Carlos Travezaño: La vacuna digital

La “nueva normalidad” impuso a los negocios y gobiernos una nueva tarea: incrementar la confianza en plataformas digitales. A medida que la pandemia sigue retando a los sistemas de salud, políticos, económicos y sociales; otra amenaza invisible se acelera: los ataques cibernéticos.

Cada vez más, nuestra vida depende de actividades digitales: transacciones financieras, teletrabajo, compras online, etc. Por ello, necesitamos madurar una conciencia colectiva de los riesgos a los cuales estamos expuestos.

A inicios del 2021, el BID indicó que los daños económicos provenientes de ataques en red, en algunos países, podrían llegar a sobrepasar el 1% del PBI; y en naciones con infraestructura crítica, podría alcanzar hasta un 6%. **Este riesgo hace necesaria la implementación de una política integral sobre ciberseguridad, para salvaguardar la privacidad y propiedad de sus usuarios.**

 Alonso Segura: “El modelo económico se puede ajustar sin un cambio constitucional”

 Gonzalo Galdos: Liderazgo en los tiempos de cambio

Mecanismos

En las empresas urge implementar mecanismos que consoliden la ciberseguridad frente a tendencias de la movilidad del trabajo. En marzo del 2020, cerca de 5,2 millones de huéspedes de una cadena global de hoteles se vieron afectado ciberdelincuentes accedieron –a través de la cuenta de dos empleados– a información confidencial.

En el 2018, también accedieron a su sistema de reservaciones robando más de 5 millones de números de pasaportes.

A inicios de la pandemia, Zoom tuvo que superar rápidamente sus problemas de seguridad para recuperar la confianza de sus usuarios y responder al mercado. **Logró incrementar sus ingresos en un 326%.** Un mayor acceso y uso de tecnologías requiere del fortalecimiento de una cultura de ciberseguridad e implementación de herramientas. El riesgo es constante.

Tecnologías

La adopción de tecnologías como IoT (Internet de las Cosas) también ha vuelto a los edificios vulnerables. Acceder y controlar virtualmente nuestros equipos e instalaciones tiene múltiples beneficios; pero a mayor conectividad, mayores serán los riesgos para mitigar.

En 2014, a través de un sistema HVAC, unos atacantes accedieron al sistema financiero de una cadena minorista y a la información de tarjetas de crédito de más de 40 millones de clientes.

Para disfrutar de los beneficios de la revolución industrial 4.0, la explosión del Big Data y el Data Analytics necesitamos políticas más sólidas, inversión en investigación, un trabajo más articulado entre Estado y empresas; **debemos cerrar la brecha de profesionales calificados, en 600.000 personas para Latinoamérica e instaurar una cultura de prevención entre nuestros colaboradores.**

Quizá no hay forma de contener al 100% los ciberataques, pero la prevención y reacción rápida es un esfuerzo no negociable.