



Campaña

Todos somos **Gestores de riesgo**

—
Emails y RRSS

Itaú presenta:

Todos somos Gestores de Riesgo

Con *Marcelo Lagos*

Ciberseguridad, Fraude, Prevención de Lavado de Activos,
Riesgo Operacional y Seguridad de la Información.





Email Teaser





Email Lanzamiento

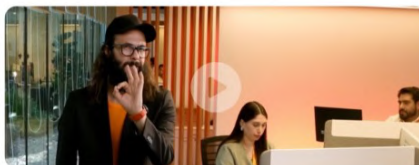


Hola Sebastian Andres,

La historia de Chile nos ha enseñado a estar siempre alertas, a prevenir y a actuar a tiempo ante el riesgo de desastre. Por eso, en Itaú creemos que no hay mejor manera de enfrentar el riesgo que anticipándonos a él.

Para fortalecer nuestra cultura de Gestión de riesgos que venimos apalancando desde siempre en el banco, **lanzaremos una serie de capítulos junto a Marcelo Lagos**, Geógrafo y Gestor de Riesgos, cuya voz ha acompañado a millones de chilenos, siendo protagonista en momentos de incertidumbre.

Junto a él abordaremos temas claves para resguardar lo que más valoramos: la confianza de nuestros clientes. Hablaremos de cómo estar preparados para enfrentar temas de: **Ciberseguridad, Fraudes, Prevención de Lavado de Activos, Riesgo Operacional y Seguridad de la Información.**



Todos somos
gestores de riesgo



Banner **Lanzamiento**

Itaú presenta:

Todos somos Gestores de Riesgo

Con *Marcelo Lagos*

Ciberseguridad, Fraude, Prevención de Lavado de Activos,
Riesgo Operacional y Seguridad de la Información.

Una serie para
anticiparnos a
lo inesperado.

Ver video



Email Ciberseguridad



Capítulo 1: Ciberataques, anticipándonos a un desastre digital.

Hola ituber,

Así como un temblor puede desencadenar un tsunami, un simple clic en un correo sospechoso puede desatar un ciberataque: **una verdadera catástrofe digital.**

En este primer capítulo, **Marcelo Lagos** nos invita a comprender mejor cómo cuidarnos del riesgo de **Phishing** y a reaccionar rápido frente a las señales de alerta.

! Si un mail te parece extraño o contiene un enlace sospechoso, **NO HAGAS CLIC.** Reporta de inmediato a: seguridadinformacion@itau.cl, phishing@itau.cl o haz clic en el botón Reportar Phishing.



Descubre qué nos tiene que decir Marcelo al respecto:



Todos somos gestores de riesgo



Banner **Ciberseguridad**

Todos somos Gestores de riesgo

Capítulo 1:
Ciberataques, anticipándonos
a un desastre digital.

Con *Marcelo Lagos*



En este primer capítulo te invitamos a comprender mejor cómo cuidarnos del Phishing y a reaccionar rápido frente a las señales de alerta.

Ver video



Email Backstage



Hola ituber,

Cada gran campaña tiene una historia detrás, y la de hoy no es la excepción. Durante una jornada única, Marcelo Lagos se sumó a nuestro equipo para grabar los primeros capítulos de: **Todos Somos Gestores de Riesgo**.

Allí compartió cómo su experiencia en desastres naturales conecta directamente con los riesgos que enfrentamos día a día en Itaú.

👉 No te pierdas el video del detrás de cámaras y descubre cómo se construyó esta campaña de magnitud 9.0





LinkedIn Backstage

Itaú Chile
 442.574 seguidores
 6 días · 🌐

Todos somos gestores de riesgo: una campaña exclusiva para itubers junto a Marcelo Lagos

La historia de Chile nos ha enseñado a estar siempre alerta, a prevenir y a actuar a tiempo ante el riesgo de desastre. En [Itaú Chile](#), creemos que no hay mejor manera de gestionar el riesgo que anticipándonos a él.

Junto a Marcelo Lagos, Geógrafo y Gestor de riesgos, cuya voz ha acompañado a millones de chilenos en momentos de incertidumbre, desarrollaremos una serie de contenidos que abordan temas clave sobre riesgos para el banco. A su vez, la evolución de la campaña busca fortalecer nuestra cultura de gestión de riesgos que hemos venido apalancando desde siempre, resguardando la información de nuestros clientes e itubers. Porque en Itaú Chile, todos somos gestores de riesgo.

👉 Conoce el detrás de cámara de esta campaña

[#Culturaltubers](#) [#GestiónDeRiesgos](#) [#TodosSomosGestoresDeRiesgo](#)

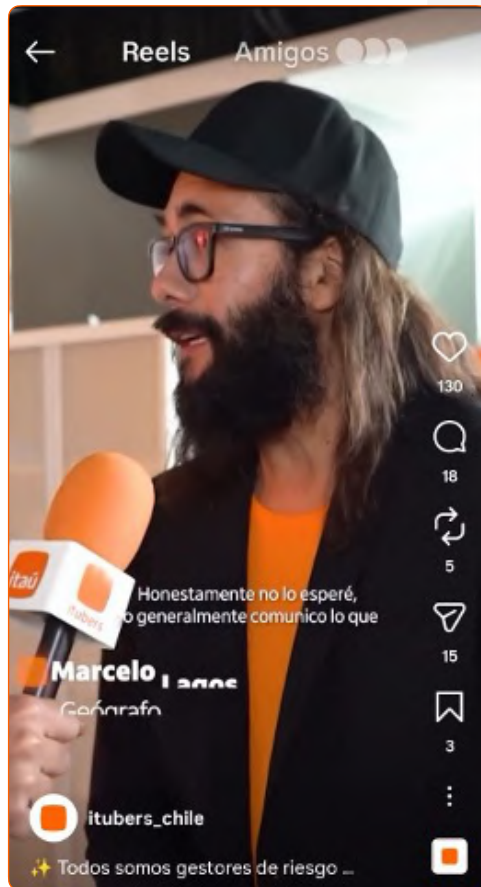
Seba León
Estratega Marketing Itaú Chile

1:45 1x CC

2 comentarios · 4 veces compartido



Instagram **Backstage**





Email Fraude



Capítulo 2: Fraudes, sus señales más comunes.

Hola ituber,

En la naturaleza ciertas señales pueden confundirnos: el terreno parece firme, el cielo despejado, pero el riesgo es silencioso y siempre está en movimiento. En el mundo del fraude sucede lo mismo.

En este segundo capítulo de Todos somos gestores de riesgo, Marcelo Lagos nos enseña a reconocer las principales señales de riesgo en caso de fraudes como Vishing, Sitios Web Falsos o Malware.

Descubre qué nos tiene que decir Marcelo al respecto:





Banner **Fraude**



Todos somos
Gestores de riesgo

Capítulo 2:

Fraudes, sus señales más comunes *con Marcelo Lagos*

En este segundo capítulo te enseñamos a reconocer las principales señales de riesgo en caso de fraudes como Vishing, Sitios Web Falsos o Malware.

Ver video 



Email Lavado de activos



Capítulo 4: Prevención de Lavado de Activos

Hola ituber,

Cuando un volcán libera cenizas es una señal de alerta que exige anticipación y medidas preventivas, y en nuestro banco, ocurre algo muy similar con el lavado de activos.

Por eso, en este nuevo capítulo de Todos Somos Gestores de Riesgo, **Marcelo Lagos**, geógrafo y gestor de riesgos, nos invita a comprender la importancia de **detectar a tiempo las señales de alerta** para proteger a nuestros clientes y al banco de movimientos inusuales.

Hola ituber,

Cuando un volcán libera cenizas es una señal de alerta que exige anticipación y medidas preventivas, y en nuestro banco, ocurre algo muy similar con el lavado de activos.

Por eso, en este nuevo capítulo de Todos Somos Gestores de Riesgo, **Marcelo Lagos**, geógrafo y gestor de riesgos, nos invita a comprender la importancia de **detectar a tiempo las señales de alerta** para proteger a nuestros clientes y al banco de movimientos inusuales.



De esta forma, si actuamos de inmediato, reforzamos nuestro modo de vivir nuestra cultura, donde la ética es innegociable.

Ve el **capítulo 4** de Prevención de Lavado de Activos:



Todos somos
gestores de riesgo



Banner
Lavado de activos

Todos somos
**Gestores
de riesgo**

Con *Marcelo Lagos*



Capítulo Prevención de **Lavado de Activos**

En este nuevo episodio aprenderás a reconocer las señales de alerta para proteger a nuestros clientes y al banco frente a movimientos inusuales.

Ve el capítulo aquí



Email Riesgo operacional



Capítulo 5: Riesgo Operacional

Hola ituber,

En la naturaleza a veces una pequeña falla basta para que algo mayor ocurra. En el banco pasa lo mismo, el **Riesgo Operacional** muchas veces se esconde en detalles o decisiones que parecen mínimas, **pero que pueden generar impactos relevantes para nuestros clientes.**

Un error al registrar información, compartir un documento sensible equivocadamente, dejar pasar una alerta sin comunicarla, son detalles que deben reportarse de inmediato. **Recuerda siempre que la gestión de riesgos comienza en nuestra primera línea de defensa, los itubers.**

Operacional muchas veces se esconde en detalles o decisiones que parecen mínimas, **pero que pueden generar impactos relevantes para nuestros clientes.**

Un error al registrar información, compartir un documento sensible equivocadamente, dejar pasar una alerta sin comunicarla, son detalles que deben reportarse de inmediato. **Recuerda siempre que la gestión de riesgos comienza en nuestra primera línea de defensa, los itubers.**



En este nuevo capítulo de **Todos Somos Gestores de Riesgo**, Marcelo Lagos nos invita a mirar más allá de lo evidente y a entender que **prevenir es anticiparse**, porque gestionar el riesgo es un compromiso compartido que se construye cada día.

Revisa aquí el **capítulo 5** de Riesgo Operacional y sigue fortaleciendo nuestra mirada preventiva



Todos somos
gestores de riesgo



Banner Riesgo operacional

Capítulo 5: Riesgo Operacional

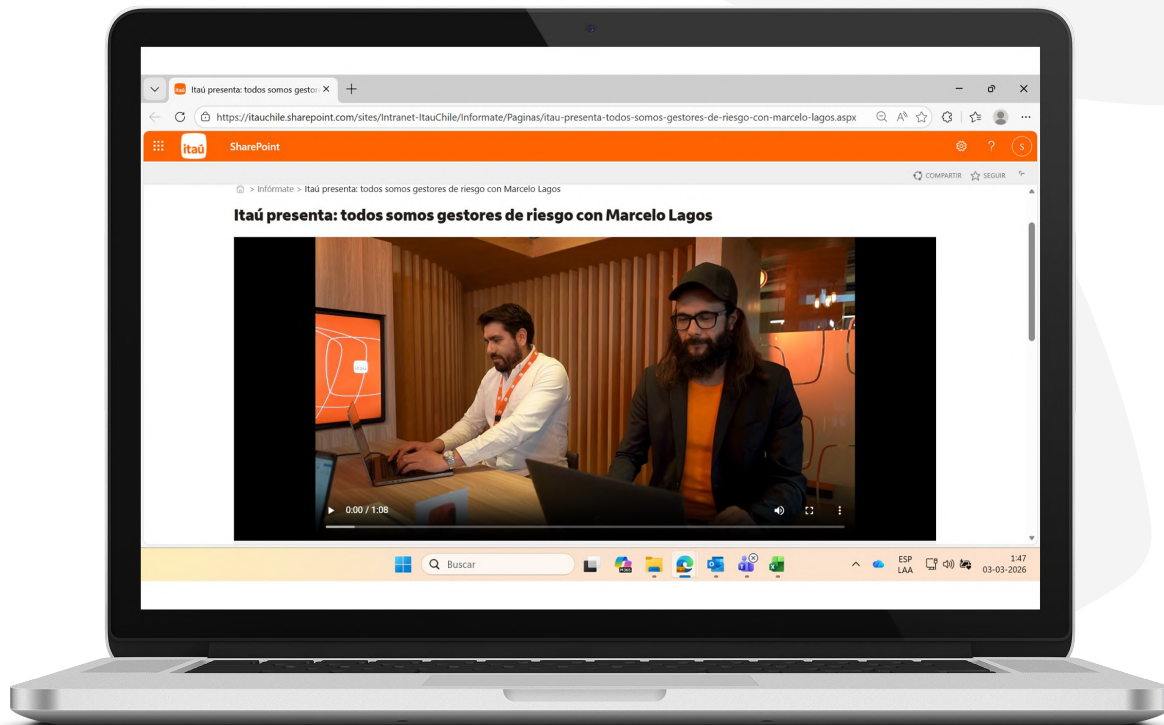
En este quinto capítulo te contamos cómo el **Riesgo Operacional** muchas veces se esconde en detalles o decisiones que parecen mínimas, pero que pueden generar impactos relevantes para nuestros clientes.

Ver video

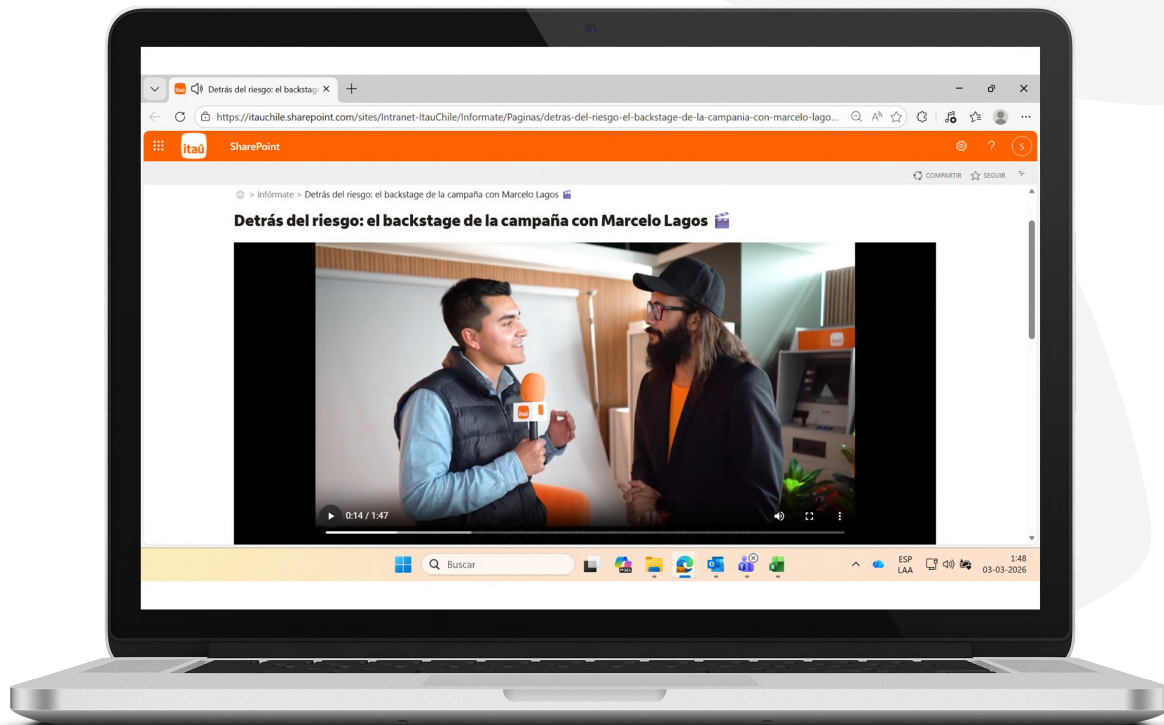




Intranet Lanzamiento



 Intranet
Backstage





Emails Mantención



¡Recomendaciones ante un caso de fraude!

Hola ituber,

Cuando tengas dudas frente a un mensaje sospechoso, lo más importante es **no apurarse**, la urgencia es la principal herramienta del fraude. Por eso cuando tengas dudas, aplica la regla P.A.R.A.:

- Para:** no hagas clic, no abras adjuntos y nunca compartas claves ni códigos OTP.
- Avisa:** reporta de inmediato a seguridad@itau.cl, idealmente en menos de 60 segundos.
- Reúne evidencia:** guarda pantallazos, la URL completa, el número de remitente, el archivo original (.eml/.msg), junto con la fecha y hora.
- Actúa:** si hubo clic o descarga de archivos, desconecta el equipo de la red, informa y cambia tus claves.



Actuar a tiempo marca la diferencia. Recuerda que tú eres la primera línea de defensa.



Todos somos
gestores de riesgo

Mientras estés en la oficina, protege tu información y dispositivos



Hola ituber,

Resguardar la información y nuestros dispositivos tecnológicos en nuestro entorno, es parte de las buenas prácticas de seguridad de la información denominado "Escritorio Limpio".

Hoy te entregamos varios tips acerca del cuidado al manipular, operar o almacenar información en tus dispositivos.

- En tu lugar de trabajo, no pegues post-it con datos sensibles, como contraseñas, UserID o información de clientes.
- Utiliza siempre el candado del notebook, anclándolo a tu escritorio.
- Evita imprimir, en caso de ser necesario resguarda los documentos de forma segura.
- Bloquea siempre tu estación de trabajo, cuando te tomes una pausa, vayas por un café u otro motivo.
- Guarda documentos, tarjetas, tokens, símbolos, llaves u otro dispositivo entregado por el banco, durante y al finalizar la jornada.
- Desecha los documentos si ya no los necesitas, de tal forma que sea imposible su recuperación.
- Borra apuntes o escritos en las salas de reuniones y retira todo material utilizado al finalizar la reunión.
- Utiliza siempre tu credencial de forma visible, con esto permites que otros puedan identificarla.



Todos somos
gestores de riesgo

Área de Protección de Datos

Saber actuar también es parte de la seguridad



Hola ituber,

En el mundo digital, cada segundo cuenta y cada clic importa. Un incidente de ciberseguridad puede ocurrir en cualquier momento y estar preparados marca la diferencia.

- Un sistema que se cae, un dispositivo extraviado o incluso un correo fraudulento, pueden convertirse en una amenaza si no actuamos a tiempo. Además, cuando se trata de un ataque malicioso como ransomware, ataques de denegación de servicios o robo de información, el impacto puede afectar directamente nuestros canales, datos y reputación como banco.

Mira el video y aprende a actuar como gestor de riesgo:



Recuerda que, ante una situación sospechosa, debes:

- Reporta a tu jefatura y a la mesa de servicio.
- No intentes resolver por tu cuenta.
- No difundas rumores, fotos ni lo publiques en redes sociales.
- Usa el botón de phishing en Outlook si recibes correos sospechosos.

¿Tienes dudas?

Escribenos a csirt@itau.cl o phishing@itau.cl

Mantener la calma y seguir los protocolos
es clave para cuidar nuestro banco.



Todos somos
gestores de riesgo

Ciberseguridad



Emails Mantención

Entérate sobre los riesgos del Ransomware



Hola #iFieldStr08!#,

El Ransomware es un tipo de ciberataque que afecta a tus dispositivos cifrando o eliminando la información contenida en él. Su propósito es solicitar un rescate en dinero o alguna criptomoneda para poder recuperar la información.

Las formas más comunes de propagación y a las que hay que poner atención son:

- 📄 Páginas web maliciosas.
- 📥 Descargas de aplicaciones y programas online.
- 📁 Dispositivos de almacenamiento externos.
- ✉️ Correos electrónicos – SMS.
- 🌐 Redes sociales y aplicaciones de mensajería instantánea.
- 📱 Códigos QR.
- 🔒 Explotación de vulnerabilidades de sistemas operativos o aplicaciones.

Es muy importante estar atento a este tipo de ataques debido a las grandes consecuencias que podría ocasionar, como pérdida de la información, robo de datos y pérdidas económicas.

Te invitamos a aplicar estas buenas prácticas:

- 🛡️ Respálate y haz copias de tu información periódicamente.
- 🔄 Mantén actualizado tus dispositivos y aplicaciones.
- 🤔 Piensa antes de hacer clic.
- 🚫 Si eres víctima no pagues el rescate, esto no asegura que recuperes la información.
- 📢 Si tienes sospechas, repórtalo de inmediato.
- 👤 ¡Sigue aprendiendo! Participa en instancias de concientización.

✅ Todos somos gestores de riesgo

Ciberseguridad

End marketing | Interno

¡Alerta! Fraude de CEO



Hola ituber,

Esta práctica delictiva consiste en que una persona se hace pasar por el CEO, gerente o integrantes del Comité Ejecutivo de Itaú, con el fin de tomar contacto y de engañar a través de un correo electrónico, videollamada, redes sociales, WhatsApp o telefónicamente.

Por eso, debes tomar precauciones y estar alerta para evitar estafas, así también sospechar cuando recibas solicitudes inusuales. Los ciberdelincuentes utilizan diferentes técnicas de engaño: usan fotografías de la persona, conocen tu nombre, datos específicos tuyos o de la persona suplantada.

Ten en consideración las siguientes recomendaciones, en caso de ser contactado:

- ✉️ **Comprueba cuidadosamente los remitentes:** fíjate bien en detalles sutiles como fallas de ortografía, dominios desconocidos o pequeñas discrepancias en las direcciones de correo electrónico que podrían delatar una estafa.
- 📞 **Duda del número telefónico que te contacta:** aún cuando te digan que es un número privado o nuevo.
- 🚫 **Desconfía de las solicitudes urgentes e inusuales:** Mantente alerta cuando recibas mensajes solicitando acciones financieras urgentes, transferencias de fondos o revelación de información sensible. Los delincuentes utilizan tácticas de miedo y urgencia para presionar a las víctimas.
- 📧 **Confirma la autenticidad del mensaje:** ponte en contacto con la persona mencionada en el correo electrónico, en persona o por teléfono, utilizando los canales oficiales.
- 👤 **Valida con tu Gestor:** coméntale a tu Gestor la situación, para que te apoye en verificar la solicitud. Si estás experimentando un intento de estafa contacta a la casilla seguridadinformacion@itau.cl

✅ Todos somos gestores de riesgo

Ciberseguridad

Cultura de Riesgo

Tu rol es clave para proteger la información



Hola ituber,

La cultura de riesgo se basa en principios fundamentales, como la confidencialidad, integridad y disponibilidad de la información. Nuestras decisiones diarias pueden prevenir o generar incidentes que afecten la seguridad de la información.

⚠️ Riesgos:

- ❌ Compartir acceso puede abrir la puerta a usos indebidos o accesos no autorizados.
- ❌ Dejar dispositivos desbloqueados o sin supervisión puede permitir que terceros accedan a información sensible.
- ❌ No reportar incidentes o conductas sospechosas puede aumentar el impacto de una brecha.
- ❌ Las brechas de datos pueden generar sanciones regulatorias, pérdida de confianza y consecuencias legales.
- ❌ Una afectación de este nivel compromete el cumplimiento normativo y la reputación del banco.

✅ Buenas prácticas:

- 🔍 Revisa antes de compartir: ¿Es el canal adecuado? ¿La persona tiene autorización? ¿Es necesario?
- 🔒 Minimiza el uso de datos: Solo trata lo estrictamente necesario.
- 🚨 Reporta incidentes sospechosos: No subestimes señales de riesgo.
- 📵 Evita enviar información sensible por canales no cifrados o no autorizados.
- 🔒 Utiliza contraseñas robustas y nunca las compartas.
- 📴 Bloquea tu equipo cuando te ausentes, incluso por breves momentos.
- 📋 Antes de recolectar o tratar datos, evalúa si realmente son necesarios para el propósito definido.

📌 Recuerda:

Puedes consultar políticas y procedimientos disponibles en la intranet del banco. Ante cualquier incidente, utiliza el canal oficial de reporte a través de **GESTIONA**.

✅ Todos somos gestores de riesgo

Área de Protección de Datos



iGracias!