
**Ingrid Inda, jefa de la División de Redes y Seguridad Informática - Ministerio del Interior:**

## “El CSIRT de Gobierno representa la continuidad y transversalidad de un proyecto y de una visión que involucra a varios actores y sectores del mundo privado y público”

Para conocer el avance y el rol actual que está cumpliendo en el Estado el Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT) de Gobierno, conversamos con Ingrid Inda, jefa de la División de Redes y Seguridad Informática del Ministerio del Interior.

**Usted estuvo a cargo de un incipiente CSIRT en el segundo Gobierno de M. Bachellet, ¿Cómo ha visto que ha cambiado con el actual?**

El CSIRT de Gobierno ha tenido una importante evolución. Recordemos que  la Red de Conectividad del Estado (RCE) nace el año 2000 interconectando a Ministerios y Servicios del Estado en una red de alta disponibilidad, entregando servicios de internet y seguridad y desde hace 10 años ya se conforma el CSIRT como servicio integral, consolidándose con la creación del Departamento CSIRT el año 2018.

Cuando desarrollamos la Política Nacional de Ciberseguridad (PNCS) en el gobierno de la ex presidenta Michelle Bachellet fijamos los principales ejes de interés nacional y que continuó con el ex presidente Piñera, y que hoy se mantiene con el gobierno de Gabriel Boric, esto nos demostró la importancia de desarrollar estos procesos dentro de un entorno participativo con enfoque de política de Estado que permite dar continuidad y crecimiento al final.

En este largo proceso, el CSIRT de Gobierno ha estado involucrado en la creación y asesoría de las nuevas legislaciones, instructivos, normas, protocolos, tecnologías y en la consolidación de una red de encargados de ciberseguridad y, hoy estamos desarrollando una ciberseguridad dirigida a los funcionarios públicos que administran y gestionan los activos informáticos de la ciudadanía, además de apoyar a las instituciones en la educación y capacitación de sus funcionarios. Por otra parte, estamos

***"Actualmente, la mayoría de las instituciones del Estado cuentan con un encargado de ciberseguridad, se ha invertido en equipos y tecnología y además el año 2015 se creó una comisión asesora para abordar temas de ciberseguridad y en la que participan diversas subsecretarías."***

compartiendo recomendaciones dirigidas tanto a técnicos como ciudadanía en general a través de nuestras redes.

El CSIRT de Gobierno representa la continuidad y transversalidad de un proyecto y de una visión que involucra a varios actores y sectores del mundo privado y público, y eso se refleja en que hoy somos un actor en el ecosistema de la ciberseguridad.

**¿Cómo han evolucionado por un lado los riesgos cibernéticos y por otro la preparación del Estado para hacer frente a estas amenazas?**

Los principales tipos de ataques cibernéticos no han cambiado en sí, se han mantenido con el tiempo. Los phishing, DDoS, ransomware, malware no son nuevos, lo que sí ha evolucionado son las técnicas que utilizan los delincuentes para no ser detectados. También se suman nuevos atacantes y grupos que antes no existían o no estaban identificados.

Paralelamente, debemos considerar la digitalización y la hiperconectividad como elementos que si bien contribuyen al desarrollo y crecimiento de un país, también son factores de riesgo. Hoy estamos viviendo la transformación digital del Estado, por lo tanto, un desafío importante que enfrentamos es la protección de nuestros sistemas y de los servicios públicos de cara a la ciudadanía, y el cuidado y resguardo de la información y de los datos sensibles.

Para hacer frente a estos cambios, el Estado también se encuentra transformándose para adaptarse a este nuevo escenario. Actualmente, la mayoría de las instituciones del Estado cuentan con un encargado de ciberseguridad, se ha invertido en equipos y tecnología y además el año 2015 se creó una comisión asesora (Comité Interministerial de Ciberseguridad) para abordar temas de ciberseguridad y en la que participan

diversas subsecretarías. Por otra parte, nos encontramos revisando nuestra política de ciberseguridad y se está discutiendo acerca de la institucionalidad necesaria, para lo cual se ha designado a Daniel Alvarez, coordinador nacional de ciberseguridad.  A la vez, tenemos que Gobierno Digital también contempla la componente ciberseguridad en su plan.

A la vez, existe conciencia en la relevancia de la capacitación y preparación no sólo de los equipos de ciberseguridad, sino también la educación para todos los funcionarios, ya que son un pilar fundamental para evitar que una amenaza se concrete. En este sentido desde hace algunos años contamos con campañas de concientización sobre los riesgos y peligros que existen en el ciberespacio y cómo evitarlos, las que compartimos con las distintas instituciones. Además, este año hemos realizado otras iniciativas que nos permitan llegar con nuestras campañas a más trabajadores.

***"El CSIRT de Gobierno elaboró un plan integral y estratégico que nos permitirá trabajar en las distintas necesidades que tenemos como Estado y que abordará a la ciberseguridad en su conjunto"***

**¿Qué rol está cumpliendo hoy el CSIRT?**

El rol principal del CSIRT de Gobierno es proveer servicios de seguridad a las instituciones del Estado que forman parte de la RCE. Para lograr este objetivo, hemos desarrollado un plan integral que nos permita abordar las distintas necesidades que tenemos como Estado y contar con las mejores herramientas para proteger a la RCE.

**¿Cómo evalúa el accionar del CSIRT en los incidentes del Estado Mayor Conjunto y del Poder Judicial?**

Siempre en este tipo de incidentes de ciberseguridad se evalúa la forma en que se actúa y sin duda uno aprende de los errores y también se valora las acciones que se toman. En ambos casos, el CSIRT de Gobierno alertó oportunamente a las instituciones del Estado, a través de los distintos canales de comunicación, por un lado, en enero de 2020, que Microsoft informó el fin de la entrega de soporte y actualizaciones de seguridad a los dispositivos con el sistema operativo Windows 7 y, en julio de 2021, compartió las vulnerabilidades y mitigaciones de los productos de Microsoft.

***"En ambos casos (EMCO y PJUD), el CSIRT de Gobierno alertó oportunamente a las instituciones del Estado, a través de los distintos canales de comunicación"***

En este sentido, creo que el CSIRT de Gobierno hizo su trabajo, quizás se podría haber insistido más en los riesgos que conllevaban, pero finalmente la responsabilidad siempre recae en las instituciones en su deber de realizar las actualizaciones que correspondan. Sin embargo, también debemos considerar que la inversión requerida en equipos y tecnología es alta, y no todas las instituciones cuentan con esos recursos, por lo tanto debemos evaluar como país de qué manera abordar esta situación para evitar y prevenir que estas amenazas se repitan especialmente en instituciones críticas para nuestro país.

**¿De qué manera el Estado aprende de estos incidentes?**

Como en cualquier crisis, lamentablemente se aprende de los errores y de malas decisiones, pero por lo mismo también es un buen momento para evaluar, analizar, planificar y concretar ideas y proyectos que van en beneficio de la protección de los activos e información de los ciudadanos. Los incidentes nos obligan a revisar nuestros procesos y aplicar gestión de riesgo y son una oportunidad para que todos tomen conciencia de la ciberseguridad, revisen y cambien sus hábitos y se tome conciencia de la responsabilidad que se tiene debido a la información que mantenemos.

Cuando nos vemos involucrados en un incidente de ciberseguridad, el primer afectado es la institución que ve en desmedro su reputación, su capacidad operacional y el problema que implica perder información, datos, etc. Por lo tanto, se busca la manera de disminuir las probabilidades que vuelva a ocurrir, ya sea invirtiendo en recursos, en capacitación y lo más importante, que se considere la ciberseguridad dentro de la estrategia y pilar de una organización. Luego, es afectada la ciudadanía que pudiera verse expuesta debido a los datos sensibles que registran los servicios públicos.

**¿Dónde estarán los principales énfasis que tendrá el CSIRT en el 2023?**

Como mencioné anteriormente, el CSIRT de Gobierno elaboró un plan integral y estratégico que nos permitirá trabajar en las distintas necesidades que tenemos como Estado y que abordará a la ciberseguridad en su conjunto.


***"El ecosistema de ciberseguridad funciona y crece en la medida que seamos capaces de cooperar y colaborar entre nosotros y no para ayudar al CSIRT sino para ayudarnos todos a proteger nuestros activos de información"***

Durante el 2022 hemos avanzado en este proyecto, el que se extenderá para el 2023. La protección perimetral de la RCE es nuestro principal foco, queremos implementar nuevos sistemas y servicios que nos permitan brindar la máxima protección contra amenazas externas e internas. Así también, trabajamos con las instituciones para evaluar, a través de auditorías internas, su nivel de madurez en ciberseguridad, entregando recomendaciones, lineamientos y propuestas de mejora.

Otras áreas a desarrollar serán la concientización ciudadana, capacitación a funcionarios y asesoría y respuesta a incidentes de ciberseguridad. Continuaremos además generando alertas preventivas de seguridad cibernética, principalmente a las instituciones del Estado, sobre nuevas amenazas, vulnerabilidades, mitigaciones, etc.

**¿Cómo el ecosistema de ciberseguridad ayuda al rol del CSIRT?**

De distintas maneras se puede contribuir a la ciberseguridad y ayudar al rol que tiene el CSIRT de Gobierno. Algunas de ellas son: notificando oportunamente los incidentes y anomalías relevantes que se identifiquen en las infraestructuras y sistemas; incorporando las recomendaciones del CSIRT de Gobierno y solicitando ayuda cuando no hay capacidad para lograr la meta planteada; compartir información y experiencias, ya sean buenas o malas, y establecer un entorno de confianza que permita avanzar, a pesar de los errores, logrando convertirlos en aprendizaje.

Es importante considerar que un ecosistema sobrevive en la medida que se entiende que todos somos parte y dependemos unos de los otros. Las malas experiencias de uno pueden impactar en otros y ser enseñanza-aprendizaje para el ecosistema de ciberseguridad.

El ecosistema de ciberseguridad funciona y crece en la medida que seamos capaces de cooperar y colaborar entre nosotros y no para ayudar al CSIRT sino para ayudarnos todos a proteger nuestros activos de información que al final se traduce en protección de nuestra continuidad operativa y de la ciudadanía.


## Daniel Álvarez Valenzuela, Coordinador Nacional de Ciberseguridad:

# “A diferencia de otras áreas, en materia de ciberseguridad contamos con una verdadera política de estado que se ha desarrollado e implementado en tres gobiernos consecutivos”

Hace unos meses se anunció el nombramiento como Coordinador Nacional de Ciberseguridad al abogado y doctor en derecho de la Universidad de Chile, Daniel Álvarez Valenzuela, cuando se conoció esta noticia, el ecosistema de la ciberseguridad lo tomó positivamente, por ser él alguien reconocido e involucrado desde ya hace unos años en el mundo de la seguridad de la información y de la academia.

“Tenemos dos objetivos de corto plazo. Evaluar la política nacional de ciberseguridad vigente y proponer la nueva política nacional para el período 2023-2028. A diferencia de otras áreas, en materia de ciberseguridad contamos con una verdadera política de estado que se ha desarrollado e implementado en tres gobiernos consecutivos”, señala Álvarez.

**Para entender bien su rol como Coordinador Nacional de Ciberseguridad ¿Cuáles son sus responsabilidades?**

1. Convocar y dirigir el Comité Interministerial sobre Ciberseguridad, que es la comisión asesora presidencial que propone la Política Nacional de Ciberseguridad, además de llevar a cabo e implementar los acuerdos que se adopten en el Comité.

2. Dirigir el proceso de evaluación de la Política Nacional de Ciberseguridad 2018-2022 y, en paralelo, dirigir el proceso de elaboración de la Política Nacional de Ciberseguridad 2023-2028.

3. Coordinar la acción legislativa del Estado en materia de ciberseguridad. En este momento, estamos coordinando la discusión del proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, que ha sido recientemente aprobado en general en el Senado. Nuestra labor consiste en buscar los consensos técnicos y políticos necesarios para la aprobación del proyecto de ley en el más breve plazo posible.

**¿Cómo evalúa el nivel de Chile en ciberseguridad, primero a nivel general y segundo del Estado en particular?**

Según diversos rankings y evaluaciones internacionales, Chile cuenta con nivel de madurez medio en materia de ciberseguridad. Si nos detenemos en particular en el Reporte del año 2020 elaborado por el BID y la OEA, utilizando una metodología de la Universidad de Oxford, Chile tiene un nivel de madurez consolidado al evaluar las siguientes cinco dimensiones específicas: Política y Estrategia; Cultura Cibernética; Formación, Capacitación y Habilidades; Marcos Legales y Regulatorios; y, Estándares, Organizaciones y Tecnologías, aunque en esta última tenemos un nivel más bajo.

Nuestra debilidad más importante pasa por la ausencia de una autoridad nacional de ciberseguridad, cuestión que subsana el proyecto de ley marco sobre ciberseguridad que se discute en el Congreso Nacional y al cual el gobierno le ha puesto suma urgencia en su tramitación.

**¿En qué aspecto Chile tiene sus principales desafíos en ciberseguridad?**

Como señala recién, uno de nuestros desafíos tiene que ver con la ausencia de una institucionalidad pública con competencias específicas en materia de ciberseguridad, que cuente con atribuciones sobre el sector público y el privado. Adicionalmente, debemos fortalecer el desarrollo de capacidades, especialmente en las personas, las instituciones, sus procesos digitales. Finalmente, creo urgente comenzar a desarrollar campañas sobre hábitos de higiene digital.

**¿Qué destacaría de la agenda legislativa en el ámbito de la ciberseguridad y protección de datos?**

Tenemos dos proyectos de ley en discusión que están avanzando en la tramitación legislativa. El ya mencionado proyecto de ley marco sobre ciberseguridad, al cual le ingresaremos indicaciones que tienen por objeto esencial simplificar su orgánica y fortalecer sus atribuciones y funciones, ampliando el ámbito de aplicación a todo el sector público y privado, con obligaciones de ciberseguridad diferenciadas por riesgos y tamaño.

En el caso del proyecto de ley sobre datos personales, está en segundo trámite constitucional en la Cámara de Diputados, y se ha avanzado sustancialmente en su discusión con el propósito que se transforme en ley, lo más pronto posible. Este proyecto es importante no solo porque incrementa en nivel de protección legal de los datos personales en Chile, sino que también porque establece la obligación de adoptar medidas de ciberseguridad a los procesadores de datos personales y la notificación obligatoria de incidentes que impliquen pérdida de los mismos, ambas cuestiones que hoy no existen en nuestra regulación.

> ***“Nuestra debilidad más importante pasa por la ausencia de una autoridad nacional de ciberseguridad, cuestión que subsana el proyecto de ley marco sobre ciberseguridad que se discute en el Congreso Nacional y al cual el gobierno le ha puesto suma urgencia en su tramitación”***

**¿Qué expectativas debiésemos tener en plazo y alcance de una “Agencia nacional de ciberseguridad”?**

El gobierno ha dispuesto la aceleración de la discusión del proyecto de ley, haciendo uso de las urgencias legislativas y además está promoviendo espacios de diálogo político para alcanzar los acuerdos que sean necesarios para su pronta aprobación. Por ello, felicitamos la decisión de las comisiones de Defensa y de Seguridad Pública del Senado, de llevar a cabo la discusión en particular de manera conjunta, para así poder despachar el proyecto de ley en el más breve plazo posible.

### Carlos Silva, encargado CSIRT de Gobierno:

# “Generamos distintos tipos de informes y alertas, con el fin de llegar con la información relevante y de forma oportuna a nuestros distintos públicos objetivos.”

Para ahondar en las amenazas más frecuentes y en cómo lograr una mayor cultura de ciberseguridad en los funcionarios públicos, conversamos con Carlos Silva, encargado CSIRT de Gobierno

**¿Como se evalúan las amenazas en este último año?**

Primero que todo, es importante destacar que las amenazas cibernéticas están presentes todos los días, y no es algo nuevo. Desde hace muchos años hemos visto cómo grandes empresas e instituciones han sido víctimas de un ciberataque y lo seguimos viviendo hasta la fecha.

Las amenazas son constantes. El tema es que hoy los delincuentes utilizan distintas técnicas y tácticas para comprometer infraestructuras, algunas de ellas críticas, es por eso que nosotros estamos observando una gran cantidad de tráfico las 24 horas del día, los siete días de la semana. Eso nos permite observar cómo cambian los ataques. Hoy son más sofisticados que antes.

A esto debemos sumar que el uso de las tecnologías implica un desafío cada vez mayor, dada la cantidad de software y hardware que utilizamos, los cuales pueden ser vulnerables.

Todos los días, los funcionarios públicos están expuestos a los diversos riesgos y amenazas desde sus dispositivos de trabajo. Y a ello hay que sumar la pericia de los atacantes, que van directamente contra los usuarios de los sistemas utilizando técnicas de ataques, como por ejemplo las campañas de phishing que contienen malware. Esta es quizás la mayor amenaza a la que se enfrentan los usuarios.

Al observar el comportamiento del tráfico que monitorea el CSIRT de Gobierno, se ha logrado identificar y bloquear más de 80 mil correos electrónicos con contenido malicioso. De ellos, el 47% contienen archivos comprimidos con extensiones como .zip, .Rar, .7z y .gz. Esos archivos contienen otros archivos que al ser ejecutados infectan a las organizaciones y son capaces de, hasta paralizarla. Además de esos tipos de archivos, hay otros que son más reconocidos por los usuarios. Me refiero a aquellos que son de tipo Word, Excel o pdf. Casi el 45% de las detecciones bloqueadas tenían este tipo de documentos adjuntos. Es por eso que siempre llamamos a seguir nuestras recomendaciones sobre no abrir archivos de correos de desconocidos o fijarse quien es el remitente del mensaje.

**¿Qué tipo de alertas son más frecuentes?**

Para el CSIRT de Gobierno todas las alertas son importantes y constituyen un potencial riesgo para las personas e instituciones. Por esto, generamos distintos tipos de informes y alertas, con el fin de llegar con la información relevante y de forma oportuna a nuestros distintos públicos objetivos.

Sin embargo, las alertas que generan mayor preocupación y revis-

ten una mayor importancia para el Estado son las alertas preventivas de seguridad cibernética, es decir, aquellos informes que advierten sobre nuevas amenazas, vulnerabilidades, mitigaciones, detección de agentes maliciosos, etc. Y que podrían afectar a las organizaciones en el momento en que las estamos advirtiendo.

***“Se ha logrado identificar y bloquear más de 80 mil correos electrónicos con contenido malicioso. De ellos, el 47% contienen archivos comprimidos”***

La relevancia radica en que al analizar y revisar el comportamiento del Estado nosotros podemos obtener una muestra de lo que ocurre en el país y llamar a tomar acciones a las organizaciones de la administración pública, las que están en convenio de colaboración y al público en general.

Desde enero hasta la fecha hemos identificado y bloqueado casi 5,2 millones de intentos de ataques para explotar alguna vulnerabilidad en la infraestructura del Estado y alrededor de 20 mil alertas a instituciones públicas, privadas y al público en general. Por ejemplo, las que se publican en el sitio del CSIRT tienen que ver con phishing, malware y vulnerabilidades, mientras que a las organizaciones se les envían tickets con las amenazas específicas sobre sus activos informáticos que podrían ser afectados por alguna vulnerabilidad.

**¿Cómo lograr una mayor cultura de ciberseguridad de los funcionarios públicos?**

La principal respuesta es la capacitación. Que los funcionarios cuenten con capacidades y habilidades para advertir que están frente a una amenaza es esencial.

Las capacitaciones son una importante parte del plan de trabajo elaborado por el CSIRT. Por una parte, nuestro principal objetivo es preparar y capacitar a los encargados de ciberseguridad y subrogantes, con el fin de entregarles más herramientas y conocimientos que les permitan proteger a sus instituciones.

Durante este año hemos logrado concretar dos instancias muy importantes en temas de capacitación para los encargados de ciberseguridad. La primera de ellas fue el desarrollo de un ejercicio de simulación de incidentes donde los participantes tuvieron que poner en práctica los conocimientos de gestión y la toma de decisiones, para afrontar y responder de manera efectiva y eficiente ante un ciberataque en el ámbito de la administración pública. La segunda iniciativa fue la inscripción gratuita al diplomado Seguridad de la Información y Ciberseguridad del Centro de Capacitación USACH. Desde agosto, cerca de 250 funcionarios están estudiando y se están capacitando en temas de auditoría, controles, implementación de SOC, entre otros temas.

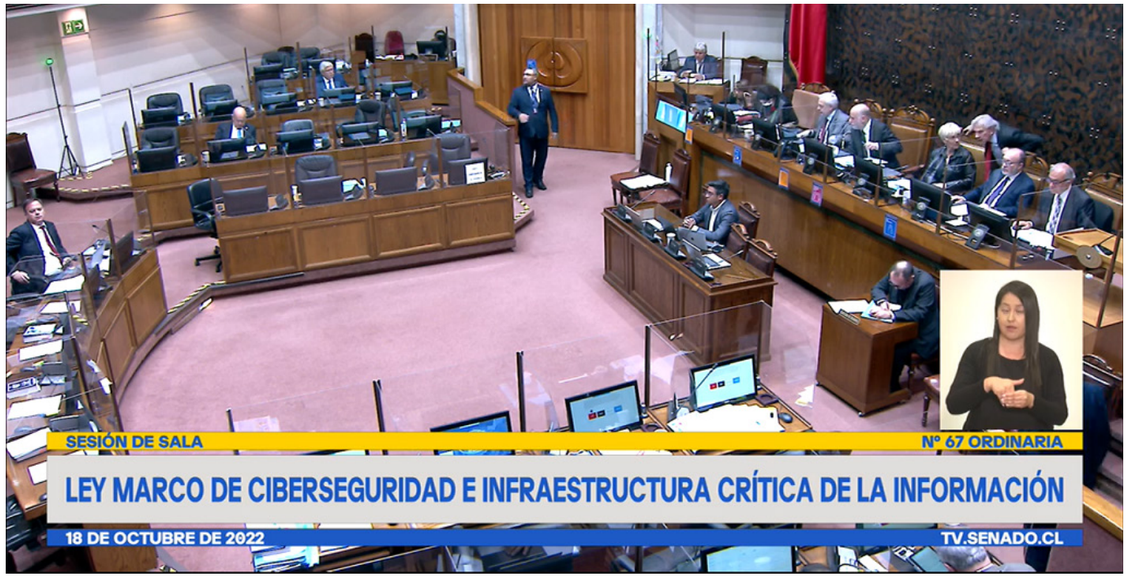
Por otra parte, también nos interesa llegar a los funcionarios públicos, a través de la concientización y educación. Para eso estamos realizando campañas utilizando distintos canales de comunicación y creando nuevas iniciativas. Sin duda es un trabajo largo, que requiere de mucha dedicación, pero también sabemos y confiamos en

***“Desde enero hasta la fecha hemos identificado y bloqueado casi 5,2 millones de intentos de ataques para explotar alguna vulnerabilidad en la infraestructura del Estado y alrededor de 20 mil alertas a instituciones públicas, privadas y al público en general. ”***

que siendo constantes, repetitivos y asertivos lograremos poco a poco crear una cultura de ciberseguridad en los funcionarios.

Estas iniciativas y parte de los proyectos que tenemos para este año y los próximos son también gracias a la colaboración y apoyo constante que tenemos por parte del sector privado, estableciendo alianzas estratégicas y convenios de colaboración.






# Senado aprobó en general Ley Marco sobre Ciberseguridad e Infraestructura Crítica

En sesión en sala realizada el pasado 18 de octubre, el Senado aprobó por unanimidad el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (BOLETÍN Nº 14.847-06).

Cabe recordar que el proyecto tiene por objetivo establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión y de responsabilidad por la infracción de la normativa.

La ley crea la Agencia Nacional de Ciberseguridad, organismo que tendrá como objetivo asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica.

En la sesión en sala estuvo presente Daniel Álvarez Valenzuela, Coordinador Nacional de Ciberseguridad y contó con la intervención de parlamentarios de los diversos sectores presentes en el Senado, quienes destacaban la importancia de la nueva normativa.

En el debate el Senador Kenneth Pugh, valoró que en el mes de ciberseguridad se apruebe este proyecto necesario para avanzar en la ciberseguridad de las personas. Por su parte el Senador Jaime Quintana, destacó que es un avance importante es establecer los principios que van a ordenar la institucionalidad en materia de ciberseguridad.

La aprobación en general del proyecto de Ley realizada por el voto a favor de los 38 senadores presentes en la votación, dio la unanimidad del Senado a que la normativa siga avanzando en el parlamento. Acordándose también que el proyecto se discutiera en particular en la comisiones unidas de defensa y seguridad pública, además de definir el próximo 11 de noviembre como el plazo máximo para recibir indicaciones.