WEB de Banco Santander.

La siguiente figura muestra gráficamente lo descrito.

Fig. 1.



Entonces, cada vez que se conecte un cliente por medio de un dispositivo, lo hará con una IP.

Los dispositivos obtienen una IP al momento de conectarse a la red, es decir, si usted con un computador se conecta a la red en un lugar físico distinto de otro lugar, su equipo tendrá asignada una IP diferente cada vez que logre la conectividad. Es decir, el cliente se puede conectar a Banco Santander desde distintas IPs. Esta condición hace que un cliente pueda tener varias direcciones IP (habituales o no habituales), dependiendo si ocupa una o más redes para conectarse.

Sólo se obtendría siempre la misma IP cuando el equipo se encuentre configurado con una IP fija en el equipo y este equipo siempre se conecte a la misma red (el mismo lugar), de lo contrario se le asignará una IP (DSHP dinámica) diferente.

Como ya se dijo, los clientes de Banco Santander cuando se conectan al sitio web del Banco para realizar transacciones, lo hacen por medio de dispositivos, permitiendo la plataforma la conectividad simultáneamente con más de uno de ellos a la vez (normas de seguridad que están revisadas y autorizadas por la CMF, ya que dicho organismo es el nuevo regulador desde el año 2019).

Para la conectividad del cliente al Banco Santander, si y sólo sí, el cliente debe tener sus credenciales que son de su exclusiva responsabilidad y conocimiento, las que le permitirán acceder a sus productos y realizar transacciones.

Debido a estas variables señaladas de conectividad que son exigidas por la entidad reguladora CMF (Comisión para el Mercado Financiero), se entiende que Banco Santander no debería tener restricciones de acceso ni de monitoreo sobre accesos de Ips de los clientes a la plataforma del Banco.

• **Conclusiones.**

- La conectividad al sitio WEB de Banco Santander se realiza por medio de dispositivos, ya sean estos: a) un Computador; b) una Tablet o un c) Smart-Phone (celular).
- Cada vez que se conecte un cliente por medio de un dispositivo, lo hará por medio de una IP.
- El cliente se puede conectar a Banco Santander desde distintas IPs (pudiéndose conectar desde distintos lugares). Esta condición hace que el cliente obtenga una dirección IP no habitual. Entendiéndose por IP habitual, al mismo número de IP que se asigna al dispositivo al momento de conectarse a la red y a su vez IP no habitual, es la que se le asignan distintos números de IP al conectarse a la red.
- El cliente se puede conectar al sitio WEB de Banco Santander con más de un dispositivo a la vez de forma simultánea.
- El cliente para conectarse al sitio WEB de Banco Santander debe contar sus credenciales que son de su exclusiva responsabilidad y conocimiento, las que le permitirán acceder a sus productos y realizar transacciones.
- Debido a estas variables señaladas de conectividad que son exigidas por la entidad reguladora CMF (Comisión para el Mercado Financiero), se entiende que Banco Santander no debería tener restricciones de acceso y el deber del cliente es utilizar redes seguras y resguardar en debida forma, y con máxima confidencialidad, las credenciales que le permiten acceder a dichas redes.

Causa rol 17.367-L

En Iquique, a veintidós días del mes de julio del año dos mil veintidós. Siendo el día y horas, se lleva a efecto la prosecución de la audiencia de contestación, conciliación y prueba decretada para el día de hoy, con la asistencia de la parte denunciante infraccional y demandante civil, representada por el abogado don José Francisco Gallegos Torres y, la asistencia de la parte denunciada infraccional y demandada civil representada por el abogado don Marco Antonio Hernández Güiza.

Contestación.

La parte denunciada y demandada civil, viene en contestar por escrito la denuncia infraccional y demanda civil, solicitado se tenga como parte integrante de la presente causa y para todos los efectos legales.

El Tribunal provee: a lo principal: téngase por contestada la denuncia infraccional y por acompañada. Al primer otrosí: téngase por contestada la demanda civil de indemnización de perjuicios y, por acompañada. Al segundo otrosí: téngase por acompañados los documentos con citación, los que deberán ser ratificados en la etapa procesal respectiva.

El Tribunal llama a las partes a conciliación, esta no se produce.

El Tribunal recibe la causa a prueba, fijando como hecho substancial, pertinente y controvertido.

1.- efectividad de los hechos denunciados.

2.- efectividad del daño, naturaleza y monto demandado

Prueba testimonial

La parte denunciada infraccional y demandada civil, no formula preguntas de tacha a la testigo.

La parte denunciante infraccional y demandante civil, viene en presentar los siguientes testigos. Comparece doña Ina María Choque Castillo, chilena, casada, 63 años de edad, estudios técnicos, técnico, cédula de identidad N° 8.150.782-1, domiciliada en Malaquita N° 4238, población quebrada blanca, de esta ciudad, quien debidamente juramentada expone. a los puntos. Esto fue de oído, el día 4 de junio de 2021, llame telefónicamente a la señorita Verónica, por un asunto particular en realidad, y la note que estaba complicada, le pregunte si le pasaba algo, y me comentó que había sufrido una estafa, de parte de una persona que se hizo pasar telefónicamente por una ejecutiva del Banco Santander, quien le habría manifestado, que el banco estaba cambiando los plásticos de las tarjetas con un sensor contra estafa. Esta ejecutiva le habría entregado telefónicamente los números de la cuenta corriente, cuenta vista, los números de las tarjetas de crédito, los inicios y final, manifestó además que ella tenía dos seguros tomados con el Banco, y que ella para hacer los cambios, debía digitar los números que la ejecutiva le iba a indicar de la tarjeta de coordenadas, que coincidía con los números que tenía la tarjeta que ella mantenía. Hago presente que la ejecutiva la había identificado con sus dos nombres y sus dos apellidos. Por esta razón la ejecutiva le dio las coordenadas, las que Verónica digito en el teléfono, la señora Verónica se dio cuenta que era una estafa, solo al recibir un correo



Gmail, al mismo teléfono con el que estaba hablando y ahí le pareció raro, y corto la llamada. La señora Verónica trata de entrar a la página web del Banco, pero las claves habían sido cambiadas. Inmediatamente llama al call center del banco, donde pide que bloqueen sus productos porque había sufrido una estafa, la llamada se cortó y, tuvo que volver a llamar, y la atendió un ejecutivo, del que no me recuerdo, pero sí que era una mujer, a quien se le explica nuevamente que había sufrido una estafa, y le pide que revise los productos. La ejecutiva le responde que los productos están bloqueados y, le indica una cantidad xx, de los productos que habían alcanzado a sacar dinero. Verónica consulta si tiene que ir a Carabineros o a la PDI, la señorita le indica que no era necesario ya que estaba todo bloqueado. Al día siguiente Verónica vuelve a llamar al banco, ya que no podía ver la cuenta digital, se contacta con un ejecutivo del Banco quien le indica que efectivamente que sus cuentas estaban bloqueadas. Ella pide que sean revisados sus productos, el ejecutivo le da otro valor, superior al indicado anteriormente, al día siguiente ella se dirige al Banco, y la atendió a una ejecutiva, a quien nuevamente le pide revisar sus productos y, nuevamente el valor había variado. Además se entera que si debía haber ido a la PDI, situación que ella lo había hecho por si sola. Ella rompió en llanto por todo lo que le había pasado ya que las cantidades difieren del día tres, que es el día de la estafa. Es cuanto puedo declarar.

El Tribunal provee: téngase por aceptada la declaración de la testigo.

1.- repreguntada la testigo para que diga, si sabe o conoce que Banco Santander haya da dado solución al problema de la demandante.

R. solo de una parte, no completa.

2.- para que diga la testigo si sabe o conoce el monto de esta parte.

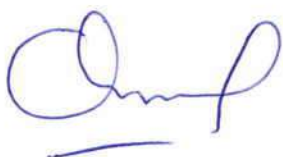
R. no me recuerdo.

3.- para que señale la testigo, como se encuentra la demandante anímicamente a la fecha.

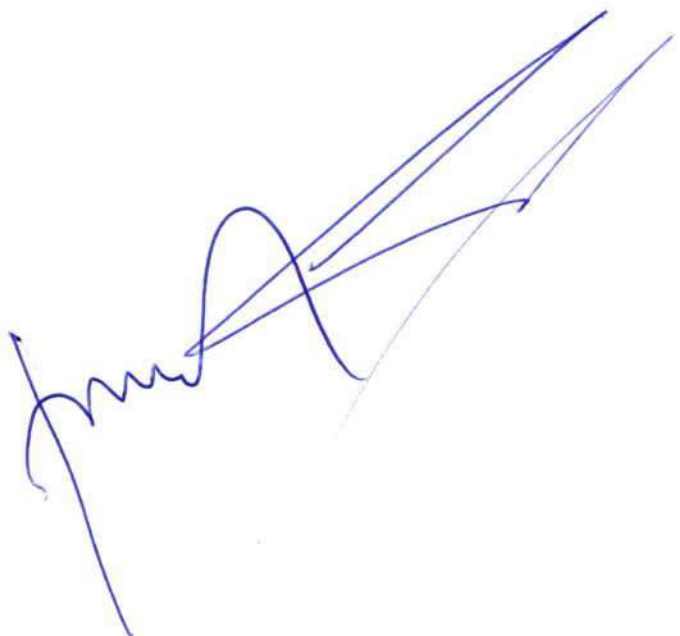
R. bastante complicada, ya que se encuentra en tratamiento con una Psiquiatra y con un psicólogo y, con medicamentos.

La parte denunciada infraccional y demandada civil, no contrainterroga a la testigo.

La parte denunciante y demandante civil, viene en solicitar se dispense a la testigo por andeles laborales. El Tribunal provee: como se pide, previa firma



8.150.782-1



Comparece doña Laura Inés Martínez Fumey, chilena, casada, 39 años de edad, estudios superiores, trabajadora social, cédula de identidad N° 15.008.435-0, domiciliada en playa Blanca N° 2535, casa 5, de esta ciudad, quien debidamente juramentada expone. yo sé que el día 3 de junio de 2021, Verónica sufrió una estafa telefónica en al cual la llamaron supuestamente del Banco Santander, para hacer cambios de unos plásticos, y unos seguros que tenía contratados, ahí le indicaron en el proceso, que debía digitar su clave para finalizar los procesos. En algún momento dela llamada se dio cuenta que era una estafa, y corto de inmediato. Luego de esto, procedió a llamar al Banco, para notificar lo que le había pasado, y que no le fueran a robar. Para que el Banco no pagara las posibles transacciones que pudieran efectuar, porque ella no l as estaba haciendo sino que había sufrido de una estafa. Que era muy creíble, puesto que, la ejecutiva que la contactó, conocía en detalle todos sus datos personales, además, las cosas que tenía contratados en el Banco y los tramites que había hecho últimamente. Eso fue lo que llevo a ella a digitar las claves ya que conocía todos sus antecedentes que estaban en poder del Banco. Yo me enteré de esto a fines del mes de junio, en una llamada telefónica que hice a Verónica y me comento lo que acabo de expresar. Me cometo que no solo habían ocupado con sus tarjetas de créditos, sino que también habían hecho transferencia, que la habían dejado prácticamente la habían dejado sin dinero su cuenta y, elle tenía mucho ahorrado.

Cuando hable con ella por teléfono. La note muy decaída, note que no estaba durmiendo bien, que todo lo que había pasado con la estafa, la tenía muy enferma, no solo psicológicamente sino que físicamente, por lo que le comente que fuera al doctor, porque no podía estar sin dormir y angustiada de esa forma.

Después como a fines julio, volví a contactarla, yo estaba con licencia médica, para saber cómo estaba, y seguía de la misma forma, todavía angustiada visitando al psicólogo, muy mal todavía anímicamente, porque no había logrado tener una respuesta positiva del banco. En agosto la volví a llamar para invitarla a mi baby shower, para que se distrajera, sin embargo no asistió porque todavía su estado anímico no era el mejor. Entremedio sé que tuvo licencia médica psicológica por todo el daño que había sufrido debido a la estafa, pero no recuerdo la fecha. Sé que después tuvo que regresar a trabajar, y desde esa fecha a la fecha actual, ella no está recuperada psicológicamente, por los daños sufridos. Es cuanto pudo declarar.

El Tribunal provee: téngase por aceptada la declaración de la testigo.

1.- repreguntada la testigo para que diga, si sabe o conoce si banco Santander ha solucionado los problemas que ha tenido la demandante.

R. no estoy segura.

La parte denunciada infraccional y demudada civil, no contrainterroga a la testigo.

Prescrito Presunto y Ocuco

365

La parte denunciante infraccional y demandante civil, viene en solicitar se dispense a la testigo, por motivos de índole laboral. el Tribuna, provee: como se pide, previa firma.

Laural

15.008.435-0



La parte denunciada infraccional y demandada civil, no rinde prueba testimonial.

#### Prueba documental

La parte denunciante infraccional y demandante civil, vienen en reiterar los documentos acompañados a fojas 1 y siguientes, y viene en acompañar nóminas de documentos, que consta de 14.

El Tribunal provee: téngase por ratificados y por acompañados los documentos solicitando se tengan como parte integrante de la presente causa y para todos los efectos legales.

El Tribunal provee: téngase por ratificados y por acompañados los documentos.

La parte denunciada infraccional y demandada civil, viene en ratificar los documentos acompañados en el segundo otrosí de la contestación de la demanda, documentos acompañados con citación y en este acto viene en acompañar pendrive, que contiene audio de la señora Verónica Ramírez, solicitado a S.S. la custodia por parte del señor secretario del Tribunal. El Tribunal provee: téngase por ratificados los documentos y por acompañado pendrive, y se ordena su custodia en la secretaria del Tribunal. Diligencias.

La parte denunciante infraccional y demandante civil viene en solicitar se oficie al demandado Banco Santander, para que haga llegar toda la documentación que tenga respecto a los reclamos realizaos por la demandante, desde el mes junio del año 2021, a la fecha

La parte denunciada infraccional y demandada civil, viene en solicitar la siguiente diligencia, se cite a las partes a audiencia de percepción de documental, en atencional pendrive aportado por esta parte, solicitando a S.S. se fije día y hora para la audiencia de percepción de documento electrónico.

Las partes de común acuerdo, vienen es solicitar a S.S. que la audiencia de percepción de documento electrónico se fije para el día 23 de agosto a las 09:00 horas.

Respecto de las diligencias solicitadas por las partes. El Tribunal queda en resolver.

Con lo obrado y siendo las 10:55 horas, se pone termino a la presente audiencia, previa lectura se firma conjuntamente con S.S. y secretario subrogante que autoriza.

13483.1243

Causa rol 17.367-L

En Iquique, a veintidós días del mes de julio del año d dos mil veintidós Resolviendo la diligencia solicitada por la parte denunciante infraccional y demandante civil a fojas 366, como se pide. Oficiese al Banco Santander Chile, a fin remita a esta Magistratura, toda la documentación que tenga, respecto de los reclamos realizados por la demandante, desde el mes de junio de 2021, a la fecha.

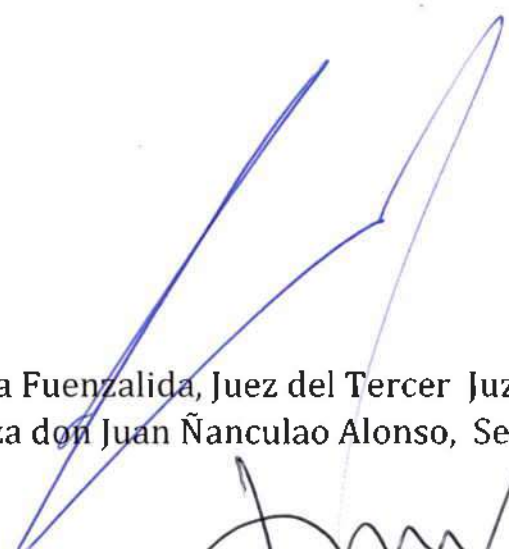
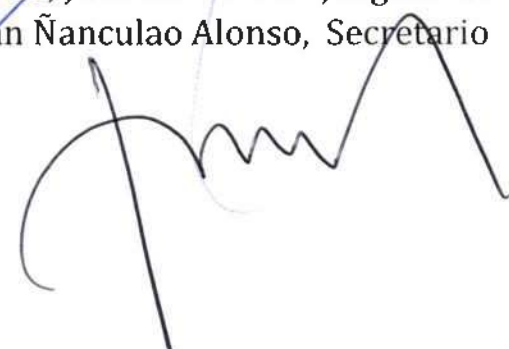
Resolviendo la diligencia solicitada por las partes a fojas 366, en cuanto a la audiencia de percepción de documento electrónico. Teniendo presente lo dispuesto en el artículo 348 bis, del Código de Procedimiento Civil, no ha lugar a lo solicitado.

Cítese a las partes a audiencia de percepción de documento electrónico, el día 29 de julio de 2022, a las 11:30 horas. Se apercibe a la parte solicitante, para que se presente con los medios tecnológicos para tal efecto, de conformidad a lo dispuesto en el artículo 348 bis, del Código de Procedimiento Civil, bajo apercibimiento de tener por no presentada la prueba electrónica.

10/2

Notifíquese.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de Policía Local de Iquique, autoriza don Juan Ñanculao Alonso, Secretario subrogante.

cuatrocientos Quince

405

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367 - L

IQUIQUE,

02 SET. 2023

CERTIFICO: Que, con esta fecha y siendo las 11:39 hrs. he procedido a notificar a don (ña) FELIPE FERNANDEZ LEON de la resolución de fecha 30 / Agosto / 2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico ffernandez@fgnabogados.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

Hacer  
acto  
Audiencia

certificación - pes

406

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367 - L

IQUIQUE, 02 SET. 2023

CERTIFICO: Que, con esta fecha y siendo las 11 : 38 hrs. he procedido a notificar a don (ña) MARCO A. HERNANDEZ GUIZA de la resolución de fecha 30 / Agosto / 2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abogadomarcohemandezguiza@gmail.com. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

c.c.: zonanorte@legaltec.cl

Presupuesto Presuete 7 ochos  
28/07

368

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE, 25 JUL. 2022

CERTIFICO: Que, con esta fecha y siendo las 17:47 hrs. he procedido a notificar a don Felipe Fernández León de la resolución de fecha 22/07/2022 (15.367), remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico ffernandez@fgmabogados.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor



Presentes Presente J. J. Pérez 369

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367 - h

cc.

IQUIQUE, 25 JUL. 2022

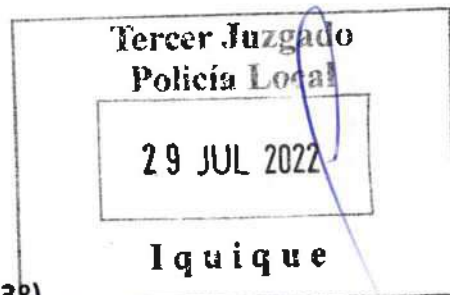
CERTIFICO: Que, con esta fecha y siendo las 17 : 47 hrs. he procedido a notificar a don Marco A. Hernández Guiza de la resolución de fecha 22/07/2022 (fs. 367), remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abogado.marco.hernandez.guiza@gmail.com. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

cc. zonamonte@lepatel.cl

Resumen Potente

3/0



DELEGA PODER


S.J. DE POLICÍA LOCAL DE IQUIQUE (3º)

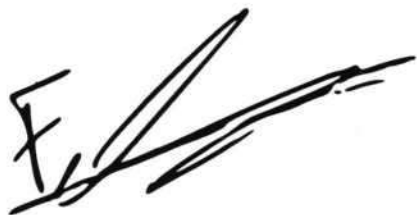
**FELIPE FERNANDEZ LEON**, abogado denunciante y demandante civil, en causa RIT N° 17367-L-2021, seguida ante este tribunal por ley del consumidor, a US. respetuosamente digo:

Que por medio de este acto, vengo en delegar poder a la abogada doña **Tamara Rojas Aguirre**, Cédula Nacional de Identidad No 17.430.213-8, domiciliada en calle Pedro González N° 2847, comuna de Iquique, para actuar en forma conjunta o por separado en este proceso, sin perjuicio de mi derecho de reasumir plenamente las facultades ya mencionadas.


**POR TANTO:**

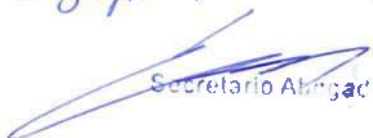
**SOLICITO A UD:** Tenerlo presente.

  
17.430.213-8



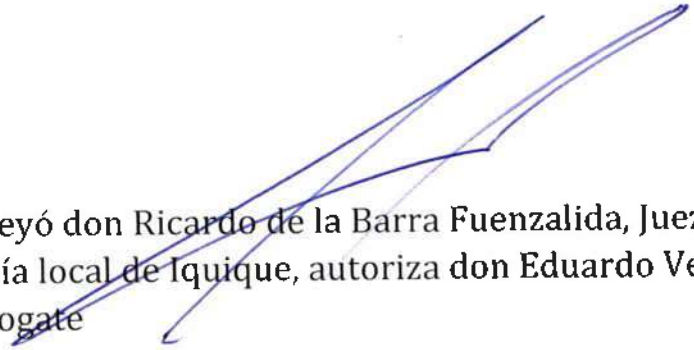
16.938.411-8

Iquique, a 29.07.2022  
Autorizo 

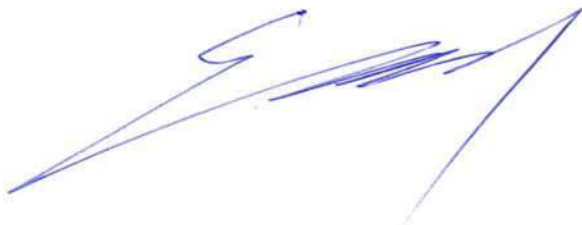
  
Secretario Abogado

Causa rol 17.367-L

En Iquique, a veintinueve días del mes de julio del año dos mil veintidós.  
Téngase presente delegación de poder.  
Notifíquese.



Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía local de Iquique, autoriza don Eduardo Veliz Soto, secretario  
subrogate



... ..  
... ..

*Tresunto Petición caso 3º*

Tercer Juzgado  
Petición Local  
29 JUL 2022

**DELEGA PODER;**

**S. J. DE POLICÍA LOCAL DE LOS IQUIQUE (3º)**

**ALBERTO SORDO BISBAL**, abogado, por la parte demandante, en autos sobre Responsabilidad para Titulares o Usuarios de Tarjetas de Pago y Transacciones Electrónicas en Caso de Extravío, Hurto, Robo o Fraude, causa Rol N° 17367-L, a SS. con respeto digo:

Que por este acto vengo en delegar poder en el habilitado de derecho don **PAULO CESAR ORDENES WILLIAMS** cedula nacional de identidad N° 16.349.892-8, de mí mismo domicilio, con quien podré actuar de forma conjunta y/o separada, y quien firma junto a mí en señal de aceptación.

**POR TANTO  
PIDO A SS.,** tenerlo presente.

**ALBERTO  
JOSÉ  
SORDO  
BISBAL**

Firmado digitalmente por  
ALBERTO JOSÉ  
SORDO BISBAL  
Fecha: 2022.07.27  
14:05:24 -04'00'

*16.349.892-8*

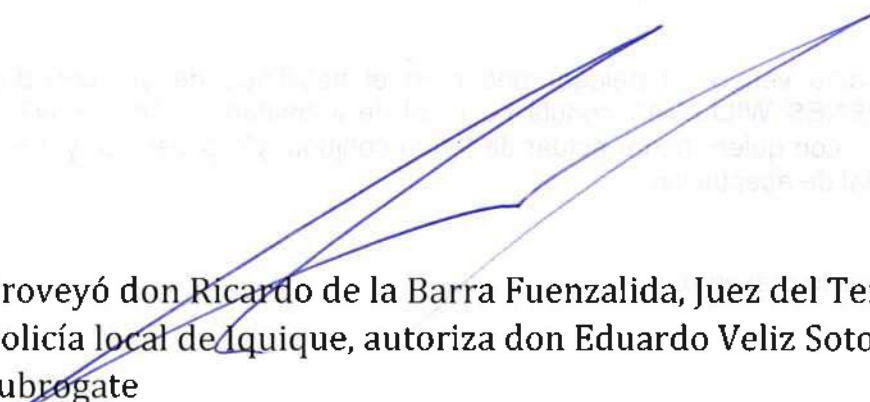
Iquique, a *29. 07. 2022*  
Autorizo *Paulo Cesar Ordenes Williams*

Secretario Asignado

Causa rol 17.367-L

En Iquique, a veintinueve días del mes de julio del año dos mil veintidós.  
Téngase presente delegación de poder.

Notifíquese.



Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía local de Iquique, autoriza don Eduardo Veliz Soto, secretario  
subrogate



## Causa rol 17.367-L

En Iquique, a veintinueve días del mes de julio del año dos mil veintidós. Siendo el día y hora, se lleva a efecto la audiencia de percepción de documento electrónico decretada para el día de hoy, con la asistencia de la parte denunciante infraccional y demandante civil, representada por la abogada, doña Tamara Rojas Aguirre y la asistencia de la parte denunciada infraccional y demandada civil, representada por el habilitado en derecho, son Pablo Cesar Ordenes Williams, quien se presenta con los medios electrónicos para tal efecto. En este acto se procede a abrir el sobre que contiene el documento electrónico a examinar. Al segundo siete, se identifica la señorita de apellido monte, y la señora Verónica Ramírez, le indica que recibió un llamado telefónico del Banco Santander. Y le indica, que la persona que la llamo muy educada, le indica todas las tarjetas que ella tiene, incluso los números de estas, y le indica que le iban a cambiar los plásticos. Me pedía que ingresara las coordenadas. Luego de ello le llegan unos correos electrónicos, en donde le informaban de un súper avance y unos giros desde su cuenta corriente. Al minuto 2.30, indica que ella tiene una cuenta en donde le depositan el 10% de la afp. Y sale una transacción a una persona de nombre Marcelino, persona que no conozco y tampoco he hecho esa transacción.. luego de ello le empezaron a llegar mensajes y trato de ingresar a cuenta y no pudo. Al minuto 3.32, le indica a la ejecutiva, que no puede acceder a su cuenta, ya que se encuentra bloqueada. Al minuto 3.41, le ejecutiva le informa que va a revisar las cuentas, y primero va a revisar la del 10% ,el día de hoy, tiene un giro en un cajero por \$200.000, a lo que responde que ella no ha girado nada. La ejecutiva le pregunta si le pidieron las claves, a lo responde que, la persona que me llamó me dijo que la tarjeta que termina en los números tanto y yo no le he dado ninguna información. Me pedía las fechas de caducaión y los nueros de seguridad. De igual forma me dijo que tenía la numeración de mi tarjeta de súper clave. La ejecutiva le consulta si la clave tenía relación con su fecha de nacimiento o rut,, a lo que responde que era el año de su nacimiento, la ejecutiva, le indica que esas claves son fáciles de adivinar. La ejecutiva le indica que al crear una clave no se debe usar fechas de nacimiento ni números correlativos. Al minuto 5.35, la ejecutiva le indica que cuando logran ingresar a la página del banco, ahí le aparecen los números de las tarjetas y toda la información de su cuenta. La ejecutiva le informa que lo que no se puede ver en la página, son la fechas de caducidad y los números de seguridad de las tarjetas. La señora Verónica le indica a la ejecutiva, que como la persona que la llamó era tan educada y tenia tanta información de ella, ella confió. Al minuto 6.54, la ejecutiva le informa que el súper giro de \$200.000 Salió de su cuenta y con la súper clave, la persona lo puede retirar en cualquier cajero, sin la necesidad de tener la tarjeta. Y adicionalmente se realizo una transferencia por \$ 200.000 a Marcelino. Luego de abonaron de la cuenta del 10% , la suma de dos millones . al minuto 7.47, la ejecutiva le informa que la suma mas grande por dos millones, se puede reversar, y que tiene que hacer una

solicitud. La señora Verónica, le consulta a la ejecutiva que es lo que tiene que hacer, ir a Carabineros; PDI, la ejecutiva le dice que cuando la contacten del banco, que diga que ella misma va a llamar al banco. La señora Verónica le indica a la ejecutiva, que al momento de recibir el llamado, decía banco Santander, departamento de cobranzas, y por eso conteste. Al minuto 10.04, la ejecutiva le informa que le bloqueo todos los productos, y va a ingresar el reclamo. Al minuto 12.45, la ejecutiva le informa que se va a reversar los montos, lo que van a quedar en su cuenta de forma transitoria a la espera de la investigación, la que dura unas doce días. La señora Verónica le consulta por su cuenta corriente y la ejecutiva, le responde que sigue igual, no hay ningún movimiento. La ejecutiva le dice que hay una compra el día de hoy en PC factorin, a lo que responde que no ha hecho ninguna compra. La ejecutiva, le consulta cuánto dinero tenía en la cuenta corriente, a lo que responde que debe tener unos dos millones de pesos, a lo que la ejecutiva le responde que tiene esa cantidad. Le dice la ejecutiva que hay un movimiento por ochocientos ochenta mil pesos. Y 185.590. Dice que no ha comprado nada. Al minuto 16.43 doña Verónica le consulta a la ejecutiva, si se puede bloquear la página para que nadie pueda ingresar, a lo que la ejecutiva le responde que si. Al minuto 19.03, la ejecutiva le consulta si un tercero le pidió entregar sus claves, a lo que responde que no. Al minuto 19.30, doña Verónica le dice a la ejecutiva, que la persona que la llamó le indico los números de la tarjeta de súper clave y ella los fue digitando en el teléfono pero no se las dije. Al minuto 21.25, la ejecutiva le consulta si recibió algún email, para bajar algún archivo, a lo que responde que le llegó un mensaje con seis dígitos y que tenía que ingresarlos y eso lo hicimos como cuatro veces. Al minuto 23.14, la ejecutiva le consulta si le han pedido revolver dinero, es decir si la han llamado para decirle que por error le depositaron, a lo que responde que no. La ejecutiva le consulta si tiene la aplicación del banco en el teléfono, a lo que responde que no, ya que le pueden robar el teléfono. Al minuto 25.50, la ejecutiva le informa que va tener que ingresar tres reclamos. Para la cuenta vista y para la que se realizó el giro. Al minuto 26.48, doña Verónica le da a la ejecutiva el número del celular del cual la llamaron 56968300089 y decía departamento de cobranza banco Santander. Al minuto 28.28, la ejecutiva le informa el monto de la compra a PC factorin es de \$ 1.967.700. le da el número de respaldo por la cuenta corriente 28251083. Al minuto 32.50, doña Verónica le consulta a la ejecutiva si tiene que ir a Carabineros, a lo que le responde que ese tipo de denuncia la debe hacer en la PDI. Al minuto 35.47, la ejecutiva le da el número de respaldo del reclamo por la cuenta vista, monto \$450.000 N° 28251203. Al minuto al minuto 37.14, la ejecutiva la informa que le bloqueo el ingreso a las cuentas vía internet, y que todas las tarjetas están bloqueadas. Al minuto 40.54, le da el N° de respaldo 28251264 y un plazo de cinco días para el reverso. Al minuto 43.02 la señora Verónica le consulta, a la ejecutiva que le de los valores que se compraron en PC factorin. Le informa N° 1 a las 13.29, por un valor

Trescientos setenta y cuatro

374

de \$896.890 código de autorización 291664. 2 \$ 185.590 a las 13.22, código de autorización 323664. Al minuto 45.20 se termina el primer audio.

Por atención preferente del Tribunal, suspéndase la presenta audiencia, y fíjese nueva fecha y hora para su prosecución. Cítese a las partes para la prosecución de la audiencia de percepción de documento electrónico el día 11 de agosto de 2022, a las 09:00 horas, quedando en este acto notificadas las partes.

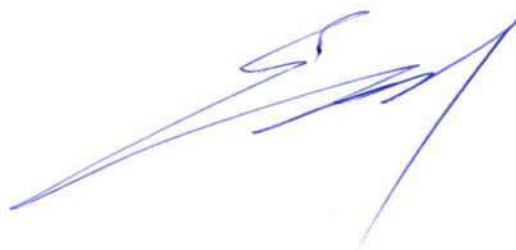
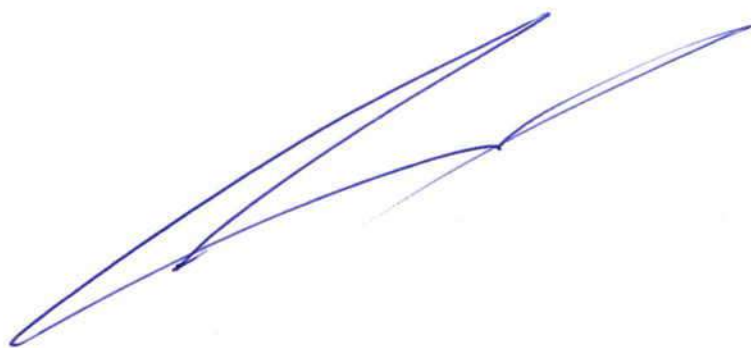
Con lo obrado y siendo las 13:25 horas, se pone termino a la presente audiencia, previa lectura se firma conjuntamente con S.S., y secretario subrogante que autoriza.



17.430.213 8



16.349.887-8





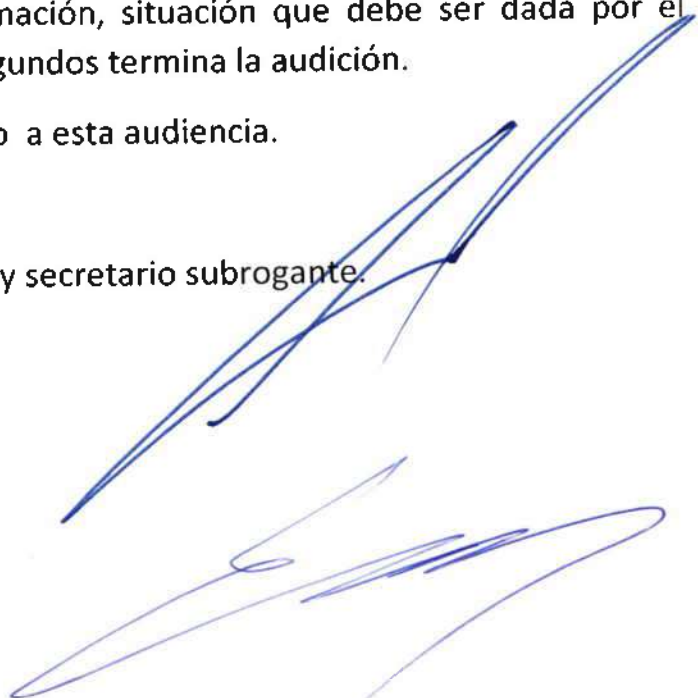
lquique a once días del mes de agosto del año dos mil veintidós.

Siendo día hora y señalada se lleva a efecto la prosecución de la audiencia de percepción de documento electrónico decretada con la asistencias de la parte denunciante infraccional y demandante civil representada por la abogada Tamara Rojas Aguirre y la asistencia de la parte denunciada infraccional y demandada civil representada por el señor abogado don Marcos Antonio Hernández Guiza.

El segundo audio, comienza con saludo de la ejecutiva del banco Santander, de nombre Johana Parra a los 18 segundos de la conversación. A los 3 minutos y diez segundos, solicita a la actora la tarjeta visa solicitando su número, a lo que la actora le señala que tiene nueva tarjeta solicitando su número, la clave y asimismo su tarjeta de coordenada, como la actora no domina el procedimiento la ejecutiva la instruye y guía para hacerlo. A los 10 minutos y diecinueve segundos, la ejecutiva señala a la actora de dos reclamos por compras no reconocidas indicando montos y señalando que la conversación para su seguridad está siendo grabada. A los 14 minutos y diez segundo indica monto de deuda \$494.890. A los 25 minutos con treinta segundos la ejecutiva le solicita l fecha y hora que activa la tarjeta, a lo que la actora le expone lo hace 25 de minutos que están conversando. A los 27 minutos y siete segundos la ejecutiva le solicita si un tercero le solicitó otorgar la clave, solamente cuando la llamaron y no la entrego a viva voz y lo tecleo en el teléfono. Al minuto 34 con cuarenta y segundos la actora le señala a la ejecutiva que las tarjetas ya están v bloqueadas. A los minutos 41. La ejecutiva le informa que está ingresando el reclamo se lo hará llegar a su correo electrónico, dado que no puede otorgar solución sino será el supervisor quien le entregar la información respectiva. A los minutos 44, la ejecutiva señala a la actora que respectiva la compra de 3 de junio le señala que la tarjeta fue bloqueada a las 14:06 y la compra se efectuó a las 13:27 y respecto de la compra del día 7 desconoce la entrega de información, situación que debe ser dada por el supervisor. A los 47 con siete segundos termina la audición.

Con Lo actuado se pone término a esta audiencia.

Previa lectura, se firma Ante SS y secretario subrogante.



Re: NOTIFICA RESOLUCIÓN 17.367-L

Felipe Fernández Leon <ffernandez@fgnabogados.cl>

Vie 12/08/2022 12:04

Para: Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

Estimad@s:

Junto con saludar, adjunto escrito para causa 17.367-L. Favor confirmar recepción.

Saludos cordiales.



**Felipe Fernández León**

Abogado

Dr. Sotero del Río N° 326, oficina N° 1309, comuna de Santiago.

(2) 2 929 97 67

www.fgnabogados.cl

**De:** Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

**Fecha:** jueves, 10 de marzo de 2022, 16:04

**Para:** Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

**Asunto:** RE: NOTIFICA RESOLUCIÓN 17.367-L

Buenas tardes:

La ubicación del Juzgado es Calle José Joaquín Pérez N° 390. Es una casona esquina, que está ubicada en la plaza 21 de Mayo.

**De:** Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

**Enviado:** jueves, 10 de marzo de 2022 17:24

**Para:** Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

**Asunto:** Re: NOTIFICA RESOLUCIÓN 17.367-L

Estimada:

Junto con saludar, le consulto por la dirección del JPL, ya que esta no está informada en la página web de la municipalidad, ni en ninguna de las notificaciones recibidas. Quedo atento.

Saludos cordiales.



**Felipe Fernández León**

Abogado

Dr. Sotero del Río N° 326, oficina N° 1309, comuna de Santiago.

(2) 2 929 97 67

www.fgnabogados.cl

**De:** Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

**Fecha:** miércoles, 2 de marzo de 2022, 10:57

**Para:** Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

**Asunto:** RE: NOTIFICA RESOLUCIÓN 17.367-L

Buenos días:

El comparendo es presencial, no tenemos implementado el sistema telemático.

atentamente

secretaria abogado

*Presente de Leon Gueta 377*  
De: Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

Enviado: miércoles, 2 de marzo de 2022 10:54

Para: Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

Cc: Verónica R <vramirezr1975@gmail.com>

Asunto: FW: NOTIFICA RESOLUCIÓN 17.367-L

Estimad@s:

Junto con saludar, les consulto si este comparendo en causa 17.367-L puede ser realizado mediante video conferencia. Si es así, favor indicar si la prueba documental puede ser enviada por esta vía, previo al comparendo. Quedo atento.

Saludos cordiales.



**Felipe Fernández León**

Abogado

Dr. Sotero del Río N° 326, oficina N° 1309, comuna de Santiago.

(2) 2 929 97 67

www.fgnabogados.cl

De: Notificaciones Tercer Juzgado <notificaciones\_3jpl@municipioiquique.cl>

Fecha: miércoles, 2 de marzo de 2022, 09:01

Para: "zonanorte@legaltec.cl" <zonanorte@legaltec.cl>, "abogadomarcohernandezguiza@gmail.com" <abogadomarcohernandezguiza@gmail.com>, Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

Asunto: NOTIFICA RESOLUCIÓN

Por medio de la presente, se procede a notificar por correo electrónico, en virtud de lo dispuesto en el inciso cuarto del artículo 18 de la Ley 18.287, en la causa rol 17.367-L "RAMIREZ/BANCO SANTANDER", la resolución contenida en el archivo adjunto.

Sin otro particular.

Eduardo Véliz

Receptor Ad-Hoc

Tercer Juzgado de Policía Local de Iquique

*Presente Actente y ochos*

*379*

**SOLICITA COPIA DE AUDIOS**

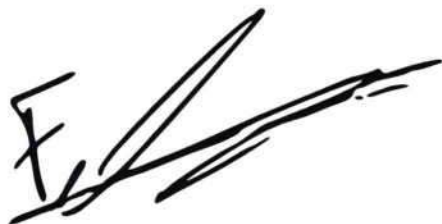
**S.J. DE POLICÍA LOCAL DE IQUIQUE (3º)**

**FELIPE FERNANDEZ LEON**, abogado denunciante y demandante civil, en causa RIT N° 17367-L-2021, seguida ante este tribunal por ley del consumidor, a US. respetuosamente digo:

Que por medio de este acto, vengo en solicitar copia de los archivos de audio acompañados por la parte denunciada demandada, los cuales fueron escuchados en audiencias de percepción de fechas 29 de julio y 11 de agosto de 2022.

**POR TANTO:**

**SOLICITO A UD:** Acceder a las copias solicitadas.



16.938.411-8

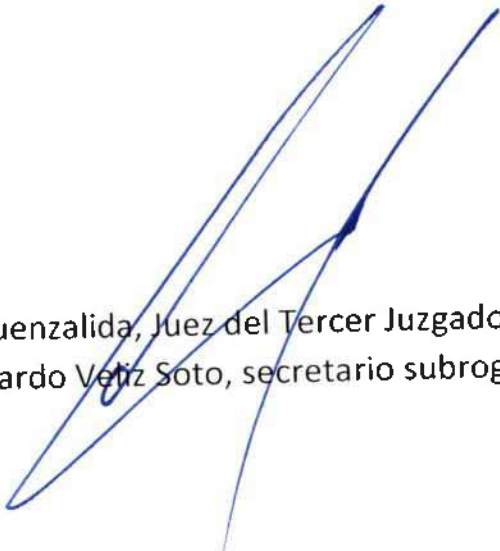
Trescientos setenta y ocho

378

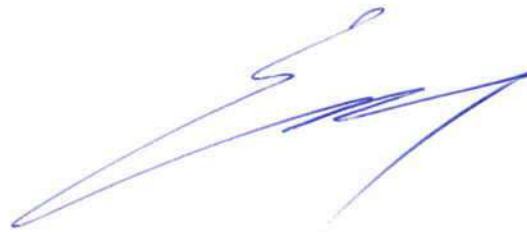
P 17367

En Iquique, a treinta y un días del mes de agosto del año dos mil veintidós  
Resolviendo la presentación de fojas 376 y siguiente. Como se pide, a costa  
del solicitante.

Notifíquese.



Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de policía  
local de Iquique, autoriza don Eduardo Véliz Soto, secretario subrogante



*Prescrita ochante*

380

TERCER JUZGADO DE POLICIA LOCAL  
JOSE JOAQUIN PEREZ N° 390  
IQUIQUE

OF.: 1100 /

ANT.:

MAT.: solicita lo que indica

Iquique, 12 de agosto de 2022

DE : TERCER JUZGADO DE POLICIA LOCAL IQUIQUE

A : AGENTE DEL BANCO SANTANDER DE IQUIQUE.

En causa rol 17.367-L caratulada Verónica Andrea Ramírez Riquelme con Baco Santander Chile, seguida en este Tribunal, por infracción a la ley 19.496, de protección a los consumidores, se ha ordenado oficiar a Ud., a fin remita a este Tribunal, toda la documentación que tenga, respecto de los reclamos realizados por la demandante, desde el mes de junio de año 2021, a la fecha.

Se solicita que dichos documentos, sean remitidos a la brevedad, por existir causa en tramitación.

Sin otro particular, le saluda

atte., a Ud.,



*[Signature]*  
RICARDO DE LA BARRA FUENZALIDA  
JUEZ

*[Signature]*  
EDUARDO VELIZ SOTO  
SECRETARIO SUBROGANTE

CC. Expediente.-

*[Signature]*  
CAMILA SANDOVAL RIVERA  
Jefe de Servicio a Clientes  
BANCO SANTANDER CHILE

31/08/2022

Trascrito pchunto juus

381

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE,

01 SET. 2022

CERTIFICO: Que, con esta fecha y siendo las 18:23 hrs. he procedido a notificar a don Felipe Fernández León de la resolución de fecha 30 Agosto 2022, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico ffernandez@fqaabogados.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

Trescientos ochenta y dos

382

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367 - L

IQUIQUE, 01 SET. 2022

CERTIFICO: Que, con esta fecha y siendo las 18 : 23 hrs. he procedido a notificar a don (ña) Marco A. Hernandez Guiza de la resolución de fecha 20/Agosto/2022, remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abogado.marco.hernandezguiza@pmail.com. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

n.c.c: ZonasMonte@lapaltec.cl



Trescientos ochenta y tres

383

**OBSERVACIONES A LA PRUEBA**

20 DIC 2022

**S.J. DE POLICÍA LOCAL DE IQUIQUE (3ª)**

Iquique

**FELIPE FERNANDEZ LEON**, abogado denunciante y demandante civil, en causa RIT N° 17367-L-2021, seguida ante este tribunal por ley del consumidor, a US. respetuosamente digo:

Que vengo dentro de plazo en hacer las siguientes observaciones a la prueba rendida por las partes en autos:

Para acreditar la infracción a las normas establecidas en la ley 19.496, y para comprobar los perjuicios sufridos como consecuencia de la mencionada infracción, esta parte se valió de prueba documental extensa, prueba testimonial, y de antecedentes que aportó la parte denunciada/demandada.

En cuanto a la prueba documental presentada por esa parte, hacemos las siguientes observaciones:

1. Denuncia en Fiscalía de fecha 3 de junio del años 2021, y aporte de antecedentes: Con este documento se comprueba que mi representada realmente fue estafada, y que ha mantenido el mismo relato desde el comienzo, a saber, que la llamó una persona que se hizo pasar por una ejecutiva del Banco Santander, la cual tenía toda su información bancaria.
2. 2 pantallazos de llamados recibidos de parte del estafador, 3 de junio del año 2021, (13:06, y 13:45): Con estos documentos se acreditan las llamadas realizadas por la estafadora, lo que complementado con la hora de la llamada al call center del banco prueba que mi representada llamó de inmediato al Banco luego de sufrir la estafa
3. Mails del banco hacia mi representada de fecha 10/6/21, 29/6/21, 1/7/21, 8/7/21, 12/7/21, 13/7/21, 27/7/21 y 28/7/21: Con estos se prueban los distintos reclamos que realizó mi representada por la estafa sufrida.
4. Mails hacia el banco, parte de mi representada, de fecha 9/6/21, 13/6/21, 29/6/21: Con esto se comprueba nuevamente que mi representada ha mantenido la misma historia, y no ha cambiado, ya que en estos correos ella le narra los mismos hechos la banco. También es dable destacar que en el correo de 29 de junio de mi representada al banco ella dice: "En este momento no puedo pensar, me roban desconocidos y después el banco... es demasiado."
5. Carta al Sernac financiero: Nuevamente se comprueba que se mantiene el mismo discurso en relación a los hechos desde el principio.

6. Cartola tarjeta Visa (super giro, transferencia entre productos, y transferencia a terceros, de fecha 3 de junio de 2021): Con esto se comprueba parte de los movimientos no reconocidos.
7. Detalle 4 compras PC Factory y 1 compra Super Repuestos SPA, 3 de junio de 2021: Con esto se comprueba parte de los movimientos no reconocidos.
8. Movimientos en cuenta corriente 3 de junio 2021 (3 compras PC Factory): Con esto se comprueba parte de los movimientos no reconocidos.
9. Mails a y desde Pc Factory de 4, 9, 13 y 15 de junio del año 2021: Con estos correos enviados a un tercero se comprueba que mi representada mantiene la misma historia desde el principio.
10. Estados de cuenta tarjetas de crédito visa y american express desde junio a diciembre 2021: Con esto se comprueba parte de los movimientos no reconocidos, y específicamente los cobros de impuestos, intereses y cuotas que se tuvo que ir pagando, ya que algunos de los movimientos no reconocidos fueron realizado en cuotas.
11. Reclamo y respuesta Sernac, 21 de julio del año 2021: Nuevamente mi representada mantiene la misma dinámica de los hechos.
12. Reclamo ante la CMF: Idem.
13. Informe psicológico, 16 de agosto de 2021: Con este documento se comprueba las consecuencias psicológicas que tuvo en mi representada el haber sido víctima de esta estafa telefónica, provocándole un episodio de depresión.
14. Formulario de constancia información al paciente GES e ingreso GES., 5 de agosto de 2021: Con este documento se comprueba la licencia médica a la que tuvo que acogerse mi representada, por el episodio de la estafa.

En cuanto a la prueba testimonial, en comparendo de estilo compareció doña Ina Choque, quien básicamente confirmo que mi representada le contó exactamente los mismo hechos que se relatan en estos autos, y también pudo atestar al estado anímico de mi representada, indicando que se encontraba con terapia psicológica y psiquiátrica.

Por otro lado, declaró la testigo Laura Martínez, quien testificó sobre los mismo hechos, nuevamente confirmando lo que doña Verónica nos relata por medio de se denuncia y querella, y también aportó haber visto a mi representada muy decaída y angustiada, que no dormía bien, por no tener respuesta favorable del banco, incluso no asistiendo al baby shower de la testigo. También indicó que doña Verónica tuvo que volver a trabajar luego de su licencia pero se veía que no estaba recuperada 100%.

Finalmente, esta parte solicitó las grabaciones de las llamadas realizadas por doña Verónica el día de los hechos, 3 de junio de 2021, el 7 de junio de 2022 y el 12 de junio de 2022, las que fueron escuchas en audiencia de percepción. Esto, ya que mi representada tuvo que hacer 3 reclamos distintos ya que cada vez que llamaba, le daban información incompleta. En estas llamadas también se puede escuchar claramente que, momento después de haber sido estafa, mi representada llama al banco para denunciar el hecho, indicando que la persona que la llamó tenía toda su información personal, toda la información respecto a los productos bancarios que ella tenía, información de sus seguros, números de tarjetas, e incluso el número de la tarjeta de coordenadas.

Por otro lado, las llamadas de los otros 2 días se habían solicitado para que el tribunal pudiese ver el estado mental en el que la dejó esta situación, llorando y poniéndose nerviosa al hablar con los ejecutivos de la parte denunciada. Extrañamente, el banco no acompaña la llamada del 7 de junio de 2022, ya que en ella mi representada estalla en llanto al ser informada de más movimientos no reconocidos provocados por la falta de seguridad del banco.

Finalmente, el banco debería aportar todos los reclamos que realizó mi representada (que fue oficiado para tal efecto con fecha 22 de julio de 2022), los que nuevamente comprobaran que mi representada mantuvo la misma historia desde el principio.

En cuanto a la prueba presentada por la contraparte, esta se limita a realizar alegaciones en cuanto a que el movimiento bancario se realizó con todas las autorizaciones que se requieren. Alegan que tienen un certificado de seguridad en su página web. Luego, aportan pantallazos en los que figura las advertencias que realiza el banco por el tema de fraudes. Básicamente, su defensa se reduce a alegar que como mi representada fue negligente, todo lo que le pasó es su culpa. Esto lo resumen de la siguiente forma: *"El tema es muy simple. Si el usuario no hubiere, digitado las en su teléfono, que terceros le pidieron entregar y ella entregó, (como lo reconoce), las transacciones no podían haberse materializado, es decir el mismo usuario se expuso al riesgo, digitando sus super clave y clave 3.0 de seis dígitos que llegó a su teléfono, y entregó, las cuales son precisamente para resguardar que quien hace las transacciones es el propio usuario."*

Es decir, su argumento es uno de causalidad. Mi representada cometió un acto que tuvo una consecuencia determinada

Pero, luego revisar la prueba presentada es claro que, si estamos viendo esto desde un punto de vista de causalidad, lo que realmente inició estos hechos es la falta de seguridad con la que cuentan los movimientos bancarios del Banco de Chile, debido

a la falta de seguridad con que opera el banco respecto a la información privada de sus clientes. Ellos se limitan a tratar de establecer que ellos tienen todas las medidas de seguridad habidas y por haber, por lo que lo sucedido no podría haber pasado. Pero, en la práctica sí pasa, y pasa a menudo, ya que los defraudadores saben que personas como mi representada tienen determinados productos bancarios, sabiendo incluso la numeración de estos productos, información que solo maneja el cliente y el banco. O que solo debería manejar el cliente y el banco, mejor dicho.

Si bien existe una acción intermediaria realizada por mi representada, al entregar claves solicitadas por la estafadora, esta estafadora nunca debió haber tenido acceso a toda la información que tenía, que ha sido latamente detallada en esta causa, lo cual fue el gatillante para que mi representada accediera a entregar cierta información solicitada.

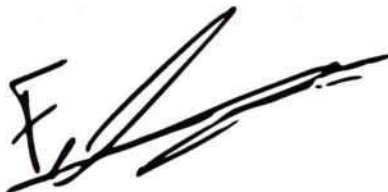
El Banco Santander debería contar con las herramientas suficientes para que estos hechos no ocurran, es decir, realizar un mejor resguardo de la información confidencial de sus clientes. Y si no las tiene, y estos hechos ocurren, debe hacerse responsable por los perjuicios que puedan ocurrir. Ninguna de las anteriores llevó a cabo la empresa demandada.

Por otro lado, la conexión de causalidad entre el actuar omisivo de la parte demandada con los daños sufridos por mi representada es patente. Debido al fraude que sufrió mi representada, su bienestar económico se vio afectado en un primer lugar ya que una suma importante de dinero le fue sustraída, y, a pesar de que el banco abono la suma de 35 UF, en este mismo procedimiento está pidiendo que se le devuelva. Esto, sin contar con los intereses e impuestos cobrados por los cupos de tarjetas de crédito de mi representada. Debido a esta pérdida, su psiquis se ha visto afectada, debido a la abrumadora situación en la que se vio, lo que le trajo como consecuencia un estrés post traumático que se ha visto agigantado por no tener respuesta alguna de la empresa demandada.

Por estas consideraciones, debe tenerse por plenamente probado, que la parte demandada de autos infringió, a lo menos, el artículo 23 de la ley 19.496 que establece que *"Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio"*.

**POR TANTO:** En virtud del artículo 430 del Código de Procedimiento Civil,

**SOLICITO A UD:** Tener por observada la prueba rendida en autos, y en su mérito, acoger la denuncia presentada en autos, determinar que la parte denunciada y demandada vulneró los derechos de mi representada, en su calidad de consumidora, al ofrecer un servicio que no garantizaba la seguridad de quienes lo ocupaban, solicitando se impongan las multas más severas disponibles según la ley 19.496, y, por otro lado, acoger la demanda civil interpuesta.



Resumen de Cuenta y Causa

385

Causa rol 17.367-L

En Iquique, a veintisiete días del mes de diciembre del año dos mil veintidós.

Téngase presente en su oportunidad.

Notifíquese

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de Policía Local de Iquique, autoriza doña Jessie Giacconi Silva, Secretaria Abogado

Prescritos Ochoenta y seis

386

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367 - L

IQUIQUE, **05 ENE. 2023**

CERTIFICO: Que, con esta fecha y siendo las 16 : 30 hrs. he procedido a notificar a don (ña) Felipe Fernández León de la resolución de fecha 27 / diciembre / 2022, remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico fernandez@fpmabopados.cl. Doy fe.



JUAN A. SAAVEDRA FERRADA  
Receptor

Trescientos ochenta y siete

387

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17367 - L

IQUIQUE, 05 ENE. 2023

CERTIFICO: Que, con esta fecha y siendo las 16 : 38 hrs. he procedido a notificar a don (ña) Marco A. Hernandez Guiza de la resolución de fecha 27 / diciembre / 2022, remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abopado.marco.hernandezguiza@gmail.com. Doy fe.



JUAN A. SAAVEDRA FERRADA  
Receptor

c.c.: zonamonte@lupaltec.cl

*Presente adjunte y odu 360*

Re: Causa 17367-L-2021

Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

Vie 20/01/2023 14:58

Para: Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

CC: Verónica R (mediante Google Drive) <vramirezr1975@gmail.com>

Estimad@s:

Nuevamente consulto por la sentencia de esta causa. Han pasado más de 5 meses desde que se presentó toda la prueba, y aun no resolución "autos para fallo", o sentencia. Si no tengo respuesta tendré que presentar el reclamo correspondiente ante la Corte de apelaciones. Quedo atento.

Saludos cordiales.



**Felipe Fernández León**

Abogado

Dr. Sotero del Río N° 326, oficina N° 1309,

comuna de Santiago.

(2) 2 929 97 67

www.fgnabogados.cl

---

**From:** Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

**Date:** Monday, 19 December 2022, 11:44

**To:** Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

**Cc:** "Verónica R (mediante Google Drive)" <vramirezr1975@gmail.com>

**Subject:** Causa 17367-L-2021

Estimad@s:

Junto con saludar, consulto por la causa 17367-L-2021, ya que se llevó a cabo audiencia de percepción de audio el 11 de agosto, y a la fecha no se ha resuelto "autos para fallo" o similar, o no se ha notificado a esta parte de esa resolución.

Por otro lado, adjunto escrito para su presentación en la causa. Favor acusar recibo.

Saludos cordiales.



**Felipe Fernández León**

Abogado

Dr. Sotero del Río N° 326, oficina N° 1309,

comuna de Santiago.

(2) 2 929 97 67

www.fgnabogados.cl

---

**From:** Felipe Fernandez Leon <ffernandez@fgnabogados.cl>

**Date:** Wednesday, 7 September 2022, 09:47

**To:** Tercer Juzgado Municipalidad de <tercerjuzgado@municipioiquique.cl>

**Subject:** Re: NOTIFICACION R. 17367-L RES. FECHA 30/08/2022

Estimad@s:

Sigo esperando respuesta.

Saludos cordiales.



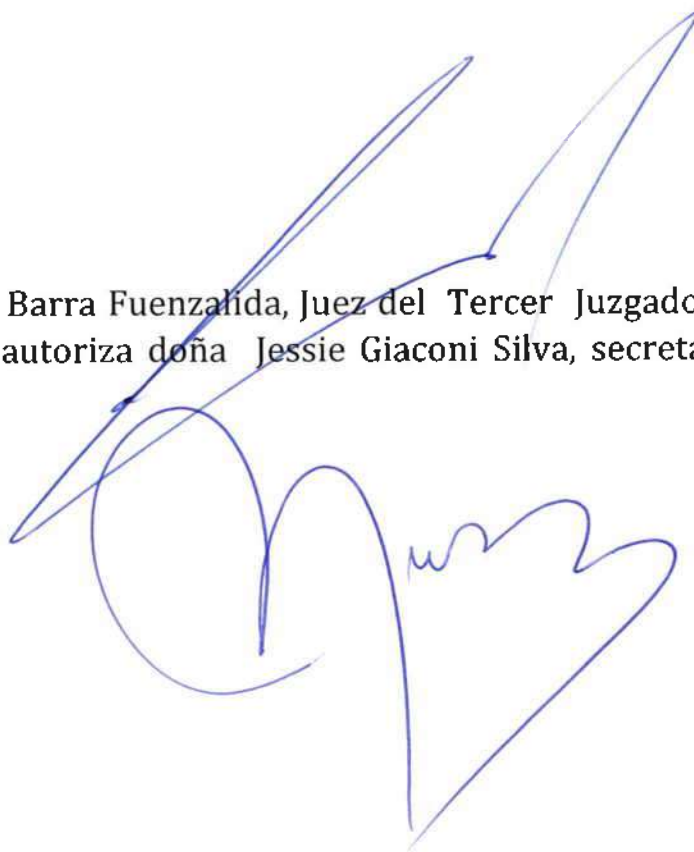
Prescrites ochute y more

389.

Causa rol 17.367-L

En Iquique, a dieciocho días del mes d enero del año dos mil veintitrés  
No habiéndose recibido respuesta por parte del Banco Santander, al oficio  
N° 1100, de fecha 12 de agosto de 2022, en el que se ordenó remitir a este  
Tribunal, toda la documentación que tenga respecto de los reclamos  
realizados por la demandante, doña Verónica Andrea Ramírez Riquelme,  
Rut 12.858.024-7, desde el mes de junio de 2021, a la fecha.  
Notifíquese y ofíciase.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía Local de Iquique, autoriza doña Jessie Giaconi Silva, secretaria  
abogado



Treserats monute

390

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17-367-L

IQUIQUE, 24 ENE. 2023

CERTIFICO: Que, con esta fecha y siendo las 16:28 hrs. he procedido a notificar a don (ña) Marco A. Hernandez Guiza de la resolución de fecha 18 | enero | 2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abogado.marco.hernandezguiza@gmail.com. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

c.c: zoumante@kba/tec.cl

Prescrita Monte Juro

301

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE, 24 ENE. 2023

CERTIFICO: Que, con esta fecha y siendo las 16:28 hrs. he procedido a notificar a don (ña) Felipe Fernández Leon de la resolución de fecha 18 enero 2023 remitiéndote copia íntegra de esta debidamente autenticada al correo electrónico fernandez2@fgabogado.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

*Presunto agente J. don*

*392*

TERCER JUZGADO DE POLICIA LOCAL  
JOSE JOAQUIN PEREZ N° 390  
IQUIQUE

**COPIA**

OF. 90 /

ANT:

MAT: reitera oficio

IQUIQUE, 23 de enero de 2023

DE: JUEZ DEL TERCER JUZGADO DE POLICIA LOCAL DE IQUIQUE

A: AGENTE DEL BANCO SANTANDER IQUIQUE.

En causa Rol 17.367-L, caratulada "Verónica Andrea Ramírez Castillo con Banco Santander", seguida en este Tribunal por infracción a la Ley 19.496 de protección al consumidor, se ha decretado oficiar a Ud., a fin reiterar oficio 1100, de fecha 12 de agosto de 2022, en el que se ordenó remitir a este Tribunal, toda la documentación que tenga respecto de los reclamos realizados por la demandante, doña Verónica Andrea Ramírez Riquelme, rut 12.858.024-7, desde el mes de junio de 2021 a la fecha.

Se solicita que dicha información sea remitida a la mayor brevedad, por existir causa en tramitación

Sin otro particular.

Saluda Atte. A Ud.,



RICARDO DE LA BARRA FUENZALIDA  
JUEZ

JESSIE GIACONI SILVA  
SECRETARIA ABOGADO

*[Handwritten signature]*  
VIDE LATINI BERNALDES  
Agente  
BANCO SANTANDER-CHILE

*22/03/23.-*

Trescientos noventa y tres

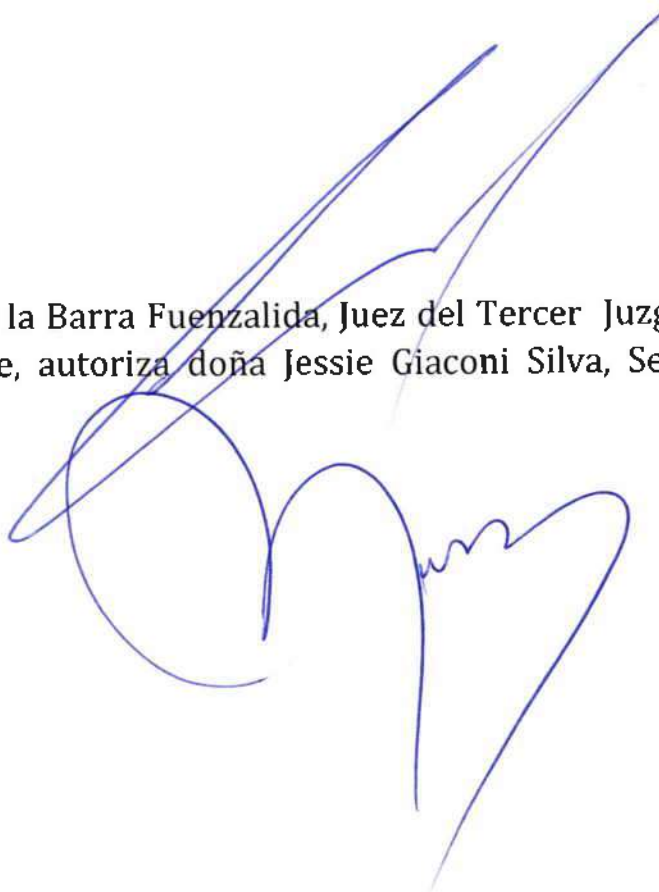
393

Causa rol 17.367-L

En Iquique, a veintinueve días del mes de junio del año dos mil veintitrés  
Visto: el tiempo transcurrido y, no habiendo recibido respuesta por parte  
del Banco del Estado Santander, al oficio 90, de fecha 23 de enero de 2023,  
otórguese un plazo a la parte querellante y demandante civil, para que  
dentro del tercero día de notificada la presente resolución, solicite  
peticiones concretas, bajo apercibimiento de dejar sin efecto dicha  
diligencia.

Notifíquese.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía Local de Iquique, autoriza doña Jessie Giacconi Silva, Secretaria  
abogado



Trescientos Noventa y cuatro 394

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE,

01 JUL. 2023

CERTIFICO: Que, con esta fecha y siendo las 12:23 hrs. he procedido a notificar a don (ña) Marco A. Hermudez Guiza de la resolución de fecha 29 Junio 2023, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico abogado marco.hermudez.guiza@pmudil.com. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

c.c.: zona monte @ legaltec.cl

Prescinto monte y fisco

395

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE,

01 JUL. 2023

CERTIFICO: Que, con esta fecha y siendo las 12:23 hrs. he procedido a notificar a don (ña) Felipe Fernandez Leon de la resolución de fecha 29/ Junio / 2023, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico ffernandez@fpabopados.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

*Tresmuntas Morale*



*396*

**CUMPLE LO ORDENADO**

**S.J. DE POLICÍA LOCAL DE IQUIQUE (3º)**

**FELIPE FERNANDEZ LEON**, abogado denunciante y demandante civil, en causa RIT N° 17367-L-2021, seguida ante este tribunal por ley del consumidor, a US. respetuosamente digo:

*qci*

Que vengo en cumplir lo ordenado por este tribunal el 29 de junio de 2023, en el sentido de desistirme de cualquier solicitud de prueba realizada de la que tenga que responder la parte demandada, ya que claramente no aportarán lo solicitado, logrando que este tribunal demoré en más de 1 años en emitir sentencia definitiva.

En virtud de lo anterior, solicito se falle la causa dentro del plazo establecido en el artículo 50 H, inciso sexto de la ley 19.496.

**POR TANTO:**

**SOLICITO A UD:** Tener por cumplido lo ordenado, y emitir sentencia lo antes posible.

16.938.411-8



Trescientos veinte y siete ) Fidei

38;

Causa rol 17.367-L

En Iquique, a cinco días del mes de julio del año dos mil veintitrés  
A lo principal: traslado.  
Notifíquese.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía Local de Iquique, autoriza doña Jessie Giaconi Silva, S



Presentes Monica y Ocho

388

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE. 08 .III 2023

CERTIFICO: Que, con esta fecha y siendo las 12 : 04 hrs. he procedido a notificar a don (ña) Felipe Fernandez Leon de la resolución de fecha 05 / Julio / 2023, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico ffernandez@fgabogados.cl. Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

Tresceros Monte Jiron

3PP

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE, 08 JUL 2023

CERTIFICO: Que, con esta fecha y siendo las 12:04 hrs. he procedido a notificar a don (ña) Marco A. Hernández Guiza de la resolución de fecha 05 Julio 2023, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico abqpsdomarcohernandezguiza@gmail.com. Doy fe.



JUAN A. SAAVEDRA FERRADA  
Receptor

c.c.: zonamonte@bpaltec.cl

cuatrosuents

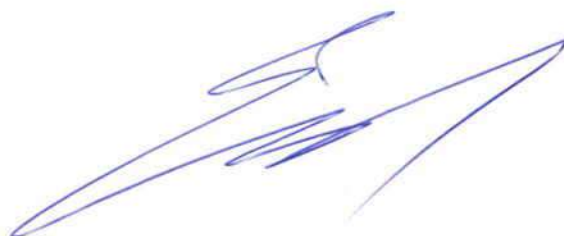
c/copia

40

Causa rol 17.367-L

En Iquique, a veinticuatro días del mes de julio del año dos mil veintitrés  
Certifique el señor secretario del Tribunal, si la parte denunciada y  
demandada civil, evacuó el traslado conferido a fojas 397  
Notifíquese.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía Local de Iquique, autoriza don Eduardo Veliz Soto, Secretario  
subrogante.



Presidencia Municipal

401

TERCER JUZGADO DE POLICIA LOCAL  
J. J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367 - L

IQUIQUE, 26 JUL. 2023

CERTIFICO: Que, con esta fecha y siendo las 18 : 10 hrs. he procedido a notificar a don (ña) Felipe Fernández León de la resolución de fecha 24 Julio 2023, remitiéndole copia íntegra de esta debidamente autentificada al correo electrónico ffernandez@fgabogados.cl. Doy fe.



JUAN A. SAAVEDRA FERRADA  
Receptor

cuatrocientos dos

402

TERCER JUZGADO DE POLICIA LOCAL  
J.J. PEREZ No. 390 - IQUIQUE

ROL No. 17.367-L

IQUIQUE,

26 JUL. 2023

CERTIFICO: Que, con esta fecha y siendo las 11:10 hrs. he procedido a notificar a don (ña) Marco A. Hernández Guiza de la resolución de fecha 24 Julio 2023, remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico abogado.marco.hernandezguiza@pmidil.com. Doy fe.

  
JUAN A. SAAVEIRA FERRADA  
Receptor

c.c.: zondante@bpoltec.cl

cuarenta y tres

403

IQUIQUE, ocho de agosto del año dos mil veintitrés

CERTIFICO, que no se ha evacuado el traslado conferido en autos. Doy fe.

Por orden del Juez

  
SECRETARIO (S)



Causa rol 17.367-L

En Iquique, a treinta días del mes de agosto del año dos mil veintitrés  
En mérito de la certificación del señor secretario del Tribunal a fojas 403,  
téngase por evacuado el traslado conferido a fojas 397, en rebeldía de la  
parte denunciada infraccional y demandada civil.

Resolviendo la presentación de fojas 396, téngase por desistida la  
diligencia solicitada por la parte denunciante infraccional y demandante  
civil a fojas 366.

Notifíquese.

Proveyó doña Jessie Giaconi Silva, Jueza subrogante del Tercer Juzgado de  
Policía Local de Iquique, autoriza don Eduardo Veliz Soto, secretario  
subrogante.



cuarenta y siete  
C/ Iquique

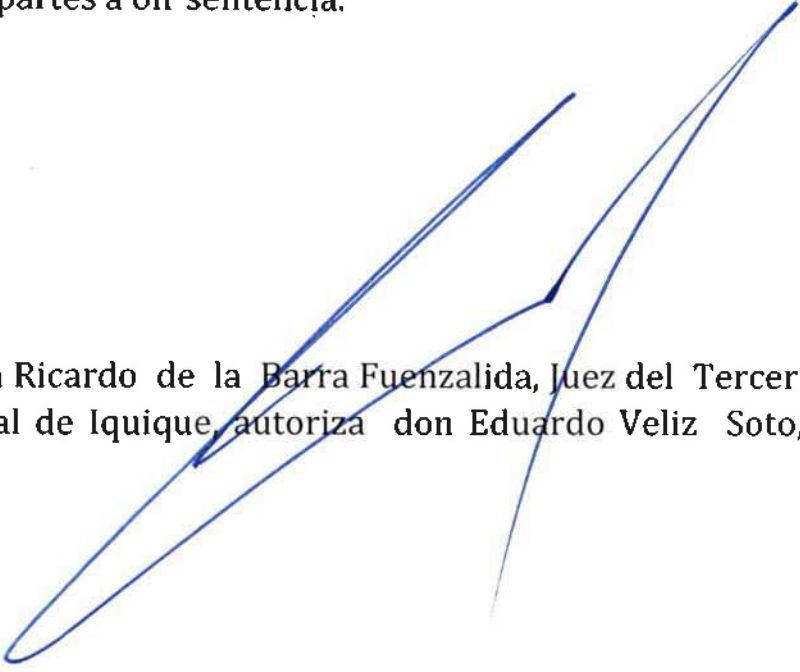
401

Causa rol 17.367-L

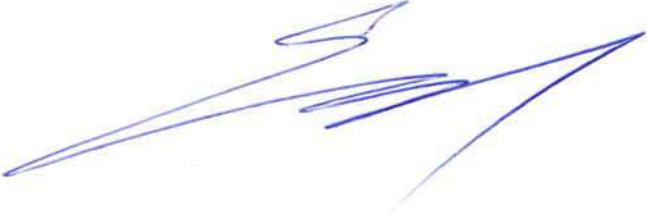
En Iquique, a veintisiete días del mes de septiembre del año dos mil veintitrés

Cítese a las partes a oír sentencia.

Notifíquese.



Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de Policía Local de Iquique, autoriza don Eduardo Veliz Soto, Secretario subrogante



matrículas ochu

408

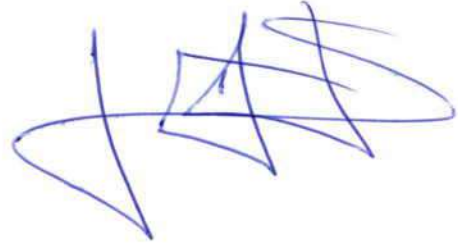
TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

IQUIQUE, 29 SET. 2023

CERTIFICO: Que, con esta fecha y siendo las 17:29 hrs. he procedido a notificar a don (ña) FELIPE FERNANDEZ LEON de la resolución de fecha 27-09-2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico ffernandez@fgnabogados.cl. Doy fe.

JUAN A. SAAVEDRA FERRADA  
Receptor



motu proprio

409

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

IQUIQUE, 12 9 SET. 2023

CERTIFICO: Que, con esta fecha y siendo las 07:29 hrs. he procedido a notificar a don (ña) MARCO A. HERNANDEZ GUIZA de la resolución de fecha 27-09-2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico [abogadomarcohemandezguiza@gmail.com](mailto:abogadomarcohemandezguiza@gmail.com). Doy fe.

JUAN A. SAAVEDRA FERRADA  
Receptor

c.c.: [zonanorte@legaltec.cl](mailto:zonanorte@legaltec.cl)



patrocinio de

410

**En lo principal:** asume patrocinio y poder; **primer otrosí:** acompaña documentos; **en el segundo otrosí:** forma de notificación; **en el tercer otrosí:** delega poder.

S.J.P.L. de Poliza Local (3°)



**Manuel José Searle Risopatrón**, abogado, en representación de **Banco Santander**, en autos sobre declaración de existencia de dolo o culpa grave del titular o usuario del medio de pago, conforme al artículo 5° de la Ley N° 20.009, caratulados "**Banco Santander con Ruiz**", ROL N° 17367-L-2021, a S.S., respetuosamente digo:

941

Que, con el mérito del mandato otorgado por escritura pública con fecha 02 de diciembre de 2022 en la 37° Notaria Pública de Santiago, otorgada por doña Nancy De La Fuente Hernández, anotada bajo su repertorio N° 3904-2022, en donde consta mi personería para actuar en presentación de la demandante, y en calidad de abogado habilitado que envisto, vengo en asumir personalmente el patrocinio y poder en esta causa.

**Por tanto**, en virtud de lo señalado,

**Ruego a S.S.**, se sirva tenerlo presente.

**PRIMER OTROSÍ:** Solicito a S.S., tener por acreditada mi personería para actuar en representación de Banco Santander Chile, teniendo por acompañado con citación, copia de la escritura pública de Mandato Judicial otorgado en Trigésimo Séptima Notaría Pública de Santiago, de fecha 02 de diciembre de 2022, el que cuenta con firma electrónica avanzada y vigencia.

**SEGUNDO OTROSÍ:** De conformidad a lo establecido por el artículo 18 de la Ley N° 18.287, que establece procedimiento ante los Juzgados de Policía Local, solicito a S.S. que las notificaciones de resoluciones dictadas en estos autos, sean enviadas por correo electrónico a la siguiente casilla; [notificacionsantander@o-a.cl](mailto:notificacionsantander@o-a.cl).

**TERCER OTROSÍ:** Que, en este acto delego poder en don **Paulo Cesar Ordenes Williams**, habilitado en derecho, cédula nacional de identidad 16.349.892-8, con domicilio en Bolívar N° 354, oficina 301, edificio Humberstone, Iquique, para que actúe en forma conjunta, separada o indistintamente con las mismas facultades.

**Manuel José Searle Risopatrón**  
Firmado digitalmente por Manuel José Searle Risopatrón  
Fecha: 2023.09.27 18:44:14 -03'00'



16.349.892-8



**Notario de Santiago Nancy de la Fuente Hernandez**

Certifico que el presente documento electrónico es copia fiel e íntegra de MANDATO JUDICIAL otorgado el 10 de Junio de 2022 reproducido en las siguientes páginas.

Notario de Santiago Nancy de la Fuente Hernandez.-

Huerfanos 1117 of. 1014.-

Repertorio Nro: 1835 - 2022.-

Santiago, 10 de Junio de 2022.-



*Nancy de la Fuente Hernandez*

123456831125  
www.fojas.cl

Emito el presente documento con firma electrónica avanzada (ley No19.799, de 2002), conforme al procedimiento establecido por Auto Acordado de 13/10/2006 de la Excm. Corte Suprema.-

Certificado Nro 123456831125.- Verifique validez en

<http://fojas.cl/d.php?cod=not71ndlfueh&ndoc=123456831125.-> .-

CUR Nro: F4754-123456831125.-

Monsieur Herr

413



Notaría  
NANCY DE LA FUENTE

1 REPERTORIO N° 1.835-2022

OT 7279.0622

2  
3  
4  
5  
6 **MANDATO JUDICIAL**

7 \*\*\*\*\*

8 **BANCO SANTANDER-CHILE**

9 **-A-**

10  
11 **SEARLE RISOPATRÓN, MANUEL JOSÉ Y OTRA**

12  
13  
14  
15 EN SANTIAGO DE CHILE, a diez de junio de dos mil  
16 veintidós, ante mí, **NANCY DE LA FUENTE HERNANDEZ**,  
17 abogada, Titular de la Trigésimo Séptima Notaria Pública  
18 de Santiago, con oficio en Huérfanos número mil ciento  
19 diecisiete, Oficina número mil catorce, comuna de  
20 Santiago; comparece: don **EUGENIO ANDRÉS LABARCA**  
21 **BIRKE**, chileno, casado, abogado, cédula de identidad  
22 número ocho millones quinientos cuarenta y ocho mil  
23 setecientos cuarenta y tres guion cuatro, en  
24 representación del **BANCO SANTANDER-CHILE**, sociedad  
25 del giro de su denominación, Rol único Tributario número  
26 noventa y siete millones treinta y seis mil guion K, ambos  
27 domiciliados en calle Bandera número ciento cuarenta,  
28 piso décimo tercero, de la comuna y ciudad de Santiago,  
29 Región Metropolitana, en adelante denominado el  
30 "Mandante"; el compareciente, mayor de edad, quien

215



icado N°  
16831125  
que validez en  
/www.fojas.cl

1 acredita su identidad con la cédula antes mencionada y  
2 expone: Que debidamente facultado según se acreditará,  
3 viene en otorgar mandato judicial a los abogados don  
4 **MANUEL JOSÉ SEARLE RISOPATRÓN**, cédula de  
5 identidad número trece millones veintisiete mil  
6 novecientos ochenta y ocho guión cero y doña **NATHALY**  
7 **DIANE PÉREZ LAGUNAS** cédula de identidad número  
8 dieciséis millones seiscientos sesenta y tres mil  
9 setecientos once guión dos en adelante también  
10 indistintamente "los mandatarios", para que individual,  
11 separada e indistintamente, interpongan antes los  
12 Juzgados de Policía Local, en representación de Banco  
13 Santander Chile, las acciones y/o demandas relacionadas  
14 a las Ley veinte mil nueve y sus modificaciones y  
15 representante a Banco Santander Chile en todas las  
16 etapas de los procesos judiciales que dichas acciones y/o  
17 demandas originen. Los mandatarios tendrán todas las  
18 facultades del inciso primero del artículo séptimo del  
19 Código de Procedimiento Civil, quedando expresamente  
20 facultados para delegar todo o parte del poder en otro  
21 abogado o habilitado de derecho, pudiendo reasumirlo las  
22 veces que estime conveniente. **PERSONERÍA**: La  
23 personería de don Eugenio Labarca Birke para actuar en  
24 representación de **Banco Santander-Chile**, consta en  
25 escritura pública de fecha doce de mayo de dos mil  
26 veintiuno otorgada ante ésta misma Notaría, la que no se  
27 inserta por ser conocida del compareciente y del Notario  
28 que autoriza.- La presente escritura ha sido extendida,  
29 conforme a la minuta redactada por la Abogada doña  
30 Maria Olga Hernández Vallejos.- En comprobante y previa

3/5



Certificado  
1234568311:  
Verifique va  
http://www.f



*Monica Luna*

415



Notaria  
NANCY DE LA FUENTE

1 lectura firma.-Se da copia.-Doy fe.-REPERTORIO N° 1-835-22

2 C.P.

3

4

5

6

EUGENIO ANDRÉS LABARCA B

8548743-4

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

4/5



icado  
6831125  
que validez en  
/www.fojas.cl

1  
C/FEA  
229.0622

25

26

27

28

29

30

Causa rol 17.367-L

En Iquique, a veinte días del mes de octubre del año dos mil veintitrés

A lo principal: téngase presente.

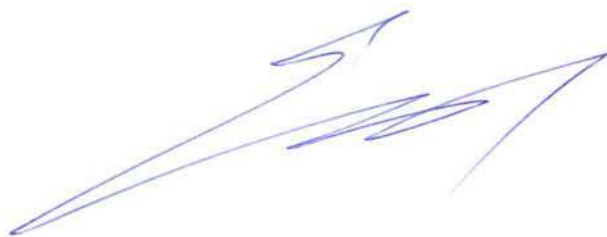
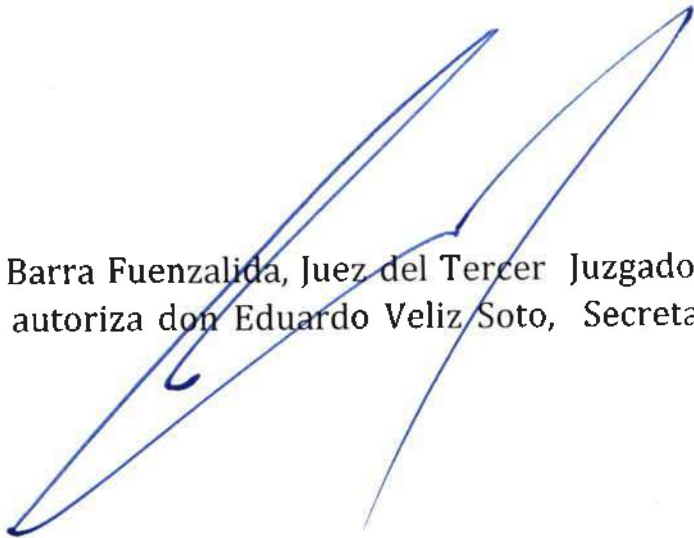
Al primer otrosí: téngase por acompañado documento con citación.

Al segundo otrosí: como se pide, notifíquese las resoluciones que se libre en estos autos al correo electrónico informado por la parte solicitante.

Al tercer otrosí: venga en forma.

Notifíquese.

Proveyó son Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de Policía Local de Iquique, autoriza don Eduardo Veliz Soto, Secretario subrogante.



Iquique, a veintiséis días del mes de octubre del año dos mil veintitrés.

Vistos:

A fojas 1, rola denuncia infraccional y demanda civil de indemnización de perjuicios, interpuesta por doña **Verónica Andrea Ramírez Riquelme**, chilena, Ingeniera en Construcción, cédula nacional de identidad y rol único tributario N° 12.858.024-7, domiciliada en Iquique, calle Patricio Lynch N° 91, departamento 1404, en contra del **Banco Santander Chile**, persona jurídica de derecho privado, Rol Único Tributario N° 97.036.000-K, representado por **Miguel Mata Huerta**, chileno, empleado, cédula nacional de identidad y rol único nacional N° 9.496.096-7, ambos domiciliados en la Comuna de Santiago, calle Bandera N°140, por infracción a las normas de la Ley 19.496, sobre Protección a los Derechos de los Consumidores, en virtud de los hechos:

Funda su denuncia en el hecho de ser cliente desde hace 14 años del Banco Santander, suscribió contrato respecto de los siguientes productos; Cuenta Corriente N° 61-95389-2; Cuenta Vista por depósito del 10% de AFP; T de Crédito American Express Platinum; Tarjeta de Crédito Visa Gold, por los cuales paga mensualmente un plan. Adicionalmente posee seguros asociados y compra acciones por intermedio del Banco.

Expresa que con fecha 03 de junio del año 2021, recibe un llamado telefónico de una señorita manifestando ser ejecutiva del Banco Santander señalándole que debía entregarle una información de su interés, pero previo a ello debía confirmar su calidad de clienta del Banco, para lo cual le formuló una serie de preguntas personales y de los productos contratados con el banco, no extrañándole las consultas y alto conocimiento que tenía la supuesta ejecutiva de sus antecedentes personales y productos ya que jamás dudó de su calidad de empleada del Banco, por lo que otorgó los antecedentes que se le requerían e incluso informó sus claves secretas y las coordenadas de la Super Clave, cuando así se lo requería; estos últimos antecedentes fueron entregados mediante pulsación de las teclas de su celular personal.

En tanto realizaba las referidas operaciones recepciona un correo electrónico del Banco Santander informando la realización de una transferencia, ante lo cual se percató que estaba siendo engañada por la presunta ejecutiva, procediendo, de inmediato, a dar por terminada la conversación telefónica que mantenía con la supuesta funcionaria bancaria, como también a dar orden de bloqueo de todos sus productos y efectuar cambio de su clave de acceso al portal web del Banco.

Al no poder verificar los movimientos realizados en sus cuentas y tarjetas de créditos, dado al bloqueo realizado, procede a llamar al Centro de Atención Telefónica del Banco Santander para inquirir antecedentes respecto de la orden de bloqueo de sus productos como también los detalles de las transacciones realizadas por los estafadores y efectuar los reclamos de desconocimiento respectiva.

Así se efectuaron los Reclamos N° 28251264 y N° 28251203, cuyas transferencias fueron recuperadas; Reclamo N° 28251083, realizado por tres compras realizadas on line a PC Factory, que alcanzaron la suma total de \$ 1.969.070, cargadas a su cuenta corriente; Se hace notar que número del reclamo fue reemplazado por el N° 28265790, a raíz de lo cual la entidad bancaria efectuó abono nominativo por la suma de \$1.037.874,

con fecha 11 de junio del 2021, reclamo que finalmente fue rechazado por el Banco Santander.

La denunciante, con fecha 7 de junio del 2021, toma conocimiento que, además de las defraudaciones antes señalada, se efectuaron tres compras en cuotas con cargos a su Tarjeta de Crédito American Express por terceros, dos de ellos a PC Factory y uno a SuperRepuestos SpA, que en su conjunto ascendieron a la suma de \$2.055.180, sin tomar en consideración los intereses que se generarían por las compras efectuadas en cuotas, por lo que formuló el Reclamo de desconocimiento N° 28264489.

Además, el día 12 de junio del 2021, la actora se percató que, el mismo día tres de junio del 2021, se habían realizado dos compras con cargo a su tarjeta de crédito VISA, en PC Factory, procediendo de inmediato a efectuar el Reclamo de desconocimiento N°28293413, por la suma de \$1.505.180.

Por los presuntos hechos fraudulentos concurrió a la Policía de Investigaciones de Chile a efectuar la respectiva denuncia, para posteriormente regresar al Banco con la finalidad de hacer entrega del certificado de la denuncia.

Percatándose, la querellante, que el Banco no le daría solución alguna, acudió al Servicio Nacional del Consumidor a efectuar el respectivo reclamo, decidiendo, al mismo tiempo, interponer las respectivas acciones judiciales, ventiladas en estos autos.

De acuerdo a lo expuesto, la actora estima que la Institución Bancaria querellada, no ha dado cumplimiento a las obligaciones que le impone la Ley N° 19.496, en especial a lo dispuesto en su letra d) del inciso primero de artículo 3°, cual es el derecho del consumidor a la seguridad en el servicio, cuyo correlato es la obligación, del prestador del servicio, a otorgar las medidas de seguridad necesarias que permitan proteger los bienes de sus clientes, obligación que se encuentra intrínsecamente relacionada con el deber de profesionalismo, consagrado en el inciso primero del artículo 23°, de la Ley del ramo, por lo que solicita que se tenga por interpuesta querrela infraccional en contra del Banco Santander-Chile, acogerla a tramitación, y en definitiva condenarla al máximo de las multas señaladas en la Ley N° 19.496, con condena en costas.

De igual modo presenta acción de indemnización de perjuicios, basada en los hechos descritos precedentemente, solicitando se condene a la parte demandada, en la suma de \$13.713.610, cantidad que se desglosa de las siguiente forma: por concepto de **A.- Daño Emergente**, a) la suma de \$8.713.610, por detrimento patrimonial sufrido a raíz de los movimientos económicos no reconocidos; y, **B.- Daño Moral**, la cantidad de \$5.000.000, en razón al menoscabo, sufrimiento psicológico padecido por la actora, daño a su imagen comercial al verse expuesta de ser informada a DICOM por el no pago de los montos o a la suma que el Tribunal estime ajustada a derecho, conforme al mérito de autos, más reajustes, intereses y costas. Fundamenta jurídicamente la acción en los artículos 3° letra d), 23, 50 a) y 50 b) de la Ley N° 19.496.

2° Desde fojas 27 a 59, rolan antecedentes que respaldan la acción infraccional interpuesta.

3° A fojas 86, rola declaración extrajudicial del abogado Alberto Sordo Bisbal, efectuada en representación de Banco Santander Chile S.A., ambos domiciliado en calle Coyancura

N° 2283, piso 11, comuna de Providencia, quien expone, en su presentación, que rechazaba todos los hechos y pretensiones de la demanda.

Manifiesta igualmente que la Sra. Ramírez realizó diversos reclamos ante el Banco desconociendo haber otorgado su autorización o consentimiento a las operaciones efectuadas el día 03 de junio del 2021.

Respecto de los SAC N° 28265790, 28293413 y, 28368046 por un monto total de \$4.206.240, se determinó su rechazo, fundado en los antecedentes recabados por el área de fraudes del Banco Santander, por lo que se procedió a efectuar los abonos nominativos de cada reclamo rechazado y a deducir la respectiva acción de responsabilidad contractual señalada en la ley N° 20.009, acción que conoce el Primer Juzgado de Policía Local de Iquique, bajo el Rol N° 4.930-E, fundado en los antecedentes logrado obtener a raíz de la investigación realizada, en que se concluyó que las transacciones, ejecutadas a través de internet, con cargo a Tarjeta de débito y tarjeta de crédito de la demandada, se habían realizado utilizando a) una plataforma segura (WEBPAY PLUS) que exige autenticación del usuario, con claves personales y datos de tarjetas; b) en las operaciones reclamadas, ingresaron correctamente los datos de la "clave secreta" para ingresar al Banco; c) igualmente se ingresaron correctamente los tres números que exige la "tarjeta de coordenadas" denominada también "super clave"; d) se conformó que a la fecha de las operaciones reclamadas, la tarjeta de coordenadas del cliente se encontraba vigente, es decir, no había sido dejada sin efecto o denunciada como sustraída ni nada similar; e) en las compras con tarjeta de crédito, se ingresaron correctamente los datos de seguridad de la tarjeta respectiva, es decir número de tarjeta, fecha de vencimiento y CVV2 = Card Verification Value =; y, f) la actora informó haber entregado claves de coordenadas en forma telefónica a un tercero.

Con lo expuesto, a juicio del banco, la usuaria incurrió en una negligencia grave de la obligación de custodia de sus productos financieros, claves y/o dispositivos de seguridad, permitiendo con ello que terceros realizaren las operaciones que desconoce, pese a que el banco advirtiera, por diversos medios de comunicación, que no solicitará claves en forma telefónica.

Así, continúa manifestando que el Banco ha cumplido con todas y cada una de las obligaciones que le correspondían, respecto a la seguridad de las operaciones de los clientes, por lo que solicita se rechace la querrela infraccional y demanda de indemnización de perjuicios.

4° A fojas 125; y, 362 rola acta de audiencia de contestación, conciliación y prueba realizada con la asistencia de la parte querellante y demandante civil; y, de la parte querellada y demandada civil.

La parte querellante y demandante civil, ratifica sus acciones en todas sus partes, con costas.

La denunciada infraccional y demandada de indemnización de perjuicio contesta por escrito las respectivas acciones, documento que se agrega a fs.140, en el cual, en primer término, niega expresamente todos y cada uno de los hechos esgrimidos por la actora, solicitando que las acciones sean rechazadas en todos sus términos con especial condena en costas. A continuación, solicita se tenga por reproducidos los descargos vertidos en declaración indagatoria.

Igualmente alega la inadmisibilidad de la denuncia presentada en atención a que el libelo carece de fundamento legal, pese a que se ampara en la Ley N° 19.496, no precisa las normas que se habrían infringido como tampoco expresa claramente las infracciones que habría incurrido su representada.

Por otra parte, manifiesta que la actora había efectuado diversos desconocimientos de autorización u otorgado consentimiento a operaciones efectuadas el día 03 de junio del 2021, siendo acogidos los reclamos SAC 28251203 y SAC 28264889, siendo rechazados los reclamos SAC 28265790; SAC 28293413; SAC 28368046, a raíz de los informes evacuados con ocasión de la investigación realizada por el área de fraudes del Banco Santander Chile, procediéndose a enterar los respectivos abono normativo.

El rechazo de los reclamos se basan en los hechos reseñados en la declaración de fojas 86, que se resumen en los siguientes hechos que constituyen negligencia grave de la usuaria: **A)** La Sr. Ramírez, pudiendo no hacerlo, entregó claves y datos de tarjetas de coordenadas en forma telefónica a un tercero; **B)** Las operaciones se realizaron con el ingreso correcto de la clave secreta de la usuaria, la cual se encontraba bajo su custodia; **C)** Las operaciones se ejecutaron con el ingreso correcto de los códigos de su tarjeta de coordenadas, la cual era mantenida bajo su custodia; y, **D)** Las operaciones con tarjeta de crédito requirieron el ingreso de CVV2, que también se encontraba bajo custodia de la actora, por lo que los efectos de un manejo no responsable y con culpa grave de la tarjeta de crédito y claves no puede ser imputable al Banco sino únicamente a su tenedora.

Lo anterior no solo fluye del resultado de la investigación realizada por la entidad financiera sino también de la propia relación de los hechos expuesta en la en su demanda al reconocer haber efectuado la entrega de las claves en forma libre y voluntariamente.

Por todo lo expuesto solicita el rechazo de las acciones interpuestas en su contra con expresa condena en costas y, si por el contrario se estimare la existencia de alguna infracción a la ley sobre protección de los derechos a los consumidores, se le condene al mínimo de la multa establecida para dichos efectos por haberse la actora expuesto impudente al riesgo.

El Tribunal llama a las partes a conciliación, no se produce.

El tribunal recibe la causa a prueba y fija los hechos substanciales, pertinentes y controvertidos.

La actora presenta a doña Ina María Choque Castillo, chilena, casada, técnica, cédula nacional de identidad y rol único nacional N° 8.150.782-1, domiciliada en Iquique, Población Quebrada Blanca, Malaquita N° 4238; Laura Inés Martínez Fumey, chilena, casada, trabajadora social, cédula nacional de identidad y rol único nacional N° 15.008.435-0, domiciliada en Iquique, Playa Blanca N° 2535, casa 5

Las partes rinden prueba documental.

La querellada y demandada acompaña prueba electrónica

5° A fojas 373 y 375, rola acta levantada respecto de la percepción de la prueba electrónica, realizada con la comparecencia de ambas partes.

6° A fojas 407, rola decreto que cita a las partes oír sentencia.

**Considerando**

**A.- En cuanto a la acción infraccional**

**Primero:** La actora funda su denuncia en el hecho de haber recibido el día 3 de junio del año 2021, un llamado telefónico de una señorita manifestando ser ejecutiva del Banco Santander señalándole que debía entregarle una información de su interés, pero previo a ello debía confirmar su calidad de cliente del Banco, para lo cual le formuló una serie de preguntas personales y de los productos contratados con el banco, no extrañándole las consultas y alto conocimiento que tenía, la supuesta ejecutiva, de sus antecedentes personales y productos, por lo que no dudó de su calidad de empleada del Banco, por lo que otorgó los antecedentes que se le requerían e incluso informó sus claves secretas y las coordenadas de la Super Clave, cuando así se lo requería; estos últimos antecedentes fueron entregados mediante pulsación de las teclas de su celular personal, conducta que motivó que le sustrajeran, entre varias operaciones, la suma de \$ 8.713.610.

**Segundo:** La actora al percatarse de haber sido víctima de fraude procedió a efectuar los Reclamos SAC N° 28251264 y SAC N° 28251203, cuyas transferencias fueron recuperadas; y, los SAC Reclamo N° 28251083, realizado por tres compras realizadas on line a PC Factory, que alcanzaron la suma total de \$ 1.969.070, cargadas a su cuenta corriente; Se hace notar que el número del reclamo precedente fue reemplazado por el SAC N° 28265790, a raíz de lo cual la entidad bancaria efectuó abono nominativo por la suma de \$1.037.874, con fecha 11 de junio del 2021, reclamo que finalmente fue rechazado por el Banco Santander.

La denunciante, con fecha 7 de junio del 2021, toma conocimiento que, además de las defraudaciones antes señalada, se efectuaron tres compras en cuotas con cargos a su Tarjeta de Crédito American Express por terceros, dos de ellos a PC Factory y uno a SuperRepuestos SpA, que en su conjunto ascendieron a la suma de \$2.055.180, sin tomar en consideración los intereses que se generarían por las compras efectuadas en cuotas, por lo que formuló el Reclamo de desconocimiento N° 28264489.

Igualmente, el día 12 de junio del 2021, la denunciante se percató que, el mismo día tres de junio del 2021, se habían realizado dos compras con cargo a su tarjeta de crédito VISA, en PC Factory, procediendo de inmediato a efectuar el Reclamo de desconocimiento SAC N°28293413, por la suma de \$1.505.180.

**Tercero:** Por su parte el Banco Santander Chile, a través del abogado Alberto Sordo Bisbal, en su declaración de fojas 86, y contestación de la denuncia y demandad de indemnización de perjuicios, manifiesta que la Sra. Ramírez efectuó diversos reclamos ante el Banco desconociendo haber otorgado su autorización o consentimiento a las operaciones efectuadas el días 03 de junio del 2021.

De los reclamos formulados se rechazaron aquellos signados bajo los números SAC N° 28265790, 28293413 y, 28368046 por un monto total de \$4.206.240, fundado en los antecedentes recabados por el área de fraudes del Banco Santander, procediéndose a efectuar los abonos nominativos respectivos de cada reclamo rechazado y a deducir la correspondiente acción de responsabilidad contractual señalada en la ley N° 20.009, acción que tuvo su fundamento en los antecedentes logrados obtener a raíz de la

investigación realizada, en que se concluyó que las transacciones, ejecutadas a través de internet, con cargo a Tarjeta de débito y tarjeta de crédito de la demandada, se habían realizado utilizando a) una plataforma segura (WEBPAY PLUS) que exige autenticación del usuario, con claves personales y datos de tarjetas; b) en las operaciones reclamadas, ingresaron correctamente los datos de la "clave secreta" para ingresar al Banco; c) igualmente se ingresaron correctamente los tres números que exige la "tarjeta de coordenadas" denominada también "super clave"; d) se conformó que a la fecha de las operaciones reclamadas, la tarjeta de coordenadas del cliente se encontraba vigente, es decir, no había sido dejada sin efecto o denunciada como sustraída ni nada similar; e) en las compras con tarjeta de crédito, se ingresaron correctamente los datos de seguridad de la tarjeta respectiva, es decir número de tarjeta, fecha de vencimiento y CVV2; y, f) la actora informa haber entregado claves de coordenadas en forma telefónica a un tercero y que se ventila ante el Primer Juzgado de Policía Local de Iquique, bajo el Rol N° 4.930-E.

**Cuarto:** Consta en autos, tanto en la exposición de los hechos de la acción infraccional, fojas 5; relación de hechos formulado por doña Verónica Andrea Ramírez Riquelme al Banco Santander Chile, fojas 101 y siguientes, no objetada; y acta levantada, con ocasión de la percepción de la prueba documental, no objetada, acompañada por la denunciada, cuya acta se agregó a fojas 372 y 375, que doña Verónica Andrea Aguirre Ramírez Riquelme reconoce haber tecleado en su teléfono celular las claves de cada uno de sus productos, la cual era el año de su nacimiento, y las coordenadas de la Súper Clave que ella le fuera dictando, importando todo ello un reconocimiento extrajudicial de su conducta descuidada en relación al manejo de sus claves secretas.

**Quinto:** Con lo expuesto, a juicio del banco, la usuaria incurrió en una negligencia grave de la obligación de custodia de sus productos financieros, claves y/o dispositivos de seguridad, permitiendo con ello que terceros realizaren las operaciones que desconoce, pese a que el banco advirtiera, por diversos medios de comunicación, que no solicitará claves en forma telefónica, todo ello conlleva a deducir que el actuar de la actora es absolutamente negligente, dado a que se trata de una persona profesional y por ende con un coeficiente intelectual, a lo menos normal, y culta, por lo que debe saber o a lo menos deducir el significado del término "Secreto".

**Sexto:** Con lo relacionado, esta magistratura y analizados los medios probatorios agregados a estos autos y en lo fundamental el reconocimiento de haber entregado su clave secreta como también las coordenadas solicitadas, todos los que analizados en su conjunto y de acuerdo a las reglas de la sana crítica, esta sentenciador ha adquirido plena convicción, que la operaciones impugnadas fueron efectuadas con absoluto conocimiento de la actora, en atención a que las claves fueron entregadas personalmente, por lo que, se debe concluir que la denunciante actuó con culpa grave y sin ninguna prudencia al no resguardar sus datos y antecedentes adecuadamente, pese a las constantes advertencias, tanto generales como en particular, efectuadas por la denunciada.

**Séptimo:** De lo expuesto, se observa que la denunciada dio pleno cumplimiento a las normas sobre seguridad exigidas en la Ley N° 19.496, al haber actuado en forma diligente en la prestación del servicio ofrecido al actor, por el contrario, la actuación descuidada e imprudente de la actora fue la causa basal del menoscabo patrimonial por ella sufrido.

**Octavo:** Por todo lo expuesto, esta magistratura deberá rechazar la denuncia infraccional que dan motivo a estos autos.



**B.- EN CUANTO A LA ACCIÓN CIVIL DE INDEMNIZACION DE PERJUICIOS**

**Noveno:** Al no haber incurrido la querellada de autos en infracción alguna a la ley N° 19.496, acorde a lo expuesto anteriormente, esta magistratura deberá rechazar la acción de indemnización de perjuicio en contra del Banco Santander Chile.

Y Visto, lo dispuesto en los demás artículos de la Ley 19.496, Ley N° 15.231, sobre Organización y Atribuciones de los Juzgados de Policía Local y Ley 18.287 sobre Procedimiento y sus posteriores modificaciones introducidas por la y Ley N° 19.816.

**Declaro:**

**1.- EN CUANTO A LA ACCIÓN INFRACCIONAL**

Absuélvase al **Banco Santander Chile**, persona jurídica de derecho privado, Rol Único Tributario N° 97.036.000-K, representado por **Miguel Mata Huerta**, chileno, empleado, cédula nacional de identidad y rol único nacional N° 9.496.096-7, ambos domiciliados en la Comuna de Santiago, calle Bandera N°140, de la denuncia por infracción a las normas de la Ley 19.496, sobre Protección a los Derechos de los Consumidores, presentada por doña **Verónica Andrea Ramírez Riquelme**, chilena, Ingeniera en Construcción, cédula nacional de identidad y rol único tributario N° 12.858.024-7, domiciliada en Iquique, calle Patricio Lynch N° 91, departamento 1404, por los razonamientos escritos en los considerandos precedentes.

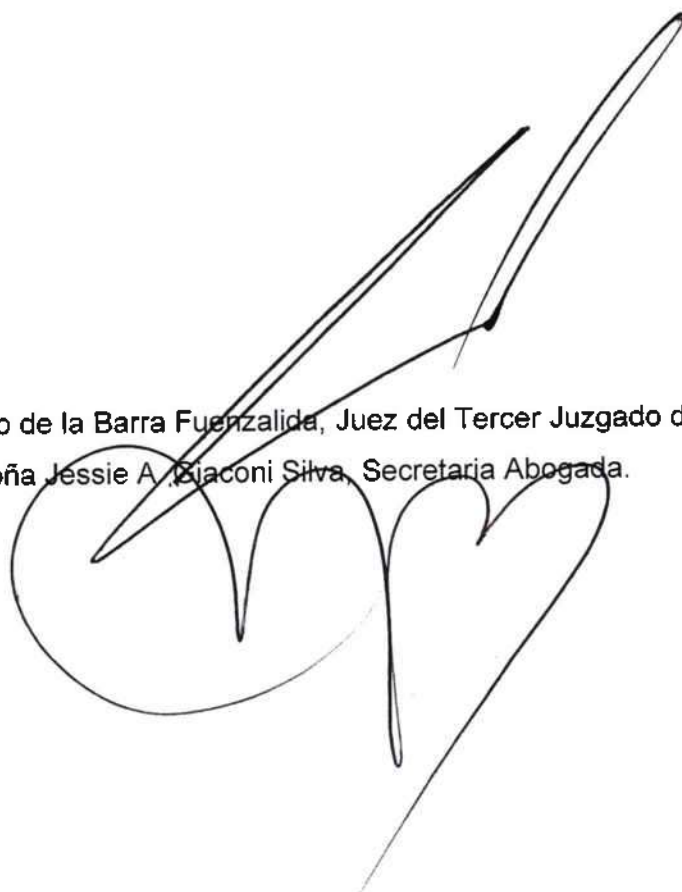
**2.- EN CUANTO A LA ACCIÓN CIVIL DE INDEMNIZACION DE PERJUICIOS**

Rechácese la demandad de indemnización de perjuicios presentada por **Verónica Andrea Ramírez Riquelme**, en contra del **Banco Santander Chile S.A.**, representado por **Miguel Mata Huerta**, todos ya individualizados.

**3.-** No se condena a la denunciante y demandante de indemnización de perjuicios al pago de las costas de autos por haber tenido motivo plausible para litigar.

**4.-** Encontrándose a firme la presente sentencia, remítase copia de esta, debidamente autenticada, al Servicio Nacional del Consumidor, Región Tarapacá  
Notifíquese, regístrese y archívese en su oportunidad.

Dictada por don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de Policía Local de Iquique. Autoriza doña Jessie A. Bjaconi Silva, Secretaria Abogada.



cuarenta y siete

421

TERCER JUZGADO DE POLICIA LOCAL

José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

IQUIQUE,

27 NOV. 2023

CERTIFICO: Que, con esta fecha y siendo las 09 : 40 hrs. he procedido a notificar a don (ña) MANUEL J. SEARLE RISOPATRON de la sentencia de autos remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico [notificacionsantander@o-a.cl](mailto:notificacionsantander@o-a.cl). Doy fe.

JUAN A. SAAVEDRA FERRADA  
Receptor



procurador Ferrada

422

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

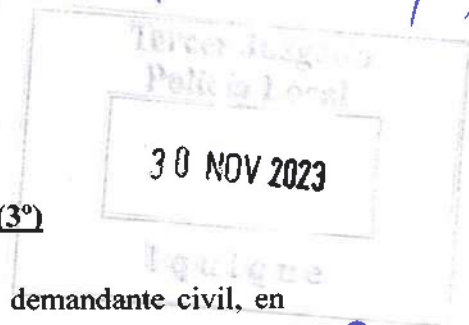
IQUIQUE,

27 NOV. 2023

CERTIFICO: Que, con esta fecha y siendo las 09:40 hrs. he procedido a notificar a don (ña) FELIPE FERNANDEZ LEON de la sentencia de autos remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico ffernandez@fgnabogados.cl. Doy fe.

JUAN A. SAAVEDRA FERRADA  
Receptor



**RECURSO DE APELACIÓN****S. J. DE POLICÍA LOCAL DE IQUIQUE (3°)**

**FELIPE FERNANDEZ LEON**, abogado denunciante y demandante civil, en causa rol N° 17367-L-2021, seguida ante este tribunal por ley del consumidor, a US. respetuosamente digo:

Cley

Que por medio de este acto, y en virtud de los artículos 32 y siguientes de la ley 18.287, vengo en interponer recurso de apelación en contra de la sentencia fechada 26 de octubre de 2023, notificada a esta parte con fecha 27 de noviembre de 2023, para que esta sea revocada por la Ilustrísima Corte de Apelaciones de Iquique, por los argumentos de hecho y derecho que paso a exponer:

**CONTEXTO:**

Doña Verónica Ramírez fue demandada por el Banco Santander Chile en base a la ley 20.009, y a la vez denunció y demandó al Banco Santander Chile por infracción a la ley 19.496 de protección a los derechos del consumidor, debido a que mi representada sufrió una defraudación en sus productos bancarios contratados con Banco Santander Chile, la cual se describe de la siguiente forma:

Con fecha 03 de junio del año 2021, mi representada recibió una llamada de una señorita que se identificó como ejecutiva del Banco Santander y que requirió entregarle información. **Primero le dijo que debía corroborar que ella fuera la cliente del Banco, pues la información era personal y ella (la supuesta ejecutiva) procedió a detallar la siguiente información de doña Verónica: Su nombre completo (dos nombres y dos apellidos); el número de mi cuenta corriente; el número de mi cuenta vista; las características y números iniciales y finales de sus tarjetas de crédito Visa y American Express; le detalló que tenía dos seguros tomados por medio del Banco Santander e incluso le dijo el número completo (siete dígitos) de su tarjeta Súper Clave.** Esta señorita conocía exactamente todos los datos registrados en el Banco, por ende, doña Verónica confió que estaba hablando con una ejecutiva del Call Center del Banco Santander.

Cabe hacer presente que nadie más que doña Verónica, y por supuesto, el banco Santander, tiene esta información y ella no se la ha entregado a nadie. El discurso de la señorita era que, por motivos de seguridad y por el cambio de la ley respecto de la responsabilidad de los bancos sobre los fraudes que afecten a sus clientes, iban a cambiar todos los plásticos por unos modernos, con GPS y que, además, le depositarían en mi cuenta los intereses pagados por los seguros que hubiera tenido contratados hasta la fecha del cambio de la ley. Incluso, le explicó la ley y pidió disculpas por la tardanza en la devolución de los intereses de los cobros por seguros. Como doña Verónica contaba con seguros contratados, **y la persona que la llamó sabía de estos seguros,**

sumado a lo anterior el hecho de que solo el banco tiene esta información, le hizo sentido lo que se le indicaba.

Luego, le indicó que, para proceder con el cambio de plásticos y la devolución de intereses, los cuales serían depositados en su cuenta y tarjetas respectivamente, debían realizar uno a uno los requerimientos por cada plástico que doña Verónica tuviera, **así que ella comenzó nuevamente a detallarle los productos que poseía, con sus números, y por cada uno de ellos, en el momento que ella le indicaba, doña Verónica debía teclear en su celular las coordenadas de la Súper Clave que ella le fuera dictando. Debo aclarar que en ningún momento doña Verónica le dijo a viva voz ni claves secretas ni coordenadas de la tarjeta Súper Clave. Cuando ella le pedía una coordenada, doña Verónica debía teclearla en su celular (tal cual cuando uno llama al Call Center y debe ingresar coordenadas, sin decirlas, solo tecleándolas en el celular) y eso hizo. Esto fue realizado en su celular personal y sin decirlas en voz alta, donde doña Verónica tecleó las coordenadas, supuestamente para autorizar el cambio de plásticos y la autorización de reembolso de intereses.**

Hasta ese momento doña Verónica no sospechaba absolutamente nada, ni que podría ser un engaño y menos que terceros estuvieran usando sus documentos. Hasta que de pronto, en el mismo celular del que estaba hablando, donde ella tiene la aplicación de su correo electrónico Gmail, llega un mail del Banco Santander por una transferencia, y en ese momento recién doña Verónica se dio cuenta que eso no era normal y entendió que era una estafa, por lo que cortó la llamada inmediatamente. Trató de entrar a la página web del Banco para ingresar a su cuenta, pero no fue posible porque no reconocía su clave, por ende, no pudo entrar a ver sus productos y sólo pudo llamar por celular al call center del Banco y esperar a que la atendieran. Cuando la atendieron doña Verónica les dijo rápidamente que estaba siendo estafada, que bloquearan todos sus productos y les avisó que habían cambiado su clave del portal web del Banco y que ella no tenía ningún acceso. Luego la llamada se cortó y ni siquiera pudo anotar el nombre de la persona que la atendió.

Como ella no tenía acceso a sus productos bancarios bloqueados, toda la información respecto a los movimientos que realizaron los estafadores iba siendo proporcionada por el call center del Banco, dándole información incompleta cada vez que llamaba, ya que en cada llamado aparecían más cobros no reconocidos, provocándole aun más daño psicológico, como se puede ver de los audios de las llamadas que fueron acompañadas y de las declaraciones de las testigos acompañadas por esta parte.

Detallo a continuación cada uno de los movimientos no reconocidos, reclamos efectuados y las respuestas entregadas por el Banco hasta la fecha, algunas realizando el abono normativo, aceptando el reclamo, y en otras no. En gris están marcadas las transacciones que el Banco ha determinado que acoge el reclamo y ha devuelto el dinero estafado, y están marcadas en amarillo aquellas que el Banco no acoge el reclamo e

indica que cursará acciones para la devolución de los montos depositados provisoriamente:

Transacciones realizadas el 03.06.2021 Hora	monto	Origen del dinero defraudado	Movimiento	n° Ingreso reclamo	Resolución del Banco
13:25	\$ 886.590	Cuenta Corriente	Compra en PC Factory	28251083	El banco internamente cambia el n° de reclamo al n° 28265790 sin avisar al cliente. Con fecha 29.06.2021 el Banco indica que, de acuerdo a su análisis de antecedentes rechaza el reclamo. Cliente reitera el reclamo con n° 28367929
13:29	\$ 896.890		Compra en PC Factory		
13:32	\$ 185.590		Compra en PC Factory		
13:33	\$ 200.000	Cuenta Corriente	SuperGiro	28251203	10.06.2021 el Banco indica que, de acuerdo a análisis de antecedentes acepta el reclamo y realiza abono a cuenta corriente
13:36	\$ 250.000		Transferencia a Cuenta Vista Banco Estado N° 9058567, del Rut 9.058.567-3 a nombre de Marcelino, correo_as@gmail.com		
13:34	\$ 2.734.180	Cuenta Vista	Transacción interna desde Cta Vista hacia Tarjeta de Crédito	28251264	Se realiza reversa y ladrones no alcanzan a utilizar el dinero. Dinero recuperado

13:22	\$ 1.010.290	T.C. Visa	Compra en PC Factory	28293413	29.06.2021 el Banco indica que, de acuerdo a su análisis de antecedentes rechaza el reclamo. Cliente reitera el reclamo bajo el n° 28380096 con fecha 02.07.2021
13:27	\$ 494.890		Compra en PC Factory		
13:06	\$ 773.190	T.C. American Express	Compra en PC Factory	28264489	16.06.2021 el Banco indica que, de acuerdo a análisis de antecedentes acepta el reclamo y realiza abono a cuenta corriente
13:24	\$ 731.990	T.C. American Express	Compra en PC Factory	28264489	El Banco elimina del reclamo n° 28264489 este monto, sin aviso ni consulta a la cliente. Cliente vuelve a generar un nuevo reclamo n° 28368046 por este monto
13:29	\$ 550.000	T.C. American Express	Compra en Súper Repuestos SpA	28264489	16.06.2021 el Banco indica que, de acuerdo a análisis de antecedentes acepta el reclamo y realiza abono a cuenta corriente

Como se puede ver, todas las transacciones se realizaron bajo la misma metodología, en una sola llamada telefónica y ocurrieron entre las 13:06 y las 13:36 hrs. del 3 de junio de 2021. Sin embargo, para el análisis del Banco, para algunas transacciones aplica la devolución del dinero y para otras no.

Debido a lo que ha sucedido, doña Verónica estuvo con licencia médica por estrés desde el lunes 7 de junio hasta el jueves 05 de agosto de 2021. Para ella ha sido horroroso todo esto ya que a pesar de contar con una serie de productos contratados, ser clienta de años del banco, incluso comprando acciones a través de esta institución, pagando todo al día religiosamente, Santander ha optado por desconocer sus obligaciones para con ella, en el sentido de no hacerse cargo de una falla en la seguridad de reserva de la información que manejan, ya que, como ya mencioné, **la única forma en la que la estafadora haya podido tener acceso a toda la información bancaria de doña Verónica, es precisamente a través del Banco Santander. Tampoco operó algún mecanismo de seguridad al detectar operaciones sospechosas que se realizaban rápidamente por altos montos, ni se solicitó la autorización vía clave 3.0, clave que llega directamente al celular vía mensaje de texto.**

Hasta el día 02 de junio de 2021, doña Verónica tenía depositado en su cuenta corriente la suma de \$4.043.696, en su cuenta Vista la suma de \$3.623.853, no usaba su línea de crédito hace muchísimo tiempo, en su tarjeta Visa sólo tenía cargado Netflix y en su tarjeta American Express estaba la compra de anteojos en una Óptica en Vitacura.

Aclaro finalmente que doña Verónica nunca perdió ninguna tarjeta de crédito, débito o Súper Clave y aún tiene en su poder las que fueron bloqueadas por la estafa; que nadie tiene acceso a su computador personal y que éste es el único lugar desde donde ella realiza transacciones bancarias; que doña Verónica no ha perdido ni prestado su celular y que tampoco utiliza la aplicación móvil del Banco. Tampoco ha viajado al extranjero.

Esta parte presentó prueba para acreditar todo lo anteriormente narrado, alegando que todo ocurrió por faltas de seguridad en la prestación del servicio por parte del Banco.

El Banco por su lado demandó a mi representada por dolo o culpa grave en la ocurrencia de este fraude para recuperar los abonos normativos depositados, al según ellos realizarse la transacción mediante todas las medidas de seguridad que mantiene la institución, mismo argumentos que virtió en este proceso, pero no pudo refutar que mi representada lo único que hizo fue digitar teclas en su propio teléfono, sin aportar más a gatillar estas transacciones no reconocidas, y que lo hizo ya que la estafadora le dijo información que solo empleados del Banco tienen.

En base a estas alegaciones, el 3° Juzgado de Policía Local de Iquique decidió rechazar la denuncia infraccional y demanda civil interpuesta por esta parte en contra de Banco Santander Chile por infracción a la ley 19.496 de protección a los derechos del consumidor, debido a que:

Cuarto: Consta en autos, tanto en la exposición de los hechos de la acción infraccional, fojas 5; relación de hechos formulado por doña Verónica Andrea Ramírez Riquelme al Banco Santander Chile, fojas 101 y siguientes, no objetada; y acta levantada, con ocasión de la percepción de la prueba documental, no objetada, acompañada por la denunciada, cuya acta se agregó a fojas 372 y 375, que doña Verónica Andrea Aguirre Ramírez Riquelme **reconoce haber tecleado en su teléfono celular las claves de cada uno de sus productos, la cual era el año de su nacimiento, y las coordenadas de la súper clave que ella le fuera dictando, importando todo ello un reconocimiento extrajudicial de su conducta descuidada en relación al manejo de sus claves secretas.**

Quinto: Con lo expuesto, a juicio del banco, la usuaria incurrió en una negligencia grave de la obligación de custodia de sus productos financieros, claves y/o dispositivos de seguridad, permitiendo con ello que terceros realizaren las operaciones que desconoce, **pese a que el banco advirtiera, por diversos medios de comunicación, que no solicitará claves en forma telefónica, todo ello conlleva a deducir que el actuar de la actora es absolutamente negligente, dado a que se trata de una persona profesional y por ende con un coeficiente intelectual, a lo menos normal, y culta, por lo que debe saber o a lo menos deducir el significado del término "Secreto".**

Sexto: Con lo relacionado, esta magistratura y analizados los medios probatorios agregados a estos autos y **en lo fundamental el reconocimiento de haber entregado su clave secreta como también las coordenadas solicitadas**, todos los que analizados en su conjunto y de acuerdo a las reglas de la sana crítica, esta sentenciador ha adquirido plena convicción, que las operaciones impugnadas **fueron efectuadas con absoluto conocimiento de la actora, en atención a que las claves fueron entregadas personalmente, por lo que, se debe concluir que la denunciante actuó con culpa grave y sin ninguna prudencia al no resguardar sus datos y antecedentes adecuadamente, pese a las constantes advertencias, tanto generales como en particular, efectuadas por la denunciada.**

Séptimo: De lo expuesto, se observa que **la denunciada dio pleno cumplimiento a las normas sobre seguridad exigidas en la Ley N°19.496, al haber actuado en forma diligente en la prestación del servicio ofrecido al actor**, por el contrario, la actuación descuidada e imprudente de la actora fue la causa basal del menoscabo patrimonial por ella sufrido. octavo: Por todo lo expuesto, esta magistratura deberá rechazar la denuncia infraccional que dan motivo a estos autos.

### **ARGUMENTOS PARA REVOCAR**

Como se puede ver, el 3° Juzgado de Policía Local de Iquique estableció que solo por el hecho de que mi representada tecleó los números que la persona que se hacía pasar por ejecutiva del Banco Santander le indicaba, se puede entender que actuó por



culpa grave, y que el Banco cumplió con el estándar de seguridad en sus productos bancarios.

Y en ese punto es clave establecer que mi representada ha mantenido su versión desde el principio respecto a solo teclear los números que la persona que se hacía pasar por ejecutiva del Banco Santander que contaba con toda su información le indicaba de su tarjeta de coordenadas, desde su primer llamado el día de los hechos (cuyo audio consta en autos), correos al banco, denuncia en fiscalía, en su declaración indagatoria, en su relato de los hechos en la presente causa, e indirectamente a través de testigos. No su clave de acceso al portal de internet, o clave de 4 dígitos. Y, como se explicó, el banco no probó que mi representada haya aportado a los defraudadores su clave de acceso al portal de internet, o clave de 4 dígitos, sino que indican que los movimientos realizados pasaron por todos sus obstáculos de seguridad.

Y teniendo lo anterior en consideración, es claro que la institución bancaria es la que debe probar su deber de cuidado, y que las operaciones fueron realmente autorizadas por el usuario, y en este sentido el artículo 4 de la ley 20.009 establece que *"El solo registro de las operaciones no bastará, necesariamente, para demostrar que esta fue autorizada por el usuario, ni que el usuario actuó con culpa o descuido que le sean imputables, sin perjuicio de la acción contra el autor del delito."*

Por otro lado, la sentencia indica que *"que las operaciones impugnadas fueron efectuadas con absoluto conocimiento de la actora, en atención a que las claves fueron entregadas personalmente,"*. Esto es un error, ya que en primer lugar no se puede decir que una operación bancaria se realizó con absoluto conocimiento cuando la usuaria ni siquiera sabía que estaba haciendo una operación bancaria como la que efectivamente se realizó. De lo que ella tenía absoluto conocimiento, era de que estaba renovando sus tarjetas, debido a que alguien con información que solo un funcionario del Banco pudo haber obtenido, se lo informó de esa manera.

A esto se suma el error garrafal del tribunal de primera instancia, al confundir lo dicho por doña Verónica en el audio de la primera llamada al Banco, para denunciar la estafa. Según el tribunal, mi representada reconoce haber tecleado en su teléfono celular **las claves de cada uno de sus productos, la cual era el año de su nacimiento**. Esto no es lo que dijo, ya que del audio aportado por el banco se escucha claramente, en el minuto 4:43: *"Ejecutiva: "lo más probable es que hayan logrado ingresar a la página..su clave de acceso a internet, tenía relación con su rut, fecha de nacimiento, o eran números correlativos? R: era un año, de mi nacimiento"*. Esto el tribunal lo confunde con que mi representada, cada vez que la falsa ejecutiva lo solicitaba, ingresaba en su celular las claves de sus productos, las cuales para todos era su fecha de cumpleaños, siendo que lo que se escucha claramente es que doña Verónica tenía el año de su nacimiento como clave de su portal de internet, y esta clave no se la entregó a nadie. Por lo demás, la clave para ingresar al portal en internet de un banco debería tener más requisitos que permitir claves con 4 dígitos.

Entonces, claramente no podemos tener por probada la culpa de mi representada (y como consecuencia, tampoco se puede tener por probado el deber de cuidado del Banco), por el solo hecho de que el banco presentó registros de que la transacción cumplió con todos los requisitos de seguridad, especialmente cuando tenemos prueba en contrario (la declaración de mi representada sin cambio en el tiempo) para acreditar que esto no fue así.

Luego, el mismo artículo 4 establece que *"En relación con las operaciones no autorizadas incluidas en el reclamo, se considerará especialmente la circunstancia de que el emisor haya enviado una alerta de fraude al usuario, identificando las operaciones sospechosas, y que exista constancia de su recepción por parte del usuario, conforme al contrato de prestación de servicios financieros correspondiente."* Esto, no ocurrió en este caso, y no se presentó prueba alguna de alguna alerta de fraude al usuario, a pesar de que estamos hablando de **11 movimiento totalizando más de ocho millones de pesos**. ¿Si no se va a emitir una alerta de fraude para este tipo de transacciones, entonces cuándo?

Por lo demás, Banco Santander no tiene campañas de prevención de este tipo de estafas, como erróneamente concluye la sentencia de primera instancia, ya que no aportaron ningún antecedente para acreditar que sus campañas están enfocadas en advertirle a sus clientes que existen personas que se hacen pasar por ejecutivos del banco, que pueden incluso tener toda tu información bancaria, y que los pueden estafar. Eso es lo que se necesitaba para prevenir hechos como el que sucedió en autos.

Entonces la pregunta aquí realmente es si la acción de mi representada al teclear los números que la persona que se hacía pasar por ejecutiva del Banco Santander le indicaba, es suficiente para acreditar la culpa de mi representada en el fraude que sufrió, teniendo en cuenta la obligación de banco de prestar un servicio seguro.

Esta parte entiende que claramente, teniendo en cuenta las circunstancias antes mencionadas, no existe culpa grave de mi representada en su actuar, y lo que queda demostrado es la falta de seguridad en los servicios ofrecidos por el Banco de Chile, ya que a nuestro juicio existen graves incumplimientos en este ámbito.

Por un lado tenemos la primera falla en seguridad por parte del Banco, la cual está relacionada con el hecho de que mi representada, una cliente del Banco Santander Chile, fue contactada por estafadores que sabían que ella era cliente del Banco Santander Chile, su nombre completo (dos nombres y dos apellidos), el número de su cuenta corriente, el número de su cuenta vista, las características y números iniciales y finales de sus tarjetas de crédito Visa y American Express; le detalló que tenía dos seguros tomados por medio del Banco Santander e incluso le dijo el número completo (siete dígitos) de su tarjeta Súper Clave, todas piezas de información que solo Banco Santander Chile tiene, por lo que, **o sus bases de información son vulnerables, o algún**

**empleado del mismo Banco está involucrado de alguna forma en estos fraudes.** Esta situación por si sola debiese exculpar cualquier accionar de los usuarios al ser contactados por estafadores que claramente los identifiquen como clientes del Banco en el cual efectivamente tienen productos, y les detalles dichos productos.

Y por el otro lado, tenemos una segunda falla de seguridad relacionada con que con solo apretar ciertos botones correspondientes a coordenadas de la tarjeta superclave en un celular en una llamada se vulnera todo el sistema de seguridad del banco. Esta es una acción que solo debiese tener efecto cuando un funcionario del Banco realice la solicitud. Un estafador no debiese tener acceso a esa tecnología ya que claramente al ingresar solo coordenadas correcta de la super clave de coordenadas se da acceso a los productos bancarios de un usuario vulnerando todos los mecanismos de seguridad del Banco, o el tecleo de las coordenadas permite al estafador tener acceso a los códigos de acceso, pin, y código enviado al teléfono. En ambos casos es clara la falta de seguridad del producto, siendo que el Banco argumenta que en base a estas medidas de seguridad es que la operación es segura. (que como ya se explicó, es todo en lo que se basó el tribunal de primera instancia para determinar la culpa grave de mi representada),

En cuanto a la ley tenemos el artículo 4 ley de la ley 20.009:

*“Tratándose de operaciones anteriores al aviso a que se refiere el artículo 2 de esta ley, el usuario deberá reclamar al emisor aquellas operaciones respecto de las cuales desconoce haber otorgado su autorización o consentimiento, en el plazo de treinta días hábiles siguientes al aviso.*

*El reclamo podrá incluir operaciones realizadas en los ciento veinte días corridos anteriores a la fecha del aviso efectuado por el usuario.*

*En relación con las operaciones no autorizadas incluidas en el reclamo, se considerará especialmente la circunstancia de que el emisor haya enviado una alerta de fraude al usuario, identificando las operaciones sospechosas, y que exista constancia de su recepción por parte del usuario, conforme al contrato de prestación de servicios financieros correspondiente.*

*Tan pronto el usuario tome conocimiento de la existencia de operaciones no autorizadas, deberá dar aviso conforme a lo previsto en el artículo 2 de esta ley.*

*En los casos en que el usuario desconozca haber autorizado una operación, corresponderá al emisor probar que dicha operación fue autorizada por el usuario y que se encuentra registrada a su nombre.*

*El solo registro de las operaciones no bastará, necesariamente, para demostrar que esta fue autorizada por el usuario, ni que el usuario actuó con culpa o descuido que le sean imputables, sin perjuicio de la acción contra el autor del delito.”*

Infracción a la Ley 19.496: El artículo 3° de la referida Ley “son derechos y deberes básicos del consumidor: d) **La seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos que puedan afectarles;**

Por último, el artículo 23 inciso 1° de la Ley N°. 19.496 sobre protección de los Derechos de los consumidores dispone que: "**Comete infracción a las disposiciones de la presente Ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio**".

De todo lo anteriormente narrado, y de las normas citadas, podemos concluir claramente que este fallo debe ser revertido, ya que este no tuvo en consideraciones las graves fallas de seguridad que mantiene el sistema de prevención de fraudes del Banco Santander Chile por las que ocurrió la defraudación, y solo se fijó en el actuar de mi representada, sin tener en cuenta las particularidades de los hechos de la presente causa aparejado con la inacción del Banco.

### **PERJUICIO**

El perjuicio en este caso es claro, y consiste en el hecho de que mi representada, si se mantiene este fallo, deberá devolver dinero al Banco, encima del dinero del que ya fue desposeída debido al fraude, en un juicio en el que claramente ella debe ser la indemnizada, perdiendo a la vez sus derechos a recibir la compensación suficiente, y que se condene al Banco a las multas correspondientes por violación a los derechos del consumidor por todos los hechos anteriormente narrados.

**POR TANTO:** Y de acuerdo con lo dispuesto en los arts. 32 y siguientes de la ley 18.287, normas citadas, y demás pertinentes al caso;

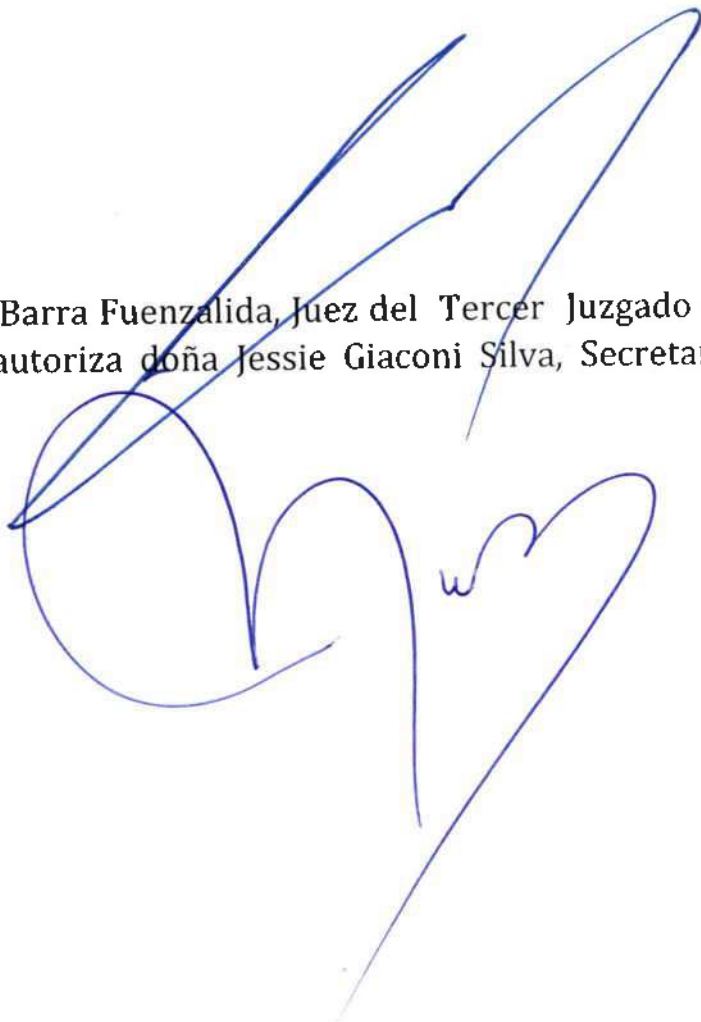
**SOLICITO A S.S:** Tener por interpuesto recurso de apelación en contra de la sentencia definitiva de autos, de fecha 26 de octubre de 2023, notificada a esta parte el 27 de noviembre de 2023, acogerlo a tramitación y ordenar que los autos se eleven a la Ilustrísima Corte de Apelaciones de Iquique, con el objeto de que éste Tribunal, en uso de sus facultades, revoque la sentencia definitiva dictada por S.S., que resolvió rechazar la denuncia infraccional y demanda civil interpuesta por esta parte en contra de Banco Santander Chile por infracción a la ley 19.496 de protección a los derechos del consumidor; y en su lugar, resuelva acoger la denuncia infraccional y demanda civil interpuesta por esta parte en contra de Banco Santander Chile por infracción a la ley 19.496 de protección a los derechos del consumidor, o lo que S.S.I. determine en derecho.



Causa rol 17.367-L

En Iquique, a un día del mes de diciembre del año dos mil veintitrés  
Téngase por interpuesto recurso de apelación. Concédase y elévense los  
autos a la Ilustrísima Corte de Apelaciones, para su conocimiento y  
resolución.  
Notifíquese.

Proveyó don Ricardo de la Barra Fuenzalida, Juez del Tercer Juzgado de  
Policía Local de Iquique, autoriza doña Jessie Giaconi Silva, Secretaria  
Abogado

A large, stylized handwritten signature in blue ink, consisting of several loops and a long horizontal stroke at the bottom.

Quinto de los Andes

433

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

IQUIQUE, 05 / DICIEMBRE / 2023

CERTIFICO: Que, con esta fecha y siendo las 10 : 07 hrs. he procedido a notificar a don (ña) Felipe Fernández Leon de la resolución de fecha 01-12-2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico ffernandez@fpmabopados.cl.

Doy fe.



JUAN A. SAAVEDRA FERRADA  
Receptor

cuatrocientos treinta y cuatro

434

TERCER JUZGADO DE POLICIA LOCAL  
José J. Pérez No. 390 - Iquique

ROL No. 17.367-L

IQUIQUE, 05 / DICIEMBRE / 2.023

CERTIFICO: Que, con esta fecha y siendo las 18:07 hrs. he procedido a notificar a don (ña) Mamuel Jr Sesale Rispatoron de la resolución de fecha 01-12-2023 remitiéndole copia íntegra de esta debidamente autenticada al correo electrónico notificacionesantander@o-a.cl.

Doy fe.

  
JUAN A. SAAVEDRA FERRADA  
Receptor

Iquique, 11 de diciembre de 2023

RESUMEN

ROL 17.367-L  
AÑO 2021  
LIBRO Tercer Juzgado de Policía Local

MATERIA Infracción a la Ley 19.496

NOMBRES DE LAS PARTES Verónica Andrea Ramírez Riquelme con Banco Santander Chile

NOMBRE APELANTE Verónica Andrea Ramírez Riquelme rut 12.858.024-7

NOMBRE APODERADO Felipe Andrés Fernández León rut 16.938.411-8 según representación de fojas 61 y siguientes.

NOMBRE APELADO Banco Santander Chile Rut 97.036.000-K

NOMBRE APODERADO Alberto José Sordo Bisal Rut 16.362.140-K según representación de fojas 92

MOTIVO DE LA APELACION deduce recurso de apelación en contra de la sentencia de fojas 417 a 420, de fecha 26 de octubre de 2023

OBSERVACIONES sobre que contiene pendrive, el que se enviara de forma física.



Secretaria abogado