LITORALPRESS

Fecha: 20-05-2026
Medio: La Prensa de Curicó
Supl. : La Prensa de Curicó
Tipo: Cartas
Título: Cartas: La resiliencia digital dejó de ser un problema tecnológico

Pág. : 9
Cm2: 165,6

Tiraje: 4.200
Lectoría: 12.600
Favorabilidad: No Definida

La resiliencia digital dejó de ser un problema tecnológico

CRISTÓBAL PÉREZ.
AI & Data Science Engineer de ComparaOnline

La fragilidad digital suele hacerse visible demasiado tarde. Una caída de sistema, una filtración, un fraude masivo o una interrupción operacional bastan para demostrar que la conectividad dejó de ser una comodidad y se transformó en infraestructura crítica para personas, empresas y mercados.

Durante años, la ciberseguridad fue tratada como una conversación técnica, reservada para áreas de sistemas, proveedores especializados o comités de tecnología. Ese enfoque quedó corto. Hoy la resiliencia digital es un asunto financiero, reputacional, operacional y, sobre todo, de confianza.

El World Telecommunication and Information Society Day 2026, celebrado este mes, pone el foco precisamente en las "líneas de vida digitales", una idea que resume bien el momento actual: los sistemas conectados ya no son solo canales de eficiencia. Son redes que sostienen pagos, salud, educación, comercio, logística, atención ciudadana y vínculos esenciales entre organizaciones y personas.

El problema es que la velocidad de adopción digital ha sido mucho mayor que la capacidad de comprensión del riesgo. Muchas empresas digitalizaron procesos sin rediseñar su cultura de prevención. Se movieron rápido para vender, atender o automatizar, pero no siempre con el mismo rigor para proteger datos, asegurar continuidad o preparar respuestas frente a incidentes.

Esa brecha se vuelve especialmente delicada cuando los usuarios ya no distinguen entre falla técnica y falla de confianza. Para una persona, que una plataforma no responda, que una cuenta sea vulnerada o que una transacción falle no es un "incidente tecnológico". Es una experiencia directa de desprotección.

En ese sentido, la resiliencia digital debe ser entendida como una capacidad institucional. No basta con firewalls, contraseñas o seguros de ciberseguridad. Se requiere gobernanza, entrenamiento, protocolos, comunicación, trazabilidad y una cultura que entienda que el riesgo digital no vive en un área específica, sino en toda la organización.

El consumidor también está cambiando. La mayor exposición a fraudes, suplantaciones y compras digitales fallidas está generando usuarios más cautelosos. Comparan más, revisan reputación, buscan medios de pago protegidos y esperan respuestas rápidas cuando algo sale mal.

Para las empresas, esto abre una discusión mayor: la seguridad digital ya no será evaluada únicamente por especialistas, sino por clientes, reguladores, inversionistas y medios. La resiliencia será una señal de gestión. Y su ausencia, una señal de vulnerabilidad.

El desafío, por lo tanto, no consiste solo en evitar ataques. Consiste en construir sistemas capaces de resistir, recuperarse y explicar lo ocurrido sin destruir confianza en el proceso. En la economía digital, el silencio, la opacidad y la improvisación pueden ser tan dañinos como la falla original.

La próxima etapa de la transformación digital tendrá menos que ver con adoptar herramientas y más con demostrar confiabilidad. Las organizaciones que entiendan esto dejarán de mirar la resiliencia como costo y comenzarán a verla como una condición básica para operar en entornos permanentemente expuestos.