LITORALPRESS

Fecha: 27-10-2020
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Ciencia y Tecnología
Título: LOS RETOS DEL PAIS PARA DAR EL SALTO EN SEGURIDAD DIGITAL

Pág. : 24
Cm2: 589,4
VPE: $ 5.222.571

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: Positiva

# LOS RETOS DEL PAIS PARA DAR EL SALTO EN SEGURIDAD DIGITAL

Contar con directrices claras en materia de ciberseguridad es clave para el desarrollo, ya que estas inciden en la infraestructura crítica y en los servicios ciudadanos. Y aunque hay avances importantes, aún queda mucho por resolver.

POR PAMELA CARRASCO T.

Hace unas semanas la noticia del acceso no autorizado a los servidores de la División de Gobierno Digital de la Secretaría General de la Presidencia y el posible robo de las claves únicas de los ciudadanos disparó las alarmas sobre la importancia de la ciberseguridad en los organismos del Estado. Una urgencia crítica en tiempos de pandemia, cuando las interacciones online con las instituciones públicas se han disparado en número y frecuencia.

El tema se está trabajando con fuerza hace unos años. En 2017, una Política Nacional de Ciberseguridad trazó una hoja de ruta y propuso metas con miras a 2022. A partir de esto se creó en 2018 el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), que depende del Ministerio del Interior y coordina la respuesta técnica frente a incidentes o ataques informáticos. También se dictó el Instructivo Presidencial N° 8, que implementó medidas como la designación de un encargado de ciberseguridad en cada servicio público y la evaluación de riesgos, vulnerabilidades, medidas y planes de acción.

"Hoy el Estado, en base a los objetivos de la Política Nacional de Ciberseguridad, cuenta con una mejor infraestructura de ciberseguridad", asegura Carlos Landeros, director nacional del CSIRT. Y cuenta que, en esta línea, hasta la fecha el Gobierno ha suscrito ocho convenios internacionales en ciberseguridad con países como Israel, España y Colombia, y también con la OEA, y cuenta con 53 convenios con empresas privadas, universidades, ONGs y órganos autónomos, de modo de generar intercambio de información estratégica y traspaso de conocimientos.

## Los pendientes

Ricardo Seguel, académico de la Facultad de Ingeniería y Ciencias de la Universidad Adolfo Ibáñez, reconoce que en los últimos años se ha reforzado la ciberseguridad en el sector público, pero dice que aún hay mucho por hacer. "Falta fortalecer las capacidades humanas, técnicas y de infraestructura tecnológica de las instituciones públicas con un plan de acción e inversión clara de parte del Estado para avanzar a un nivel de ciberseguridad gestionada", dice.

Para Excequiel Matamala, vicepresidente de la Alianza Chilena de Ciberseguridad (ACC), es fundamental invertir más en ciberseguridad y trabajar en una regulación que obligue y sancione tanto la ausencia de medidas organizacionales de prevención como la falta de inversión constante en capital humano.

"Esta parece ser la única vía para que todos los actores del ecosistema tomen en serio la importancia y real impacto de la ciberseguridad", dice.

Para Pedro Lluch, socio de servicios Legales en el área de Consultoría Tributaria de EY Chile, es necesario seguir profundizando en mecanismos de seguridad que permitan alcanzar niveles de acuerdo con los estándares internacionales. "Para ello, debemos contar con un sustento legislativo, desarrollo de cultura de seguridad y aprendizaje continuo de sus profesionales, entre otros", dice.

Pero el desafío no es sólo del Estado: se estima que en Chile se invierte alrededor de US$ 200 millones por año en ciberseguridad, lo que representa el 0,0007% del PIB. A nivel mundial, en tanto, el promedio de inversión en materia de ciberseguridad es del 0,0012% del PIB.

Alejandro Barros, consultor internacional y académico asociado del Centro de Sistemas Públicos de la Universidad de Chile, asegura que se requiere un quehacer más decidido en este tema. "El tema no tiene toda la prioridad que debería. Si a eso agregamos que nuestro marco normativo en la materia tiene serias deficiencias y aún no terminamos el proceso de actualización de dicho marco, el panorama no es del todo alentador", asegura.

Para Nicolás Corrado, socio de Deloitte experto en ciberseguridad, contar con una Ley Marco de Ciberseguridad es fundamental, ya que haría posible establecer un marco de gobernanza definitivo que tendrá la ciberseguridad dentro del Estado y "definir una serie de estándares y obligaciones que deberán cumplir tanto los organismos del sector público y privado", dice.

Carlos Landeros, del CSIRT, reconoce que la necesidad de una estructura de gobernanza "es una realidad y una deuda que como gobierno comprometimos", y afirma que están trabajando en la revisión del proyecto de ley con el grupo técnico nacido del Comité Interministerial de Ciberseguridad, para lograr el consenso y profundidad de la nueva institución. La meta es tener el proyecto de ley dentro de este año.

**Uno de los temas pendientes es tener una Ley Marco de Ciberseguridad, que establezca la gobernanza del tema en el Estado. La meta, dicen en el gobierno, es tener el proyecto de ley este año.**

## Los desafíos

Desde el gobierno están trabajando en ciertos ejes claves en materia de ciberseguridad, como la concientización y educación entre los funcionarios públicos y el refuerzo en la coordinación entre las organizaciones, de modo de brindar mayor entrenamiento y competencias profesionales a los equipos TIC y de ciberseguridad, así como renovar la arquitectura e infraestructura tecnológica.

Además, se está avanzando en la implementación y cumplimiento de estándares de ciberseguridad. "Estamos buscando la actualización de los decretos sectoriales de ciberseguridad que impongan estándares más altos en el desarrollo, implementación y administración de los sistemas de correos y sitios web, los cuales hoy en día revisten la principal amenaza de riesgos ya identificados como phishing, malware y defacement", dice Carlos Landeros.