Ciberseguridad ambidiestra: el equilibrio entre control e innovación que exige la nueva era digital

Por José Lagos,Docente Facultad de Economía y Negocios Universidad de Chile.

Durante años, la ciberseguridad fue entendida principalmente como una función de control: políticas, firewalls, monitoreo, gestión de accesos, cumplimiento normativo, auditorías y respuesta ante incidentes. Todo eso sigue siendo esencial. Sin embargo, en la nueva era digital, marcada por inteligencia artificial, ataques automatizados, ransomware, deepfakes, ingeniería social avanzada y riesgos en la cadena de suministro, proteger lo conocido ya no basta. Las organizaciones también necesitan aprender, experimentar y anticiparse. Aquí surge un concepto clave para la estrategia moderna de ciberseguridad: la ambidestreza organizacional. Una organización ambidiestra es aquella capaz de equilibrar dos capacidades que suelen competir entre sí: la explotación y la exploración. La explotación consiste en aprovechar y perfeccionar lo que ya existe. En ciberseguridad, esto significa fortalecer controles, estandarizar procesos, cumplir regulaciones, capacitar usuarios, monitorear eventos, gestionar vulnerabilidades y mantener la continuidad operacional. Es la dimensión del orden, la eficiencia y la disciplina. La exploración, en cambio, apunta a descubrir nuevas formas de protegerse. Incluye pilotos de inteligencia artificial, threat hunting, simulaciones de ataques, modelos predictivos, automatización de respuestas, nuevas arquitecturas de seguridad y análisis avanzado de amenazas emergentes. Es la dimensión del aprendizaje, la innovación y la adaptación. El desafío estratégico es que muchas organizaciones se inclinan demasiado hacia uno de estos polos. Algunas son muy sólidas en explotación: tienen políticas, comités, matrices, controles y reportes, pero poca innovación defensiva. Otras exploran intensamente nuevas tecnologías, pero no siempre logran institucionalizarlas en procesos, métricas, responsables y evidencias. En ambos casos, existe una brecha. La ciberseguridad ambidiestra busca resolver esa tensión. No se trata de elegir entre control o innovación, sino de integrar ambos mundos. Una organización verdaderamente madura no solo demuestra que tiene controles, sino que también es capaz de cuestionarlos, adaptarlos y rediseñarlos frente a amenazas cambiantes. Este enfoque puede ser evaluado incluso mediante procesamiento de lenguaje natural (NLP). Los reportes corporativos, memorias anuales, políticas, informes de auditoría y reportes de riesgo contienen señales sobre cómo una organización entiende su ciberseguridad. Cuando el lenguaje se concentra en cumplimiento, políticas, monitoreo y auditoría, predominan señales de explotación. Si aparecen conceptos como innovación, automatización, inteligencia artificial, simulación, threat intelligence o nuevas capacidades, emergen señales de exploración. Un análisis documental basado en NLP permite clasificar a las organizaciones en cuatro estados: supervivencia, cuando existen bajas señales de exploración y explotación; investigación, cuando predomina la exploración, pero falta consolidación; reforzamiento, cuando hay controles sólidos, pero baja innovación; y balance, cuando la organización combina ambas capacidades. Este último representa el estado ambidiestro. La conclusión es clara: la ciberseguridad del futuro no será solo una función técnica ni un requisito de cumplimiento, sino que deberá tener la capacidad de adaptación continua. Los directorios, Director de Seguridad de la Información (CISO), Delegado de Protección de Datos (DPO), auditores y gerentes de riesgo, deberán preguntarse no solo si la empresa está protegida hoy, sino si está aprendiendo lo suficiente para defenderse mañana. Porque en ciberseguridad, defender sin innovar conduce a rigidez e innovar sin controlar lleva a la dispersión. La ventaja estratégica estará en lograr ambas cosas al mismo tiempo.