Mesa de trabajo “Gobernanza Nacional de la Ciberseguridad"

Autor

Agesic

Fecha de creación

20/09/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la primera mesa de trabajo "**Gobernanza Nacional de la Ciberseguridad**" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad del 17 de junio al 21 de junio del 2024. Participaron representantes de: sector público, sector privado, academia, sociedad civil y organismos internacionales.

Introducción

En el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay, la semana del 17 al 21 de junio de 2024 se realizaron ocho mesas de diálogo para recoger propuestas y aportes respecto a la propuesta borrador. Participaron diferentes actores de las instituciones públicas, del sector privado, de la sociedad civil y de la academia, con el objetivo de intercambiar ideas y propuestas que permitan cocrear la ENC. En este espacio se plantearon y se dialogó sobre ideas y propuestas con respecto al alcance de la Estrategia, los principios, objetivos y acciones específicas a impulsar.

En la jornada del 17 de junio se realizó el análisis del primer pilar de la Estrategia, “Gobernanza y Marco normativo”. En este informe se detallan las propuestas y aportes compilados en la primera mesa de diálogo, centrada en “Gobernanza Nacional de la Ciberseguridad”.

Este documento presenta en forma sintética el intercambio que se dio en esta mesa.

Participantes

Agesic (Institución pública), Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Nicolás Bianchi, Nicolás Correa, Sebastián Gómez, Gabriel Hernández, Jimena Hernández, Angie Lecot, Maximiliano Maneiro, Natalí Paggiola, Mauricio Papaleo, Virginia Pardo, Maite Rodríguez, Cecilia Rossi, Karimeé Ruibal, Natalia Salazar, Fabiana Santellán, Alejandro Vargas.

AIN (Institución pública), Auditoría Interna de la Nación. Rodrigo Pagliaro, Jonathan Silva.

ANCAP (Institución pública), Administración Nacional de Combustibles, Alcohol y Pórtland. Marianela Moreno, Lucía Posse.

ANP (Institución pública), Administración Nacional de Puertos. Marcos Cocchiraro.

APBU (Sector privado), Asociación de Bancos Privados del Uruguay. Álvaro Bertolini.

BCU (Institución pública), Banco Central del Uruguay Carla Facal, Isabel Maroñas.

Banco Santander (Sector privado), Martín Rodríguez.

BID (Institución pública), Banco Interamericano de Desarrollo. José Callero, Ariel Nowersztern, María Inés Vázquez.

BROU (Institución pública), Banco República Oriental del Uruguay. Marcelo Varaldi.

Presidencia de la República, División Gestión de Gobierno Electrónico (Institución pública) Consejo Asesor Honorario de Seguridad de la Información. Soledad Suárez.

CEIBAL (Institución pública), Centro de Innovación Educativa con Tecnologías Digitales del Estado uruguayo. Daniela Gómez, Federico Quiroga.

CISO (Institución pública), Chief Information Security Officer/Jefe de Seguridad de la Información, Ministerio del Interior. Javier Jaureguiberry.

CSIRT – Chile (Institución pública), Equipo de Respuesta ante Incidentes de Seguridad Informática dependiente del Ministerio del Interior y Seguridad Pública. Cristian Bravo Lillo.

FGN (Institución pública), Fiscalía General de la Nación. Germán Martínez.

IM (Institución pública), Intendencia de Montevideo. Maria Eugenia Corti.

INDDHH (Institución pública), Institución Nacional de Derechos Humanos y Defensoría del Pueblo. Gabriela Pérez.

LACNIC (Sociedad civil), Registro de Direcciones de Internet para América Latina y Caribe. Graciela Martínez.

MI (Institución pública), Ministerio del Interior. Diego Sanjurjo, Saúl Scanzani.

MIEM (Institución pública), Ministerio de Industria, Energía y Minería. Maria José Franco.

OEA (Institución pública), Organización de Estados Americanos. Alex Crowther.

Parlamento (Institución pública), Darío Burstin.

SeCIU (Institución pública), Servicio Central de Informática Universitaria [UDELAR]. Sergio Ramírez, Javier Valena.

URCDP (Institución pública), Unidad Reguladora y de Control de Datos Personales. Flavia Baladán.

URSEC (Institución pública), Unidad Reguladora de Servicios de Comunicaciones, órgano desconcentrado del Poder Ejecutivo. Mercedes Aramendía, Fernando Hernández, Agustín Hill, Mauro D. Ríos.

URTEC (Institución pública), Ministerio de Industria Energía y Minería. Pascual Gattas.

URUDATA (Sector privado), José Callero.

UTE (Institución pública), Administración Nacional de Usinas y Trasmisiones Eléctricas. Evelyn Anton.

Resumen del intercambio

A continuación, se presenta el informe general de la mesa de trabajo “Gobernanza Nacional de la Ciberseguridad” dónde se encuentran sistematizados y sintetizados los aportes de cada subgrupo. Se mantuvo la estructura estipulada en la agenda de la actividad, que consistió en dos rondas de intercambio.

Es importante señalar que, aunque cada ronda y tema estaba claramente definido, en la mayoría de los casos la discusión superó el planteo inicial.

Parte 1. Ronda de intercambio sobre el borrador

Esta primera ronda se dividió en dos partes, en las cuales los participantes realizaron aportes sobre el borrador. En la primera parte identificaron aportes generales sobre la propuesta borrador, mientras que en la segunda identificaron aportes específicos sobre el pilar “Gobernanza y Marco normativo”.

Parte A. Aportes generales sobre la propuesta borrador

En esta primera parte, las personas participantes respondieron a la pregunta: ¿Qué aspectos consideran más relevantes en la propuesta del primer borrador de la Estrategia Nacional de Ciberseguridad para abordar eficientemente retos y desafíos en torno a la Gobernanza Nacional de la ciberseguridad?

Los participantes discutieron diversos aspectos relevantes de la propuesta del primer borrador de la Estrategia Nacional de Ciberseguridad, centrando su atención en los siguientes puntos:

Sobre el enfoque y aspectos generales

Se elogió la iniciativa, hubo consenso general sobre su necesidad.

Se resaltó que falta una perspectiva de género, un desafío que se debería enfrentar de manera más central en el documento. Este mismo debería centrarse en personas, sus derechos, necesidades, brindándoles atención y velando por la calidad de vida digital. Se enfatizó la necesidad de garantizar un proceso inclusivo y organizado que involucre a todos los actores relevantes.

También se subrayó que se debe reforzar la oportunidad económica que representa la ciberseguridad para el país.

Finalmente, se planteó que para tener éxito, los documentos estratégicos deberían asumir la realidad de que la ciberseguridad siempre estará un paso atrás del cibercrimen.

Respecto al marco normativo

Se recalcó la importancia de impulsar un marco normativo, y la necesidad de que éste sea menos ambiguo. También se hizo hincapié en que debe promover la participación y estar concebido de forma dinámica, que permita adecuarlo al contexto cambiante. Debe ser mandatorio, permear las organizaciones, y darle importancia tanto al sector público como al privado.

Sobre los pilares

Se enfatizó la importancia de hablar de gobernanza como eje central de la estrategia.

Un comentario que surgió reiteradas veces apunta a la necesidad de pilares más transversales, menos específicos, que consideren las realidades de distintos sectores de ciberseguridad.

Se planteó, respecto a esta temática, que algunos pilares quedaron desproporcionados respecto a otros. Se cuestionó si “Gobernanza” y “Marco normativo” deberían ser pilares distintos, si infraestructura necesita su propio pilar, y se propuso incorporar a la generación de una cultura de la ciberseguridad en el pilar relativo a la gobernanza. También se propuso dividir la gobernanza en tres niveles (estratégico, táctico y operativo), reconociendo la dificultad de su implementación.

Establecer actores, definición de roles, coordinación entre ellos

Se resaltó la importancia de la línea de acción i del primer objetivo (“Definir los diferentes niveles, organizaciones y responsabilidades para la gobernanza a nivel Estratégico, Operativo y Sectorial”). Se recalcó que es fundamental la cooperación (línea de acción ii) y el posicionamiento de la ciberseguridad como objetivo de gestión. También se valoró mucho el aspecto participativo de la iniciativa.

Se reconoció la necesidad de definir claramente los actores y sus roles y responsabilidades, y se hizo énfasis en que en algunos casos no quedan claros los roles de los organismos. Para evitar la duplicación de actividades, debe haber un encargado de ciberseguridad en cada organismo, cuyo único rol sea ese. Para lograr este cometido, se comentó que es necesario sensibilizar a las autoridades.

Respecto a los actores involucrados, se resaltó que es clave la identificación de actores estratégicos y sus roles en la gobernanza. Se debe definir cuáles son, por ejemplo, las infraestructuras críticas.

Se marcó que hay que establecer claramente los organismos responsables y sus jerarquías, así como jerarquizar las gerencias de ciberseguridad en los organigramas de las diferentes organizaciones. Además, se debe considerar a las pymes, dándole importancia tanto al sector privado como al público. Se destacó que la estrategia debe abarcar a todos los actores, desde ciudadanos comunes hasta actores más complejos.

A la vez, se manifestó la importancia de que la ENC sea una política de Estado, para evitar retrocesos en la implementación de la estrategia.

Capacitación y sensibilización

Se destaca la importancia del desarrollo de capacidades, y se reconoció que sus aspectos fundamentales están incluidos en la estrategia. Se resaltó la necesidad de prever recursos humanos y de sensibilizar a la población en general.

Acciones propuestas

Se recomendó: hacer hincapié en el producto mínimo viable; asegurar que la estrategia sea aplicable; definir planes de acción concretos, considerando necesidades nacionales; realizar monitoreo y seguimiento dinámico, estableciendo metas, indicadores y objetivos concretos. Se enfatizó la necesidad de control y de auditorías para la ejecución de las líneas de acción, así como del desarrollo de una metodología común.

Carencias identificadas

Se identificaron algunas carencias existentes en Uruguay que surgieron reiteradas veces: la falta de cultura de la ciberseguridad; la falta de competencias de capacidades y de recursos humanos como resultado de esto; y la falta de un marco normativo coherente y sólido. También se hizo mucho hincapié en que aún falta atribuir claramente roles y responsabilidades, y se enfatizó la importancia de esto.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

En esta parte, las personas participantes respondieron a la pregunta: ¿Qué aspectos específicos de gobernanza creen que podrían mejorarse o añadirse en el pilar “Gobernanza y Marco normativo” con el fin de establecer la Gobernanza Nacional de la Ciberseguridad de Uruguay?

Los aportes de los participantes en respuesta a esta pregunta pueden dividirse en varios ejes temáticos: se sugirió profundizar en los mecanismos de cooperación y coordinación; aclarar la política, las prácticas y los marcos de referencia; elaborar una estrategia de seguimiento; definir y concretizar los objetivos y las acciones; establecer los recursos y el presupuesto generales; y apoyarse en experiencias internacionales.

Sugerencias para profundizar en los mecanismos de coordinación

Se sostuvo que en la coordinación se debería adoptar una forma concreta, como mesas de trabajos a nivel estratégico, táctico y operativo, tal como estas mesas de diálogo. Estas instancias concretas, donde los representantes tendrían un perfil concreto de trabajo y trabajarían con métricas, podrían tener una frecuencia de una vez al mes o trimestral para que se generen metas de avances. Sin embargo, también se señalaron dudas sobre la factibilidad de una mesa de 100 participantes.

También se señaló la importancia de un plan de comunicación para lograr que la información llegue a todos los involucrados.

Aspectos que se podrían añadir al pilar “Gobernanza y Marco Normativo”

Como resultado de estas discusiones, se sugirió añadir ciertos elementos al pilar “Gobernanza y Marco Normativo”.

Se propuso afrontar el tema de la política de seguridad nacional, definiendo modalidades y autoridades responsables.

También se sostuvo que se debe definir al organismo coordinador (que podría ser AGESIC), determinando si se debe crear un órgano aparte, como por ejemplo un comité para interactuar con el sector privado.

Además, es necesario identificar actores y participantes: la definición de roles debería ser parte de la estrategia. Se señaló la importancia de la participación del sector privado en la estrategia para garantizar su apropiación y éxito, y se marcó la necesidad de incluir también a la academia y a la sociedad civil en la gobernanza. Se subrayó la importancia de establecer prácticas diferenciales entre público y privado, y se marcó la necesidad de especificar las obligaciones de los organismos según su nivel operativo.

Se propuso una nueva línea de acción: *La distribución de potestades regulatorias y responsabilidades entre los diversos*

organismos debe ser clara y permitir una rápida adaptación del marco normativo a los cambios de circunstancias.

Gobernanza de seguimiento

Se hizo mucho énfasis en la necesidad de enfocarse en el seguimiento y monitoreo en el marco de la gobernanza.

Para esto, se sugirió establecer indicadores, metas de la estrategia, áreas de progreso y definir mecanismos de medición. Se recalcó que es necesario incluir métricas en el pilar de gobernanza porque si no se mide no se puede gestionar, y se tiene que hacer público en qué se está avanzando y en qué no.

Se subrayó, además, que el seguimiento de indicadores debe ser estricto, porque de lo contrario genera problemas en el pasaje de lo estratégico a lo operacional. Se resaltó la diferencia entre la teoría y la práctica, remarcando que a menudo la implementación se dificulta por falta de presupuesto, de coordinación y de recursos humanos. Por lo tanto, es importante prever los riesgos y las barreras.

También se planteó la posibilidad de establecer un estándar a seguir a nivel nacional, que permitiría hacer una medición general del país

Definición, precisión y concretización de los objetivos y líneas de acción

Se denunció una falta de precisión y concreción respecto a las líneas de acción planteadas. Reiteradas veces se sostuvo que se deben concretizar los objetivos y, luego, las líneas de acción. Para esto es necesario definir a qué nivel de detalle se busca llegar en la ENC.

Además, se afirmó que la gobernanza debe ser más específica en algunos temas, sobre todo en la definición de roles y responsabilidades y en las métricas. El marco tampoco quedó claro: se sostuvo que las definiciones son demasiado ambiguas (habría que empezar por definir el término “gobernanza”), y que falta la designación del ente rector y de los aspectos que aún se deben trabajar. Debería haber, en este sentido, un claro responsable.

Respecto a esto último, se señaló que falta un diagnóstico del sistema de gobernanza actual.

Finalmente, un comentario que surgió mucho fue la necesidad de claridad en los términos y procedimientos que permitan generar un marco legal. Frente a esto, se recalcó en reiteradas ocasiones la necesidad de elaborar un glosario para el público.

Establecimiento de los recursos necesarios

Se manifestó la necesidad de presupuesto y de recursos humanos, equipos, y recursos para ayudar a los decisores.

De nuevo se destacó que faltan capacidades y se debe profesionalizar más. Se propuso una formación obligatoria para todos, desde los técnicos hasta los jerarcas.

Se enunció a lo largo de la ronda la necesidad de incluir el involucramiento activo de los altos mandos. Para lograr su compromiso se propuso:

1. Generar un marco legal o regulatorio;
2. Generar una cultura sobre la temática;
3. Mostrar los riesgos ligados a un incidente de ciberseguridad.

Se reiteró la necesidad de fijar un plan de riesgo para priorizar el presupuesto.

Experiencias internacionales

Se afirmó que es clave tomar las experiencias internacionales como referencia, por ejemplo, para actualizar la normativa. Sin embargo, también se argumentó que es imprescindible tener presente nuestra realidad ya que las experiencias internacionales en muchos casos no son aplicables en Uruguay.

Parte 2. Aportes Estratégicos, Priorización e Identificación de actores para el pilar de la mesa

La segunda parte de intercambio sobre el borrador propuesta se dividió en tres partes centradas en aportes estratégicos que incluían plantear objetivos, proponer actividades específicas y analizar su viabilidad.

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Los objetivos fueron generalmente y en gran medida validados por las personas participantes en las mesas.

Se propusieron ciertas modificaciones en la redacción:

- Respecto al segundo objetivo, “La ciberseguridad como objetivo de gestión”, se sugirió agregar “nacional” para que se refiera a la gestión nacional.
- En la segunda línea de acción de este mismo objetivo (“Definir el conjunto de organizaciones mínimo que deberán contar con estos objetivos”), se propuso reemplazar “deberán contar” por “deberán cumplir”.

Además, ciertos actores sostuvieron que los objetivos de gobernanza deberían ser más específicos y especificar actores, roles y responsabilidades con el fin de encuadrar efectivamente la capacidad de actuar y de impulsar acciones.

Se señaló el fomento de la cooperación y la concientización entre empresas, aunque se marcaron ciertas dificultades de compartir estrategias de seguridad por razones comerciales.

También se criticó que los objetivos no mencionan las necesidades previas, por lo que sería útil sacar conclusiones a partir de una comparación pasado-futuro que permita identificar brechas y aprender de lo que ha funcionado y lo que no. A partir de eso, habría que proponer posibles vías de evolución de la gobernanza.

Finalmente, se sostuvo que se debe evaluar la viabilidad y entablar una discusión acerca de cómo aprovechar los recursos que ya existen para no duplicar esfuerzos.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Las personas participantes aportaron actividades y acciones para el pilar “Gobernanza y marco normativo”.

En varios subgrupos se desarrollaron propuestas en función de cada objetivo:

Objetivo 1. Establecer la gobernanza nacional de ciberseguridad:

- En la línea de acción ii, agregar “coordinación y comunicación”;
- Coordinar el diálogo como línea transversal a todas las acciones: trabajar para involucrar a los actores que no están involucrados a nivel estratégico;
- Mapear a los actores involucrados y sus roles en la estrategia;
- Establecer roles, relevar funciones y asegurarse de que no se superpongan;
- Representar a los actores por inciso y por sector (público, privado, academia) para que sea más abarcativo;
- Establecer una capacitación obligatoria en ciberseguridad como requisito para el ingreso a la función pública y definir los procedimientos;
- Crear una comunidad técnica para el intercambio de conocimiento;
- Incluir presupuesto y recursos, fundamentales en la gestión, en las líneas de acción (punto debatido);
- Desarrollar una hoja de ruta;
- Contar con potestades administrativas;
- Definir un órgano rector asociado con el Comité de Gestión;
- A futuro, crear un Ministerio de Tecnología;
- Coordinar y difundir las actividades del comité asesor o de gestión;
- A corto plazo, incorporar en el comité tanto a nivel estratégico y a nivel de gestión a otros actores: por ejemplo, la academia;
- Definir la competencia de control;
- Definir indicadores, recursos humanos y recursos;
- Establecer una agenda digital a nivel nacional de ciberseguridad;
- Mirar hacia fuera para descubrir buenas prácticas a nivel internacional.

Objetivo 2. La ciberseguridad como objetivo de gestión

- A través de incentivos y capacitaciones obligatorias, brindar métricas para ir evaluando las tendencias y el avance (no esperar a hacer una evaluación anual);
- Crear un incentivo por madurez en ciberseguridad a través de las auditorías;
- Jerarquizar;
- Asegurarse de que sea una política de Estado;
- Desarrollar capacidades;
- Invertir en tecnología;
- Medir el riesgo de forma transversal, gestionar la ciberseguridad dentro de las organizaciones;
- Certificar empresas en Ciberseguridad;
- Operacionalizar, medir y profesionalizar;
- Incluir la tercera línea de acción del segundo objetivo: “Elaborar los marcos legales y regulatorios necesarios” en el tercer objetivo: “Desarrollar la legislación, el marco normativo y regulatorio”.

Objetivo 3. Desarrollar la legislación, el marco normativo y regulatorio

- En la línea de acción ii, reemplazar “desarrollar” por “trabajar en el desarrollo y actualización”;
- Instrumentar un marco normativo de ciberseguridad e implementar el marco en la mayor cantidad de ámbitos posibles;
- Establecer una ley sobre delitos de ciberseguridad;
- Establecer y mejorar los aspectos procesales;
- Desarrollar una agencia de coordinación;
- Monitorear las políticas y tendencias internacionales.

Se planteó que este objetivo debería generar los marcos para los dos objetivos anteriores.

Además, se sostuvo que se debería añadir un cuarto objetivo para la implementación de la hoja de ruta y de los mecanismos de control.

Por otro lado, en algunos subgrupos se propusieron actividades y acciones globales relevantes al pilar “Gobernanza y Marco normativo”, sin incluirlas en un objetivo específico:

- Definir una línea de base para documentar los avances. Reforzar los aspectos positivos de las estructuras existentes y concentrarse en los puntos débiles.
- Definir un encargado de ciberseguridad en cada servicio público, que reciba cursos en línea, capacitaciones y recursos.
- Crear un marco claro para garantizar la seguridad jurídica.
- Establecer mecanismos de participación con el sector privado, la sociedad civil y la academia.
- Definir los niveles de criticidad de los servicios que ofrecen los organismos, y tener un modelo de madurez que obligue al cumplimiento de los niveles de criticidad.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

Las personas participantes realizaron análisis de viabilidad, priorizaron ciertas acciones e identificaron actores relevantes.

Se sostuvo que en cuanto a la priorización, las acciones son interdependientes. Sin embargo, se hizo hincapié en la necesidad de garantizar recursos (materiales y humanos), presupuesto, y asignar roles y responsabilidades.

Se destacó que hay que enfocarse en los roles y las responsabilidades y en determinar quién va a definir los términos y la atribución de responsabilidades. Se debe reforzar el marco de referencia.

Respecto a los actores, se hizo hincapié en la necesidad de descentralización de la estrategia: se recalcó que se deben tomar en cuenta los gobiernos locales, ya que tienen más cercanía con el ciudadano. También se resaltó la importancia de que estén involucradas la academia y la sociedad civil. Se planteó la posibilidad de crear un observatorio independiente. Se recomendó identificar a los actores por inciso, por sector (público o privado), y también incluir al gremio. Se propuso crear un Comité

Estratégico y Operativo. Se marcó la importancia de identificar y catalogar activos críticos.

Se aclaró que en cada organigrama debería ser posible encontrar a los responsables correspondientes de ciberseguridad, con datos obligatoriamente actualizados. Se identificó a AGESIC como actor referente que recibiría y actualizaría un directorio, que se sugiere sea de acceso público o compartido con la comunidad.

Se propuso hacer una evaluación de riesgos y revisar los marcos legales en relación con la gobernanza general. Se subrayó que es clave la definición de niveles de criticidad de servicios y el establecimiento de un modelo de madurez.

Se enfatizó la necesidad de la seguridad como objetivo estratégico de las empresas, y la necesidad de auditar la implementación.

Se hizo hincapié la importancia de poder fiscalizar públicamente.

También se identificaron potenciales actores: se mencionó al Poder Ejecutivo, la Presidencia, el Ministerio de Defensa, el Ministerio de Relaciones Exteriores (para desarrollo, actualización y monitoreo de las políticas internacionales), el Ministerio del Interior, el Poder Legislativo, la Fiscalía, los representantes de las infraestructuras críticas de la información, AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento), URSEA (Unidad Reguladora de Servicios de Energía y Agua), URSEC (Unidad Reguladora de Servicios de Comunicaciones), ANTEL (Administración Nacional de Telecomunicaciones), el Ministerio de Defensa Nacional, DINATEL (Dirección Nacional de Telecomunicaciones), y el Banco Central.

Anexos

A continuación, se detalla el intercambio realizado y los emergentes surgidos en cada subgrupo.

Subgrupo 1

- Moderadora: Ninoschka Dante, Agesic
- Relatora: Isabel Álvarez, ICD
- Participaron 11 (once) personas de 8 (ocho) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

Agesic (Institución pública) - Angie Lecot

Resalta que en el documento se hace hincapié en la resiliencia, la estructura y la confianza, además menciona que falta información sobre el comportamiento de las personas, especialmente al entrar en lo más específico.

Comenta que en el párrafo de la visión donde se indica "... aumenten la confianza de la población..." debería modificarse para no solo considerar la confianza, sino que sean críticos al hacer uso de.

En la parte de resiliencia de los pilares, falta claridad en el punto de cómo llevar adelante la resiliencia. En particular, se menciona el término "...mínimo producto viable." pero no queda claro a que se refiere con ese mínimo producto viable y si es para llevar adelante la resiliencia.

Por último, menciona que deben incorporarse distintas perspectivas y no solo hablar de equidad, sino que incluyan perspectivas.

BID (Institución pública) - Ariel Nowersztern

Concuerda con Angie Lecot. Agrega que hay que hacer hincapié en el producto mínimo viable y en equidad de género. Es necesario reforzar la oportunidad económica de la ciberseguridad en el país. Se podría exportar servicios de ciberseguridad. Hay que reforzar en la estrategia y centrarse en las personas, sus derechos, los daños ocasionados a las personas, la atención a las personas. Se requiere una visión enfocada en personas, derechos, necesidades, atención y calidad de vida digital

URUDATA (Sector privado). José Callero.

Sostiene que los pilares refuerzan la sectorización de la problemática, y que se encasillan mucho los temas cuando deberían ser más transversales. Plantea que los pilares deberían reforzar y generar visiones comunes, más que objetivos específicos. Tiene que haber algún elemento aglutinador que genere algo transversal, que junte conceptos.

Agesic (Institución pública) - Natalia Salazar

Remarca los aspectos positivos de las mesas de diálogo. Es fundamental la cooperación participativa sin temor a la interferencia. Propone que no se hable del miedo a lo malo sino de lo que se puede lograr de manera positiva.

INDDHH (Institución pública) - Gabriela Pérez

Menciona los puntos del documento que ve como positivos: la definición de roles, la importancia de posicionar la ciberseguridad como un objetivo de gestión. Pide el respaldo de otros organismos públicos para conseguir presupuesto. Como aspecto negativo, habla del mínimo producto viable.

SECIU (Institución pública) - Javier Valena

Valora el aspecto participativo de la ENC.

AIN (Institución pública) - Rodrigo Pagliaro

Considera que es un documento positivo que ataca los pilares de los distintos sectores. Menciona que tal vez algún pilar podría estar dentro de otro.

MI (Institución pública) - Diego Sanjurjo

Celebra el documento y recalca que es muy necesario para el país.

Agesic (Institución pública) - Fabiana Santellán

Concuerda con Ariel Nowersztern respecto a la oportunidad que representa la ciberseguridad del punto de vista económico, no solo en el mercado sino para reforzar nuestra posición como país. Podría representar una ventaja desde el punto de vista de los inversores en comparación con el resto de la región. También comparte con José Callero que los pilares deberían ser transversales y, además, que algunos quedaron desproporcionados respecto a otros. Se pregunta si “Gobernanza” y “Marco

normativo” deberían ser pilares distintos.

IM (Institución pública) - Maria Eugenia Corti

Menciona que la Industria nacional en ciberseguridad debería estar plasmada en una estrategia. Sería positivo a nivel país teniendo en cuenta las amenazas y el estado actual de capacitación y de capacidades. Habla de infraestructura crítica y de la necesidad de considerar a las pymes, de pensar en la escala de las empresas a nivel nacional. Además, concuerda con que los pilares deberían ser más transversales, ya que se encuentran muy divididos. Hay que verificar que se estén contemplando todas las dimensiones, ya que le parecen entreveradas. Siente que no se aborda la dimensión de recuperación y de cómo responder. El pilar de infraestructura de información no le pareció claro, ya que no se define el término “infraestructura crítica”. Plantea que quizá, a diferencia de otros temas como el marco normativo o la política internacional, no debería constituirse en un pilar. Por último, pide no dejar tan abierto el marco normativo, ya que está muy ambiguo, y darle más impulso al marco de ciberseguridad.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

Agesic (Institución pública) - Fabiana Santellán

Subraya que se debe pensar en la preocupación que motivó a escribir esto. Uruguay está en un momento de crecimiento en cuanto a ciberseguridad a nivel técnico y político. Es un buen momento para ordenar la cancha y definir la línea, y el país se merece tener una línea clara, estratégica y común. Recalca que habría que afrontar el tema de la política de seguridad nacional, bajarlo a como se hace y quien lo implementa en los tres niveles. Invita a preguntarse cómo lo queremos manejar como país, teniendo muy presente nuestra realidad, ya que las experiencias de otros países pueden, en ciertos aspectos, no ser aplicables acá. Se debe adecuar la estrategia a la realidad uruguaya.

Agesic (Institución pública) - Angie Lecot
Le parece que la política, las prácticas y los marcos de referencia no están tan claros. Se pregunta cuál va a ser el marco de referencia más allá del marco normativo.

El objetivo 1 (“Establecer la gobernanza nacional de la ciberseguridad”) incluye líneas de acción relativas a los mecanismos de vinculación y cooperación, agregando esto al marco de referencia. Si bien la gobernanza tiene que fijar las directrices falta considerar en dicha línea un marco de referencia más específico. A su vez, no solo se deben considerar mecanismos de coordinación sino también definir marcos de referencia vinculados a otras áreas de conocimiento, ej: software y datos. Para ello se podría tomar el marco de ciberseguridad y bajar a un nivel de detalle mayor con marcos específicos.

A nivel de la definición del objetivo, fata hincapié en la institucionalización.

BID (Institución pública) - Ariel Nowersztern

Recomienda fortalecer el tema de los antecedentes. La gobernanza es la primera línea de acción, pero duda acerca de hasta dónde debe llegar la estrategia y a partir de cuándo se está entrando en detalles. En la estrategia hay que definir la gobernanza, el ente rector y los aspectos que aún se deben trabajar.

URUDATA (Sector privado). José Callero.

Dice que los objetivos no le parecen claros, y recomienda concretizarlos. Una vez concretizados se pueden definir las acciones, que también deben ser más específicas.

INDDHH (Institución pública) - Gabriela Pérez

Pide profundizar en los mecanismos de cooperación y coordinación, y establecer indicadores y metas de la estrategia. También propone establecer áreas de progreso y definir cómo medirlo. Se pregunta de dónde vendría el financiamiento.

SECIU (Institución pública) - Javier Valena

Pregunta a qué nivel de detalle se buscaba llegar.

AIN (Institución pública) - Rodrigo Pagliaro

Pide más concreción, y subraya que se debe definir al organismo necesario. Propone a Agesic como articulador de este proyecto. No cree que sea necesario crear un órgano aparte; podría funcionar con las estructuras existentes. Tiene que haber un comité de crisis para poder interactuar y discutir con el sector privado, con el que debería haber un contacto directo. Están en juego temas muy sensibles que requieren soluciones rápidas.

MI (Institución pública) - Diego Sanjurjo

Sostiene que para entender la necesidad de un mayor orden del que ya existe, falta diagnosticar cuál es el sistema de gobernanza actual. Debería haber un claro responsable, y se tiene que hacer público en qué se está avanzando y en que no.

IM (Institución pública) - Maria Eugenia Corti

Recomienda que la gobernanza sea más específica en algunos temas: roles y responsabilidades, métricas. Si no se mide no se puede gestionar, por lo que es esencial incluir métricas en el pilar de gobernanza. El marco no está claro; hay cosas que deberían ser mucho más concretas. Las definiciones son demasiado ambiguas. Los roles deberían ser parte de la estrategia.

URUDATA (Sector privado). José Callero.

Cierra el bloque pidiendo que no quede todo en el aire.

Ronda 2. Aportes Estratégicos, Priorización e Identificación de actores para el pilar de la mesa

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

En esta parte, se partió de la base que hay un camino recorrido que no se puede obviar. Hay que aprender de lo que no funcionó, y comparar lo ideal con lo actual. Las estructuras y estrategias existentes funcionan y han tenido su rédito. Esto es un proceso evolutivo de algo que aún no alcanza. Se planteó que se deben hacerse comparaciones entre el pasado y el presenta para sacar conclusiones. No necesariamente hay que cambiar todo, sino que más bien ir viendo a lo largo del tiempo. Sin embargo, también se criticó que los objetivos no mencionan las necesidades previas.

Se indicó que se debe determinar hasta dónde queremos llegar con esto, e identificar brechas o proponer posibles vías de evolución de la gobernanza. Actualmente el documento no tiene especificidad. Se planteó la necesidad de hacer más específicos los objetivos de gobernanza, los roles y las responsabilidades, así como definir quiénes van a estar involucrados en la gobernanza. Esto depende de los objetivos y de un estudio que permita ver qué es lo que ya existe y qué falta. Se necesitaría un seguimiento para ver las brechas.

También se añadió que se requiere un ecosistema, una estructura concreta. Se debe generar y encuadrar la capacidad de actuar y de impulsar acciones. Es necesario impulsar al sector privado.

Se mencionó que hay muchos caminos posibles: se pueden fortalecer las estructuras existentes, o puede ser que se necesite una organización aparte como hay en Chile y Colombia. Hay que definir lo que se adecua mejor al país, y evaluar la viabilidad. Hay que determinar cómo dialogar para obtener una ejecución seria, aprovechar los recursos y no duplicar esfuerzos.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Se volvió a recalcar que la gobernanza ya existe, y que se debe reforzar lo positivo de lo que ya existe.

Se recomendó no duplicar leyes y decretos, sino bajar lo que ya existe a la práctica, concentrándose en los puntos débiles.

También se reiteró la necesidad de establecer vías de comunicación, especificar los roles y responsabilidades asegurándose de que las responsabilidades no se superpongan, pensar en qué otros organismos tienen conocimiento en estos temas.

Se planteó que deberían establecerse mecanismos de participación con el sector privado, la sociedad civil y la academia, ya que su visión es vital. Además, se estableció que es necesario un marco claro para garantizar la seguridad jurídica tanto para el sector público como para los privados. Las víctimas deben saber adónde acudir.

Pregunta sobre la gobernanza de seguimiento, cómo unir gobernanza con monitoreo, cómo plasmar este seguimiento. También se planteó la interrogante sobre el funcionamiento actual de las líneas de acción propuestas en el objetivo para considerar posibles ajustes a lo que no funcionó.

Se propusieron nuevas redacciones para líneas de acción i y iv del objetivo.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

Se reiteró que es la clave que estén involucradas la academia y la sociedad civil, y se planteó la necesidad de tener actores independientes. Se destacó nuevamente que hay que enfocarse en los roles y las responsabilidades. También se debe determinar qué actor va a definir los términos (por ejemplo, “infraestructura crítica”), resaltando que cuando nadie sabe lo que tiene que hacer no se hace.

Se subrayó que los gobiernos departamentales tienen más cercanía con el ciudadano; la estrategia tiene que tomar en cuenta a los gobiernos locales, cuya visión es muy diferente a la del gobierno. Se vive muy distinta la digitalización en el interior: se debe poder llegar a la ciberseguridad en el campo con un lenguaje diferente. Es clave tener bien claro cómo es Uruguay: no es solo Montevideo.

Se enfatizó la importancia de poder fiscalizar públicamente.

Se pidió evaluar la gobernanza existente y tener un abordaje temático a nivel global. Falta reforzar el marco de referencia.

Subgrupo 2

- Moderadora: María Noel Fernández, Agesic
- Relatora: Marta Susana Manent, ICD
- Participaron 11 (once) personas de 8 (ocho) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

Agesic (Institución pública) - Nicolás Correa

Plantea la necesidad de definir los actores fundamentales y las interacciones entre ellos para poder llevar adelante la estrategia abarcando todas las dimensiones.

Agesic (Institución pública) - Natalí Paggiola

Afirma que es necesario definir estructura organizativa, la alineación entre partes y los diferentes niveles que se plantean. Destaca que hay que realizar un seguimiento y monitoreo dinámico ajustado a la volatilidad del área y que esta instancia brindará un panorama realista para crear acciones oportuna y adecuada.

Agesic (Institución pública) - Alejandro Vargas

Presenta la importancia en esta etapa de definir actores, roles y responsabilidades.

Banco Santander (Sector privado) - Martín Rodríguez

Destaca la relevancia de que la estrategia no quede como un modelo teórico.

Presidencia de la República, División Gestión de Gobierno Electrónico (Institución pública) - Soledad Suárez

Comenta que “la ciberseguridad se hace entre todos”. El fin último de la gobernanza es que permee hasta el último nivel, que se generen comités de trabajo y que se revise continuamente. Menciona que esta estrategia fija pilares, pero no se bajan a tierra aspectos concretos.

CSIRT - Chile (Institución pública) – Cristian Bravo Lillo

Responde a las consultas que realizaron los otros panelistas. Sobre la consulta respecto a los objetivos actuales explica que se promulgó la ley marco de seguridad completando la normativa y se creó la Agencia Nacional de Seguridad y el CSIRT nacional, que ahora presta servicios al sector público y un sector del ámbito privado.

También añade que participan todos los actores. Comenta que el proceso en Chile no ha sido orgánico, sino que se realizó a partir de pruebas y reconfiguraciones. En ese sentido diferencia a lo que está ocurriendo en Uruguay, donde afirma que se está realizando un proceso orgánico y paulatino, que se está dando de manera organizada. Asimismo, plantea que es muy participativo. Nuevamente compara con el caso chileno, donde algunos sectores privados no se consideraron representados y en la segunda etapa recién se logró mayor participación.

URSEC (Institución pública) – Agustín Hill

Pregunta por qué no están consideradas todas las infraestructuras críticas, sino sólo las infraestructuras críticas de información. Los cables de fibra, por ejemplo, también son críticos a nivel de la ciberseguridad.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

Agesic (Institución pública) - Natalí Paggiola

Propone modificar la redacción de la línea de acción II (“Definir los mecanismos de coordinación entre ellos”): agregar “colaboración y comunicación”. En cuanto al objetivo “La ciberseguridad como objetivo de gestión”, propone agregar “nacional”.

En Gobernanza, la falta de líneas de acción para asegurar presupuesto adecuado, los recursos humanos y financieros, esto, para implementar los planes de acción y que la Gobernanza sea duradera.

Sostiene que, para ser una línea de acción y que la gobernanza sea duradera, es necesario asegurar el presupuesto adecuado, los recursos humanos y financieros. También identificar en la ENC cada objetivo, para que en la etapa de seguimiento poder hacer un mapeo de estos objetivos con los KPI. Plantea agregar un glosario de términos, considerando que estará dirigido al público y que habrá consulta pública.

Resalta que para englobar la voluntad política tiene que haber un liderazgo, no solamente roles alineados.

Menciona que cuando se dé el monitoreo, es necesario monitorear las dependencias de la región, no sólo las de Uruguay, y tenerlo en cuenta para actualizar la normativa.

Agesic (Institución pública) - Nicolás Correa

Sostuvo durante la sesión que:

Es fundamental identificar a todos los actores.

Es valioso aprender de otros países de la región con los que se comparten experiencias.

Es relevante que todos planteen sus necesidades como parte del proceso.

Las altas autoridades/jerarquías no pueden involucrarse porque no tienen conocimientos, por lo que parte de lo que hay que avanzar es en generar una cultura que les permita comprender las problemáticas.

Los proveedores locales deben participar del proceso e involucrarse. Asimismo, deben saber que las soluciones que ofrezcan/propongan deben cumplir con las regulaciones.

Propuso que la Agesic otorgue un certificado para que las empresas auditoras puedan dar certificados a privados.

Banco Santander (Sector privado) - Martín Rodríguez

Aporta que el modelo/instrumento que se cree tiene que ser flexible, ya que siempre cambia el cómo atacar. Agrega que la información tiene que llegar a todo el ecosistema y no sólo a quienes estén directamente involucrados.

Considera crucial, coincidiendo con Soledad Suárez, que haya planes de formación y capacitación continua de todos como algo obligatorio, entre los funcionarios y que lo cumplan como parte de su tarea.

Consulta respecto a las funciones que cumpliría la Agencia Nacional de Ciberseguridad.

Presidencia de la República, División Gestión de Gobierno Electrónico (Institución pública) - Soledad Suárez

Sostiene que es importante revisar la composición de la gobernanza, evaluar si la estructura es eficiente y si es necesario cambiarla. Plantea que habrá que realizar una auto-revisión de lo que se cree, evaluando si es eficiente para gobernar lo que hay debajo.

Afirma que tiene que haber planes de formación y capacitación continua para todos los funcionarios como algo obligatorio que sea cumplido como parte de su tarea.

En relación con el sector privado, considera que para aquellos privados que ofrecen soluciones en ciberseguridad, debería haber una revisación de los proveedores o recomendaciones a los que vayan a contratar. Se debe evaluar y guiar. Se sugiere que desde la Agencia que se cree se recomiende a esos proveedores y que cada vez más empresas contraten a esos proveedores. Que también deban ponerle foco a cumplir con determinados requerimientos, participar de reuniones y que los jefes sepan que esos empleados tienen que participar.

CSIRT – Chile (Institución pública) – Cristian Bravo Lillo

Plantea que lo que funciona a nivel autoridades es analizar casos de ataques que hayan ocurrido. Trae como ejemplo que en el Ministerio de Defensa se filtraron aproximadamente dos mil correos, lo que fue un escándalo. Desde entonces, el Ministerio no fue más indiferente. Otro ejemplo es un portal que cayó por un ataque a IAFX Network y que hizo que no funcione, generando pérdidas millonarias. Plantea que hay que recopilar datos de los ataques.

Comparte que en Chile aún no se han implementado planes de formación y capacitación continua con carácter obligatorio para los funcionarios, dado que se han centrado en lo técnico y aún falta lo humano.

Responde la consulta de Martín Rodríguez (Banco Santander) que la Agencia Nacional de Ciberseguridad que se crearía cumpliría las funciones de regular para todos los sectores. Aclara que cuando se reciben las licitaciones pueden recibirse documentos contradictorios en requerimientos. La Agencia central regularía específicamente para cada sector y se aseguraría de que no haya conflicto entre las regulaciones que reciben los regulados. Esto es importante para las PyMES, que tienen que recibir nociones claras de qué es lo que tienen que cumplir.

En el marco de los intercambios sobre el rol de la Agencia y los proveedores, Bravo Lillo expuso que en la ley hay un título sobre certificaciones. Pueden ser instituciones públicas y también otros privados los que certifiquen.

FGN (Institución pública) - Germán Martínez

Expone que se conformó un Comité de Seguridad que en Fiscalía no existía del que participaban los altos mandos; actualmente

están integrándose otras instancias del Comité. Señala que aun las autoridades no tienen claridad respecto a qué es lo que está faltando ni se ha logrado sentido de pertenencia. Menciona que los actores internos quieren defenderse de un caso que los afectó y no saben cómo defenderse y esto se aplica dentro de los Comités pero sin entender qué se está discutiendo.

Resalta que lo final son las métricas, en qué mejoramos.

Plantea que las autoridades ven estas acciones de capacitación y control como tareas extras que se les agregan, pero deberían verlo como parte de su trabajo.

Consideró que es necesario pedir requisitos para el ingreso a la función pública. Propuso que uno de los requisitos podría ser contar con un diploma de Agesic en ciberseguridad.

Agesic (Institución pública) - Alejandro Vargas

Subraya la relevancia de asentar los procedimientos, ya que las personas cambian pero los procedimientos quedan.

CISO – Ministerio del Interior (Institución pública) – Javier Jaureguiberry

Sostiene que debería generarse un marco legal o regulatorio para que haya un involucramiento de las altas gerencias, ya que los jerarcas dejan mucho a los cuadros técnicos, pero deberían involucrarse.

En el marco del debate sobre el rol de las altas autoridades, plantea que su conocimiento o desconocimiento de la temática no debe ser una traba y que para lograr su participación es necesario mostrar cuál es el riesgo, hablarles del impacto que un incidente podría tener.

Ronda 2. Aportes Estratégicos, Priorización e Identificación de actores para el pilar de la mesa

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Varios participantes validaron los objetivos.

También se hicieron ciertas propuestas, que incluyeron:

- Incorporar en el Objetivo II la palabra “nacional” después de “gestión”;
- En la segunda línea de acción del segundo objetivo, reemplazar “deberán contar” por “deberán cumplir”.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Se agruparon las propuestas en función de los objetivos:

Objetivo 1. Establecer la gobernanza nacional de ciberseguridad

- En la línea de acción ii, agregar “coordinación y comunicación”. Se deben definir los mecanismos de coordinación entre ellos.
- Los actores deberían estar representados por inciso y por sector (público, privado, academia) para que sea más abarcativo. El presupuesto y los recursos son fundamentales en la gestión.

Objetivo 2. La ciberseguridad como objetivo de gestión

- Brindar métricas para el Observatorio en ciberseguridad como de la Agenda Digital.
  Justificación: Para no esperar a la evaluación anual que se proponen en la ENC, que los representantes brinden métricas mensual o trimestralmente para ir visualizando el avance. Entre estas se pueden evaluar los incentivos y capacitaciones, para estudiar las tendencias.
- A través de incentivos y capacitaciones obligatorias, se propuso brindar métricas para ir evaluando las tendencias. Por ejemplo, que un representante de cada inciso mensualmente brinde métricas al Observatorio de Ciberseguridad para evaluar el avance. No se debería esperar a hacer una evaluación anual.
- También se propuso crear un incentivo por madurez en ciberseguridad a través de las auditorías.
- Se sugirió establecer una capacitación obligatoria en ciberseguridad como requisito para el ingreso a la función pública. En este punto se abrió un debate acerca de si se deberían incluir planes de actualización a lo largo de la carrera, y se llegó a la conclusión de que, en todo caso, los procedimientos deben estar bien definidos.
- Se hizo hincapié en la creación de una comunidad técnica para el intercambio de conocimiento, ya que la carencia de esta es un problema muy común en la región. Son pocos los que trabajan en ciberseguridad y en el Estado hay menos

recursos que en el sector privado.

- También se discutió acerca de si en este objetivo hay que agregar el asunto de Presupuesto. Hubo acuerdo que debería estar como línea de acción el asegurar presupuesto.

Objetivo 3. Desarrollar la legislación, el marco normativo y regulatorio

- Reemplazar “desarrollar” por “trabajar en el desarrollo y actualización” en la línea de acción ii.
- Monitorear las políticas y tendencias internacionales.

Además, se propusieron varias actividades de forma general:

Se propuso definir una línea de base para después documentar el avance de cada una de las áreas.

También se planteó que haya un encargado de ciberseguridad en cada servicio público, que reciba cursos en línea, capacitaciones y recursos (por ejemplo, templates).

Se hizo hincapié en que debería haber una manera de llamar a los jefes de ciberseguridad de otros servicios. Existe un directorio de contactos, pero debe implementarse una obligación de actualizarlo.

Se mencionó, por otro lado, que hay que tener en cuenta que en el Parlamento hay una ley de ciberseguridad, para no reiterar, mencionando que incluye el tema de formación.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

Se valoró identificar a los actores por inciso, por sector (público o privado), y también incluir a la academia y al gremio.

Se mencionó que los actores serían: Poder Ejecutivo, Presidencia, Ministerio de Defensa, Ministerio de Relaciones Exteriores (para desarrollo, actualización y monitoreo de las políticas internacionales), Ministerio de Interior, Poder Legislativo, Fiscalía, y representantes de las infraestructuras críticas de la información.

Se identificó como actores el Gremio (PIT-CNT) porque en las buenas prácticas dicen que son quienes generar resistencia y se deben incluir en la toma de decisiones, además de la Academia.

Se identifica a Agesic como actor referente que recibe y actualiza el directorio, y se sugiere que debería ser de acceso público o compartido con la comunidad.

Se aclara de todos modos que en cada organigrama debería ser posible encontrar a los responsables correspondientes, aunque depende del sector. Algunos, como la Banca, cuentan con información ordenada y otros no y no siempre los datos se encuentran actualizados.

Por ello, se recuerda que mantener esa información actualizada es obligatorio y que hacerlo también es parte de generar esta comunidad.

En cuanto a la priorización, se consideró que son todos interdependientes.

Subgrupo 3

- Moderadora: Arianne Palau, Agesic
- Relatora: Sabrina Piffaretti y Daniel Miranda, ICD
- Participaron 17 (diecisiete) personas de 9 (nueve) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

Parlamento (Institución pública) - Darío Burstin.

En relación con la definición de roles, mencionada en el borrador, propondría elaborar un marco legal para la participación. La gobernanza debería permitir que el marco normativo sea dinámico, que haya potestades suficientes en las autoridades, y que no sea necesario que cada vez que haya un problema haya que cambiar el marco legal. Menciona la necesidad de adecuarse a un contexto cambiante que requiere un marco normativo ágil.

ANCAP (Institución pública) - Marianela Moreno.

Lo fundamental y lo más importantes está: gobernanza, roles, participación de los actores públicos y privados, así como el desarrollo de las capacidades, ya que uno de los problemas que más nos golpea hoy es la falta de profesionales con esta especialización. Otro de los problemas significantes se encuentra en la compra de paquetes de tecnologías. Plantea la posibilidad de certificar esos paquetes para asegurar que reúnan los requisitos de ciberseguridad.

Agesic (Institución pública) - Gabriel Hernández

Destaca la necesidad de que se establezca un objetivo de gestión de las organizaciones a nivel de la ciberseguridad, para lo cual sería importante hacer mandatorio ese marco. A nivel público es más sencillo, pero a nivel privado es un desafío importante para la gobernanza. Propone que la ciberseguridad se tome como un objetivo central a nivel privado y que esto permee a las organizaciones.

URCDP (Institución pública) - Flavia Baladán

Menciona tres puntos para que la gobernanza sea más efectiva: primero, hay que trabajar mucho el desarrollo de capacidades y apuntar a una mayor capacitación. Para poder llevar esto a la práctica, es importante preverlo en recursos humanos. Además, se deben empezar a coordinar acciones de ciberactividades, para lo que es importante trabajar en las funciones de cada organismo. Finalmente, considera que se debe también priorizar este tema en las instituciones.

BCU (Institución pública) - Isabel Maroñas

Está de acuerdo con el borrador y cree que es importante el tema de la coordinación, en especial en los niveles estratégico, táctico y operativo. Es importante también la generación de cultura: en el marco de la gobernanza se debe generar esa cultura de ciberseguridad, que falta mucho en el país y en las instituciones. Es necesario que se brinden los recursos.

AIN (Institución pública) - Jonathan Silva

La capacitación es importante, porque hay 700 puestos de ciberseguridad que no están cubiertos (dato de un informe de Agesic). En el sector público la inversión en tecnología es deficitaria, lo que se plantea como un reto. Es necesario que haya algún tipo de control: en el sector público, Agesic debería poder auditar a los organismos. Falta mayor control de parte del Estado. Lo ideal sería llegar a un punto donde el riesgo se mida en todos los organismos, y tener una metodología común que sea transversal a todas las organizaciones.

BCU (Institución pública) - Carla Facal

Es importante que se definan claramente muchos aspectos porque en algunos casos no queda claro el rol de cada uno de los organismos.

Ceibal (Institución pública)- Federico Quiroga

Coincide con la participación anterior y menciona que es importante la segregación de roles. Actualmente como no se tienen recursos hay otras áreas que se encargan de la ciberseguridad y eso genera una duplicación de actividades. Es importante que el encargado de ciberseguridad tenga eso como única función, por lo que es importante sensibilizar a las autoridades. Por lo demás, aprueba el borrador.

URSEC (Institución pública) - Mercedes Aramendía

Primero, sería bueno poner más énfasis en la educación en ciberseguridad, incluso en la población en general. Segundo es

importante jerarquizar la temática para que sea transversal y se convierta en una política de Estado. Se debe vincular la educación y la sensibilización con la importancia del tema y los riesgos que conlleva a nivel público y privado.

Agesic (Institución pública) - Karime Ruibal

Una agenda digital es una buena herramienta y Uruguay tiene mucha experiencia. La gestión del conocimiento también es imprescindible, y los procesos de gestión del conocimiento tienen que estar incluidos desde la gobernanza. Reconoce que faltan esfuerzos orientados a este objetivo.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

Agesic (Institución pública) - Karimesole Ruibal

Comenta que el seguimiento de indicadores debe ser estricto, porque sino en ese pasaje de lo estratégico a lo operacional hay muchos problemas. Sería importante ver cuáles son los riesgos y las barreras, porque lo crítico está en lo operacional. Menciona como clave tomar las experiencias internacionales como referencia y apuntar a la eficiencia.

URSEC (Institución pública) - Mercedes Aramendía

Afirma que se debe profesionalizar más la temática, y que necesitamos una ley que tipifique los ciberdelitos y acompañe la parte procesal.

Ceibal (Institución pública) - Federico Quiroga

Los objetivos estratégicos se podrían tomar a nivel país, para lo cual es necesario que se establezca un estándar a seguir. Esto puede generar una mejora continua. Sería bueno en este escenario hacer una medición general del país.

BCU (Institución pública) - Carla Facal

El marco de ciberseguridad de Agesic existe, pero ¿por qué no trasladar lo que se tiene en Agesic hacia las otras organizaciones? Propone un marco de gobernanza más abarcativo; un modelo más amplio y formal de ciberseguridad. Esta propuesta podría implementarse mediante un modelo de gobernanza.

AIN (Institución pública) - Jonathan Silva.

Sostiene que el marco de Agesic se está aplicando en algunas empresas, pero la resolución de hacer un análisis de brecha y un plan de acción no es vinculante y queda diluido en un plan de acción. Hay organismos que no tienen la suficiente madurez tecnológica para implementar esto.

BCU (Institución pública) - Isabel Maroñas

A la coordinación habría que darle una forma concreta, como mesas de trabajos a nivel estratégico, táctico y operativo, tal como estas mesas de diálogo. Estas instancias concretas, donde los representantes tendrían un perfil concreto de trabajo y trabajarían con métricas, podrían tener una frecuencia de una vez al mes para que se generen metas de avances.

URCDP (Institución pública) - Flavia Baladán

Resalta que es importante considerar la diferencia entre lo público y lo privado. Es imprescindible esta diferenciación para establecer prácticas diferenciales, ya que se observan distintos niveles de cumplimiento. También es importante avanzar en la parte normativa, con el fin de crear las condiciones necesarias para que se puedan establecer gobernanzas.

Agesic (Institución pública) - Gabriel Hernández

Tiene muchas preocupaciones. Coincide en que tiene que haber regularidad y seguimiento para que haya un plan que funcione y se operativice, pero más allá del nivel normativo hay que poner recursos para que puedan haber fuerzas de trabajo que se ocupen de esto. Habría que tener equipos y ayudar a los que toman las decisiones a enfatizar el tema de ciberseguridad y establecer presupuestos. Es necesario volcar recursos en la operación para ponerla en marcha de manera efectiva.

ANCAP (Institución pública) - Marianela Moreno

Menciona la diferencia entre la elaboración de políticas ideales y su implementación, y enfatiza la necesidad de hacer foco en este último punto. Subraya que se definen hermosas políticas, pero que luego cuesta implementarlas porque no hay presupuesto, gente, etc. Sostiene que se debe hacer más foco en lo que planteaba Isabel Maroñas, es decir mantener estas mesas para aprender de los que ya recorrieron el camino, para buscar sinergias. Hay que tener en cuenta los procesos de gestión del conocimiento, ya que pueden ayudar a simplificar lo operacional.

Parlamento (Institución pública) - Darío Burstin

Menciona una propuesta de redacción para una línea de acción: *La distribución de potestades regulatorias y responsabilidades*

entre los diversos organismos debe ser clara y permitir una rápida adaptación del marco normativo a los cambios de circunstancias.

Ronda 2. Aportes estratégicos, priorización e identificación de actores para el pilar de la mesa

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Consideran que los objetivos son correctos a nivel general y los dan como validados.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Los y las participantes analizan los objetivos de forma grupal en base a los aportes del trabajo anterior. A continuación se detallan sus propuestas de acciones y actividades en base a cada objetivo.

Objetivo 1. "Establecer la gobernanza nacional de la ciberseguridad"

- Desarrollar una hoja de ruta;
- Contar con potestades administrativas;
- Definir un órgano rector asociado con el Comité de Gestión;
- A futuro, crear un Ministerio de Tecnología;
- Coordinar y difundir las actividades del comité asesor o de gestión;
- A corto plazo, incorporar en el comité tanto a nivel estratégico y a nivel de gestión a otros actores: por ejemplo, la academia;
- Definir la competencia de control;
- Definir indicadores, recursos humanos y recursos;
- Establecer una agenda digital a nivel nacional de ciberseguridad;
- Establecer roles;
- Mirar hacia fuera para descubrir buenas prácticas a nivel internacional;
- Relevar funciones;
- Coordinar el diálogo como línea transversal a todas las acciones: trabajar para involucrar a los actores que no están involucrados a nivel estratégico.

Objetivo 2. "La ciberseguridad como objetivo de gestión"

- Jerarquizar;
- Asegurarse de que sea una política de Estado;
- Desarrollar capacidades;
- Invertir en tecnología;
- Medir el riesgo de forma transversal;
- Gestionar la ciberseguridad dentro de las organizaciones;
- Certificar empresas en Ciberseguridad;
- Operacionalizar, medir y profesionalizar.

Objetivo 3. "Desarrollar la legislación, el marco normativo y regulatorio"

- Instrumentar un marco normativo de ciberseguridad e implementar el marco en la mayor cantidad de ámbitos posibles;
- Establecer una ley sobre delitos de ciberseguridad;
- Establecer y mejorar los aspectos procesales;

- Desarrollar una agencia de coordinación.

También se hicieron otros aportes generales:

Agesic (Institución pública) - Gabriel Hernández

Señala que la tercera línea de acción del segundo objetivo (“Elaborar los marcos legales y regulatorios necesarios”) debería estar incluida en el tercer objetivo (“Desarrollar la legislación, el marco normativo y regulatorio”). Se debería añadir un objetivo para la implementación de la hoja de ruta y de los mecanismos de control. Además, el tercer objetivo debería generar los marcos para los dos objetivos anteriores.

URCDP (Institución pública) - Flavia Baladán

Frente a esto, argumenta que si bien el marco regulatorio es de ayuda, no soluciona todo. Por lo tanto, en el marco regulatorio se deben diseñar acciones concretas.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

No se llegó a trabajar este punto

Subgrupo 4

- Moderadora: Mariana Ferraro, Agesic.
- Relatora: Marcelo Castillo y Mauro Parada, ICD
- Participaron 13 (trece) personas de 11 (once) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

Identificar aportes generales sobre la propuesta borrador: ¿Qué aspectos consideran más relevantes en la propuesta del primer borrador de la Estrategia Nacional de Ciberseguridad para abordar eficientemente retos y desafíos en torno a la Gobernanza Nacional de la ciberseguridad?

MIEM (Institución pública) - María José Franco

Destaca la importancia de convocar a todos los actores y adoptar una perspectiva holística que abarque todas las realidades. Apoya la idea de que el cibercrimen es un pilar importante, pero reconoce que la estrategia debe ir más allá de ello, abarcando una estrategia nacional inclusiva.

BROU (Institución pública) - Marcelo Varaldi

Subraya la importancia de hablar directamente sobre la gobernanza y no solo sobre la estrategia general.

Propone dividir la gobernanza en niveles: estratégico, táctico y operativo, y reconoce la dificultad de implementar estos niveles.

Señala la brecha entre el "qué" y el "cómo" en la implementación, destacando que muchos se preocupan, pero pocos se ocupan en la práctica.

Menciona que su organización está regulada y auditada, lo cual mejora su posición frente a los riesgos, y sugiere que esto podría extrapolarse a la estrategia nacional.

URSEC (Institución pública) - Mauro D. Ríos

Critica la constante queja de estar siempre detrás del cibercrimen debido a limitaciones legales y éticas, sugiriendo asumir esta realidad en los documentos estratégicos.

Reitera la importancia de jerarquizar la ciberseguridad y resalta que la gobernanza debe ser manejada a un nivel superior para ser efectiva.

Comenta que la Agesic tiene antecedentes positivos y propone que las resoluciones de Agesic sean obligatorias para la Administración Central.

LACNIC (Sociedad civil) - Graciela Martínez

Considera que las líneas de acción deben tener metas claras para su ejecución.

Enfatiza la necesidad de continuidad en la estrategia, independientemente de los cambios de gobierno, involucrando a todos los partidos políticos.

Propone el uso de una matriz de riesgos para priorizar y analizar la ciberseguridad al mismo nivel que otros riesgos.

Agesic (Institución pública) - Mauricio Papaleo

Explica que la estrategia nacional se definirá por decreto, y que se debe incluir la forma de llevarla a cabo y los organismos involucrados.

Destaca la importancia del consenso y el desafío del presupuesto, subrayando que cada gobierno debe aplicar la estrategia sin cambiarla significativamente.

Propone una ley que defina la gobernanza en el país, sugiriendo un consejo de alto nivel para establecer la estrategia.

Menciona que la seguridad debe ser un objetivo estratégico y destaca la importancia de cumplir con el marco de ciberseguridad establecido por la ley Nº 20.212.

BID (Institución pública) - María Inés Vázquez

Sugiere identificar los actores estratégicos y sus roles en el sistema de seguridad, para saber quiénes son los responsables a

nivel superior.

UTE (Institución pública) - Evelyn Antón

Señala el problema del presupuesto y la necesidad de priorizar recursos, sugiriendo revisiones de riesgo antes de implementar cambios. Menciona que la seguridad debe jerarquizarse dentro de las organizaciones para evitar depender de otras necesidades del negocio. Destaca que la ciberseguridad debe competir al mismo nivel de análisis que otros riesgos.

SeCIU (UDELAR) (Academia) - Sergio Ramírez

Propone definir objetivos de gestión de ciberseguridad y los organismos que deben cumplirlos, sugiriendo que estos objetivos sean claros y prioritarios. Resalta la importancia de tener objetivos claros para evitar que se les dé importancia solo cuando ocurren incidentes.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

Identificar aportes específicos sobre el pilar a analizar en la mesa. ¿Qué aspectos específicos de gobernanza creen que podrían mejorarse o añadirse en el pilar “Gobernanza y Marco normativo” con el fin de establecer la Gobernanza Nacional de la Ciberseguridad de Uruguay?

LACNIC (Sociedad civil) - Graciela Martínez

Enfatiza la importancia de nombrar los organismos y tener una estrategia de riesgos, ya que esto es fundamental para priorizar otros riesgos críticos y determinar el presupuesto necesario. En cuanto a la gobernanza, cuestiona la viabilidad de una mesa con cien participantes y sugiere analizar la media en otros países y los planes de comunicación efectivos que han implementado.

Respecto a las líneas de acción, menciona la necesidad de definir los niveles de organizaciones y responsabilidades en la gobernanza y establecer mecanismos de integración. Se pregunta cómo se definirán las organizaciones que participarán en la gobernanza y cuál será el plan de comunicaciones, ya que una de las causas de fracaso es que, a menudo, se definen las responsabilidades y luego cada uno sigue caminos diferentes, lo que dificulta la cohesión y efectividad.

MIEM (Institución pública) - María José Franco

Plantea que al incorporar la ciberseguridad en la gestión, cada sector (vertical) debe hacer un análisis de riesgo específico, aunque pueda haber un análisis general como base. Pregunta cómo será la participación del sector privado, ya que la estrategia parece enfocarse más en lo público. Sostiene que es necesario que tanto el sector público como el privado se apropien de la estrategia.

Aunque está claro que los privados estarán involucrados, cuestiona si tendrán un rol dentro de la gobernanza y cuál sería ese rol. Destaca que, para que las empresas incorporen la ciberseguridad en sus modelos y cumplan con la ley, deben estar activamente involucradas en la gobernanza. Si no se les incorpora adecuadamente, será una debilidad, ya que necesitarán presupuesto para cumplir con las exigencias de la estrategia.

BROU (Institución pública) - Marcelo Varaldi

Sugiere que se puede cubrir la cuestión adoptando el marco de seguridad de Agesic para toda la población. Explica que esto debe salir de la estrategia nacional de ciberseguridad, aplicándose tanto a sistemas públicos como privados. Menciona que, independientemente de si la infraestructura es pública o privada, debe ser parte del análisis de riesgo y de la estrategia.

URSEC (Institución pública) - Mauro D. Ríos

Señala que, aunque nos centramos en ciberseguridad, se necesita una estrategia de seguridad informática integral, ya que la ciberseguridad es solo una parte y el eslabón más débil es el ser humano. En URSEC, tienen 25 políticas de seguridad y están actualizando diez, pero al ejecutarlas a menudo se desvían de lo planeado, lo cual debería mencionarse en las estrategias. Además, al hablar de sociedad civil, no sólo deben considerarse ONGs sino también otras organizaciones que trascienden fronteras. Propone que la seguridad de la información se aborde de manera general dentro del marco de la ciberseguridad para prevenir fugas de información.

Ronda 2. Aportes estratégicos, priorización e identificación de actores para el pilar de la mesa

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Se trabajó en base a ejes temáticos y se desarrollaron sugerencias en distintas áreas.

Definiciones y glosario

Ante la interrogante sobre si se acordó un glosario y un concepto de seguridad y cibercrimen, se fijó la recomendación de iniciar

con un glosario como práctica internacional.

Se comentó que se está trabajando en un decreto que incluirá un glosario.

Identificación de involucrados y comunicación

Se volvió a manifestar que es necesaria la incorporación del análisis de riesgos en la gestión de objetivos de ciberseguridad. Hay que establecer criterios para definir los actores y líneas de acción, y mejorar la comunicación y coordinación.

Obligatoriedad, cooperación y concientización

Se mencionó la necesidad que sea obligatorio compartir información en algunos países y cómo habría que considerar la obligación de reportar e interoperar en Uruguay, considerando marcos sancionatorios en otros países como por ejemplo el caso de Chile.

Se señaló el fomento de la cooperación y la concientización entre empresas, aunque se marcaron ciertas dificultades de compartir estrategias de seguridad por razones comerciales.

Definición de actores clave

Se marcaron como actores claves a incluir en la gobernanza a: Agesic, URSEC, DINATEL y Ministerio del Interior. Luego otros participantes agregaron al Banco Central, URSEA, Ministerio de Relaciones Exteriores y Ministerio de Defensa. Además de ese espacio de gobierno central, se agregaría un Consejo Consultivo con amplia participación.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Se propuso mapear a los actores involucrados y sus roles en la estrategia.

También se sugirió definir los niveles de criticidad de los servicios que ofrecen los organismos, y tener un modelo de madurez que obligue al cumplimiento de los niveles de criticidad.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados:

Se propuso hacer una evaluación de riesgos y revisar los marcos legales en relación con la gobernanza general. Se subraya que es clave la definición de niveles de criticidad de servicios y el establecimiento de un modelo de madurez.

Sobre la infraestructura crítica, se manifestó que hay que realizar un set general de responsables para el marco normativo.

Se propuso crear un Comité Estratégico y Operativo: definir organizaciones responsables del marco normativo y crear un Comité Táctico y Operativo por sectores.

Se marcó la importancia de identificar y catalogar activos críticos.

Se enfatizó la necesidad de la seguridad como objetivo estratégico de las empresas, y la necesidad de auditar la implementación.