La urgencia de concientizar sobre la gobernanza de datos

No cabe duda de que el último año ha sido complejo para muchas empresas e instituciones en términos de ciberseguridad. Y es que, a la fecha, son cientos los trámites, procesos y soluciones que se han digitalizado: pagos de cuentas, solicitud de permisos e información personal de instituciones y personas.

En este nuevo escenario, **la gobernanza de los datos se ha convertido en una labor crítica que requiere control y regulación desde adentro.** Es decir, dejarlo fuera de la estrategia de negocio hoy es un error garrafal ya que implica mayor riesgo de vulnerabilidades, filtraciones de datos y robo de información que puede afectar a la confiabilidad y visibilidad de una compañía.

Con la digitalización de los trámites, hay empresas y negocios que tienen sus datos críticos expuestos sin saberlo. Es por ello que minimizar los riesgos con soluciones de gobernanza de datos que se preocupen del ciclo completo de la información, es clave: almacenamiento, accesos, control y plan de crisis en caso de filtración.

Ciertamente, a Chile le falta camino por recorrer. Pero l**a verdad es que ningún país en el mundo tiene el camino 100% listo.** Hoy, poco a poco hay mayor concientización sobre la importancia de educar y crear nuevas políticas y métodos de enseñanza a una ciudadanía más digital. Y es que el recorrido es largo ya que implica responsabilidades más allá de una nube o manipular información delicada, requiere de concientización sobre nuestra identidad digital.

El proceso de digitalización fue bastante más vertiginoso que el de protección. Este último, es el que ahora se debe potenciar, lo que conlleva a maximizar los niveles de control respecto a la información.

Educando al ciudadano digital

Las empresas y las personas se digitalizaron con mucha agilidad y rapidez, lo que ocasionó un cambio para siempre. La presencialidad seguirá existiendo, pero la necesidad de que tanto personas, escuelas, gobierno e instituciones estén preocupados de la gobernanza de datos y protección de su identidad digital podrá determinar el futuro de la ciberseguridad en el país.

Para ello, **la educación es clave**. Si bien, previo a la pandemia existió una restricción con respecto al uso de pantallas en niños menores de quinto básico, hoy esa limitación ya no es válida. La educación actual es en base a una pantalla con internet y frente a un montón de estímulos y amenazas.

El paradigma debe cambiar. **Un niño hoy tiene la capacidad de formarse y crecer con herramientas digitales, con mayor facilidad que el adulto.** De hecho, actualmente, son los niños y jóvenes quienes ayudan a las personas mayores a entregar datos, sacar la clave única y solicitar permisos. Se ha impulsado a que ese control de datos sea personal, pero en el fondo, hay muchas personas que dependen de otras.

Mecanismos de concientización

Hay que comprender que la ciberdelincuencia es un negocio. Si bien la enseñanza desde el colegio podría resultar clave, también **es necesario que el adulto conozca los riesgos y los evite.** Para ello, es necesario considerar que no todos los ciudadanos son digitalizados, y muchos lo son a la fuerza.

Sin duda, debe existir una política que regule ciertos estándares y procesos y que pueda entregar recursos para esto. **Un recurso viable y pertinente es la masificación a través de las municipalidades.** Al ser organismos pequeños, pueden acceder a grupos de ciudadanos a través de programas de digitalización y ciberseguridad.

No hay que dejar de lado la necesidad de crear conciencia a través de las vivencias. Tanto pymes como personas naturales, no creen que puedan ser víctimas de ataques de seguridad, pero lo cierto es que estas amenazas están siendo cada vez más dirigidas a estos grupos. Un buen método de reacción es la simulación, hacer creer al empleado de una empresa que cayó ante un phishing, o bien, con mecanismos de comunicación a través de propagandas.

Un largo camino hacia una cultura cibersegura

El desafío es grande y no será inmediato. Esta gobernanza debe ser parte del sello de toda institución, quienes son las primeras que deben estar absolutamente concientizadas y estar al día con los controles que podrían afectar a su negocio.

La ciberseguridad, así como la seguridad física, es cíclica y debe ir evolucionando al igual que un espiral. **Se requiere de voluntad y la capacidad de crear conciencia en el usuario.** Una vez que éste acceda a una aplicación o información, inmediatamente habrá que incorporar ciberseguridad, no es una cosa primero y luego la otra, debe ser una condición.

Chile sigue liderando en la región en cuanto a digitalización y ciberseguridad. De hecho, el Gobierno acaba de anunciar una Agencia Autónoma de Datos Personales, organismo público, de carácter técnico, autónomo, descentralizado, con personalidad jurídica y patrimonio propio. Ante amenazas cada vez más sofisticadas y profesionales, hay que controlar y monitorear, para bien o para mal. La clave está en no quedarse atrás en la carrera.