

La mayor amenaza digital es la ciberseguridad

Hernán Orellana, profesor de la Escuela de Administración, Facultad de Economía y Administración PUC*

Las amenazas y eventos de ciberseguridad registrados en Chile se han duplicado en el primer semestre del año 2023 comparados con los mismos datos del año 2022. Según un estudio de EY, Chile se encuentra por debajo de la media latinoamericana y mundial en número de incidentes y filtración de datos. Estos delitos representan a nivel mundial, en términos de beneficio económico, el doble del lucro del narcotráfico.

Frente a esta realidad, se hace hoy urgente para todas las organizaciones llevar adelante un plan de ciberseguridad que les permita proteger sus activos de información, que son críticos para su operación y protección. Este plan de ciberseguridad debe incluir la generación de una política de ciberseguridad por parte del directorio de la organización, quién además debe asegurar que los recursos económicos y humanos estén disponibles para ejecutar la política, junto con desarrollar un sistema de gestión que permita ir midiendo en el tiempo en el avance del plan, con indicadores de gestión y cierre de brechas que permitan reconocer dicho avance.

Sin este plan ni las acciones derivadas, las organizaciones no tienen las herramientas necesarias para responder a las crecientes amenazas, poniendo en riesgo su actividad, a sus clientes, empleados y a sus proveedores. En una mirada más amplia, la falta de sistemas de gestión de ciberseguridad, públicos y privados, son un gran riesgo para la transformación digital del país, porque traicionan los estándares mínimos de confianza pública en los sistemas digitales. El gran motivador de la transformación digital es la experiencia del usuario, que por razones de ciberseguridad puede verse afectada.

En el marco legal, tenemos que la nueva ley 21.459 de ciberseguridad puso a Chile al día internacionalmente y agregó nuevos delitos informáticos como el de Receptación de Datos Informáticos, que castiga a quién utilice o almacene datos obtenidos ilícitamente, y el de Fraude Informático. Sin embargo, desde el punto de vista de las empresas, la principal novedad de esta ley es que agregaron los delitos informáticos a la ley 21.393, que persigue la responsabilidad penal de las personas jurídicas. Por lo tanto, las empresas deben incorporar en sus modelos de prevención del delito penal a estas nuevas tipologías de delitos.

Desde el punto de vista de la confianza de sus clientes, la reputación empresarial y la responsabilidad legal, la atención a la ciberseguridad y la gestión de sus riesgos es un imperativo para los directorios.

Hernán Orellana es Director de empresas y asesor en digitalización e innovación, con amplia experiencia en gobierno corporativo, ética de negocios y sustentabilidad. Director en BCI.