

ASICI

Asociación Internacional
de Ciberseguridad



TALLER: “SIMULACIÓN DE UN ATAQUE DE INGENIERÍA SOCIAL: EL PRIMER FIREWALL ERES TÚ”

OBJETIVOS

OBJETIVO GENERAL

Concientizar y entrenar a los participantes para reconocer, prevenir y responder ante intentos de manipulación psicológica y ataques de ingeniería social, fortaleciendo la cultura de seguridad organizacional.

OBJETIVOS ESPECÍFICOS

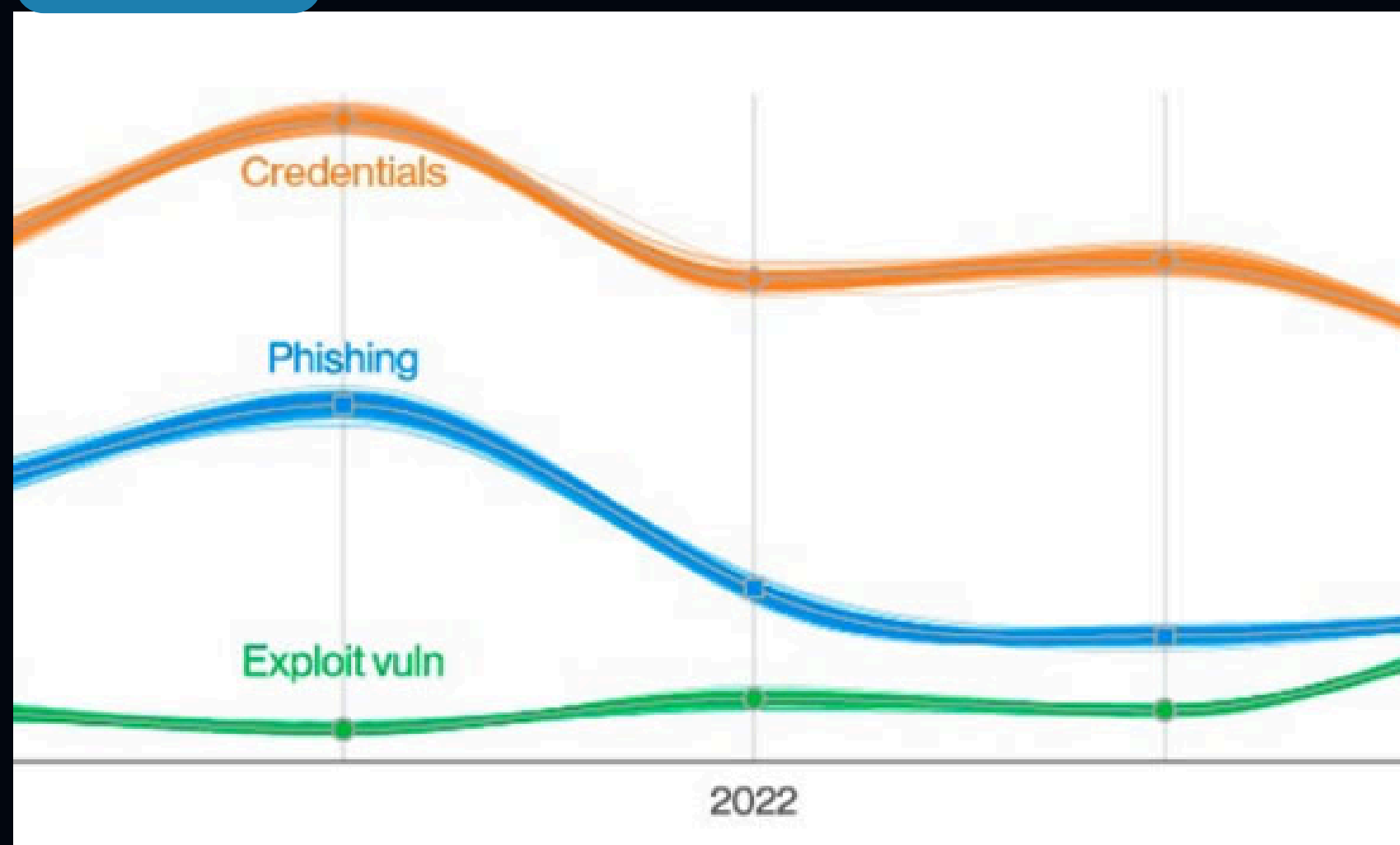
1. Comprender los principios psicológicos detrás de la ingeniería social.
2. Identificar las técnicas más comunes utilizadas por atacantes (phishing, vishing, smishing, pretexting, baiting, etc.).
3. Analizar ejemplos reales y ejecutar una simulación práctica de ataque y defensa.
4. Fortalecer las capacidades de respuesta individual y grupal ante incidentes.
5. Promover hábitos de seguridad digital cotidiana dentro y fuera del trabajo.



¿POR QUÉ HABLAMOS DE INGENIERÍA SOCIAL?

El 90% de los incidentes de ciberseguridad comienzan con un error humano.

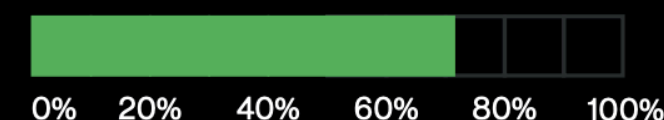
No se vulnera el sistema, se vulnera la mente.



Help people-proof your systems.

74% of all breaches include the human element through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

74%



MODALIDADES

Modalidades Remotas o Digitales

PHISHING

SPEAR PHISHING

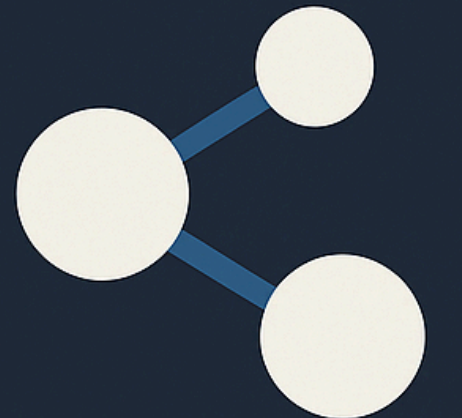
WHALING

SMISHING

VISHING

QUISHING

BUSINESS EMAIL COMPROMISE (BEC)



MODALIDADES

Modalidades Presenciales/Híbridas

TAILGATING

DUMPSTER DIVING

SHOULDER SURFING

PRETEXTING

BAITING

SCAREWARE



CASOS REALES



TWITTER 2020: EMPLEADOS ENGAÑADOS POR TELÉFONO

Éxito de un ataque
de ingeniería social
que comprometió
varias cuentas



BANCO DE CHILE 2018: CORREO INTERNO DE SPEAR PHISHING

Ataque dirigido que
afectó sus operacione



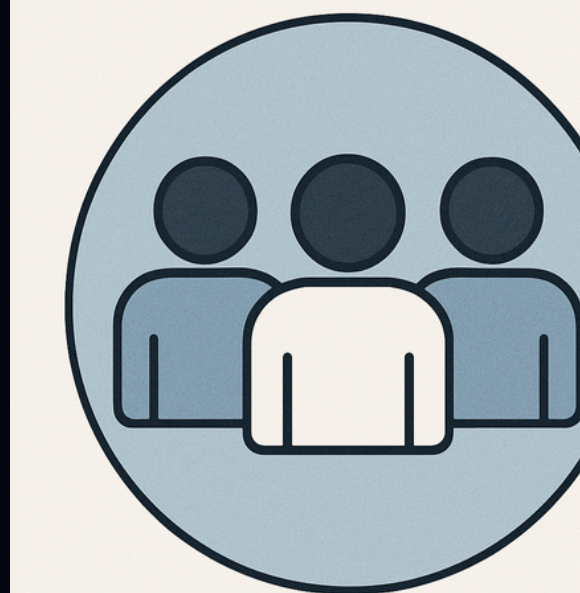
UBER 2022: ACCESO CONCEDIDO POR ENGAÑO A SOPORTE

Atacante que
comprometió sistemas

El atacante no entra por la red... entra por la
confianza.

“EL ARTE DE HACKEAR EMOCIONES”

Robert Cialdini, un investigador de la persuasión, definió seis principios universales que los atacantes aplican a la perfección.



Autoridad - “TI requiere su clave de acceso de inmediato”

Reciprocidad - “Te comparto este documento, ayúdame revisándolo.”

Compromiso/ Coherencia - “Como ya colaboraste antes, necesito otro dato.”

Simpatía - “Qué gusto verte en el evento, mira esta foto.”

Escasez/Urgencia - “Último día para reactivar tu cuenta.”

Prueba Social - “Todos ya enviaron su validación, falta la tuya.”

DINÁMICA - ¿ABRIRÍAS ESTE CORREO?

Nos vamos a Quizz
Para una breve
Dinamica



¿QUE REVISAR?

REMITENTE - ¿El dominio del correo coincide exactamente con el oficial de la empresa? ¿El nombre mostrado es distinto del correo real (spoofing visual)? ¿Usa cuentas genéricas o corporativas?

ASUNTO - ¿Es alarmista, urgente o emocional? ¿Incluye emojis, mayúsculas o signos de exclamación excesivos?

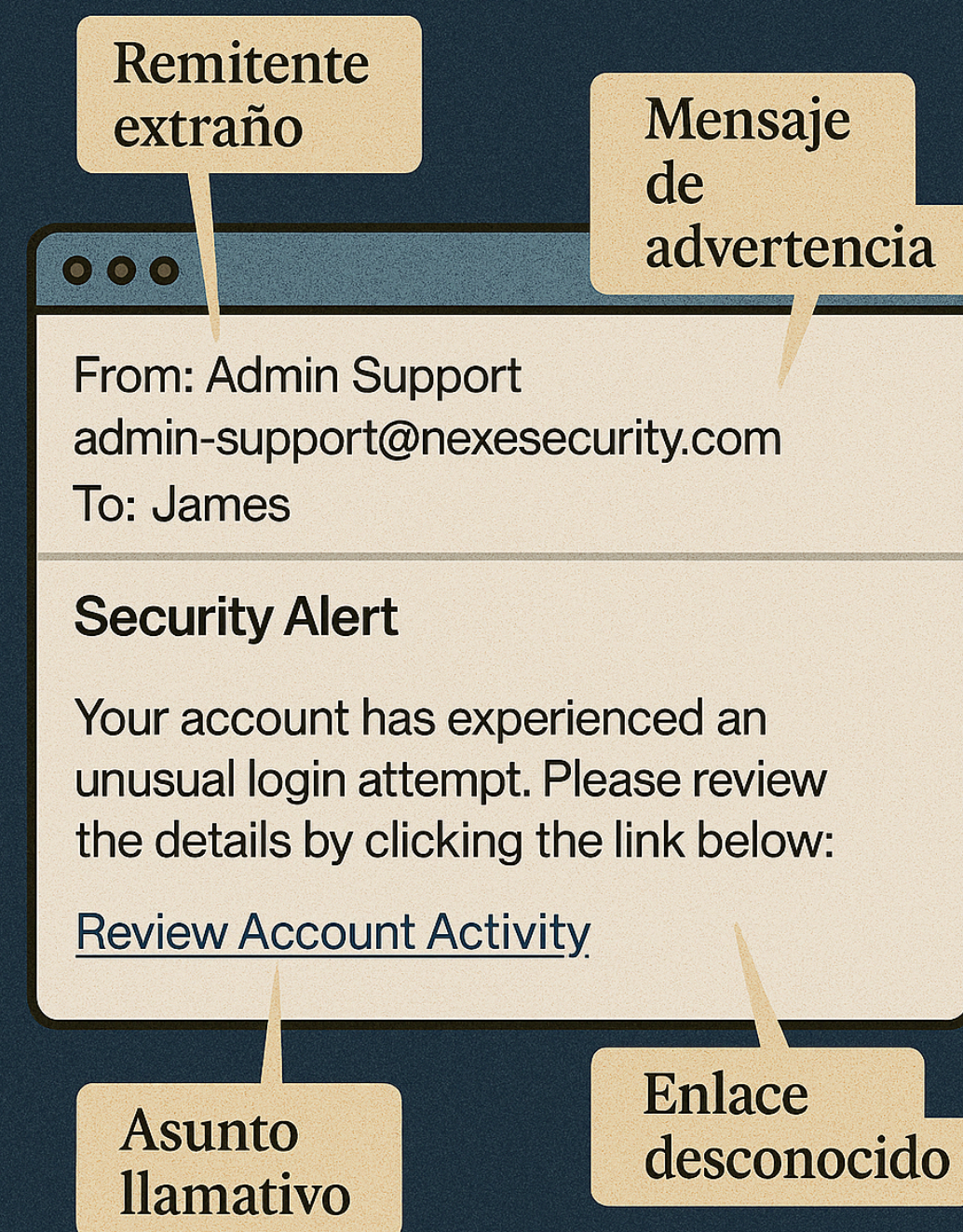
TONO Y CONTENIDO - ¿Genera miedo, curiosidad o presión para actuar rápido? ¿Pide datos personales, contraseñas o accesos que normalmente no se solicitan por correo? ¿Usa lenguaje genérico o saludos impersonales? ¿Tiene errores de ortografía, puntuación o formato visual extraño?

ENLACES Y ADJUNTOS - ¿Coincide el texto visible del enlace con la URL real al pasar el cursor? ¿El dominio parece sospechoso, largo o con letras reemplazadas (micrOsoft.com, secure-teams.net)? ¿Los adjuntos tienen extensiones raras o comprimidas (.exe, .zip, .scr, .bat)? ¿Te pide habilitar macros en un archivo de Office?

FIRMA Y LEGITIMIDAD - ¿Incluye firma corporativa real (nombre, cargo, teléfono interno, logo)? ¿O es genérica ("Soporte Técnico", "Centro de Seguridad")? ¿Faltan detalles institucionales o hay inconsistencias visuales?

CONTEXTO - ¿Esperabas ese correo? ¿Tiene sentido con tus tareas, proyectos o contactos recientes? ¿Hay algo fuera de lugar (horarios, idioma, formato, exceso de familiaridad)?

PRINCIPIOS PSICOLÓGICOS ACTIVADOS - Evalúa si el correo intenta: Imponer autoridad ("Soy de TI"). Generar urgencia o miedo ("última oportunidad"). Crear afinidad o confianza ("nos vimos en el evento"). O alguno de los principios que vimos



¿QUE HACER?

No hagas clic hasta confirmar la fuente.

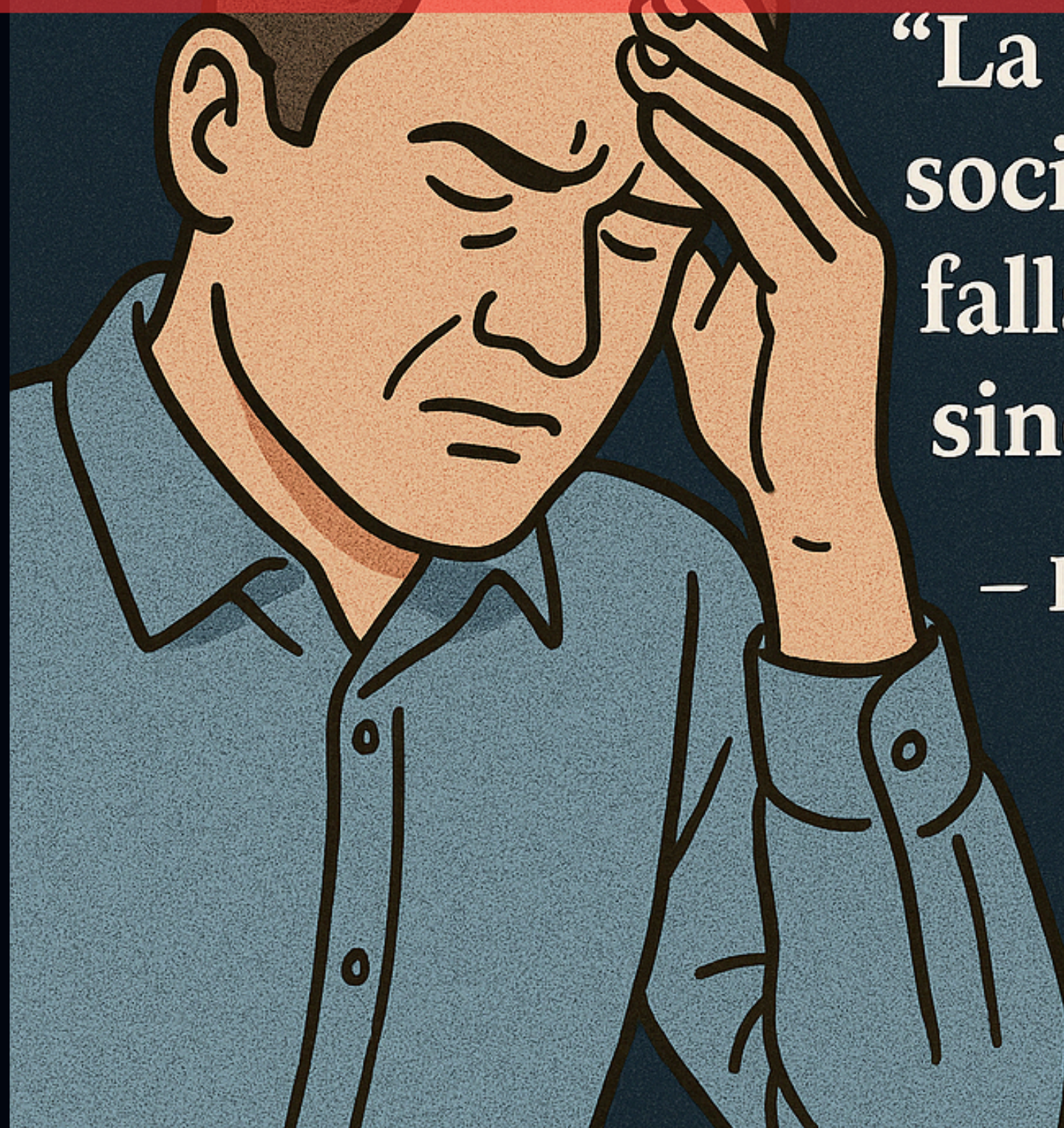
Verifica por un canal alternativo (Teams, teléfono, chat interno).

Reporta el mensaje sospechoso al área de seguridad o usa el botón de “report phishing”.

Si hiciste clic o entregaste información, cambia la contraseña inmediatamente y notifica al área TI.



TODOS SOMOS VULNERABLES



“La ingeniería social no explota fallas tecnológicas, sino humanas.”

— Kevin Mitnick

CICLO DE UN ATAQUE

“Los ataques de ingeniería social no son casuales.
Cada paso está planificado con precisión.”



FASE 1: INVESTIGACIÓN

A través de OSINT y Reconocimiento

“El atacante te estudia antes de escribirte.”



FASE 2: ENGAÑO

Aquí se da el contacto inicial

“Aquí se lanza el anzuelo.”



FASE 3: EXPLOTACIÓN

“El atacante no pide todo de una vez. Lo consigue poco a poco.”



FASE 4: EJECUCIÓN

“Con la información obtenida, el atacante actúa.”



Creada el 11 de julio - 22:34 hs

Número de operación 70791509096

⑤ Transferencia de dinero

\$ 19.000,00

✓ Aprobada

Estados anteriores >

👤 Le transferiste a

cuenta
corriente

Carlos

be

Código de identificación:

LOEJWV9U3GL16KM2QMD0GZ



Gastaste en Pendiente de categoría

[Ir a Gastos de la categoría](#)



Ver comprobante

Comprobante de transferencia

Sábado, 11 de julio 2025, 10:51 hs.

\$ 1.000

De

RUT: **.***.839-*

Mercado Pago

Número de cuenta: [redacted]

Para

Carlos Ramirez

RUT: **.***.198-*

S [redacted]

Tipo de cuenta: Cuenta corriente

Número de cuenta: [redacted]

PIENSA COMO UN ATACANTE

“Para protegerte, tienes que pensar como ellos.”

Preguntarnos:

·¿Qué intenta conseguir?

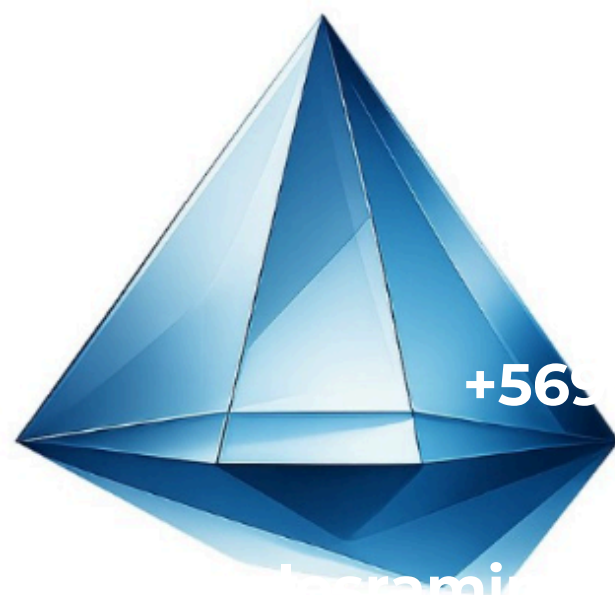
·¿Por qué me contacta a mí?

·¿Qué información le estoy entregando sin darme cuenta?

La mente crítica es el antivirus más potente.



CONTACTO



PRISMA
COMPLIANCE
<https://www.prisma.compliance.cl>

Carlos Ramírez Rodríguez
Ingeniero de Sistemas

Founder & Chief Executive Officer

+56 9 50923135

carlos.ramirez@prisma.compliance.cl

www.prisma.compliance.cl