Crónica Chillán

Fecha: 16/03/2026 Audiencia: 7.200 Sección: OPINION
Vpe: $149.068 Tirada: 2.800 Frecuencia: 0
Vpe pág: $664.000 Difusión: 2.800
Vpe portada: $664.000 Ocupación: 22,45%

C

Columna

Carolina Leal
Ingeniera estadística y Máster en Finanzas,
experta en análisis de datos y riesgos digitales

Una responsabilidad colectiva

Qué cómodo resultaba pensar que la ciberseguridad era un problema que debían solucionar los especialistas: ingenieros, expertos en tecnología o equipos de TI dentro de las organizaciones. Pero esto es insuficiente, hoy debemos estar conscientes de nuestro rol y responsabilidad. Parte importante de nuestras actividades cotidianas las hacemos en línea, comunicación, compras, trámites, etc. Y si dejamos entrar una vulnerabilidad, entonces el sistema completo se ve afectado, similar a lo que pasa con los sistemas de salud.

La evidencia apunta en esa dirección. Diversos estudios citados por el Foro Económico Mundial y por informes de la industria señalan que la gran mayoría de los incidentes de ciberseguridad involucran el factor humano, ya sea por errores, descuidos o engaños mediante técnicas de ingeniería social. Ahora bien, no significa que las personas seamos el problema, sino que somos el puente que encontraron los atacantes para llegar a vulnerar los sistemas, persuadir a alguien les resulta más fácil, que vulnerar directamente un sistema tecnológico.

Por eso, los hábitos digitales individuales importan más de lo que parece. Reutilizar la misma contraseña en múltiples servicios, o pegarla en un post-it de la pantalla del computador (¡es que lo he visto!), ignorar actualizaciones de seguridad o compartir información sensible sin verificar la fuente son prácticas que amplían la superficie de riesgo para todo el sistema.

Algo similar ocurre en salud pública. Las vacunas, las campañas de prevención y las medidas sanitarias funcionan mejor cuando existe una conciencia colectiva sobre su importancia. En el ámbito digital sucede lo mismo. La resiliencia frente a ataques no se construye únicamente con tecnología, sino con cultura de seguridad.

Hoy cada persona administra una cantidad creciente de información digital: datos financieros, cuentas de comercio electrónico, redes sociales, fotografías, documentos personales y hasta historiales médicos. Esa información tiene valor económico, y donde hay valor aparecen incentivos para robarla o explotarla.

Acciones simples pueden marcar una diferencia significativa: utilizar contraseñas robustas y únicas, activar autenticación multifactor, desconfiar de mensajes urgentes que solicitan información personal y verificar la legitimidad de enlaces o aplicaciones antes de interactuar con ellos.

Y como un verdadero antes y después hablamos de la pandemia. En particular, en nuestros trabajos, la seguridad informática estaba centrada en proteger redes corporativas o servidores internos. Antes, el perímetro era relativamente claro. Después, ese límite prácticamente desapareció. Las organizaciones operan con trabajo remoto, servicios en la nube, dispositivos personales y múltiples plataformas digitales. Y aquí el usuario pasa a formar parte del sistema de defensa.

Las instituciones y las relaciones sociales dependen cada vez más de infraestructuras digitales. Mantener la confianza en ese ecosistema es un desafío colectivo.