CATÁLOGO · 2026

SANTIAGO · CHILE

twoko

Offensive Prevention

Creamos soluciones de ciberseguridad vanguardistas para protegerte de los problemas actuales.

TWOKO.IO · SALES@TWOKO.IO

Ciberseguridad, al siguiente nivel.

Somos tu próximo socio estratégico

Robustecer la seguridad de las empresas, aportando un alto grado de predictibilidad y resiliencia en la operación TI, es clave — y eso lo sabemos en **TWOKO**. Investigamos, identificamos y explotamos vulnerabilidades para estar mejor preparados a los ataques de cibercriminales.

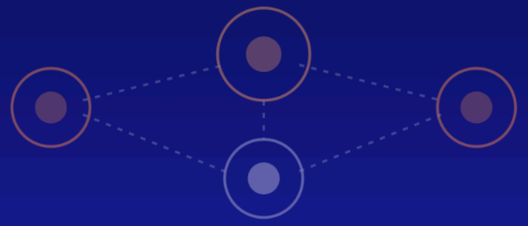
Nuestro objetivo

Ser un socio estratégico que garantice dos puntos críticos: **continuidad operacional** y **éxito en los negocios**. Por eso, desarrollamos un conjunto completo de soluciones diseñadas para proteger los activos digitales de nuestros clientes.

Cercanía, profesionalismo y proactividad.

Una mirada transversal para afrontar los problemas del ahora. Tres pilares que sostienen cada compromiso con nuestros clientes.

01



Equipo multidisciplinario

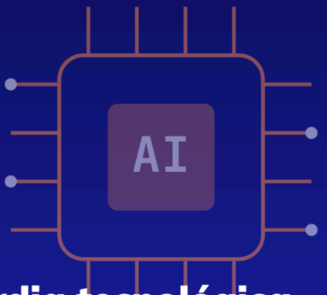
Expertos altamente capacitados que trabajan de cerca con cada cliente para ofrecer soluciones a la medida.

02

Enfoque integral 360°

Soluciones de seguridad, monitoreo proactivo, educación y respuesta rápida a incidentes — bajo un mismo paraguas.

03



Vanguardia tecnológica

Últimas tecnologías y mejores prácticas en seguridad de la información para reducir vulnerabilidades y prevenir incidentes.

Conoce nuestros servicios.

La ciberseguridad requiere rigurosidad, experiencia y conocimiento. En Twoko diseñamos servicios para protegerte de las amenazas actuales con una **mirada proactiva**.

01	Cyber Posturement 360°	PROTECCIÓN INTEGRAL
02	Cyber Intelligence I+D	INTELIGENCIA AVANZADA
03	Ethical Hacking	PENTESTING
04	Ethical Phishing & Smishing	INGENIERÍA SOCIAL
05	Análisis de vulnerabilidades	ANÁLISIS DINÁMICO
06	Agentes de Inteligencia Artificial	NUEVO
07	Red Team	OPERACIONES OFENSIVAS

PLATAFORMA

Sentinel Brand

Brand protection + Threat Intelligence LATAM

SERVICIO **01.**

Cyber Posturement 360°

Un servicio integral diseñado para ofrecer **protección completa y proactiva** a tu organización frente a las amenazas cibernéticas. Identifica y mitiga. Fortalece y evalúa.

IDENTIFICA · MITIGA · FORTALECE · EVALÚA

Cinco frentes, una sola postura defensiva.

01

Inventario de servicios

Dominios, IPs y componentes críticos expuestos. La gestión de activos es la base de un programa sólido — las brechas en el inventario ralentizan detección y respuesta.

02

Pentesting a inventario

Infraestructura / Web (3 IPs o URLs), Cloud (3 API o URLs) y una aplicación móvil. Pruebas exhaustivas para descubrir y mitigar vulnerabilidades reales.

03

Ejercicios de phishing

94% de las organizaciones globales son víctimas de phishing. Con plan de entrenamiento, se reducen los errores en un **60%**.

04

Data Leaks

Monitoreo en deep y dark web para detectar filtraciones. El costo promedio de una brecha de datos alcanza los **USD 4.5M**.

05

Capacitaciones

Seis sesiones de dos horas, enfocadas en la cultura de ciberseguridad — desde conceptos básicos hasta cómo reportar correos maliciosos e incidentes.

94%

DATO RELEVANTE

de las organizaciones a nivel global son víctimas de ataques de phishing — la postura preventiva no es un lujo.

FUENTE INTERNA
TWOKO LABS · 2025

SERVICIO 02.

Cyber Intelligence I+D

Investigación y desarrollo de soluciones avanzadas en ciberinteligencia. Un servicio que te entrega **ventaja proactiva** en la identificación, análisis y mitigación de amenazas emergentes y sofisticadas.

Investigación avanzada

Investigaciones profundas sobre tendencias en amenazas, vulnerabilidades y tácticas usadas por actores malintencionados.

01

Desarrollo de soluciones personalizadas

Creamos soluciones a medida para cada cliente, asegurando que estén preparados para enfrentar las amenazas más avanzadas.

02

Análisis de Inteligencia

Técnicas avanzadas para proporcionar información valiosa y accionable, permitiendo tomar decisiones informadas.

03

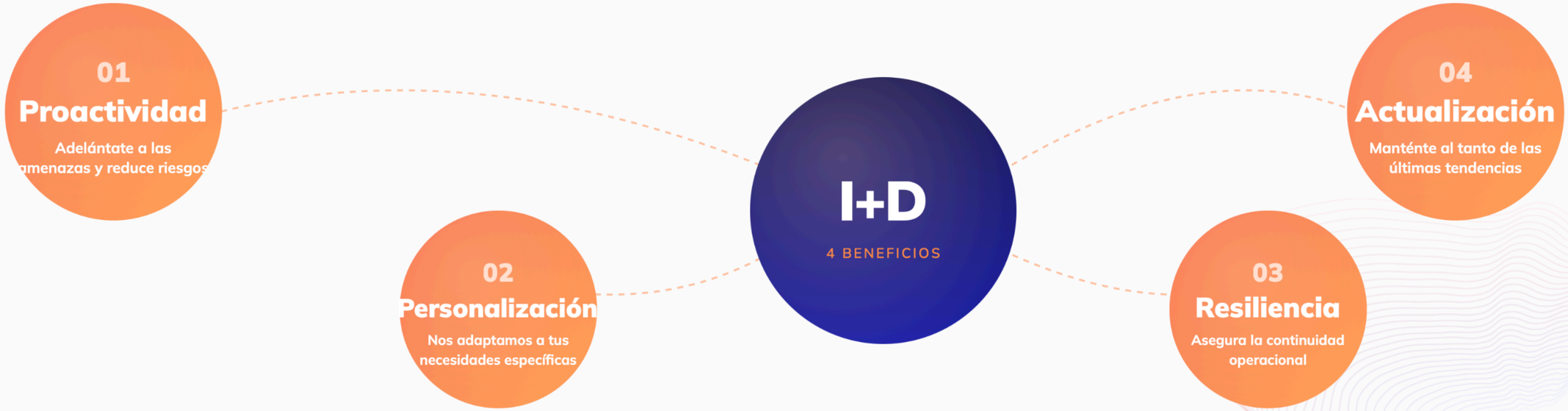
Monitoreo Continuo

Sistemas de monitoreo 24/7 que permiten detectar y responder a amenazas en tiempo real, minimizando el impacto.

04

Cuatro razones para incorporar ciberinteligencia hoy.

La ciberinteligencia es un pilar clave para toda organización actual. Estos son los cuatro beneficios que entrega Cyber Intelligence I+D.



SERVICIO **03.**

Ethical Hacking.

El **pentesting** es un proceso de evaluación que identifica y explota vulnerabilidades en redes computacionales. Simulamos un ataque por parte de un ciberdelincuente para evaluar la seguridad y determinar dónde están las brechas que podría explotar.

Aplicamos las mismas técnicas y herramientas que los atacantes — con consentimiento, marco controlado y un informe accionable de cierre.

OBJETIVOS DEL EJERCICIO

01 Evaluar la seguridad

02 Validar defensas

03 Probar incidentes de seguridad

04 Mapear la superficie de ataque

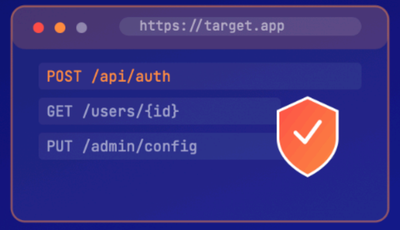
05 Medir riesgos

06 Recomendar mitigaciones

Dos frentes, una misma disciplina ofensiva.

A · WEB / API

Ethical Hacking Web / API



Identificamos vulnerabilidades y debilidades de seguridad en aplicaciones web **antes** que los ciberdelincuentes puedan descubrirlas. Usamos las últimas herramientas y técnicas de actores maliciosos.

B · MOBILE

Ethical Hacking iOS · Android · HarmonyOS

Centrado en dispositivos móviles para evaluar su seguridad y detectar vulnerabilidades. Identificamos y solucionamos problemas **antes** de que sean explotados por atacantes malintencionados.

SERVICIO 04.

Ethical Phishing & Smishing.

VECTOR · EMAIL

Ejercicios de Phishing

Simulamos ataques de correos maliciosos reales con el propósito de **educar a los empleados** y mejorar la seguridad de la organización. Diferentes objetivos: obtención de datos personales, credenciales de acceso o descargas de archivos.

VECTOR · SMS

Ejercicios de Smishing

Variante del phishing que utiliza mensajes de texto (SMS) para obtener información confidencial. Al incluir smishing en nuestras pruebas, proporcionamos una **cobertura más amplia** de las amenazas de ingeniería social actuales.

SERVICIO **05.**

Análisis de vulnerabilidades.

Un **análisis dinámico** consiste en asegurarte de que el código de tu aplicación funciona de manera segura.

Se llama dinámico porque las pruebas se realizan mientras el código se ejecuta, simulando la operación del programa para evaluar su comportamiento — lo que permite levantar hallazgos de seguridad con precisión y contexto.

Agentes de Inteligencia Artificial.

Aplicaciones prácticas de IA en **departamentos de ciberseguridad** — agentes especializados que aprenden, recuerdan y operan 24/7 dentro de tu infraestructura.

01

Automatización de tareas repetitivas

Libera al equipo de tareas rutinarias para enfocar el talento en lo estratégico.

02

Normativas y compliance

Agentes alineados a marcos regulatorios — auditables, trazables y soberanos.

03

Opciones de implementación

Identificamos casos de uso con mayor impacto, factibles desde el día 1.

04

Eficiencia de los recursos

Operación continua 24/7 que multiplica la capacidad de tu equipo actual.

El impacto sobre los equipos.

01

Aumento de productividad y eficiencia

Libera a los equipos de tareas repetitivas para concentrar esfuerzos en labores estratégicas. Más capacidad operativa, menos fatiga.

02

Velocidad de los procesos 24/7

Al trabajar de forma continua, los agentes aceleran flujos DevSecOps, operaciones internas, documentación y respuesta — sin descanso.

03

Memoria persistente y aprendizaje

Los agentes locales aprenden y mantienen contexto a lo largo del tiempo — agilizan procesos y reducen errores que dependen de memoria humana.

METODOLOGÍA

Las tres fases del proyecto

1 **REQUERIMIENTOS**
Revisión del contexto, definición de alcances y esperables.

2 **IMPLEMENTACIÓN**
Despliegue de la infraestructura y de los agentes de IA.

3 **CIERRE**
Validación de resultados y lecciones aprendidas para el equipo.

Cinco semanas para tener tu primer agente en producción.

Una metodología iterativa que valida el caso de uso antes de cada paso siguiente. Sin sorpresas, con entregables al final de cada semana.

1

SEMANA 01

Contexto

Levantamiento de características, mapeo de funcionalidades, reglas de negocio y requerimientos de ciberseguridad.

2

SEMANA 02

Diseño

Propuesta de diseño con integración a plataformas (JIRA, BB). Validación de máquina, accesos y requerimientos.

3

SEMANA 03

En marcha

Verificación de ambiente, SO, librerías, RAG, integraciones (API y MCP) y estructura de permisos.

4

SEMANA 04

Casos de uso

Revisión de casos de uso del agente, verificación de resultados y puesta en marcha en producción.

5

SEMANA 05

Cierre

Entrega de documentación, informe de resultados y capacitaciones para tu equipo interno.

¿A QUIÉN?

BANCA & FINANCIEROS
Riesgo operacional, fraude, CS

TELCOS · SOC
SOC interno y SOCs de clientes

DESARROLLO & PARTNERS
DevOps, DevSecOps, pentest

OIV · NORMATIVO
Cumplimiento regulatorio

Tres planes, un mismo estándar de entrega.

Equipo de desarrollo especialista en CS (JP + 2 devs). Los valores incluyen **3 meses de soporte post cierre**.

PLAN A

USD 3K–5K

- Hasta **4 integraciones**
- Equipo de desarrollo dedicado
- **12 meses** de soporte

Ideal para iniciar con un caso de uso de alto impacto.

MÁS POPULAR

PLAN B

USD 5K–15K

- Hasta **9 integraciones**
- Equipo de desarrollo dedicado
- **18 meses** de soporte

Volumen creciente de agentes y procesos a automatizar.

PLAN C

DESDE USD 15K

- Desarrollo a medida de **múltiples agentes**
- Equipo de desarrollo dedicado
- **Soporte ilimitado**

Para organizaciones que adoptan IA como pilar central.

SERVICIO **07.**

Operaciones de Red Team.

Evaluamos la capacidad real de tu organización para **detectar, contener, mitigar y prevenir** ataques — mediante las últimas técnicas de explotación de vulnerabilidades y obtención de información confidencial.

Un ejercicio real, pactado, con métricas claras de respuesta. Diseñado para poner a prueba — y entrenar — a tus equipos de ciberseguridad.

Sentinel Brand.

Protección de marca y threat intelligence para **fintechs y empresas LATAM**. Detecta suplantación, filtraciones y exposición digital — y acelera takedowns con evidencia pre-armada.

<6h
TAKEDOWN PROMEDIO
desde detección a resolución

10 +1
SUBMÓDULOS
de auto-investigación determinista

~⅓
COSTO vs AXUR
a precio similar o menor

MULTI-TENANT

100% DETERMINISTA · SIN LLM EXTERNO

LEY 21.719 · GDPR · CMF

STEALER LOCAL-FIRST

DASHBOARD EJECUTIVO

10 superficies de ataque, una sola consola.

Dominios suplantadores

Typosquatting, combosquatting, NIC.cl/.ar, Registro.br, Certificate Transparency. Detección el mismo día del registro.

Phishing activo

SSL inspect, Playwright + screenshot, phishing-kit fingerprint, 11 feeds TI cruzados con probes activos.

Apps móviles falsas

Google Play, App Store y APK markets. Allowlist por publisher oficial → cero ruido.

Redes sociales

Cuentas falsas FB / IG / Threads + Meta Ads. Detecta también ads pagados que imitan al cliente.

Stealer logs LATAM

Hudson Rock + procesamiento local (RedLine, Lumma, StealC). **Únicos en LATAM** con stealer local-first.

Data leaks / breaches

BreachForums.io mirror, foros darkweb, HIBP, IntelX y DeHashed (opt-in). Cobertura post-takedown FBI 2025.

Deep web / VIPs

Onion crawling vía Tor. CEOs, emails y RUT en foros y Telegram — PII chilena fuera de scope gringo.

Exposición OSINT propia

.git, .env, Swagger / GraphQL, buckets S3/GCS/Azure abiertos, 35 patrones de secrets en GitHub.

DNS / SSO

SPF, DMARC, DKIM, MTA-STS, DNSSEC, OpenID discovery. Patrón "mail legacy + creds SSO actual".

Marketplaces

Mercado Libre — listings sospechosos cada 6h. Cobertura LATAM-first donde los players globales no llegan.

Inteligencia determinista, no caja negra.

01 **Auto-investigation determinista**

Cada finding crítico dispara **10 sub-módulos** en paralelo (DNS / WHOIS / cert history / 11 feeds TI / stealer / GitHub / Wayback / cross-findings / brand correlation / Telegram) → veredicto con evidencia trazable. Sin LLM, 100% auditable.

02 **Precision gate · 9 reglas**

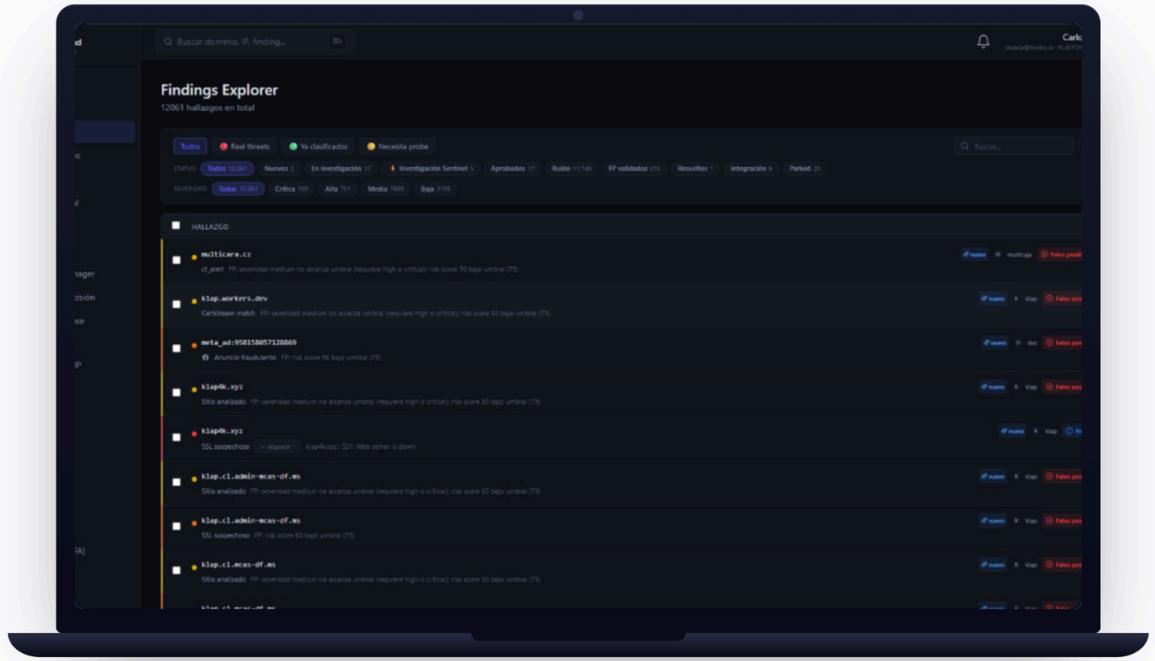
Suprime o degrada falsos positivos antes de molestar al cliente. **~90 % de findings son ruido** y nunca llegan al dashboard.

03 **Intelligence Sweep al onboarding**

Apenas se conecta la marca corre 8 steps OSINT (WHOIS post-leak, Shodan, BreachForums, prensa técnica…). **Valor desde el día 1**.

04 **Brand Attack Timeline**

Línea de tiempo con likelihood + bandas de severidad. Recalculada automáticamente con cada hallazgo.



/FINDINGS — TRIAGE PRIORIZADO

128 ABIERTOS · 24 EN COLA

Lo que nos diferencia de Axur y ZeroFox.

Soberanía, costo y precisión auditable — diseñado desde LATAM, para los marcos regulatorios de LATAM.

6 diferenciales

01 Soberanía LATAM
Datos locales que no fluyen a USA ni Europa.

02 Stealer local-first
Únicos en procesar dumps sin enviar credenciales a un tercero.

03 Registries LATAM en tiempo real
NIC.cl, NIC.ar, Registro.br — los players globales llegan tarde.

04 Auto-investigation determinista
Evidencia auditable, no "black box LLM".

05 Takedown sub-6h
SLA agresivo gracias a evidencia pre-armada por el investigator.

06 Costo
~⅓ del benchmark Axur, a precio similar o menor.

6 controles de compliance

DET 100 % determinista
Sin LLM externo en el core — crítico para Ley 21.719, GDPR y CMF.

PII PII sanitization
Screenshots con OCR + blur antes de almacenarse.

AUD Audit log append-only
Triggers en DB rechazan UPDATE/DELETE — evidencia legal-grade.

RET Retention policies
Purga automática según la política del cliente.

MFA MFA + ARCOP + DPO
Controles para cumplimiento CL / EU integrados de fábrica.

LCL Soberanía LATAM
Datos en infraestructura local — sin pasar por USA / EU.

twoko
Offensive Prevention

¡Hablemos!

Estamos listos para diseñar el siguiente paso de tu programa de ciberseguridad. Cuéntanos qué necesitas — te respondemos en menos de 24 horas hábiles.

COMERCIAL
sales@twoko.io

SITIO WEB
twoko.io

SEDE
Santiago, Chile