PARA ENFRENTAR LA AMENAZA DIGITAL

NELSON GUILLÉN BELLO

Entre las noticias que nos llegan sobre las manifestaciones sociales en Chile, una pasa desapercibida. Mientras la presencia ciudadana en las calles aumentaba, la policía de Carabineros era víctima de un ataque cibernético: Información de distinto grado de sensibilidad fue hecha pública en el lapso de una semana.

No se trata de un fenómeno aislado. Sabemos de los temores que han surgido en España frente al riesgo de un "hackeo" o ataque cibernético a su red eléctrica. Hemos sido testigos de una masiva filtración de datos privados de usuarios de la aplicación Instagram. La interferencia de un poder extranjero en el proceso electoral norteamericano continúa acaparando titulares de prensa. Suma y sigue.

La cuarta revolución industrial, la revolución digital, ha traído consigo no sólo el desarrollo de una formidable variedad de servicios para las personas y avances científicos y productivos. Con ella también han hecho su aparición amenazas con las que apenas comenzamos a familiarizarnos. Una de estas es el desarrollo de tecnología y prácticas orientadas a obtener, contra la voluntad de sus propietarios y titulares, información privada o sensible que se encuentra almacenada en internet. Esta amenaza constituye un riesgo estratégico para países y organizaciones, además de atentar contra la privacidad de las personas y contra su derecho al uso de las tecnologías para acceder a niveles crecientes de bienestar.

Para hacer frente a estas amenazas, el gobierno del presidente Medina ha constituido el Consejo Nacional de Ciberseguridad, ha elaborado una Estrategia Nacional de Ciberseguridad estructurada en torno a desafíos regulatorios, de protección de infraestructuras críticas, y de educación y capacitación, así como ha creado el Centro Nacional de Ciberseguridad. El Banco Central ha liderado, en paralelo, un amplio esfuerzo por regular las condiciones de seguridad digital necesarias para el adecuado funcionamiento de la cadena de pagos en el país.

Pero no es suficiente. Es indispensable asegurar que cada uno de los sectores estratégicos del país cumpla con los mejores estándares de ciberseguridad para proteger la continuidad de sus operaciones y servicios, resguardar su infraestructura crítica y proteger los derechos de las personas.

Con ese desafío a la vista, y en nuestro rol de coordinadores del sector de telecomunicaciones en el Consejo Nacional de Ciberseguridad, desde INDOTEL hemos convocado a una Mesa Técnica de Trabajo junto a los principales proveedores de servicios del sector en conjunto con representantes del Centro Nacional de Ciberseguridad y del Banco Central. Nuestro objetivo es concordar una estrategia para minimizar la exposición de las empresas de telecomunicaciones a riesgos cibernéticos, así como elevar su capacidad de responder con éxito a ataques de este tipo.

Adicionalmente, la mesa busca armonizar el trabajo del sector con las regulaciones que implementa el Banco Central, de manera de facilitar a la protección de la cadena de pagos en el ámbito que compete a las empresas de telecomunicaciones como proveedores de servicios críticos para la banca y la industria financiera.

Como presidente del Consejo de INDOTEL he tenido la oportunidad de apreciar, de primera mano, la velocidad y profundidad del desarrollo digital en el país. Hoy estoy consciente que enfrentamos ya no sólo el desafío de derrotar la brecha digital, asegurando el acceso masivo a las redes a toda la población dominicana, sino que además el de garantizar que ese acceso se de en condiciones de seguridad.

El desafío de la seguridad digital es complejo y tiene largo alcance. Es hora de hacernos cargo.

Publicado en el periódico Listín Diario.
15 de noviembre 2019