LITORALPRESS

Fecha: 03-02-2026
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Columnas de Opinión
Título: Columnas de Opinión: Cibercrimen: La distracción veraniega es el mejor negocio

Pág. : 4
Cm2: 197,8

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Cibercrimen: La distracción veraniega es el mejor negocio

MÓNICA RETAMAL F.

PLAZA de IDEAS

US$ 130 cuesta hoy hackear una cuenta de Facebook; US$ 162 una de Gmail y US$ 500 una casilla corporativa (BCG, 2025). Cuando los delitos tienen precios de referencia, oferta segmentada y servicios a la medida, ya no estamos frente a un problema técnico, sino ante un mercado ilícito establecido que no se sostiene con *hackers* solitarios, sino con organizaciones criminales que se aprovechan de la distracción y baja alfabetización digital de sus víctimas. De hecho, las mediciones siguen tratando estos delitos como un fenómeno aislado, sin capturar la sensación de inseguridad digital que acompaña la vida cotidiana de millones de chilenos que —en su mayoría— consideran que ser estafado digitalmente es algo "inevitable" (Mastercard, 2025).

En Chile, los delitos más denunciados son estafas y uso malicioso de tarjetas (Fiscalía, 2025). En 2024 se registraron casi cinco veces más ataques que en 2023 (FortiGuard Lab), lo que significa que el ruido escaló exponencialmente y fue automatizado, personalizado y más barato gracias a la IA, estimándose un daño económico mundial de US$ 10,5 billones (10% más que en 2024, según Cybersecurity Ventures).

Los sectores más expuestos son los de uso cotidiano: gobierno, banca, *retail*, salud. Y el escalón más débil es el usuario y su forma descuidada de manejar sus cuentas: contraseñas recicladas, apertura de enlaces con tono urgente y excesiva confianza en mensajes recibidos que "parecen legítimos". Por eso no sorprende que estafas tradicionales, como "el cuento del tío", hayan mutado con tanto éxito a WhatsApp, correo o redes sociales, con datos filtrados y mensajes cada vez más verosímiles. Los períodos de menor vigilancia —vacaciones, feriados, viajes— amplifican las amenazas existentes, porque cambian nuestros hábitos con más conexiones móviles, más redes públicas y menos verificación.

Chile invierte apenas el 0,08% de su PIB en ciberseguridad, menos de la mitad del promedio mundial (BCG, 2025), y a nivel institucional la respuesta sigue siendo incipiente y profundamente asimétrica. Aunque el país dio un paso relevante con la Ley Marco de Ciberseguridad y la creación de la Agencia Nacional de Ciberseguridad, el foco se concentra en organismos públicos, servicios esenciales y operadores de importancia vital. Sin embargo, deja fuera al 97% del tejido productivo: las pymes. Estas no cuentan con presupuestos, personal ni herramientas para prevenir, detectar o recuperarse de incidentes, operando sin monitoreo, respaldos robustos ni protocolos de respuesta. A diferencia de países OCDE, donde la política pública combina regulación con financiamiento, asistencia técnica y alfabetización masiva, en Chile la ciberseguridad sigue abordándose como un problema sectorial y no sistémico, generando una brecha riesgosa entre lo que la ley exige y lo que miles de organizaciones —y sus usuarios— pueden efectivamente cumplir.

Frente a un delito industrializado y automatizado, debemos instalar capacidades a todo nivel y desarrollar una comprensión social del riesgo que haga menos rentable el engaño. De lo contrario, cualquier ley será siempre insuficiente. Porque la ciberseguridad ya no es solo un problema técnico ni policial, sino ciudadano y la confianza digital se construye, se practica y, sobre todo, se enseña.