CIBERSEGURIDAD, LA NUEVA ALFABETIZACIÓN

# Clases de seguridad digital desde 3°básico: la ofensiva chilena para frenar el phishing

Chile avanza en seguridad de la información, pero su mayor desafío sigue siendo educar a la población, debido a que los riesgos más graves provienen de hábitos básicos no corregidos. Para abordar este desafío, la ANCI plantea una agenda que combina regulación, diseño centrado en el usuario y educación desde la escuela.

IRINA TORO SALGADO

**A un año de la promulgación de la Ley Marco de Ciberseguridad (21.663), Chile cerró un ciclo clave en la construcción de su institucionalidad digital. La Agencia Nacional de Ciberseguridad (ANCI), que nació como un programa interno del Estado, hoy opera como regulador multisectorial con competencias sobre organismos públicos, bancos, telecomunicaciones, instituciones de salud y proveedores tecnológicos.**

A solo días de dejar la dirección nacional, Daniel Álvarez hace un balance optimista: "La ANCI pasó de ser una pyme del Estado a una autoridad con información diversa, que ahora recibe notificaciones de incidentes que afectan directamente a las personas. Antes veíamos solo los phishing contra Tesorería o el SII; hoy llegan casos de ciudadanos que perdieron sus claves o fueron engañados por llamados fraudulentos", precisa.

Chile figura entre los países más avanzados de América Latina y alcanzó el puesto 20 en el National Cyber Security Index. Pero ese liderazgo convive con amenazas básicas que nos hacen vulnerables.

Según los datos de la ANCI, el 40% de los incidentes reportados se origina en problemas de usuario y contraseña. Álvarez explica que esto no es solo una falla técnica, sino cultural:usuarios que repiten la misma clave en múltiples servicios, adultos mayores que siguen cayendo en estafas telefónicas y sistemas bancarios cuya usabilidad no siempre acompaña a quienes tienen menos habilidades digitales.

"Un solo incidente puede comprometer 20 o 30 servicios distintos y usualmente cuesta dos veces más caro que las medidas preventivas que lo hubieranevitado. Nos digitalizamos sin hacernos la pregunta por la seguridad", resume.

La ausencia de doble autenticación (2FA) es otro punto crítico. Aunque es una medida simple y gratuita, de eficacia probada —reduce entre 70% y 95% el riesgo de intrusiones— su adopción sigue siendo baja.

Más grave aún es el diagnóstico sobre respaldos y planes de continuidad:empresas que tenían "todo respaldado", pero nadie sabía restaurarlo; planes de emergencia que existían solo en el papel; incidentes que pudieron resolverse en dos días y terminaron tomando un mes.

Uno de los hallazgos más complejos del año fue la evaluación del sector tecnológico.De más de 60 mil empresas analizadas a partir de datos del SII y Chile-Compra, solo 1% clasificó preliminarmente como Operador de Importancia Vital (OIV). Cientos presentaron oposiciones y muchas aseguraron que "la ciberseguridad no es parte de su negocio".

> *La ANCI está trabajando en tres frentes: definición de perfiles profesionales y técnicos, contenidos en educación básica, y formación en seguridad en Liceos Técnicos Profesionales.*

Para Álvarez, esto revela un problema estructural: "La industria TI está en un nivel de madurez muy bajo. Muchos proveedores no ven que, aunque solo desarrollen código o revendan software, sostienen operaciones críticas del país. Es como la minería en los años 2000: hoy no entras a una faena sin estándares, y TI debe moverse hacia eso".

## Coordinación entre sectores

Las campañas de phishing afectan por igual a bancos, compañías de telecomunicaciones, comercio y fintech. Pero hasta ahora, cada sector respondía por su cuenta. Para enfrentar esto, la ANCI articuló una mesa integrada por los reguladores de telecomunicaciones, comercio, bancos, instituciones financieras y gremios, con el objetivo de entregar una respuesta rápida y transversal: bloquear en horas —y no en días— campañas maliciosas que circulan por mensajes, llamadas o redes sociales.

La ENUSC 2024 confirma la urgencia. Los delitos digitales subieron con fuerza en un año: los fraudes de 5,3% a 7,6%; las estafas, de 3,3% a 3,7% y la victimización de hogares por delitos digitales, de 8,3% a 11%.

La ANCI también cambió su forma de comunicarse.De mensajes técnico dirigido a especialistas, pasó a una comunicación masiva centrada en los riesgos cotidianos, que incluye campañas en redes sociales con mensajes breves y pedagógicos, el uso del CiberPudú como personaje educativo, el Fono 1510 para reportar phishing, y materiales para adultos mayores y niños. "Tuvimos que cambiar la forma de comunicar, porque ahora el mensaje le llega directamente al ciudadano", explica Álvarez.

## Habilitación en la educación ténico-profesional

El legado más estructural de la ANCI puede estar en el ámbito educativo, donde se está trabajando en tres frentes: definición de perfiles profesionales y técnicos, contenidos en educación básica y formación en seguridad en Liceos Técnicos Profesionales.

Primero, y a petición del Ministerio de Hacienda, junto a ChileValora y SENCE se definieron diez perfiles de especialistas que se necesitan en materia de ciberseguridad para las empresas e instituciones, los que hoy sirven de referencia para la educación técnica y superior.

Segundo, basándose en un modelo de laboratorios de ciberseguridad implementado en escuelas secundarias de Colorado, Estados Unidos, Chile prepara una malla de ciberseguridad para liceos técnico-profesionales con el objetivo de formar analistas de nivel uno directamente desde la educación media, lo que juicio de Álvarez, tendrá un impacto social enorme: "Un analista básico gana cerca de $800 mil. Para un joven recién egresado, eso cambia la trayectoria de vida", advierte.

De hecho, un piloto realizado con diez jóvenes madres en un colegio de Renca hace dos años ya mostró resultados: la mitad de ellas están trabajando en el sector.

Y tercero, la ANCI junto al Ministerio de Educación también impulsa la incorporación de seguridad digital y protección de datos en el currículum escolar, desde tercero básico. Si bien es un proyecto de más largo plazo, cuenta con evidencia internacional clara:la educación temprana es la única forma de reducir el riesgo estructural.

Chile ha construido una institucionalidad sólida, reconocida internacionalmente. Pero la modernización técnica no basta si la cultura digital no cambia. "Somos un referente en la región, pero aún nos enfrentamos a problemas básicos. La seguridad digital no es solo tecnología: es educación, hábitos y sentido común", concluye Daniel Álvarez.

El desafío para los próximos años será doble: seguir fortaleciendo la regulación y, al mismo tiempo, alfabetizar en seguridad digital a toda una sociedad que entró al mundo digital sin manual de instrucciones.

"Tuvimos que cambiar la forma de comunicar, porque ahora el mensaje le llega directamente al ciudadano", explicó Daniel Álvarez, director de la ANCI

COMERCIO DIGITAL Y SISTEMAS DE PAGO

# Integraciones: el motor del auge del e-commerce

Según cifras del Banco Central, Chile registra más de 374 pagos digitales anuales por persona, con un crecimiento de más de un 18% en el último año.

CRISTIÁN MÉNDEZ

La integración entre plataformas de comercio digital y sistemas de pago se ha convertido en el esqueleto tecnológico que sostiene al e-commerce moderno. Este concepto, que muchas veces opera de forma invisible para el usuario, "permite que una tienda online y un sistema de pago funcionen como si fueran una sola cosa", explica Ricardo Fuentes, director de Ingeniería Comercial de la Universidad Andrés Bello sede Concepción.

La pandemia aceleró esta dinámica. Con las restricciones sanitarias, miles de comercios vieron en lo digital no solo una oportunidad, sino la única forma de seguir vendiendo. Ese salto masivo demandó plataformas capaces de ofrecer pagos rápidos y confiables, exigencia que se mantienen.

"Hoy, la experiencia del usuario no se mide solo por la calidad del producto, sino por la fluidez y confianza en el proceso de pago. Si un cliente percibe riesgo o complejidad al pagar, la tasa de abandono aumenta", enfatiza Ricardo Blümel, gerente División Negocios y Productos de Transbank.

A medida que esta adopción se masificó, también se evidenciaron los beneficios económicos y operativos. Ricardo Fuentes detalla que se "han reducido costos de transacción y permitido que una pyme compita en igualdad de condiciones" con otros comercios.

Menos manejo de efectivo, menos errores administrativos y la posibilidad de vender a cualquier lugar del país se transformaron en ventajas decisivas, impulsando además la inclusión financiera. Según el académico, "muchas personas que antes dependían del efectivo hoy pueden participar plenamente del comercio digital", clave para sostener un sistema que, según cifras del Banco Central, registra más de 374 pagos digitales anuales por persona y que según proyecciones de la Cámara de Comercio de Santiago este 2025 superará los $9 billones en ventas, lo que representaría un aumento del 10% respecto a 2024.

Foto: La experiencia del usuario no se mide solo por la calidad del producto, sino por la fluidez y confianza en el proceso de pago.

Ese contexto es el que explica la relevancia de integraciones como la recientemente desplegada entre Shopify y Transbank. Shopify es una de las plataformas de comercio electrónico más utilizadas en el mundo: permite a emprendedores crear tiendas online completas sin conocimientos técnicos avanzados. Al integrar Webpay Plus, esos mismos negocios pueden activar un sistema de pago seguro, local y reconocido.

"En este contexto, como compañía nos aseguramos de que en cada integración que implementamos se incorporen los más rigurosos estándares de seguridad, brindando tranquilidad tanto a comercios como a consumidores", destaca el ejecutivo de Transbank.

Para emprendedores, esto implica vender desde el celular y recibir pagos de tarjetas de débito, crédito o prepago en segundos. Y, según adelanta Blümel, este es solo el comienzo: "Seguiremos trabajando en integraciones y colaboraciones estratégicas que contribuyan a transformar el ecosistema de pagos en Chile".

Un ciberataque cada 11 segundos se produce en el mundo y cada vez son más sofisticados debido al uso de IA.

CIBERDEFENSA COGNITIVA DISTRIBUIDA

# La ciberseguridad avanza hacia sistemas nerviosos digitales de defensa

A través de IA es capaz de percibir, analizar y actuar en tiempo real, donde todas las herramientas funcionan como sensores.

CRISTIÁN MÉNDEZ

La aceleración de los ciberataques impulsados por IA ha obligado a la ciberseguridad a replantear su arquitectura de defensa. Diversos estudios e informes detallan que en el mundo se produce un ataque cada 11 segundos "y cada vez son más sofisticados debido al uso de IA", comenta Héctor Muñoz, jefe de Seguridad Digital de la Universidad de Talca.

Este hecho ha provocado una reconfiguración a nivel global de la protección tecnológica que está dejando atrás el enfoque tradicional basado en firewalls, SOC y análisis centralizado por uno que convierte la seguridad "en un sistema nervioso digital capaz de percibir, analizar y actuar en tiempo real, donde todas las herramientas funcionan como sensores y una capa cognitiva integra señales, recuerda incidentes y consulta inteligencia externa para responder de forma automática y proactiva", explica Germán Rodríguez, CTO de Tenpo.

Es lo que se conoce como Ciberdefensa Cognitiva Distribuida en la cual los sistemas -agrega Héctor Muñoz- deben "aprender, adaptarse y colaborar como redes neuronales" para avanzar así "hacia una ciberseguridad realmente resiliente a través también del uso de la IA".

Una de las primeras fintech chilenas en adoptar este modelo es Tenpo, hecho que incluso les significa ganar el premio Plata en los Premios Fintech a los Innovadores Financieros en las Américas 2026.

Su CTO destaca que esta tecnología automatiza "más del 90% de los casos, reduce cientos de horas operativas y ofrece una protección profunda y escalable, similar a un sistema inmune que anticipa y neutraliza ataques de alta velocidad". Esto ha permitido a Tenpo responder a comportamientos anómalos en segundos, con prevención de fraudes, bloquea amenazas antes de que estas se materialicen", destaca.

Rodríguez detalla que esta arquitectura "extiende una capa de seguridad inteligente hasta la App, identificando incluso atacantes con IOCs humanos". Según explica, esta capacidad permite asegurar transacciones sin fricción, manteniendo la experiencia del cliente intacta un aspecto crítico en un mercado donde la confianza es un activo estratégico.

Sin embargo, implementar esta tecnología a gran escala no es trivial. Rodríguez reconoce que "el primer choque son los costos de integración", ya que las empresas suelen acumular múltiples plataformas que no conversan entre sí. También advierte sobre la escasez de talento especializado y la importancia de definir una gobernanza robusta: "Si vas a automatizar decisiones importantes, tienes que dejar claríisimo qué puede hacer la automatización sola y cuándo debe intervenir un humano", comenta.

EDITOR: Arturo Catalán A.; SUBEDITORA: Camila Miranda K.; REDACTORES: Claudia Betancourt, Cristián Méndez, Irina Toro, Trinidad Valenzuela
DISEÑO: Estudio Pixel; FOTOGRAFÍA: Hypo Photos; GERENTE COMERCIAL: Juan Carlos Encina; EJECUTIVO COMERCIAL: Juan Carlos Herrera; REPRESENTANTE LEGAL: Alejandro Arancibia;
DIRECCIÓN: Avenida Santa María 5542, Santiago de Chile; TELÉFONO: 22330 1221; CORREO: finanzasytecnologia@mercurio.cl