

“ Nuestra vida depende de servicios digitales. Pedir una hora, comprar, hacer una transacción electrónica, dependemos de tecnologías digitales todo el día, para pedir un auto, para pagar cuentas incluso. ”
Daniel Álvarez Valenzuela, Director Nacional de la ANCI.

ENTREVISTA A JEFE NACIONAL, DANIEL ÁLVAREZ

Región de base tecnológica: Biobío focaliza interés de nueva Agencia Nacional de Ciberseguridad

El director nacional de la recién instalada entidad detalla cómo podría proyectarse territorialmente, en nuestra zona y de la mano de la academia, para convertirse en un polo de la industria en el área.

Eduardo Baseañán
 contacto@diari CONCEPCION.CL

La Ley 21663, promulgada el 26 de marzo de 2024 sentó las bases para la creación de la Agencia Nacional de Ciberseguridad (ANCI) y un sistema de respuesta ante incidentes de ciberseguridad. Entre sus cimientos, recién fundados, se encuentran definidos los métodos en los que la ANCI operará a nivel regional. Pero ¿en qué radica la importancia de la creación de este nuevo estamento público?

“Nuestra vida depende de servicios digitales. Pedir una hora, comprar, hacer una transacción electrónica, dependemos de tecnologías digitales todo el día, para pedir un auto, para pagar cuentas incluso. Por lo tanto, necesitamos garantizar que esos servicios digitales estén operativos 24/7 a lo largo de todo el país. Cuando tenemos una emergencia de ciberseguridad, al final, los afectados son los ciudadanos que no pueden llevar a cabo su vida de manera normal”, explicó el director Nacional de la ANCI, Daniel Álvarez Valenzuela, quien es abogado y doctor en Derecho por la Universidad de Chile.

Es que con solo 16 días de instaurada la agencia, más de 40 personas contratadas en el nuevo servicio, busca instalarse en Santiago, para luego, proyectar sus líneas de acción en regiones.

Atribuciones

Si bien, la Ley asevera que la ANCI tendrá diversos objetivos, su director nacional, explicó que “la agencia efectivamente va a ser un servicio público que tiene por misión esencial garantizar la ciberseguridad tanto en el sector público como en el sector privado a nivel nacional”, pero cumplirá tres grandes atribuciones. La primera, según detalla Álvarez,



serán atribuciones clásicas de una superintendencia, “un organismo que norma, regula y fiscaliza”.

La segunda gran atribución, tiene relación a la respuesta ante incidentes: “cuando alguna institución pública y, a partir de marzo, alguna institución privada tenga un ciberataque en aspecto significativo, la agencia va a poder, no solo ayudar en la respuesta a incidentes, sino que también ayudar en el proceso de recuperación de las capacidades que sean afectadas”, agregó.

El tercer atributo único del nuevo servicio es el de la concientización, la educación y “la sensibilización de la población en estos temas que hoy día con las tecnologías digitales están presentes a lo largo de todo el país”, expresó Álvarez.

Pero ¿cómo se enfocarán estas atribuciones en las regiones? La ley autoriza a la ANCI en dos ámbitos relativos a los territorios. “Es un servicio de alcance nacional, porque las mayores capacidades tecnológicas en Chile salen del nivel central”, pero también,

la norma permite el “establecimiento de oficinas regionales”, explicó.

Grandes posibilidades

A medio mes de instaurada la Agencia, su director nacional, observó al Biobío como un territorio que se podría proyectar como una base tecnológica. “En el caso particular del Biobío, es una región que tiene una industria de base tecnológica interesante, hay empresas desde criptografía cuántica hasta investigación académica en estos temas, por

lo tanto, es probable que tengan algún nivel de representación en estos órganos que se crearon con la agencia”, agregó.

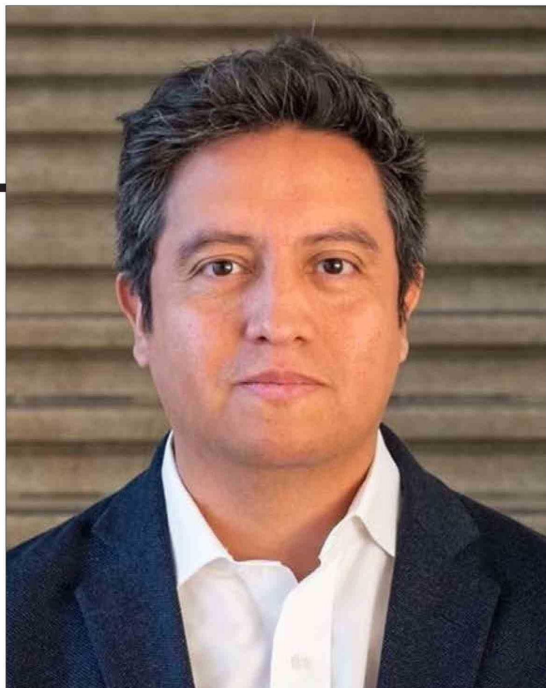
Y es que, el vínculo con el mundo empresarial y las universidades, son también, es una parte que está incluida en el organismo. En ese sentido, su objetivo, según detalla la Ley (artículo 11) se fomentará la investigación, capacitación y desarrollo de la industria local de ciberseguridad en colaboración con universidades e instituciones académicas.

“No solo serán universidades, se vinculan con centros de formación técnica, los institutos profesionales, es mucho más diverso. Hay varias líneas de trabajo. Las más importantes, en nuestra opinión, tienen que ver con, primero, nosotros tenemos capacidades nacionales destacadas en materia de ciberseguridad en diversas instituciones de educación superior”, afirmó el director nacional.

Además, sumó que “universidades regionales como la de Valparaíso, la Universidad de Concepción, Universidad Católica de la Santísima Concepción, la UFRA, en fin, múltiples universidades que han tenido desarrolladas en el tiempo estas capacidades”, afirmó.

Es que, un reciente estudio del Ministerio de Ciencias y Tecnologías identificó las instituciones de investigación en materia de ciberseguridad y “aparecer varias regiones destacadas desde Valparaíso hasta del Biobío, y ahora, el desafío que tenemos ahora es aglutinar esta investigación que se realiza de manera más atomizada y orientarla a objetivos país”, dijo Álvarez.

Esto puede propiciar la creación de una industria nacional de ciberseguridad y además, tener bases científicas tecnológicas en materia de ciberseguridad.

DANIEL ÁLVAREZ, director nacional de la ANCI.

“En el caso de la región del Biobío, las universidades e incluso las empresas de bases científicas tecnológicas, por ejemplo, tuvimos un par de muy buenas iniciativas de proyectos que están funcionando. Por lo tanto, el unir ese esfuerzo que se está haciendo de manera diversa en distintas regiones del país nos debería permitir mejorar no solo nuestro nivel de madurez, sino que incrementar la oferta de servicios y también la sofisticación de estos servicios”, proyectó el director de la ANCI, en el territorio regional.

Vínculo con el mundo privado

Pero además del nexo con la academia, la ANCI tendrá como misión vincularse tanto con el mundo privado, como con los organismos públicos.

Consultado, respecto de las diferencias presupuestarias entre municipalidades y posibles desigualdades administrativas al momento de abordar problemáticas de ciberseguridad, el director, aseveró que “para nosotros es indiferente el tamaño de la municipalidad, lo que nos intere-

sa es que todos los municipios y también los encargados informáticos o los encargados de ciberseguridad, puedan recibir formación desde el nivel básico hasta el nivel lo más avanzado posible”, explicó.

Reconociendo las diferencias en torno a la alfabetización digital, Ál-

varez afirmó que “nuestras capacitaciones llegan a los encargados de ciberseguridad en los tres niveles, en servicios nacionales, en gobiernos regionales y en gobiernos locales”.

Es que incluso, en marzo se va a llevar a cabo una conferencia anual de informáticos municipales, donde se

reunirán los informáticos de las 346 comunas del país. “Ellos, son el eslabón más débil desde el punto de vista administrativo y vamos a realizar un esfuerzo especial por capacitar incluso a funcionarios municipales, que son usualmente los que han estado más alejados de eso”, afirmó.

En ese sentido, la proyección para este año es incrementar la cantidad de capacitaciones, así como también, “aumentar la diversidad de ofertas de capacitaciones, y también el público objetivo que le alcanza. La idea es ir cubriendo tanto del sector público como del sector privado, la mayor cantidad de sectores posibles”, sumó el director.

Toma de razón y selección

Ahora bien, la norma en cuestión establece también, el vínculo con las empresas en torno a la ciberseguridad y la infraestructura crítica.

Aun así, mientras Contraloría toma razón del reglamento que establece los criterios de selección de estas infraestructuras, el director nacional, adelantó que serán consi-

derados todos los “servicios esenciales, aquellos que por su naturaleza determinan el funcionamiento del país, el sector eléctrico, telecomunicaciones, combustibles, transportes, por mencionar algunos, además de los organismos de la Administración del Estado a nivel nacional, regional y local”.

Además, en el caso de las pequeñas y medianas empresas, la Ley establece diferencias en cuanto al cumplimiento de obligaciones de ciberseguridad. ¿Cuáles son algunas de estas obligaciones? Por ejemplo, notificación de incidentes, gestión de los incidentes o medidas preventivas, por nombrar algunas.

“Cualquier obligación que establezca la Agencia, se debe tener en consideración el tamaño de la empresa. (...) No va a haber la misma carga regulatoria para una pequeña o una mediana. Eso es una garantía legal”, explicó el recién asumido director nacional de la ANCI.

OPINIONES

Twitter @DiarioConce
contacto@diarioconcepcion.cl