https://transformacionpublica.cl/

Transcripción Coloquio 28.05.2021:

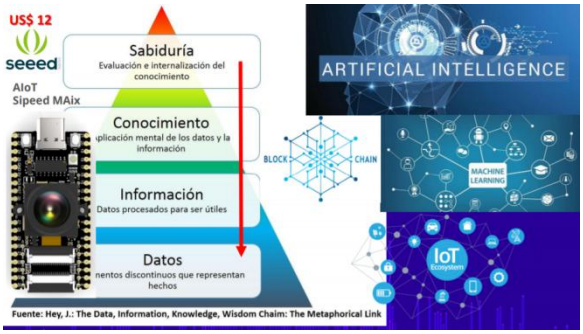
El ecosistema de la transformación digital en el Estado

Macarena San Martín: Bienvenidos a nuestro nuevo coloquio, organizado por Transformación Pública, esta es una nueva actividad, coordinada por este grupo de personas que somos uno apasionados por el valor que entrega la buena función pública, en especial en este tiempo de transformaciones. En este tiempo en que la Ley de Transformación Digital del Estado está impulsando a muchos servicios a hacer cambios radicales, queremos de alguna manera aportar en esta guía de cómo se han hecho las cosas, cómo se pueden hacer, qué cosas han funcionado y qué cosas no. Pueden revisar esta conversación en YouTube

Hoy tenemos de invitado a un gran orador, que nos va a mostrar su mirada respecto del Ecosistema de la Transformación Digital en el Estado. Personalmente, a mí me ha sido de gran interés ver la evolución que he podido verificar en sus presentaciones a lo largo del tiempo, porque nos está mostrando una forma en que el Estado se puede organizar y su mirada respecto a los problemas de ciberseguridad e interoperación que tenemos en el Estado. Me refiero al senador por la Región de Valparaíso, el señor Kenneth Pugh Olavarría. El senador Pugh tiene una larga trayectoria en la Armada de Chile, donde se desempeñó entre el año 1979 y 2013, retirándose con el grado de vicealmirante. Allí comenzó a formarse en los temas asociados a tecnología, desde sus estudios como ingeniero naval electrónico, y luego un magíster y dos diplomados. En la actualidad, desde su lugar en el senado, donde fue electo para el periodo legislativo 2018-2026, ha sido el impulsor de iniciativas como la Ley 21.113-2018 que declara a octubre como el mes de la ciberseguridad en Chile. Y actualmente, entre otras, impulsa una iniciativa que esperamos se convierta en reforma, a través del Boletín 13.582-07 para incorporar a la constitución el derecho ciudadano para relacionarse digitalmente con el Estado. Dada esta trayectoria, resulta importante conocer su mirada, provocarnos, y así tener esta buena conversación que esperamos, al final de su presentación.

Senador Kenneth Pugh: (03:53) Muchas gracias Macarena, agradezco a Transformación Pública esta iniciativa fantástica, porque ustedes la llevan desde la pasión y con conocimientos. Me gustaría hacerles una pequeña presentación de la articulación de la sociedad con el mundo digital y el nuevo rol que debe cumplir el Estado. Me he permitido también acuñar esta suerte de visión de un “Chile hacia una República digital”. Estamos discutiendo esto, va a ser un tema esencial. Y aquí viene algo que es fundamental,

tenemos que entender que esto tiene una base. Y por eso espero por la razón y la fuerza de los datos, o por la razón o la fuerza de los datos, porque los datos son esenciales. Son tan esenciales, son la base de la pirámide del conocimiento.



Ustedes pueden ver en la pirámide del conocimiento que en la antigüedad los datos eran obtenidos desde donde se podía y se registraba en libros. Salían expediciones en barco, una de ellas, la de Magallanes, en la que descubrió nuestro estrecho y dio la primera vuelta al mundo. Bueno, esos datos empezaron a ordenarse como información y las comunidades comenzaron a tener conocimiento, pero muy pocos llegaron a ser sabios. Los sabios eran las personas que lograban extractar y tomar lo mejor. Y cada comunidad los valoraba mucho. Esa es la historia de la humanidad escrita.

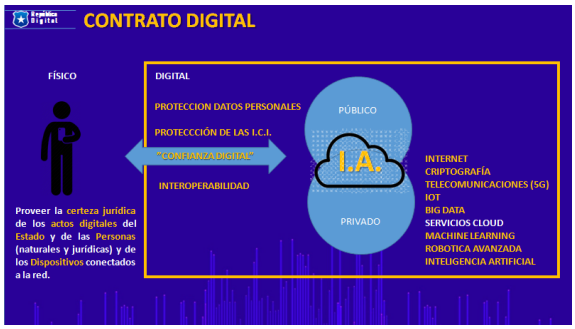
(05:33) Pero, ¿qué ha pasado hoy en día? Tenemos los datos en los dispositivos que se llaman IoT, que están tomando datos incluso sin conectarse físicamente. Lo están haciendo a través de las redes inalámbricas, podemos hablar mucho de ello. Pero esos datos son procesados, esa información y conocimiento se genera porque las máquinas empiezan a aprender a trabajar y finalmente se construye lo que hoy conocemos como la inteligencia artificial. Este es el mundo actual, este es el ecosistema que hemos construido, el primer ecosistema construido por la humanidad. Todos los ecosistemas anteriores, sean terrestres, marítimos, aéreos, el espacio exterior, algunos dirán: “salió solo”, otros mencionan a Dios, otros dirán lo que quieran, pero lo que hemos construido entre todos es este ciberespacio. ¿Qué nos pasa ahora, para comprender la complejidad? Que si no se hace con seguridad, y ustedes mismos lo explicaban, todo esto se puede caer. Han aparecido algunas técnicas como el Blockchain, que permite darle trazabilidad a la información y tener integridad de los datos. Por lo tanto, los datos ya sabemos de dónde vienen, cuáles son y no van a ser alterados por terceros. Sin embargo, lo que se ha apreciado, es que esta sabiduría colectiva que tenía el sabio hoy está en la base, en el dispositivo, y ese es un tema no menor. Por lo tanto, estamos en una nueva sociedad digital, con un nuevo ecosistema que se está construyendo con dispositivos, que además no necesariamente tienen que estar alambrados, y que están tomando decisiones. Ese es el ecosistema construido que tenemos que entender.

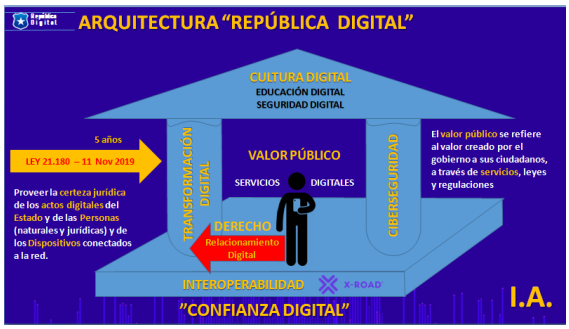
Somos 7,7 billones de personas, pero si sumamos a todos estos nuevos dispositivos a este nuevo espacio, tenemos más de 50 billones de habitantes que conversan, que entregan datos sobre las cosas que ocurren. Ese es el entorno en el cual estamos insertos y todo esto fluye con el comercio. El comercio es el que habilita las rutas y las rutas han sido de navegación. Ustedes pensarían que esas líneas son la carga marítima. Sí, la carga marítima viaja por el mar, el 94% de ella, pero más importante, es todo lo que acompaña a la data. Y esto es desde el siglo XIX. La data viaja por cables de fibra óptica, anteriormente eran cables de telégrafo submarino. Todas esas líneas que ustedes ven en el globo, bajo el mar, es el verdadero ciberespacio, es donde están ocurriendo todas estas transacciones. Si vemos así nuestro ecosistema es complejísimo, de carácter global. Se necesitan estructuras críticas como estos cables de fibra óptica, los servidores, todo lo que sea el despliegue. Bueno, de esto estamos hablando, esta es la globalización del siglo XXI, la globalización digital, donde converge el mundo físico con el mundo digital. Es por eso que es tan importante invertir. Fíjense que la inversión no es sólo del Estado. El Estado, a través de un proyecto que viene del gobierno anterior, que se llama "fibra óptica austral", desplegó un cable al le hemos puesto el nombre de Magallanes. Dicho cable de fibra óptica va a tener ese nombre, porque todos los cables tienen nombre. Este otro es el que llegó vía Google y se llama "Curie", reconociendo a Marie Curie, y une a Valparaíso con San Francisco. Pueden ver en la foto a Jayne Stowell, la encargada de los cables de Google (negociadora estratégica de infraestructura global), junto a la Ministra de Transportes Gloria Hutt. Google ha hecho una inversión gigantesca para tener independencia y poder mover sus datos. Pero también lo tenemos que hacer los estados, tenemos que entrar entonces a complementar los servicios, porque es imposible que un solo actor lo haga.

(09:36) Chile está proyectando un cable de fibra óptica hacia Australia, pasando por Nueva Zelanda, pero no podemos dejar nuestros territorios insulares desconectados. Entonces, la mejor forma de conectar a nuestro país, de conectarlo de verdad, es primero con la conectividad digital. La brecha de conectividad tenemos que disminuirla a cero y hay planes, incluso de los que podemos conversar más adelante en otro seminario.

¿Dónde está el problema? El problema es cómo compatibilizamos el mundo físico de las personas, con este mundo de lo digital. Ya sabemos que va a haber una convergencia y algunas películas de ciencia ficción muestran que nos implantan cosas, o personas implantadas a las máquinas. ¿Qué se requiere? Un nuevo contrato. Tenemos un contrato social de la época de Rousseau, entre personas, expresado en una constitución. Tenemos que relacionarnos con este mundo digital y lo primero que tenemos que establecer, el primer canal, es el de "confianza digital". No podemos entrar en un mundo en el que no confiemos en él, y gestionar el riesgo. Pero, ¿cómo vamos a crear ese puente de oro de la confianza digital? En primer término, hablar de la confianza digital nace de todas las tecnologías: Internet, criptografía, telecomunicaciones, IoT, Big data, servicios cloud, machine learning, robótica avanzada, inteligencia artificial.

La inteligencia artificial va a empezar a sustituir trabajos mecánicos apoyando a las personas, pero no reemplazando a las personas. Y esto es lo primero que debemos aclarar, porque la primera de las situaciones que se producen de forma natural en los ecosistemas es el temor. Yo tengo temor porque me puede reemplazar una máquina. Pero si empiezo a confiar, la confianza se va creando. Y esta es una de las condiciones más importantes, porque además yo tengo certezas, esto sirve para muchas cosas más. ¿Para qué? Para los procesos del Estado.





Interoperabilidad es clave, porque sin interoperabilidad es imposible crear la confianza digital. Y si uno tuviera que acompañar la interoperabilidad, para decir: ¿cómo lo hacemos para que siempre funcione? Para eso están las otras medidas que considera la ciberseguridad, que van desde la protección de los datos personales hasta la protección de la infraestructura crítica de la información: todos los cables de fibra óptica, los servidores, la redes. Entre todo eso, tenemos que ser capaces de confiar en la interoperabilidad. Ella es la única que nos va a garantizar la certeza jurídica. Y esto es fundamental no sólo para los abogados, sino para poder realizar todo lo que queremos hacer con la digitalización del Estado. Garantizar la certeza digital de los actos digitales del Estado, de las personas que se relacionan con el Estado, personas naturales y jurídicas de las empresas y también de todos los dispositivos que estén conectados a la red. Y cuando

hablo de dispositivos conectados a la red con certeza jurídica, por ejemplo, podemos tener en los postes de luz, cada cierta distancia un medidor de ruidos molestos. Y bueno, si hay ruidos molestos, el dispositivo informará con la cadena de custodia digital, con confianza digital, y eso puede alertar inmediatamente y generarse el control de una infracción, sin la necesidad de tener un aparato de fiscalización físico gigante.

Necesitamos la ayuda de las tecnologías. Para que le hagan bien a la sociedad tenemos que regularlas, para generar estos canales de confianza, punto de partida para nuestra transformación digital. Porque si no tenemos claro esto desde un principio, no sacamos nada con digitalizar por digitalizar. Sería básicamente transformar el computador en máquina de escribir y seguir haciendo lo que hemos hecho todos los años desde la invención de la imprenta. La confianza digital, es la que permite crear nuevos procesos que van a transformar realmente al Estado.

(15:07) Partamos entonces construyendo la casa digital del Estado, de la futura República Digital. La base es la confianza digital, sin ella no partamos. La confianza digital requiere de modelos de gobernanza que se basen en estándares, por ejemplo, y yo lo pongo en la misma plataforma, X-ROAD. Ese es un estándar abierto, gratuito, desarrollado por los gobiernos de Finlandia y de Estonia, que se distribuye para ser la capa técnica de los modelos de gobernanza. Tiene KSI Blockchain, permite toda la trazabilidad de la data con su integridad y sobre él uno construye. Hay países que ya lo usan para el traspaso de datos seguro: Colombia, desde el año pasado está cambiando toda su plataforma de interoperabilidad del Estado con confianza digital basada en X-ROAD. En el cono sur, en la provincia de Neuquén en Argentina ya está funcionando casi dos años con una experiencia extraordinaria. Los estamos probando ahora en la Región de Valparaíso. Con la Provincia de Mendoza estamos haciendo el primer piloto, se llama Puente Andino, con privados, porque obviamente al Estado le cuesta, más aún, confiar en otro Estado. Bueno, el desafío más grande es lograr confianza digital con los vecinos. Si necesitamos movimientos de personas, movimiento de carga, debemos tener servicios que sean capaces de conectarse. El mejor ejemplo de cómo no lo estamos haciendo bien, es hoy el proyecto más importante, ya instalado, en el Paso Los Libertadores se construyó un edificio gigantesco, nuevo, maravilloso, con cuatro servicios chilenos, tres servicios argentinos, viviendo los 7 en el mismo edificio, pero hay 7 servidores que no se conectan. Se pasan en pendrive la información de un servicio a otro. Bueno, eso es no estar en el siglo XXI. No sólo tenemos que transformar nuestro Estado, sino que tenemos que transformar la relación entre los estados. Puente Andino es una forma ¿Qué se tiene que hacer? Transformación digital, obviamente. Debemos tener servidores conectados, data interoperando y todo lo que conlleva, que lo vamos a ver pronto. Tenemos este pilar de la transformación digital. Y el

sistema debe tener también algo que es muy importante, que viene a ser el techo: Cultura digital, con educación digital y seguridad.

Pero si ustedes se fijan, todo eso que estamos construyendo se cae si no consideramos algo que siempre tiene que ir al lado, que es la ciberseguridad. Entonces, no podemos construir una casa digital si no tenemos fundaciones sólidas, de confianza digital, con una plataforma de interoperabilidad adecuada, si no tenemos pilares robustos que permitan el desarrollo digital, pero que tengan ciberseguridad. Y esto debe tener su techo, un cambio cultural completo, porque la transformación digital a la larga es transformación de personas. Son las personas las que se transforman, las personas y los procesos, porque, la tecnología está disponible, las personas entienden la tecnología y cambian los procesos. Entonces, cambiemos a las personas para cambiar los procesos y usemos la tecnología para agregar valor público y así tener mejores servicios digitales.

Entendiendo estos mejores servicios digitales, junto con todo lo que es la modificación a la legislación, como ese valor público agregado, no sacamos nada con servicios públicos que no tienen toda la regulación que se requiere para sus empleos. Entonces, el valor público se da en los dos lados. En el cambio de las reglas, las formas en que se generan, cómo se controlan y en los servicios digitales que están entregándose. Es convertir los estados y los gobiernos al servicio de las personas. Gobierno como servicio. Es el servicio digital del Estado como algo potente, tan potente, que no es necesario postular a un beneficio. Nada más absurdo que las postulaciones a los beneficios. Es no entender las capacidades del Estado.

Por eso yo valoro que tengamos aprobada la Ley 21.180. Con mucha satisfacción siempre reconozco la gentileza del entonces Presidente, Senador Jaime Quintana, quien pidió permiso a la sala para que en la última sesión para despachar esta ley se me autorizara para ser el Presidente accidental del Senado. Y así fue, la sala lo otorgó y pude presidir y despachar ese proyecto de ley en su último trámite, para que se convirtiera hoy en la Ley 21.180. Tenemos el reglamento publicado, por lo tanto, el plazo de 5 años partió contando. Y aquí es donde todos tenemos que ponernos de acuerdo para sacarla adelante.

¿Qué propongo entonces? La contraprestación. Si el Estado está obligado a transformarse, bueno, ahora el ciudadano tiene que tener algo a cambio. Ese es un nuevo **derecho al relacionamiento digital del ciudadano con el Estado**. Y, ¿por qué? Porque yo ciudadano tengo el derecho a tener elementos, que se los voy a explicar a continuación, que me permiten pedirle al Estado digitalmente todo. Y si yo tengo ese derecho, el Estado me tendrá que conectar primero. Entonces, el conectarse a internet, el derecho a acceder a un servicio público, el darle internet a todo el mundo, es para relacionarse digitalmente

con el Estado. Entonces, ese solo hecho de tener un derecho garantizado en materia de relacionamiento digital, conlleva no solo la conexión al dispositivo, incluye además la identidad, los procesos, todo. Es la forma de interactuar con este ecosistema digital. Yo espero que ustedes me ayuden, es lo único que yo les pido. Ayúdenme a llegar con este mensaje, transformemos este mensaje que lo podamos poner en nuestra Constitución. Y con ustedes vayamos a hablar con todos los constituyentes y explicarles porqué creemos que es tan importante este momento histórico que estamos viviendo. Podemos construir perfectamente una República digital, con una base sólida, con todos estos principios que estamos hablando y con un nuevo derecho garantizado para los ciudadanos. Bueno, seríamos visionarios.

Entremos entonces en los pilares de la transformación del Estado. El Estado tiene muchos datos, dispersos y los pide siempre datos. De hecho uno solicita permiso a la Comisaría virtual y me siguen pidiendo los mismos datos que ya tiene. Y me los siguen pidiendo y me los siguen pidiendo. Llevamos años haciendo esto y seguimos aguantando. Y es lo que nos falta.

Primero tenemos que educar digitalmente a la gente que trabaja en el Estado. La educación digital no es usar el Excel. De hecho, si ustedes quieren destruir a una organización, regálale Excel, porque todos los datos van a estar sueltos, no van a estar controlados, nadie sabe la versión, las prioridades cualquiera las cambia, los valores en las celdas se borran. O sea, si ustedes quieren destruir un Estado, regálale una planilla de cálculo, de cualquiera marca. Eso no es digitalizar el Estado. Entonces, la primera educación digital es: ¿para qué sirven estos medios digitales? , ¿Cómo podemos resolver las tareas digitales?, ¿Qué habilidades y competencias del siglo XXI debo tener, para desarrollarlas? No las tenemos definidas, hasta el momento creemos que es solamente hacer clases de Excel.

(22:21) Lo segundo, debemos estar todos conectados. No puede ser que tengamos comunas que no estén conectadas con fibra óptica. Y cuando digo todas, las 345, incluidas las dos insulares, el Archipiélago de Juan Fernández, y Rapa Nui, Isla de Pascua. Ya llegamos, y ¡qué bueno!, a la comuna más austral del mundo: Puerto Williams.

Lo tercero, la digitalización de los servicios. Tenemos que entonces que invertir en las tres áreas: en las personas, para que entiendan el valor que tiene la digitalización y todo lo que se puede hacer; la conectividad para funcione bien, con un buen ancho de banda. Y, la más crítica: digitalizar los servicios. Digitalizar los servicios no es hacer el formulario en la pantalla, no es llenar un PDF, eso no es digitalizar, es no entender para qué estamos. El papel es un soporte de una transacción. En la práctica, la transacción es suficiente, no se necesita absolutamente nada más. ¿Para qué quiere un Certificado de nacimiento si usted

sabe cuando yo he nacido y usted mismo verifica digitalmente la transacción y luego lo comprueba? Entonces, no me pidan certificados, ni siquiera me pida los certificados digitales, eso es un absurdo. ¿Para qué quiero imprimir un papel si lo que necesito es un servicio del Estado? El Estado tendrá que verificar los antecedentes y para eso los tiene. Entonces, tenemos que cambiar la forma en que digitalizamos los servicios, fundamental partir desde la base.

Lo primero, una buena y nueva identidad digital. No tenemos identidad digital, no se está ocupando. La identidad digital viene de la mano con un proceso que se está licitando en estos momentos. Yo les pido que lo sigan porque es muy importante, porque aquí es donde está la clave donde comienza nuestro proceso de transformación. Es dándole una buena identidad digital, una identidad digital segura, que no sea clonada. Que cuente con los dispositivos especiales, la tecnología que lo permita, para que además la identidad sea parte de la comprobación de seguridad, ya sea leer o verificar con los elementos que tenga, pero como uno de los factores, no el único. Debemos tener segundos y terceros factores de autenticación, para decir que efectivamente somos la persona que dice ser, y esto se puede lograr con diversos medios.

(24:56) Después, habilitar las firmas electrónicas avanzadas, para que nuestra voluntad se exprese con el más alto estándar de seguridad y se comprometa completamente. La firma electrónica avanzada, FEA, son fáciles de integrar con las identidades digitales. Y finalmente, disponer de domicilios digitales. Y esto no es la casilla e-mail que nadie verifica, sino que es el lugar donde alguien ingresa, un espacio que está en el ciberespacio. Básicamente, reside en un disco duro donde están almacenados siempre todos los documentos, todo lo que la persona necesita saber, más los accesos que pueda tener.

Si ustedes se fijan, en el ejemplo que hemos puesto, esto debiera cambiarle la vida a Marcela. Ella debiera entregar una sola vez el dato y nunca más se lo debe pedir el Estado. O sea, el Estado lo guarda bien y lo usa. Y después, con técnicas Push (empujar), el Estado entrega servicios digitales a Marcela, o se comunica con ella. O si Marcela requiere algo a través de las APIS (interfaces de programación de aplicaciones) que se desarrollan por el

mismo Estado o por privados, ella obtiene nuevos servicios. Este modelo de relacionamiento digital del ciudadano con el Estado no es solo la Clave Única, esto es mucho más, esto es entender un nuevo Estado que tenemos que construir. Quienes ya lo han hecho, les pongo el ejemplo de Estonia, que lo ha llevado a la sofisticación. De hecho ellos miden separado el Índice de Desarrollo Digital de todos los países y el Índice de Ciberseguridad. Recuerden los dos pilares que les hablaba. Estonia lo hace.

Y no solo eso, tienen una Academia de Gobierno Digital, los invito a seguirla. Ellos además desarrollaron este instrumento de medición para saber cómo están, con métricas. ¿Quiénes están avanzando? Chile estaba en el número 52 el 2018, ahora ya vamos en el número 36, lo cual es muy bueno, pero sólo avanzamos en ciberseguridad. En transformación digital seguimos en el mismo nivel 65. O sea, subimos en la escala porque hemos tomado más medidas de Ciberseguridad, no es porque nos hayamos transformado mejor digitalmente, o sea, hay un desafío pendiente. Estonia también privilegia la protección de los datos personales y la protección de la infraestructura crítica, que son los dos elementos esenciales que, les decía, debe tener todo modelo. Tomemos el ejemplo de Estonia, porque ellos nos dicen que no se puede hacer transformación digital sin ciberseguridad, esa es la primera de las conclusiones.

Veamos cuáles son los grandes riesgos mundiales, el año en que partí con las primeras leyes hablando de ciberseguridad, no había ninguna antes, teníamos 2 de los 4 riesgos más grandes de la humanidad en el mundo tecnológico: los ciber ataques y todo lo que era fraude de identidad para el robo electrónico. Hoy en día, curiosamente, apareció la pandemia, sigue la ciberseguridad, pero ya se habla de fallas de ciberseguridad. Tenemos los dispositivos, todo, pero se nos olvidó poner el ticket en la casilla, o habilitarlo. Bueno, ahora tenemos la capacidad y la podemos usar.

(28:05) Pero, ¿qué es lo que nos pasa? Fallamos en usar las capacidades de ciberseguridad que tenemos. Eso es lo que le está ocurriendo al mundo en 2021. Y los riesgos siguen siendo tan importantes y tan graves. Ocurren con frecuencia, y cuando ocurren, el impacto que generan es muy alto. Chile ha sido desde el inicio de las mediciones un

referente latinoamericano. Somos el país que tiene la mayor cantidad de conexiones a internet móviles. El 2016 la OEA publicó este Reporte de ciberseguridad, consultando si estábamos preparados o no. A mí me llamó mucho la atención. Ya estaba retirado en esa época, era asesor externo del Ministerio del Interior, en el desarrollo de la Política Nacional de ciberseguridad que salió al año siguiente, 2017. Pero el 2016 no me di cuenta de algo que me percaté después, que ese modelo que nos estaba midiendo había sido desarrollado por la Universidad de Oxford. La Universidad de Oxford hizo el Modelo de madurez de las capacidades de ciberseguridad para naciones, el instrumento de métrica que nos permite entender cómo este proceso de transformación digital se tiene que hacer de forma segura. Y la ciberseguridad, primero, hay que declararla, tenemos una política desde 2017, pero la estrategia es la que nos está fallando. Nuestra política actual al 2022 mezcla cosas de una política y cosas de una estrategia. La política tiene que ser permanente y veremos qué aspectos cambian, pero una política tiene que orientarnos. Y la estrategia tiene que ser la forma en que vamos a abordar, año a año, con los presupuestos, con las métricas, con todos los elementos que nos permitan llevarla adelante. Yo lo que espero es que seamos capaces el próximo año, en que tenemos la tarea de actualizar la Política nacional de ciberseguridad, de separarla en dos. Dejarla en una política permanente y hacer una estrategia que sea a 4 años, para que cada gobierno se encargue de avanzar y se comprometa a cumplir.

(30:34) Lo segundo, el fomento de una sociedad responsable en el uso de las tecnologías, y esto es cultura. Esta cultura es precisamente lo que hablamos en la primera ley, lograr el cambio cultural en las personas, entendiendo qué estamos enfrentando. Lo tercero, bien importante, el desarrollo de conocimientos de ciberseguridad. Si los países no entienden de qué están hablando y no son capaces de desarrollar incluso sus propias herramientas, no van a saber nunca enfrentar esta amenaza cambiante que tenemos. Una vez que tenemos estos 3 elementos, recién podemos empezar a formular el marco jurídico y regulatorio. Tenemos que entender que los 3 elementos van antes para lograr impulsar un marco jurídico, porque sin los otros es imposible. Y finalmente tenemos que hacer la gestión del riesgo, a través de los estándares, la tecnología y las organizaciones. Entonces,

estos 5 elementos se miden por separado, porque cada uno de ellos es un elemento propio de sostén, cada uno aporta a que esto funcione bien. Eso motivó a que fuéramos a Oxford para tratar de entender el desarrollo del conocimiento en ciberseguridad, cómo se había hecho. Ahí estuvimos con el profesor Michael Goldsmith, él es el padre del Modelo de madurez de capacidades de ciberseguridad para las naciones. Como este es un tema de Estado fuimos con el senador Álvaro Elisalde, actual Presidente del Partido Socialista, porque como Estado tenemos que enfrentar esto como una tarea permanente y debemos ser capaces de resolverla.

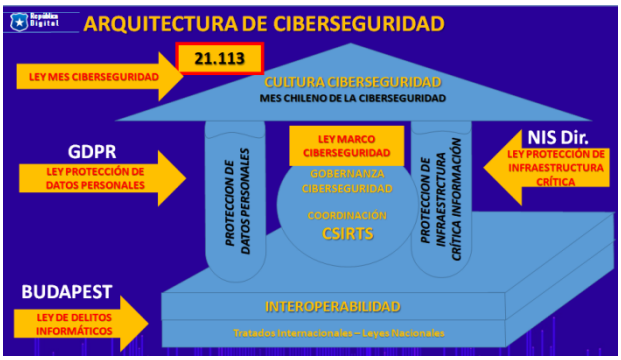
(32:07) ¿Quiénes están haciendo lo mismo en otro lado? En Australia en la Región de Victoria, 8 universidades se unieron en el Oceanía Cyber Security Centre (OCSC). Y ellos también usan este modelo de madurez. La gracia es que a nosotros el modelo de madurez nos sirve porque todo el continente ha sido medido. Tenemos 2 mediciones: 2016 y 2020.

Es una métrica que nos permite ver si nuestra política pública está funcionando o no, sin ser auto complacientes. Aquí vienen quizá las primeras recomendaciones: ¿qué métricas estamos usando para ver cómo avanzamos en transformación digital? Yo les estoy mostrando las del área de la ciberseguridad. Me gustaría con ustedes ver cuáles tenemos en transformación digital. En el área de la ciberseguridad, en estas 5 perspectivas medidas, podemos ver que hay aspectos en los que hemos subido. En general todo ha sido de 2 a 3, o sea, estamos a mitad de camino. Tenemos un par de cosas que somos buenos, pero el resto estamos 2 a 3. ¿Qué hacemos entonces? Política pública. ¿Cómo logramos mejorar y cómo logramos que esto nos vaya ayudando a transformar el Estado? Este va a ser el desafío para el trabajo de actualización de la política, el próximo año. Tenemos que salir, basados en estos antecedentes, con algo mejor.

Y sumémosle que todo lo que ya conocíamos crece de forma exponencial. Porque tenemos nuevas tecnologías. se licitó y ya se entregó todo el espectro 5G, en 26 Gigas, que es la frecuencia más alta para automatización avanzada y 3,5 Giga Hertz, que es la que vamos a ocupar nosotros en nuestros teléfonos, y que probablemente es la que más va a ocupar el Estado. Pero la cantidad de dispositivos que se van a conectar es gigantesco, y

eso hay que reconocerlo, vamos a aumentar la superficie de exposición al riesgo. O sea, va a haber mucha mayor probabilidad que nos ataquen, y si alguno de esos ataques es exitoso puede producirse un problema grave.

(34:10) Y lo otro que hemos detectado: se mantiene la brecha de género de mujeres en tecnologías digitales y en ciberseguridad. En Chile es menos de un 9%. Y aquí hay una pérdida de capital humano valioso. Las mujeres son talentosísimas, tienen experiencias increíbles. Yo fui en España a ver el Centro de ciberseguridad de una empresa que opera cables submarinos a nivel global y en el área de mayor especialización la gran mayoría eran mujeres. Yo pregunté si tenían una política especial, y no: son las que mejor califican. Aquí hay que entender que nos estamos perdiendo de un segmento importantísimo, porque no hemos hecho la difusión correcta ni dar las oportunidades. Porque esto nace de la misma cultura que tenemos. En ciberseguridad debemos cambiar la cultura y los números. Estas son cifras que también podemos ir midiendo para ver si efectivamente la política pública que vamos desarrollando permite que esto vaya avanzando.



¿Qué hay que construir? la arquitectura de ciberseguridad. Ya hablábamos de la interoperabilidad, la base, todo lo que es la plataforma, pero eso se sostiene sobre un marco global: los tratados internacionales y las leyes. La primera ley importante, la Ley 21.113-2018, que permite tener un mes dedicado a 2 cosas: primero, la promoción y difusión de conocimiento. Las amenazas cambian todos los años, no se repite nada, siempre estamos viendo cosas nuevas: hay ideas nuevas y hay tecnologías nuevas,

entonces hay que actualizarse todos los años. Lo segundo: los ejercicios nacionales de ciberseguridad, igual como se tiene en los colegios, con las operaciones DEYSE, que a edad temprana saben evacuar en caso de terremoto. Como se hace ahora con las evacuaciones de tsunami. Bueno, lo mismo acá, debemos ser capaces de probar si sabemos, si es que somos atacados de forma masiva, qué vamos a hacer. No cuesta nada. ¿Pero qué hemos incorporado? Las competencias. Igual que en el fútbol, campeonatos nacionales e internacionales, donde nuestros equipos puedan mostrar sus destrezas y habilidades.

(36:5) Lo segundo: lo que se está haciendo con la Ley 19.628 sobre Protección de Datos Personales, aquí se incorpora el Reglamento Europeo de Protección de Datos Personales, porque es un estándar mundial de muy buen nivel y lo hemos adaptado a nuestra legislación. Esto está en el primer trámite legislativo, está en la Comisión de Hacienda del Senado. Yo he pedido que le den suma urgencia, porque no podemos quedarnos con esta ley atrás, porque impide que podamos desarrollar todo el sistema.

La tercera ley está relacionada con el marco global internacional. El mismo año 2017 en que la presidenta Bachelet publica la Política nacional de ciberseguridad, Chile adhiere a la Convención de Budapest, que permite perseguir el Cibercrimen transnacional. El Cibercrimen no tiene fronteras y el único mecanismo es a través de estos instrumentos internacionales. Por lo tanto, tomamos aquellos aspectos que están en dicha convención, y se pusieron en la Ley 19.223 de delitos informáticos. Ley que es del año 1993, antes que naciera la gran mayoría de los adultos jóvenes que están usando las tecnologías. Bueno, esa ley tenemos que actualizarla. La buena noticia es que está en su tercer trámite legislativo. Ya fue despachado de la cámara de diputados al Senado y estamos próximos a promulgarla. Hay un pequeño detalle respecto de hasta dónde se va a considerar investigación avanzada en ciberseguridad o delito. Vale decir, quién se metió, hasta dónde, qué hizo, para separar los investigadores de los delincuentes. No queremos que se confundan los dos roles, ni que algunos usen los dos roles. Son dos roles necesarios si queremos una industria nacional de ciberseguridad.

¿Qué falta? Falta y no se ha ingresado todavía algo que permita regular la Protección de la infraestructura crítica. La recomendación es usar las normas NIS europea, no las NIS americana que es algo más genérico, las NIS europeas son mucho más prácticas y claras. Y todo esto con una Ley Marco de ciberseguridad. Espero que se ingrese durante el segundo semestre, se ha estado trabajando, y esto permitiría darle forma a este ecosistema con el pilar de la seguridad. El ecosistema se soporta con estos elementos, si no los tiene obviamente va a ser frágil. Y un ecosistema frágil no da confianza. Entonces, tenemos que avanzar en consolidarlo, desplegarlo, instalar fibra óptica, instalar 5G, empezar a cambiar

los procesos pero con ciberseguridad, porque si no la hay, va a ser abandonado, nadie va a querer meterse, los riesgos son muy altos.

Esa ley de delitos informáticos entonces, tal como lo señalé, es la primera que se va a promulgar muy pronto. Estamos con el senador José Miguel Insulza, los dos apoyamos bastante para que esto ocurriera en la Comisión del Senado, que me tocó integrar cuando tramitamos esa ley. Y el Estado ha tomado las buenas prácticas, no teniendo todavía una autoridad nacional, el Estado ya dispuso un Instructivo Presidencial con varias medidas y normas, todo lo que se debe tener para enfrentar de forma transitoria, con una gobernanza transitoria, esta situación.

¿Qué sigue? seguir desplegando la ley 21.113 todos los años. Todos los años en el mes de octubre tenemos que hacer difusión de conocimiento y ejercicios nacionales. Los ejercicios nacionales son fundamentales, y la difusión de conocimiento comienza desde el Parlamento.

El año pasado con la senadora Adriana Muñoz hubo una sesión especial del Senado y escuchamos a los referentes europeos: la Directora del Instituto de ciberseguridad español, y también Chema Alonso, un investigador de ciberseguridad avanzado, uno de los hackers más reconocidos. Y era increíble ver a este hombre con su gorro de lana hablando a los senadores. Eso es lo que tenemos que lograr, que se entienda el problema para que

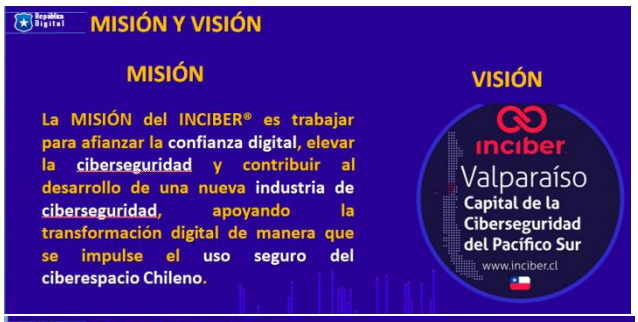
se pueda legislar con toda la información. Durante el mes tuvimos seminarios internacionales, al creador y dueño de Kaspersky y sus sistemas de anti virus, él es ruso, pero esa es la gracia de las redes, permiten poner a las personas en contacto, intercambiar información.

(41:10) Chile puede tener un rol protagónico en todo este proceso de transformación brutal que está viviendo la sociedad. Esto no le está pasando sólo a Chile, el mundo entero está siendo transformado: cultural, social, económica y políticamente. Las redes, las tecnologías digitales, lo que está disponible, es un medio que nos puede ayudar a hacerlo mejor. Para crear un sistema que nos dé la tranquilidad que si estamos digitalmente funcionando, nuestros datos van a estar protegidos. Y si no están protegidos, porque nosotros dimos un consentimiento para que se usaran para un fin específico y eso se vulnera, denunciarlo a la Agencia nacional de protección de datos personales. Una agencia que ojalá tenga la máxima autonomía posible, para que ella multe o al Estado o al privado, al que no haya hecho uso correcto de los datos que yo he entregado. Entonces, ahí se parte garantizando el derecho constitucional, con una institucionalidad, con autonomía, para que pueda regular esto.

También, los que ataquen la infraestructura crítica sepan que van a tener una fuerza que se va a encargar de evitar que eso ocurra. Necesitamos entonces de este centro de protección de infraestructura crítica. La Autoridad nacional de ciberseguridad que es la que está en discusión, no sabemos la forma, el organigrama que va a tener, pero lo que sí sé es que va a tener que trabajar en red. No existen sistemas jerarquizados, y por eso el trabajo de los CSIRT, los centros de respuesta a incidentes son fundamentales. Y tienen que estar en cada uno de los lugares: la red de conectividad del Estado, de las FFAA, las infraestructuras críticas, el de los bancos, todos los deben tener.

Y es esencial el conocimiento. Si no tenemos gestión del conocimiento, desarrollo de talento, Chile va a ser un esclavo digital. Necesitamos tener independencia digital, y por eso he propuesto la creación de este Instituto de ciberseguridad. El INCIBER, para acrecentar la confianza digital y ayudar a desarrollar la nueva industria de ciberseguridad. Hay gente que se ríe y me dice "es que no hay industria de ciberseguridad". Yo les digo que en 1978 estábamos en una crisis grande con Argentina. Bueno, el 78 no existían salmones en Chile, llegaron el 79. Chile hoy es la segunda potencia más grande exportadora de salmones del mundo. Las industrias se pueden desarrollar, se pueden regular mucho mejor, pero no necesitan que estén antes, tenemos que encontrar las oportunidades. Lo hizo España con su Instituto de ciberseguridad. Rosa Díaz, su directora, nos ha ayudado y contamos con el apoyo fuerte del Gobierno español para sacarlo

adelante. Y también Estonia, con la Presidenta de Estonia que estuvo de visita en Chile, firmamos los convenios, y con ella inauguramos capacidades.



Quiero mostrarles el antiguo edificio tecnológico CORFO en Curauma, se compró para la PDI, y se instaló en un piso el lugar para el laboratorio avanzado de ciberseguridad. Nuestra PDI necesita de herramientas avanzadas y especializadas para perseguir ciber delitos, que no están disponibles en el mercado. Están trabajando 2 universidades locales, U. Santa María y la UAB, para desarrollar estas herramientas especializadas. El evidencia del delito puede estar en la memoria RAM de un PC, si se apaga el computador se acabó la evidencia y no hay delito, así de complejo es perseguir el ciber delito.

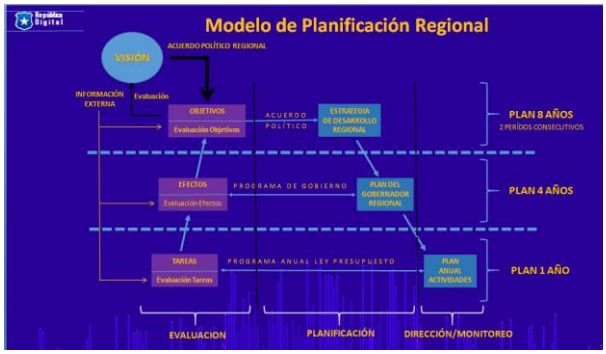
(44:30) Pretendemos como región ser la primera región con interoperabilidad, con el ejemplo de Mendoza: desarrollar un polo tecnológico. El Estado necesita articularse en los territorios, son las cosas importantes que el Estado tiene que hacer. La digitalización permite la descentralización, la confianza digital permite entregar responsabilidades a terceros, y así funcionar desconcentrados. Hoy está todo concentrado en Santiago y en procesos en papel. Si queremos lograr una regionalización efectiva tenemos que entregarlo de forma acertada, transaccional, como la cartola del banco: los recursos están, se ocuparon o no, con respaldos y todo funcionando. Y vamos a tener Contraloría y auditorías en línea ¿por qué? porque vamos a tener procesos transaccionales. Esto es lo que esperamos lograr en Valparaíso, para la comunidad. El Parque Barón se está desarrollando, son 14 hectáreas. Este es un convenio entre la Empresa Portuaria de Valparaíso y el MINVU. A ese parque nosotros queremos agregarle con las universidades e institutos de educación superior de Valparaíso, un parque de pruebas de todo lo que son

las transformaciones digitales, inteligencia artificial, sistemas 5G. Esto se puede hacer, basta poner un alambrado, poner las antenas, poner las redes especiales. Y tenemos caminos industriales, tenemos muelles, espacio para que vuelen helicópteros. Y verificar si efectivamente las creaciones chilenas funcionan, porque además va a haber otro equipo, que es el equipo ciber que va a estar tratando de destruirlo. Lo mismo que les decía a ustedes, un buen sistema es capaz de resistir un ataque, porque en ciberseguridad lo que se requiere es que los sistemas sean robustos. Y si se llegan a caer tienen que ser resilientes. Esa capacidad de respuesta es la que uno mide con los ejercicios.

Eso es lo que buscamos para Valparaíso, tener todos estos medios, oficinas, centros de pruebas, laboratorios avanzados, tanto con las policías como con las FFAA. Y se materializa en personas. Cuando les hablaba del INCIBER, tienen al oficial de la PDI que está a cargo, la doctora Romina Torres de la UAB, las personas que están en mi equipo legislativo del Senado, el doctor Xavier xxx de la U. Santa María, y otras personas, estos son los elementos humanos que están detrás desarrollando estos ecosistemas. No nos olvidemos de las personas, en las personas reside el conocimiento, y son ellos los que transforman la sociedad.

(47:23) Para ir terminando, quiero compartir por primera vez el modelo que podríamos acordar, para lograr aunar esfuerzos. No sabemos cómo van a funcionar los gobiernos regionales, pero esto se tiene que hacer con transformación digital. Entonces, lo primero es acordar una visión, si nos ponemos por ejemplo el 2030, los ODS, los objetivos de desarrollo sostenible de la ONU, un acuerdo político. Tomemos los objetivos, hagamos el

acuerdo político, desarrollemos nuestra estrategia de desarrollo regional, es fundamental. Es lo que tienen que comprometer los gobiernos en estos momentos. Y esa estrategia es la que tiene que orientar al Plan del Gobernador Regional. Los Gobernadores van a partir ahora, deben ser capaces de generar su Programa de gobierno de 4 años, que converse, que podamos medir los efectos y saber si vamos cumpliendo los objetivos de nuestro plan estratégico regional. Y ahí viene el desafío del año a año, que es construir el Plan anual de actividades con el presupuesto. Y ese programa tiene que venir en la Ley de presupuesto y se tiene que medir cada una de las tareas comprometidas



Si somos capaces de conectar estos 3 niveles: el nivel del largo plazo, de la estrategia del Gobierno regional, que puede ser 8 o 10 años, la propuesta va a ir por lograr algo que se conecte, junto con el proceso de medición. Tengo que ir entregando información, planificación, ejecución, y viendo que esto se vaya reciclando. Todo se monitorea a base de la ejecución anual, esa es la que permite darle dirección al sistema. En el monitoreo debiéramos estar viendo las transacciones, las cosas que están ocurriendo digitalmente, para saber si esto funciona o no. Podríamos empezar a estructurar un sistema en cascada, con realimentaciones. Estos sistemas son ultra estable.

(49:34) Con fases: planificación, ejecución, dirección y el monitoreo. Y finalmente la fase de evaluación. La idea es tratar que los gobiernos regionales tengan planes al menos para 8 años, porque por ley pueden tener una reelección. Especificar a dónde vamos y hasta dónde podríamos llegar. Los planes de 4 años, que serán los planes que cada Gobernador quiera instalar. Y finalmente el Plan anual, para asignar los recursos en el Parlamento. Y esto se puede medir, y se puede ver si está resultando o no, para lograr la máxima efectividad de todas las inversiones, tanto del Gobierno central, que son las más grandes. Luego las que va a hacer el Gobierno regional con el FNDR, en el Consejo Regional. Y finalmente las inversiones privadas. Cómo articulamos las 3 para que sean parte de este plan y podamos medirla, ese es el desafío. ¿Y dónde llevarlo a cabo? Por ejemplo, Isla de Pascua, Rapa Nui, se presta como un lugar ideal de prueba para políticas públicas 2.0.

(51:45) Esto lo discutimos con José Inostroza en la Comisión Desafíos del Futuro, porque estamos viendo cómo podemos hacer un sistema integrado de datos para mejorar la política pública, temas de ciberseguridad, de plataforma, entre otros.

Finalmente, todo este trabajo parlamentario está sirviendo también a otros países. Junto con la OEA creamos el Laboratorio de ciberseguridad para los Parlamentos de las Américas, con un Consejo de innovación. También hemos trabajado con el Parlamento Andino, para que estas normas sean parte de lo que ellos han desarrollado. Y como les expliqué, todo desde el Senado, en la Comisión en la cual estamos sesionando permanentemente.

Quiero felicitarlos, creo que el tema que ustedes están manejando es muy importante para el país, más aun en estos momentos trascendentes de la creación de una nueva República, que tiene que partir con lo mejor que podamos aportarle. Y si tenemos algo, es el conocimiento, la experiencia, lo que a ustedes les ha tocado vivir.

(53:13) José Inostroza: Senador, muchísimas gracias. Haciendo un elogio, creo que en síntesis es muy contundente la presentación. Toca muchos aspectos, es bien impresionante, así que hay una amplitud interesante y estratégica. Lo felicito, está muy bien fundamentado conceptualmente. Y está en un buen nivel en el sentido de que no entra en detalles técnicos. Lo coloca muy bien a nivel de arquitectura conceptual y eso se agradece muchísimo. También hay que destacar el aspecto político, que explícitamente usted señale que esto es un esfuerzo de Estado, transversal, y vemos como está trabajando en equipo con mucha gente. Y por cierto, el entusiasmo. Ha generado mucha energía, mucha narrativa, que en este caso es muy importante. Antes de dar la palabra al resto quisiera hacer la siguiente pregunta: tenemos dificultades para iniciar una narrativa que entusiasme a mucha más gente, porque estos temas son caracterizados como muy técnicos y cuesta hacer el puente y la comprensión estratégica, incluso en el mundo político. Buena parte de nuestros problemas tienen que ver con gestión, sistema, en la última capa, con datos. Podría dar muchos ejemplos en materia de salud, políticas sociales, etc. Cuesta hacer ese puente y a veces nos quedamos mucho en el tecnicismo.

Partir con la pregunta de cómo usted ve este tema de hacer una narrativa más estratégica para que podamos movilizar a todos los actores, a toda la sociedad, para poner mucho más esfuerzo, energía, coordinación, recursos, planificación, sustentabilidad.

(55:36) Senador: Muchas gracias José. La construcción del relato es fundamental, porque es una visión compartida y común. Tenemos la mejor oportunidad cuando estemos debatiendo el Chile que estamos construyendo. Es por eso que organizaciones como ustedes es tan importante que estén presente. No solo en la Comisión del Senado. Lo bueno es que hay mucha gente joven, que se le puede hablar en un lenguaje que ellos entienden. Y por eso hay que construir un relato, para aquellos que saben cómo va la vida. Otros, por la pandemia se vieron forzados a hacer uso de las tecnologías digitales. Pero lo que sí la gente sabe, y se ha instalado con las tecnologías, es que las cosas tienen que ocurrir más rápido.

La respuesta que debe tener el Estado es uno de los elementos que tenemos que ver para solucionarlo. Todos queremos que el Estado funcione mejor y más rápido. Las soluciones tecnológicas están, y hay muchas. Tenemos que tener el convencimiento de dejar de hacer las cosas de una manera para hacerlas distinta. Es la capacidad que va a tener la gente joven. Nosotros no tenemos que llegar y decir "mira, esto es lo que tienes que hacer", sería lo peor, sería destruir la capacidad de construir acuerdos. Pero sí estimularlos con conocimiento, con ideas, con casos, experiencia. Te aseguro que van a llegar a lo mismo que estamos concluyendo ahora. Apoyemos el proceso, seamos capaces de generar el acompañamiento digital, para lograr que esto converja a algo bueno para todos. La gracia es que se da la oportunidad, es el minuto, no lo perdamos. El relato lo vamos a construir, lo vamos a ayudar y entre todos vamos a ser capaces de sacarlo adelante.

José: Felipe Vera, miembro de Transformación Pública, tiene una pregunta general.

Felipe: Muchas gracias por su charla. Elementos técnicos e intelectuales de un nivel muy alto. En relación a lo visto Senador, ¿cómo aseguramos en el tiempo una estrategia a largo plazo y buenas políticas en el ámbito de la confianza digital y ciberseguridad? Esto a pesar de los cambios de gobierno. ¿Cómo aseguramos aquello desde su punto de vista?

Senador: he llegado al convencimiento que en temas digitales lo mejor es adoptar uno, al menos uno de los estándares internacionales que estén en boga, hay muchos, uno tiene que elegir uno. ¿Y, por qué? porque desde ese momento tú eres parte de algo que está federado, algo que supera lo que tú eres capaz de hacer. Porque si uno desarrolla algo propio, el próximo que venga dice: “no, lo mío es mejor”. Y vamos a estar en ese juego absurdo y vamos a perder el tiempo en eso. Recomiendo usar el Reglamento General de

Protección de Datos que se emplea en toda Europa. Lo mismo en lo que decía de los Estándares de Interoperabilidad, si ya lo está ocupando Colombia, Estonia y Finlandia.

Primero, recomendaría definir qué estándares creemos que son los mejores y los adoptamos. No discutamos más y empecemos a usarlos, porque después cambias con el estándar, vamos madurando en ese mismo estándar. El camino sería elegir el estándar que queramos, y después ser parte del desarrollo de ese estándar. Esa sería la propuesta que recomendaría. Podemos colaborar además en el perfeccionamiento del mismo estándar.

Felipe. perfecto, y esto aplica también para otros ámbitos de proyectos tecnológicos e innovación.

Senador: Muchos, es una buena política pública general que podrías emplear.

José: Hay una consulta de Octavio Espinoza, quien tiene mucha experiencia en esta materia

(1:00:44) Octavio: Senador, lo felicito pues su presentación da una mirada muy holística y sistémica de cómo abordar este tema que es bastante complejo. Estamos hablando de una mirada que debe tocar múltiples aristas y componentes, y en ese sentido me parece muy buena la sugerencia de incorporar en la carta magna que se está trabajando estos elementos. Quería consultarle cuál sería su sugerencia de los elementos fundamentales que deberán estar en esta Constitución que permitan impulsar el desarrollo de este Estado digital tan anhelado por nosotros.

Senador: bueno, ahí están los derechos digitales. Todo el mundo sabe que necesitamos derechos digitales, que parten desde la protección de los datos personales que están todos digitalizados, hasta elementos que van mucho más allá. La frontera en estos momentos creo que están en los neuro-derechos. Y la protección es para los dos lados, para evitar que alguien te los robe y evitar que alguien implante un dato personal que no corresponde en una base de datos, o implante algo en tu cerebro. Todo eso conlleva un conocimiento de la forma en que nos vamos a ir relacionando a futuro. Si esta Constitución va a ver el período de convergencia de lo digital con lo humano, tiene que tener previsto eso. Podría incluso anticipar que esta Constitución se va a hacer para un período de convergencia en la sociedad, en donde lo humano y lo digital se van a fusionar a niveles que van a superar lo que nosotros creemos, y esto está ocurriendo muy rápido. Esos derechos digitales tienen que tener eso en vista, el qué está ocurriendo con los ecosistemas, los ecosistemas naturales, que los vamos a proteger, pero también este ecosistema, este ciberespacio.

Lo segundo viene dado con la institucionalidad. La carta magna define todos los derechos, pero también la institucionalidad. La institucionalidad de este nuevo Estado digital tiene que ser prioritaria, tenemos que buscar y forzar que las cosas se hagan de manera digital, pero de manera digital segura. Y ahí viene el derecho para garantizar a las personas que se pueden relacionar digitalmente con el Estado, sin necesidad de que tengan que hacerlo personalmente, esa es la máxima expresión de la consagración de un derecho, porque ya no tienes que hacerlo en persona, sino que es tu identidad digital la que empieza a hacer estas acciones.

Para terminar en una sociedad madura, evolucionada, lo más importante que yo dejo siempre para el final en la transformación digital del Estado, es el voto electrónico. El voto electrónico debiera ser lo último que tú debieras usar, entendiendo que ya fuiste capaz de avanzar con todo el resto. Que tu identidad eres tuya, que eres tú y nadie más que tú, que no estás afectado por condiciones que no puedas ejercer. Es un proceso gradual, la forma en que se va a redactar lo verán quienes están en estos momentos elegidos para ello, pero sí tenemos que tener los principios comunes: qué esperamos que exista. Y partir de lo básico hasta lo más complejo, y entender que la Constitución tiene que garantizar que eso ocurra bien.

Es más, la Constitución tiene que garantizar la transformación digital segura del Estado, con la conectividad de todas las personas. El derecho a conectarse, a ser parte de esta forma de vida es tan importante como el derecho al agua. Necesitamos consumir mínimo 2 litros de agua para no morir. Por eso tenemos 100 litros diarios garantizados por la ONU, por cada persona son 3 m3 al mes, mínimo. La pregunta es cuántos kilobytes o megabytes mínimos necesitamos para poder funcionar. Eso para reflexionar. El agua y la conectividad son necesarias. Y las dos cosas se tienen que entregar porque es imposible que a futuro puedas vivir sin una de las dos. Y eso tiene que quedar garantizado, para que después hagamos nuestras leyes. Pero los grandes principios que nos permitan entender por qué necesitamos y para qué. Y el para qué es entendiendo que va convergiendo un mundo físico y un mundo digital, cada vez más junto, inseparable e irreemplazable, no hay vuelta atrás. Hay que hacerlo con los medios digitales y obviamente redactarlo y garantizarlo de esa forma. Eso sería una idea que puedan trabajar. No pretendo redactar lo que tienen que decir, pero sí pedirles que tengan considerados estos principios.

(1:06:35) Macarena. Dos preguntas Senador. La primera, respecto al tema de la confianza, que planteó al comienzo de su presentación, porque uno de los problemas que probablemente se nos va a ir abriendo en términos de la confianza va a ser la confianza en las decisiones que se están tomando a través de sistemas automatizados, como

inteligencia artificial o machine learning. Y por lo tanto, desde su perspectiva, cuáles serían los mecanismos para mejorar la confianza en esas decisiones automatizadas.

El segundo punto tiene que ver con el tema de las personas. Hoy día probablemente tenemos una falta de cultura interna en el país respecto a las necesidades de aumentar la ciberseguridad. A su vez, eso se traduce en que no se ha desarrollado suficientemente la industria y probablemente hay personas pero no hay suficiente oferta, o la oferta es muy mala. Porque conozco personas que son contratadas y se les exige que hagan de todo, desde Jefe de Informática hasta encargado de seguridad y monitoreo de plataforma, o en realidad se les paga muy poco a personas que son realmente especializadas. ¿Cuál es su opinión de cómo podríamos mejorar la valoración del recurso humano en el caso de los especialistas en ciberseguridad?, porque especialistas tenemos, pero la valorización de esos especialistas es en la que tenemos una gran carencia.

Senador: El tema de los sesgos es un tema no menor. Lo que necesitamos, más que algoritmos éticos, son programadores éticos. Programadores y programadoras. De hecho la primera programadora en el mundo es una mujer Lady Ada Lovelace. Las mujeres han estado siempre presentes en la programación, por algo en algún minuto dejaron de estar y queremos que vuelvan. Pero si los programadores éticos funcionan bien, van a poder dar los elementos para que cualquier persona de la organización pueda explicarle a aquel que se siente discriminado, qué paso. Y eso lo hemos puesto en la Ley de protección de los datos personales, de tal forma que no se justifique en que “el sistema dice” o “el algoritmo dice”, sino que tengan que explicarlo. Las empresas y organizaciones que tienen las mejores prácticas también quieren saber por qué el algoritmo decidió eso. Esto es algo que a todo el mundo le interesa y ese es el lado bueno. El lado bueno es que aunque no lo quieran, y uno lo fuerce, eso de explicar lo que debe tener cada empresa. Y los mismos programadores sean capaces después de entregar la información necesaria de por qué se tomó la decisión, para que lo entienda una persona. Yo no puedo entender un algoritmo. Usted use lo que quiera para tomar las decisiones, pero debe tener la capacidad de explicar, en forma humana, persona a persona, por qué se tomó la decisión. Entonces, es una sana medida y es bueno tanto para la empresa u organización como para la persona que siente que fue discriminada. Eso a la larga es transparencia y límites.

Las cosas siempre van a tener sesgos, uno tiene que tener métodos para evitar los sesgos, pero cuando empieza a ser el sesgo del sesgo del sesgo, uno termina no sabiendo qué está haciendo. La persona racional que está a cargo del proceso es la que debe tener las herramientas para ser el que decida y declare: “Yo revisé y esto es así”, o “revisé y también estoy con la duda”. Lo cual es muy honesto.

Usemos la tecnología de la mejor forma. No se trata de usarla, entregarla y que una inteligencia artificial haga, no. Las personas van a seguir funcionando. La transformación digital no es perder la pega, es mejorarla. Porque en vez de ser el digitador va a ser el analista que va a operar. No se va a perder la persona, la persona se va a usar de mejor forma. Creo que eso sería lo primero.

Lo segundo, ¿cómo identificar y remunerar bien a las personas en el ámbito de las competencias de la ciberseguridad?, es difícil, porque todavía no existen las escuelas, los grados, las certificaciones. ¿Cuáles certificaciones? Las internacionales, porque el mercado internacional es el global, puedes ser incluso consultor sin moverte del escritorio. Esta es una advertencia a las empresas en Chile. Las personas son tan buenas, que si usted no las trata bien, se le van a ir. Esto, porque hay una demanda de profesiones de ciberseguridad muy grande. Y si calificas muy bien, vas a poder tener no solo el estándar nacional, sino el internacional. Mi consejo va por ese lado, para eso yo propongo el Instituto Nacional de Ciberseguridad, para detectar talento a edad temprana. En España, parten las academias de hackers a los 14 años, pues tienen madurez digital. Si con YouTube ya saben hacer muchas cosas. No menos, porque la ley de protección de datos personales los considera menores de edad y sus datos no pueden ser tratados. Se protege por las dos razones. Las cuentas Facebook no se abren antes de los 13 años, para proteger a los menores. Antes son huérfanos digitales y es responsabilidad de sus padres. Una vez que tú has detectado talentos tienes que desarrollarlos. Es clave contar con las distintas certificaciones que permitan acceder a puestos más importantes, certificados por una autoridad competente, no como algunos que se dicen expertos. Eso se está regulando y es parte del proceso de maduración. Yo espero, como tenemos 5 años para implementar la Ley de transformación digital, el plan de madurez es a 5 años y ver qué somos capaces de crecer. Porque hay demanda en el mundo, es una buena noticia, todos los que entren en esta área tiene pega en todo el mundo.

(1:13:36) José: Le vamos a dar la palabra a Adrián Medrano.

Adrián: Muchas gracias, excelente presentación. Hemos disfrutado de esta integración sistémica, de diversos aspectos clave para la transformación digital del país. Me parece genial la propuesta de Isla de Pascua, sería un ejemplo vistoso de gran aporte. Respecto de la Ley de transformación digital, está promulgada, es de pronta implementación, pero los reglamentos requieren una bajada técnica. En la actualidad hay mesas técnicas que están trabajando con destacados servidores públicos de diversas instituciones del país, en aspectos tales como interoperabilidad, seguridad de la información, ciberseguridad, documentos de expedientes electrónicos, certificaciones, autenticación. Sería excelente contar con su participación y su visión en estas mesas. También si las tiene a la vista y que

nos comente de la relevancia respecto de su tratamiento, dado que estas especificaciones o normas técnicas son una bajada de los reglamentos que van a ser muy influyentes en los proyectos informáticos que se desarrollen en el futuro. Así que es en cierta medida un planteamiento y una pregunta de la viabilidad de participar en estas mesas de trabajo.

Senador: El reglamento está en una segunda consulta pública para poder ver cómo mejorarlo. Esto quiere decir que está abierto el espacio de escucha. Pero nos falta una verdadera reforma digital del Estado. Y ser bastante radical. Hoy no tenemos una autoridad, está disperso, cada uno tiene un área distinta. Una fórmula, puede que les guste o no, es este proceso que estamos viendo de separación de los ministerios del Interior y el de Seguridad Pública, para tener un Ministerio de Seguridad Pública y Protección Civil especializado, y dejar a Interior como un ministerio de Gobierno Central, para ver el tema de trabajo con todos los ministerios. De Gobiernos Regionales, porque los nuevos gobernadores de signo político distinto con el Presidente de turno, deben tener un tratamiento que no es la SUBDERE. Y de Gobierno Digital. Entonces, tenemos una oportunidad extraordinaria de separar ministerios y especializarlos. Y dejar Gobierno Digital con la red de conectividad del Estado para hacer la transformación digital, en Gobierno, en la autoridad política. Si esto es un tema político, no un tema técnico. Debe ser con fuerza e impuesto, sino las cosas no ocurren. Sin miedo, llamo a todos los funcionarios públicos, a la ANEF, a entender que se hace con ellos. Tenemos que ser capaces de acordar la fórmula y ejecutarla. Las condiciones están dadas: una nueva Constitución, un nuevo marco, podemos especializar este ministerio. Ahí vamos a tomar los estándares. No podemos hacer bajadas técnicas sin estándares acordados.

Estamos construyendo con lo que hay, pero falta darle profundidad. Podemos avanzar en esta propuesta de Gobierno Central, Gobiernos regionales y que Gobierno Digital sea la autoridad transformadora, visible, con recursos y capacidades. Que los que quieran ser candidatos a la presidencia lo tomen como un tema relevante. Si esto no se lidera no funciona y vamos a seguir tratando de ajustar las cosas, haciendo convenios entre todos, pasándonos las bases de datos enteras, locuras espantosas. No más de eso. Esto se hace con estructuras distintas, con nuevos ministerios, adoptando estándares internacionales, generando conocimiento. Este es el momento de partir de nuevo, porque con más de lo mismo, vamos a llegar a los mismos resultados. Pero es un desafío. Por lo pronto está bien, se sigue abriendo la consulta, vamos a ver cómo funciona, pero necesitamos hacer algo más radical. Mi propuesta, si es que me quieren acompañar, es proponer un Ministerio de gobierno fuerte, donde Gobierno Digital sea uno de los pilares esenciales de este nuevo ministerio.

(1:18:59) José: Le daré la palabra a Néstor Reyes sobre identidad digital.

Néstor: Buenos días. Entendiendo que la confianza sobre este esquema digital es muy necesaria. Entendiendo que se divide no solamente en la estructura digital que se pueda levantar, que también se divide en un porcentaje de educación, cómo propone usted hacer un aseguramiento digital, en el sentido de fortalecer los criterios que hoy día establece la confianza del ecosistema. Porque no solamente poniendo algoritmos robustos garantizamos esto. Esa es mi pregunta.

Senador: Esta es la frontera en que está todo el mundo viendo cómo hacerlo de la mejor forma, yo no tengo la respuesta, así de sincero. Este es un tema de frontera. Esta es la discusión: "cómo lo vamos a hacer". Por lo pronto, lo esencial es siempre ir a la base, y la base es acordar aquellos elementos mínimos que permitan garantizar la certeza jurídica de los actos digitales. ¿Cuáles? los elementos que definamos. ¿Para qué? Para poder despejar dudas. Uno debe tener algunos elementos para poder resolver un problema, que te den una cierta estabilidad. Puede no ser la respuesta más estable, pero al menos una respuesta acordada. Y esa respuesta acordada debe tener 3 o 4 elementos básicos, como las patas de una mesa.

¿Qué es lo que uno podría prever? Y aquí viene el tema del desarrollo de las nuevas tecnologías, que van a tener un cambio brutal muy pronto. Todos los sistemas criptográficos están siendo cuestionados por la computación cuántica, todos los sistemas de identidad están siendo cuestionados por la capacidad que tienen los algoritmos de meterse entre medio. Cuando me hablas de un sistema biométrico, alguien lo puede engañar con la foto, pero es detectable. Pero si te alteran el "man in the middle" y te generan con inteligencia artificial la cara, va a aparecer al otro lado como si fuera cierta. Esto es súper complejo, hasta el ADN también se puede fabricar. Definamos un mínimo aceptable, que digamos: "con estos elementos, en esta condición sí puede ser". Esos son los mínimos que se están discutiendo. Y por eso se está hablando bastante de la capacidad para tener varias autenticaciones simultáneas, porque es muy difícil poder generarlas simultáneas como ciber ataque. Si alguien quiere quebrar algo, romper algo, va a encontrar los puntos débiles, pero cuando tú haces algo simultáneo, 4 patrones o 4 cosas, es muy difícil que eso pueda ser de alguna manera interpretado. Entonces, da mayores seguridades. No tengo una respuesta certera de lo que debiéramos hacer, está en evolución, pero sin lugar a dudas, cualquier cosa que hagas, va a ser mejor de lo que tenemos ahora. Uno debe ser crítico de la condición actual. ¿En qué condición estamos? ¿Cuáles son los elementos que se están empleando? ¿Qué fragilidad tienen? Si las fragilidades son grandes, ¿Qué podemos hacer que sea mejor? Y encontrar una condición de estabilidad un poco mejor. Pero, ¿Cuál de todas ellas? No me gusta imponer, prefiero que esa sea una de las decisiones de Gobierno Digital, porque hay un costo político de decir: "esto es lo que vamos a decidir y adoptar". Lo podemos seguir conversando, me

gustaría saber lo que tú piensas, los datos, la evidencia, las formas, las propuestas. Porque podríamos ayudar a crear algo que oriente, que ayude y que sirva. Por lo pronto, preferiría dejarlo como he contestado. De la frontera, no tengo como para decirte: “esto es lo mejor”.

(1:23:45) José: nos quedan sólo unos minutos. Voy a destacar algunos comentarios y también preguntas que están haciendo nuestros participantes. Dany Muñoz de Argentina nos está comentando una experiencia de interoperabilidad, en Neuquén específicamente, basado en la experiencia de Estonia, agradecemos la referencia. Y también Claudio Parra nos está preguntando su opinión sobre el convenio reciente entre Microsoft y Codelco. Pregunta por la relación entre transformación digital, ciberseguridad y los convenios con las grandes empresas, en los que obviamente hay una serie de trade-off, si pudiera explayarse sobre eso senador.

Senador: Primero, saludos a Neuquén, un agrado que nos estén escuchando. Gustavo Giorgetti es la persona con la que nos hemos relacionado en Argentina. Gustavo fue el primero en ir a Estonia, 15 años atrás, entender el estándar X-Road y llevarlo a Argentina. Llegó a Neuquén y trató de crear su propio X-Road. Él hizo lo que hacemos los latinoamericanos, pensar: “yo soy capaz de hacerlo mejor”. Después de varios años de probar, dijo: “quiero trabajar de verdad”. Bueno, Gustavo hoy en día se dedica a eso, a instalar X-Road y a mejorarlo. Porque es mejor trabajar en algo que varios pueden contribuir. Lo segundo, es una de las situaciones que tenemos que ver, que está directamente relacionado con la capacidad de uso de elementos que son propiedad de privados, llamémoslo así. Pero cuál es la propiedad del privado, es la infraestructura, el disco duro, el cable de fibra óptica, el router, el sitio. Estamos hablando de las nubes. Microsoft decidió traer a la región AZURE, son 3 datacenters conectados, robustos y respaldados. Una inversión gigantesca. Pero el valor de la inversión no son los fierros, es la data. Entonces aquí es donde uno es libre de tener la data donde uno quiera. Y la data se mueve con un clic. O sea, la saco de Microsoft, la meto a Amazon web service o la meto en algo del Estado. Pero si el Estado invierte en sus propios servidores, te aseguro que nos vamos a quedar atrás al minuto 1. Esto es muy dinámico, es una locura entrar a invertir en algo que está cambiando dinámicamente. Necesitamos a terceros que den capacidad de hospedaje, almacenamiento. Y si vemos que no nos gustaron las condiciones nos cambiamos. El licitar espacio al más bajo costo es lo mejor para el Estado, porque le va a permitir resolver el problema. Si el problema es ¿Qué hago con los datos? ¿Qué política pública? Y los datos los tiene que custodiar el Estado, pero los datos finalmente son de las personas. Entonces las personas que dieron su consentimiento para que esos datos fueran usados, esos datos son tratados y permiten tener mejores servicios digitales. En CODELCO decidieron, probablemente por licitación, hacerlo con Microsoft. Podrían haberlo hecho

con HUAWEI, con Google, con Amazon, que son los grandes proveedores. Incluso con GTD, una empresa chilena que también tiene data service. Eso se licita, son procesos competitivos. Las migraciones no son grandes problemas, la competencia es bastante buena en lo que cada uno ofrece. Es como elegir la electricidad. Esto se hace en Inglaterra: tú puedes decidir si quieres consumir electricidad generada con energía renovable no convencional. Por internet decides y te llega esa electricidad y no la fósil contaminante. Con esa política sacas todos los productores de electricidad con combustibles fósiles. Lo mismo acá, los datos puedes ponerlos en cualquier lugar y van a estar necesitamos de eso.

Ahora, sería una locura tratar de competir, uno crear sus propios datacenters, excepto, aquellos datos donde el disco duro a proteger tiene que ser protegido por el Estado. Porque el disco duro lo puede sacar cualquiera y la data es muy sensible. Entonces hay dos opciones, la primera es que el privado construye el "facility" que le llaman, y un organismo del Estado toma control de él para la seguridad física. Lo segundo es que el mismo Estado, en un lugar muy seguro, decida tener sus servidores, aunque sean viejitos. Esa es la data que tiene que estar con seguridad física, más que la seguridad digital que tú le puedas dar. Ahí viene algo bien importante, que son los niveles de seguridad de la información, el "need to know", con los niveles de clasificación, con las medidas de seguridad física que debe tener la información. Eso también debe ser parte de las respuestas que debemos tener.

Yo agradezco que las empresas grandes hayan venido a apostar a Chile, estamos construyendo un Chile nuevo digital y qué bueno que estén disponibles todos. Los tenemos a todos. Ahora tenemos que sacarles rendimiento, esto no es solo almacenar el dato, es qué hacemos con los datos y cómo estos datos nos permiten mejores políticas públicas. Sólo para resumir: "más data y menos guata". Necesitamos que nuestra política pública se base en evidencia y esos datos los usemos muy bien. Muchas gracias por las preguntas, estamos llegando al término. Y, agradecerles por la invitación.

(1:30:02) José: Muchas gracias Senador y a todos los participantes. Va a cerrar esta sesión Macarena con un reflexión final, pero antes me gustaría dejarlos invitados al siguiente coloquio, el 11 de junio. Estamos hablando de nuestra querida y vieja Contraloría General de la República, que es como la quinta esencia en el imaginario de la burocracia y el papel, pero que maravillosamente ha estado empujando una transformación digital interesante, en materia de ciencia de datos, para efectos de la fiscalización. Para esa exposición vamos a contar con don Ernesto García, que es el Jefe de Estudio y Gobierno de Datos de la Contraloría.

Macarena: Nuevamente agradecer al Senador por su disposición, por su tremenda presentación. Y no solamente ver el bosque. Me encanta esta infraestructura de la casa, o del palacio que ha ido armando, que espero lo vayamos fortaleciendo, construyendo y logremos desarrollarlo como país. Dejaba una reflexión, uno de los últimos puntos que comentó en relación a la información nacional: si no queremos perder nuestra independencia en términos de datos e información, es una discusión abierta de cuáles son los datos que debemos que proteger y cómo. Creo que hemos tenido tal vez inocencia en algunos casos y dejación en otros, respecto a qué es lo que debemos proteger y cómo. Así es que nuevamente los dejamos invitados para la siguiente sesión. Agradecemos la exposición del Senador y la conversación posterior con quienes hicieron preguntas. Gracias y nos vemos en nuestro siguiente coloquio en que veremos el poder de los datos y el uso que les da la Contraloría. No se lo pierdan.