CHILETECNOLÓGICO
30/05/2025 Audiencia: 320.543 Sección: SOCIEDAD
$7.541.031 Tirada: 126.654 Frecuencia: SEMANAL
$20.570.976 Difusión: 126.654
ada: $20.570.976 Ocupación: 36,66%

COLUMNA DE OPINIÓN

Tres desafíos para los CEO en torno a ciberseguridad

NICOLÁS GOLDSTEIN,
presidente ejecutivo de Accenture Hispanoamérica

En estos tiempos en que todo pasa por lo digital, hablar de ciberseguridad ya no es solo cosa del equipo de tecnología de las empresas. Hoy, los gerentes generales —los CEO— tienen un rol que no pueden seguir postergando. Con la nueva Ley de Protección de Datos Personales y la Ley Marco de Ciberseguridad, la responsabilidad ya no se puede delegar. Y eso trae tres desafíos clave para quienes lideran compañías actualmente en Chile.

El primer gran desafío es entender de qué estamos hablando; comprender el lenguaje y los riesgos de la seguridad informática. Hoy, saber de ciberseguridad no es opcional para los altos ejecutivos. En un estudio reciente de Accenture, 96% de los CEO a nivel global dijo que la ciberresiliencia es clave para el crecimiento de sus empresas, pero solo 33% contestó tener conocimientos sobre el tema. Esto es como ser el capitán de un barco y no saber leer el radar. Puede que tengas una gran tripulación, pero si no sabes hacia dónde te diriges ni cómo detectar una tormenta, el naufragio es cosa segura.

Además, los gerentes generales deben estar preparados en ciberseguridad no solo porque la ley lo exige —aunque, ojo, las multas pueden llegar al 4% de los ingresos anuales—, también porque los clientes hoy demandan que las empresas protejan sus datos. Y si no lo hacen, pierden la confianza. Por ejemplo, en otro estudio que realizamos en Accenture, 65% de los chilenos afirmó que cambiaría de banco si supiera que su información fue vulnerada. La confianza se construye lentamente, pero puede perderse en un clic.

El segundo desafío es invertir en serio. Adoptar nuevas tecnologías para proteger los datos no es un lujo, es una necesidad. Sin embargo, muchos no están invirtiendo de manera integral, lo hacen para áreas de negocio o proyectos específicos. Esto es como instalar una puerta blindada y dejar las ventanas abiertas. La seguridad tiene que ser total, no parcial.

En ese sentido, las empresas deben avanzar hacia un enfoque de "confianza cero" (o *zero trust*). Es decir, no confiar en nadie, por defecto, ni siquiera dentro de la red corporativa. Cada acceso debe verificarse, siempre. Así también, el CEO debe trabajar de la mano con el *chief data officer* y el CISO (el encargado de seguridad de la información). No basta con contar con buenas herramientas: se necesita gobernanza, protocolos claros y, sobre todo, saber quién es responsable de cada eslabón de la cadena.

También es clave anticiparse. En Chile, la nueva legislación exigirá contar con modelos de prevención de infracciones y reportes ante la futura Agencia de Protección de Datos. No hacerlo puede tener consecuencias legales, financieras y reputacionales.

El tercer desafío —y quizás el más difícil— es impulsar una cultura organizacional en torno a la ciberseguridad. A pesar de su importancia, solo 15% de los CEO encuestados por Accenture dijo haber dedicado reuniones de directorio a hablar de este tema, y 54% cree que invertir en estrategias de seguridad cuesta más que un ciberataque.

Pero la realidad es otra. Una filtración de datos puede generar daños irreparables en la confianza del público. Y esa confianza, una vez perdida, no se recupera fácilmente, si es que se recupera. Esto es como dejar la puerta de tu casa entreabierta, porque crees que vives en un barrio tranquilo. Puede que nada pase por mucho tiempo, pero el día en que algo ocurra, el impacto no será solo material; es la tranquilidad la que se pierde, y recuperarla es mucho más difícil.

Por eso, capacitar a los equipos, promover buenas prácticas y hablar de estos temas de forma abierta es esencial. Así como se discute el clima laboral o las metas del trimestre, se debe discutir sobre amenazas digitales, planes de respuesta y protocolos frente a incidentes.

El mensaje es claro: la ciberseguridad no es un tema de sistemas, es un tema de negocio. Y los CEO que lo entiendan a tiempo serán los que marquen la diferencia.

ADEMÁS DE QUE LA LEY LO EXIGE, LOS GERENTES GENERALES deben estar preparados en seguridad cibernética porque los clientes hoy demandan que las empresas protejan sus datos.

> "En un estudio reciente de Accenture, 96% de los CEO a nivel global dijo que la ciberresiliencia es clave para el crecimiento de sus empresas, pero solo 33% contestó tener conocimientos sobre el tema. Esto es como ser el capitán de un barco y no saber leer el radar".