Santiago de Chile, 7 de julio de 2022
Fundación Chilena del Pacífico

FUNDACIÓN CHILENA DEL PACÍFICO

COMUNICADO

Webinar exploró los avances y desafíos de la ciberseguridad en industrias estratégicas de Chile

La actividad, organizada por la Fundación Chilena del Pacífico, abordó el desarrollo y los desafíos de la era digital para Chile en materia de ciberseguridad, en el contexto del Asia Pacífico y tanto desde la perspectiva y esfuerzos de los sectores público y privado como de los pasos en alianza entre ambos mundos.

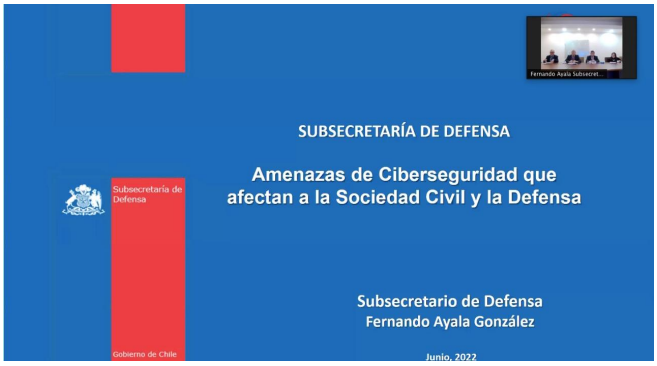
Los desafíos y los avances de la ciberseguridad en nuestro país en el contexto del Asia Pacífico, los esfuerzos públicos y privados y de las alianzas entre ambos sectores para hacer frente a la amenazas que nacen del creciente desarrollo de la era digital fueron los temas centrales de un reciente *webinar* de la Fundación Chilena del Pacífico, actividad en la que participaron el Subsecretario de Defensa, **Fernando Ayala**; la presidenta y CEO del Toronto Region Board of Trade y presidenta del Grupo de Trabajo Digital del Consejo Asesor Empresarial de APEC (ABAC), **Janet De Silva**; y el director Legal y de Asuntos Corporativos de Microsoft en América Latina, **Robert Ivanschitz.**

El seminario abordó cómo el aumento de la digitalización en Chile y el mundo, un escenario que se vio acelerado como efecto de la pandemia, ha provocado un mayor riesgo digital y creado la necesidad de avanzar en el desarrollo de estrategias y políticas de ciberseguridad adecuadas.

La actividad también exploró los avances en el Foro de Cooperación Económica del Asia Pacífico (APEC) -de cuyo Consejo Asesor Empresarial (ABAC) la Fundación Chilena del Pacífico ejerce como secretaría nacional- para enfrentar los riesgos por ciberataques. Los panelistas analizaron políticas regionales y nacionales de ciberseguridad, ejemplos de las respuestas de los gobiernos ,aprendizajes para Chile, , la importancia del desarrollo de tecnología avanzada, el valor de la capacitación profesional , , entre otros aspectos, como puntos clave para aprovechar con seguridad la era digital.

Una mirada desde el sector público

"La ciberdefensa es una de las principales prioridades que hemos definido en nuestro trabajo a partir del 11 de marzo", sostuvo el Subsecretario de Defensa, **Fernando Ayala,** quien explicó que, dada la alta amenaza en la era digital, es necesario normar y regular la ciberseguridad e *"invertir en equipos, capacitar a profesionales y a la población".*



Presentación del Subsecretario de Defensa Fernando Ayala.

COMUNICADO

El Subsecretario enfatizó su importancia ya que, agregó, *"estamos atrasados en defendernos"* y sostuvo que algunos expertos señalan que en el futuro cercano *"se usará tanto el gatillo como el mouse"*.

Ayala destacó las dificultades y magnitud del impacto para Chile que ocasionaría un ciberataque a las instituciones del Estado, a las empresas y a las personas. Enfatizó la importancia de invertir en ciberseguridad y afirmó que *"acciones cibernéticas de hostilidad y/o delictuales pueden afectar tanto a instituciones gubernamentales como privadas, pudiendo desestabilizar gobiernos y generar caos"*, por lo que dijo que es necesaria una política de ciberseguridad.

Dentro de las tendencias en ciberseguridad, el Subsecretario de defensa destacó la *"zero trust"* o tolerancia cero, que se refiere a nunca confiar y siempre verificar; la ciberseguridad impulsada por inteligencia artificial; el foco en los dispositivos móviles como nuevos vectores de ataque y la concientización y capacitación para desarrollar una cultura de ciberseguridad.

En cuanto a la política nacional de ciberseguridad, el Subsecretario se refirió a sus objetivos y pilares. Sus cuatro pilares son: resguardar la seguridad de las personas en el ciberespacio; proteger la seguridad del país; promover la colaboración y coordinación entre instituciones; gestionar los riesgos del ciberespacio. Y sus objetivos, agregó, son: desarrollar infraestructura de la información robusta y resiliente; que el Estado cuide los derechos de las personas en el ciberespacio; ayudar a una cultura de la ciberseguridad; fomentar la cooperación en ciberseguridad con otros actores; y la promoción de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos".

En Chile, la gobernanza de ciberseguridad, señaló Ayala, considera el empleo de los medios de ciberdefensa, la cooperación internacional (con países como Argentina, Colombia, Ecuador, España, Estonia, EE.UU., Israel, México, entre otros), así como la promoción de la transparecia y la confianza entre los Estados y el desarrollo de capacidades. A su vez, contempla la colaboración con la academia por medio de acuerdos e instancias de colaboración nacional público-privadas, señaló.

Los desafíos en Chile, según el Subsecretario, son *"fomentar una cultura digital segura"* e *"incentivar la inversión, investigación y el trabajo conjunto del sector público, privado, de la academia y la ciudadanía"*.

Una mirada desde el Consejo Empresarial de la APEC

"Vemos que lo digital lo abarca todo", señaló la presidenta y CEO del Toronto Region Board of Trade y presidenta del Grupo de Trabajo Digital del Consejo Asesor Empresarial de APEC (ABAC), **Janet De Silva**, quien a su vez sostuvo que *"el aumento de la digitalización significa un aumento del riesgo"* y que *"priorizar la ciberseguridad es*

COMUNICADO

una precondición para una economía digital".

"Observamos que lo ciber, al igual que la economía digital, no tiene fronteras, así que lo mejor es abordarlo como un colectivo de la APEC en vez de país a país y empresa a empresa", afirmó De Silva. Agregó que, desde un punto de vista cultural, la ciberseguridad ya no es sólo responsabilidad de los expertos y técnicos, sino que es responsabilidad de los individuos y de los gobiernos, *"un desafío humano y técnico"*.

Presentación de Janet de Silva sobre el "Desafío de la Ciberseguridad".

De Silva señaló que el riesgo de un ciberataque no está bien dimensionado, puesto que la interconectividad de las economías y los negocios llevan a que un ataque contra uno podría tener grandes implicancias en otras economías. Afirmó que *"la región de APEC es una de las más atacadas globalmente, teniendo la brecha más grande de ciber talento en el mundo"* y que, si bien ésta ha tenido la ciberseguridad en su agenda desde el 2001, la pandemia ha cambiado la urgencia con la cual requerimos actuar.

Según De Silva, hoy debemos actuar con urgencia en las siguientes seis áreas: desarrollo de ciber capacidad; enfoques en red del talento; coordinación y armonización de la normativa; intercambio de información; inversiones prioritarias en nuevas tecnologías; apoyo a las Pymes.

Respecto de la brecha en ciberseguridad en la región de Asia Pacífico, De Silva puso un particular énfasis en que "*existe mucho trabajo por hacer para cerrar la brecha"* y que existe una falta de estandarización, lo que supone un riesgo para otras economías. *"Nuestra mejor respuesta es una respuesta regional"*, afirmó Janet De Silva, y agregó que *"si queremos prepararnos mejor para los ataques y generar una mayor ciber-resiliencia, tenemos que cerrar la brecha"*.

Una mirada del sector privado

El director Legal y de Asuntos Corporativos de Microsoft en América Latina, **Robert Ivanschitz,** se refirió al cibercrimen en Chile, que, en 2022, presenta un *"60% de aumento en ciberataques"*, lo que *"está hacia los máximos históricos"*, afirmó. Señaló que, en el año 2022, ha habido un aumento de más del 400% del *ransomware*[1] dirigido a empresas en nuestro país.

[1] Según el diccionario de Cambridge, corresponde a *"un software diseñado por criminales para impedir que los usuarios de ordenadores accedan a su propio sistema informático o a sus archivos a menos que paguen dinero"*.

Santiago de Chile, 7 de julio de 2022
Fundación Chilena del Pacífico

COMUNICADO

Ivanschitz destacó el caso de Costa Rica y sostuvo que el presidente Rodrigo Cháves *"ejerció un liderazgo nunca antes visto"* frente al ciberataque de abril a varias entidades gubernamentales. Agregó que es la primera vez que un país declara emergencia nacional frente a estos ataques, lo que tiene -afirmó- tiene consecuencias importantes: *"uno, acelera la cooperación internacional; dos, acelera la cooperación del mundo privado y el destino de recursos; y tres, ayuda a todos a concientizar que esto es tan terrible o tan catastrófico como un terremoto, es decir, se rompen de forma automática las instituciones"*.

"Ciberseguridad en Chile: ¿Qué nos estamos jugando?. Por Robert Ivanschitz

Ivaschitz se refirió a la guerra en Ucrania y destacó el aumento de la utilización del ataque cibernético como un elemento adicional a una guerra tradicional. Afirmó que *"la guerra en Ucrania no comenzó el 24 de febrero con la invasión rusa; comenzó meses antes con los ataques constantes que se hacían de las distintas agencias de espionaje ruso frente al gobierno ucraniano, a las empresas de telecomunicaciones y a las empresas que prestaban los servicios"*. Ivanschitz puso enfasis en que es importante entender que hoy *"no sólo nos econtramos frente a actores muy organizados y muy poderosos, sino actores que realmente cuentan con todo lo que significa el tener la fuerza de un Estado-nación por detrás"*.

El experto destacó que, entre las enseñanzas del conflicto entre Rusia y Ucrania, es posible extraer que el uso de las armas de carácter cibernético tiene un rol preponderante, creando una *"necesidad de defensa cibernética basada en cuatro pilares: detectar, defender, disruptir y detener"*. Proteger nuestra integridad cibernética es un objetivo común entre sector público y privado, destacó Ivanschitz, haciendo un llamado a ir detectando de forma continua este tipo de situaciones, a desarrollar capacidades técnicas que beneficiarán al país y a disminuir la brecha digital.

Para ver el vídeo del *webinar* hacer click en este enlace