

## Premios EIKON Chile 2024

<b>Capítulo:</b>	General.
<b>Categoría 19:</b>	Relaciones con los consumidores.
<b>Programa:</b>	Ciberseguridad.
<b>Compañía:</b>	Itaú Chile.
<b>Área/empresa responsable:</b>	Gerencia de Marketing Itaú.
<b>Personas responsables:</b>	Equipo Itaú: Daniel Malavazzi Mariotto, Constanza Vasquez, Pablo Celis. Equipo Loca: Carolina Virgilio, Daniela Campusano, Jaime González, Sebastián Alvarado Equipo Jelly: Andrea Ramirez, Emily Andrade, Manu Chatlani.

### Tuit:

#### Juntos Contra Robos y Fraudes

En un mundo digital en evolución constante y cada vez más acelerada, la ciberdelincuencia se vale de los avances tecnológicos para vulnerar a las personas.

Itaú es el banco más recomendado de Chile por sus clientes, según el estudio Ipsos ServITest Personas 2023, al igual ocurrió en 2022, lo que se refleja en uno de los valores fundamentales de Itaú – su centralidad en los clientes – y en su visión de futuro de ser la empresa de servicios financieros más centrada en el cliente del mundo.

Frente a las amenazas crecientes de los ciberataques no solo a los clientes del banco, sino a todas las personas que están dentro del sistema financiero, Itaú ha tomado la delantera en la lucha contra los ciberataques.

La campaña “Juntos Contra Robos y Fraudes”, lanzada en abril de 2023, fue un éxito rotundo: redujo en 60% los montos defraudados a sus clientes a lo largo de los 12 meses.

Una cruzada iniciada por Itaú para alertar y enseñar a todas las personas, sin hacer diferenciación entre naranjas, azules, rojos o verdes, a protegerse contra los ciber estafadores, contando con videos educativos, presencia activa en redes sociales y correos electrónicos con tips de seguridad.

Una postura que logra juntar la estrategia corporativa de la compañía, educación financiera, visibilidad y frecuencia y, encima de todo, el bienestar y cuidado con los clientes y cada persona.

#### Introducción

Un informe publicado en diciembre de 2023 por la multinacional de ciberseguridad Trellix apuntó que más de la mitad (51,8%) de las ciber estafas de Chile son direccionadas al sector bancario y de servicios financieros.

A eso, se suma que el 70% de las estafas bancarias en el país se realizan a través de canales digitales, según la CMF, que también reporta una pérdida bruta de la banca por fraudes por US \$276,3M, cifra un 105,7% superior a la de 2022.

Esto afecta directamente a Itaú, no solo por los costos que toca asumir por las reposiciones de fondos relacionados a este tipo de fraudes, sino también por los niveles de desconfianza que genera en las personas esta realidad. De esta manera Itaú se puso como meta reducir los costos por reposición en al menos 30%.

Instituciones policiales precisan que el incremento de las estafas financieras a personas se explica, entre otras causas, por el incremento del comercio electrónico por sobre el presencial. Se suma la masificación del uso de smartphones para efectuar pagos en línea y el uso de APPs bancarias, generando nuevos *modus operandi* para los delincuentes.

A lo anterior, se agrega una falta de información y bajo nivel de educación financiera entre la población, como demuestra el informe de la Asociación Nacional de Bancos.

Itaú, consciente de que esta realidad va más allá de un potencial riesgo para el negocio, es un riesgo para sus clientes, el asset de mayor valor para el banco. Dentro de este contexto, se hace necesario desarrollar una acción concreta, masiva y transversal, adoptando la educación financiera y la ciberseguridad como uno de los pilares comunicacionales prioritarios.

De esta manera se plantearon como objetivos de comunicación.

1. Educación: alertar y concientizar a las personas sobre los riesgos cibernéticos.
2. Prevención: promover y enseñar de manera didáctica medidas de protección.
3. Relacionamiento: construir un vínculo de confianza con los clientes, demostrando la importancia de combatir las estafas en conjunto.
4. Mitigación: reducir el número de casos, de montos defraudados y de malas experiencias para los clientes.

### **Propuesta/enunciado de campaña**

“Juntos Contra Robos y Fraudes” es la plataforma de comunicación de Itaú para informar, educar y concientizar a sus clientes – y a todas las personas – sobre las ciber estafas.

El aumento progresivo de los ciberataques y de víctimas, así como de las ideas cada vez más complejas e ingeniosas para llevar a cabo una estafa, hicieron a Itaú promover un llamado que extrapolaba el banco y la competencia, y abarcaba a todas las personas que hacen parte del ecosistema financiero, independientemente de cuál solución o marca elegían.

Ejemplo de esto fue que en todos los contenidos de la marca se consideraba a toda la banca, remarcando el mensaje de que “Itaú ni ningún banco va a pedir tus claves o datos personales”. Así, Itaú buscó cumplir un rol social, extendiendo una temática esencial a todo el mundo financiero, con la mirada puesta en hacer fuerza común contra los robos y fraudes digitales.

La plataforma siempre consideraba apuntar estas premisas:

- Mecanismos de fraude: dar a conocer en forma clara los distintos métodos a través de los cuales una persona podría ser víctima de una estafa, priorizando los más comunes o ingeniosos (llamadas telefónicas de falsos funcionarios del banco, estafas por SMS o WhatsApp y mensajes o correos electrónicos con links maliciosos).
- Mecanismos de prevención: educar sobre cómo mantenerse resguardado y cómo reaccionar frente a una eventual estafa (por ejemplo, no entregar datos personales o claves bancarias, chequear la veracidad de un mensaje e, incluso, identificar un sitio web falso).
- Alcance, frecuencia y constancia: la prevención a las ciber estafas es un acto continuo que se actualiza con las transformaciones de la tecnología y los métodos criminales, demandando una generación de contenido constante y alta frecuencia para garantizar la concientización de las personas.

Para alcanzar lo pretendido, Itaú desarrolló una mesa de trabajo colaborativa entre distintas áreas del banco: Marketing, Ciberseguridad, Tecnología, Canales Digitales, Experiencia del Consumidor y Banca Minorista. El propósito de la mesa consistía en controlar los impactos sobre los clientes de los fraudes, estar al día respecto del surgimiento de nuevas modalidades y responder rápidamente para su prevención. De esta manera se establecen contenidos actualizados según la contingencia y se masifican para alertar a las personas haciendo un llamado a no bajar la guardia.

### **Desarrollo/ejecución del plan**

La plataforma fue lanzada a inicio de abril de 2023 y se mantiene en la actualidad.

A través de una estrategia digital para educar a los clientes y a la comunidad, se usaron distintos assets para potenciar la eficiencia del mensaje.

Videos en YouTube y RRSS, presencia de rostros e influencers, como Pancho Saavedra, Cristián Riquelme y Dani Cachilupi, correos electrónicos, todo sumado con un acompañamiento diario de los casos de estafas. Una verdadera operación de guerra contra los ciber criminales.

De esta forma, se construyó así una comunicación cercana, integradora y diferente, que recreaba situaciones de estafas muy cotidianas que podrían haber sido vividas por las personas y les presentaba como identificarlas y, más importante, cómo enfrentarlas de manera segura.

La narrativa traía las personas como protagonistas, reforzando la centralidad de la marca en los clientes, abordando un tema serio de manera didáctica y liviana, mucho más preocupado en enseñar y concientizar que amedrentar.

Tácticas y acciones realizadas:

1. Desarrollo de videos hero para las principales amenazas

Casos	Mensajes de seguridad asociados
(Llamada telefónica) Un supuesto funcionario bancario llama por teléfono desde un número desconocido a una cliente del banco, le informa que ha ganado un premio y solicita sus claves para abonar el monto a su cuenta. Ella se da cuenta y reacciona. <a href="#">Link 1.</a> <a href="#">Link 2.</a>	“Ningún banco solicita claves vía telefónica”.
(Estafa por chat o mensaje de texto) La víctima tiene un amigo (cuya cuenta ha sido suplantada), quien le solicita dinero ante una emergencia sufrida, un accidente, un asalto, otro, y le manda datos de su cuenta para que le haga un abono. <a href="#">Link 1.</a> <a href="#">Link 2.</a>	“Confirmar identidad de quien envía el chat o mensaje antes de hacer cualquier pago”.
(Estafa vía chat con link falso) La víctima recibe un mensaje desde un número desconocido que le avisa que ha ganado puntos extras en su tarjeta de crédito y le envía un falso link al que debe ingresar para hacer efectivo el premio o beneficio. <a href="#">Link 1.</a> <a href="#">Link 2.</a>	“Ningún banco envía links para solicitar ingresar datos”.
(Estafa Contingencia) La víctima recibe un mensaje informando sobre una compra online efectuada. El mensaje indica que debe ingresar al link donde se le solicita abonar una suma de dinero para “liberar” el envío, lo que genera que la víctima entregue sus datos bancarios <a href="#">Link.</a>	“Nunca hagas click en los links que lleguen por SMS. Nunca des tus datos personales, números de tarjeta y no compartas tus códigos de verificación. Ingresa la url manualmente en tu buscador. Sospecha de estos SMS, pueden ser una ciberestafa”.

2. Desarrollo de 60 videos complementares para RRSS: presencia de rostros conocidos e influencers para reforzar puntos clave y detalles, bien como un instrumento de guerrilla rápido y eficiente frente a una amenaza urgente.
3. Mailing: Itaú envía correos exclusivos sobre contingencia de fraudes de ciberseguridad que se estén dando en el momento. Además, ha implementado de manera permanente la inclusión de tips de seguridad en todos los correos electrónicos que habitualmente envía a sus clientes, que en Chile suman cerca de 1,2 millones, entre personas naturales y personas jurídicas. Entre los mensajes que se adjuntan, se cuentan:
  - Nuestros correos electrónicos no contienen links ni botones.
  - Prefiere dispositivos y conexiones seguras para iniciar sesión en tu App o en Itáu.cl y mantén actualizado tu antivirus.

- Recuerda que puedes hacer tus transacciones de manera rápida, fácil y segura con Itaú Pass.
- Para nuevas configuraciones de Itaú Pass continuaremos solicitando 3 números de tu tarjeta de coordenadas.
- Nunca entregues tus claves por medio de una llamada o e-mail.

### **Resultados y evaluación**

“Simple y directo. Un buen consejo para todos. Se comparte!”

“Me encanta como explica :D Gracias”

“Esa sí que es una buena información”

“¡Amamos este reel!”

Estos mensajes no son phishing, ni mucho menos fakeing. Es una pequeña muestra de cómo la campaña “Juntos Contra Robos y Fraudes” fue recibida por las personas.

Cómo se hace con cualquier contenido educativo, alcance debe ser sumada a refuerzo y repetición. A lo largo de los últimos 12 meses, fueron casi 43 millones de views en más de 60 contenidos distribuidos en YouTube, Instagram y Tik Tok.

Un esfuerzo recompensado con la reducción de un 60% en las compensaciones realizadas por fraudes a clientes por el lado del negocio entre abril del 2023 y marzo del 2024. Pero, más importante, un esfuerzo recompensado dentro del punto de vista de marca y social, con la reducción de otros 60% en los impactos negativos en la vida y en el bolsillo de las personas.

Un punto a destacar es que ya en el primer mes se logró una baja del 50% en las compensaciones por fraudes a los clientes, lo que indica la necesidad de promover contenidos como estos, que buscan cuidar antes de vender.

En Itaú, todo empieza con una simple pregunta: “¿eso tiene valor para el cliente?” Como se ve claramente por los resultados obtenidos, esto no es solo una campaña publicitaria, es una herramienta relevante de educación y de construcción de un relacionamiento con las personas que excede el ámbito comercial. Para ser el servicio financiero más centrado en las personas del mundo, se puede tener seguridad que un paso importante ha sido dado en Chile.