Mesa de trabajo “Ecosistema e Industria de la ciberseguridad"

Autor

Agesic

Fecha de creación

08/10/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la octava mesa de trabajo **'Ecosistema e Industria 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, en 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 21 de junio se realizó el análisis del pilar de la Estrategia “Cultura y Ecosistema”. En este informe se detallan las propuestas y aportes compilados en la última mesa de diálogo, centrada en “Ecosistema e industria de la ciberseguridad”.

Este documento presenta en forma sintética los intercambios que se dieron en esta mesa.

Participantes

Agesic (Institución pública), Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento. Estefanía Almeyda, Alejandro Arancio, Mateo Cabrera, Claudio Martínez, Adolfo Nidegger, Maite Rodríguez, Fabiana Santellán.

ANCAP (Institución pública), Administración Nacional de Combustibles, Alcohol y Portland. Andrea Parada.

ANII (Institución pública), Agencia Nacional de Investigación e Innovación. Fabio Bonanno, Mauricio Rinaldi.

ASSE (Institución pública), Administración de los Servicios de Salud del Estado. Gerardo Otero, Adriana Peluffo, Stella Rossi.

Atos Uruguay (Sector privado), Joaquín Pérez.

BCU (Institución pública), Banco Central de Uruguay. María Isabel Maroñas.

BID (Institución pública), Banco Interamericano de Desarrollo. Ariel Nowersztern.

BPS (Institución pública), Banco de Previsión Social. Álvaro Arias.

CERTuy (Institución pública), Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Natalí Paggiola.

CGN (Institución pública), Contaduría General de la Nación. Guillermo Freire.

CUTI (Sector privado), Cámara Uruguaya de Tecnologías de la Información. Ana Lucero.

Datasec (Sector privado), Carlos Serra.

DGI (Institución pública), Dirección General Impositiva. Guillermo Dornelles, Carlos Vidal.

Dinatel (Institución pública), Dirección Nacional de Telecomunicaciones. Virginia Alonso.

EY Uruguay (Sector privado), José Luis Vera.

Fortinet (Sector privado), Gastón Sancassano.

Galileo Latam (Sector privado), Mauro Flores.

Grant Thornton (Sector privado), Ignacio Lagomarsino.

IM (Institución pública), Intendencia de Montevideo. Luis Garcimartín, Fernando Rodríguez.

LIDECO (Sociedad civil), Liga de Defensa Comercial. Bernardo Quesada.

MIEM (Institución pública), Ministerio de Industria, Energía y Minería. Gabriel Artucio, María José Franco.

Ministerio del Interior (Institución pública), Javier Jaureguiberry.

Ministerio de Defensa (Institución pública), Claudio López.

MRREE (Institución pública), Ministerio de Relaciones Exteriores. Daniel Pesce.

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

OWASP (Sociedad civil), Open Worldwide Application Security Project. Gerardo Canedo.

Patria Investments (Sector privado), Leonardo Martinez.

QoxIT (Sector privado), Pablo Alzuri.

SECIU – UDELAR (Academia), Servicio Central de Informática – Universidad de la República. Sergio Ramírez, Javier Valena.

Teledata (Sector privado), Alejandro Pereyra.

Tilsor (Sector privado), Rodrigo Martínez.

UTE, (Institución pública), Administración Nacional de Usinas y Transmisiones Eléctricas). Alejandro Álvarez.

URSEC (Institución pública), Unidad Reguladora de Servicios de Comunicación. Fernando Hernández, Agustín Hill, Mauro Ríos, Nelson Rodríguez.

URUDATA (Sector privado), José Callero.

Resumen del intercambio

A continuación se presenta el informe general de la mesa de trabajo “Ecosistema e industria de la ciberseguridad” donde 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.

Cabe destacar que, si bien cada ronda y parte se centraba en un tema delimitado, la discusión en la mayoría de los casos excedió la pregunta inicial.

Parte 1. Ronda de intercambio sobre el borrador

Durante esta primera ronda las personas participantes realizaron aportes sobre el borrador, identificando tanto aportes generales sobre la propuesta como aportes específicos sobre el pilar “Cultura y Ecosistema”.

Se les preguntó: ¿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 al ecosistema y la industria de la ciberseguridad? ¿Qué aspectos específicos de ecosistema e industria creen que podrían mejorarse o añadirse en el pilar “Cultura y Ecosistema” con el fin de potenciar el ecosistema y la industria de la ciberseguridad en Uruguay?

Las respuestas a estas dos preguntas quedan detalladas de manera conjunta a continuación.

Los y las participantes aplaudieron la iniciativa, y compartieron sus observaciones y sugerencias sobre el borrador de la estrategia. En términos generales, se destacó la importancia de incluir la cultura como ecosistema con un enfoque en la ciudadanía. También se hizo hincapié en que falta en todo el documento una línea de acción previa que es conseguir financiamiento y recursos humanos. Se sostuvo que la descripción de objetivos es genérica y no indica claramente el propósito final, haciendo que las líneas de acción parezcan aplicables a cualquier país. Se pidió una simplificación de los mecanismos y procedimientos.

Los aportes específicos de los y las participantes se encuentran sistematizados en ejes temáticos:

Educación, concientización y capacitación

Se definió el tema de formación como prioritario para abordar la ciberseguridad en todos los niveles, y para ir formando esa fuerza laboral que se necesita. Se propuso crear nuevas carreras y/o posgrados en ciberseguridad, implementar cursos a nivel de la administración pública, y ofrecer pasantías en organismos a los estudiantes. También se subrayó que se debe cambiar el currículo de educación de la educación media en adelante.

También se sostuvo que se debería hacer más énfasis en el fomento de la cultura de los tomadores de decisión, ya que sino no se tratará de una visión estratégica a largo plazo. Se debe capacitar en percepción del riesgo para que la estrategia sea una política de Estado.

Se hizo hincapié en la necesidad de concientizar a todas las personas de los organismos, ya que todos tienen un cierto rol que cumplir. Aquellos que trabajan en la administración pública deben estar capacitados en ciberseguridad.

Se enfatizó que falta mano de obra de nivel técnico, y se debe buscar una línea de acción rápida y efectiva en el tema de capacitación. Se planteó que el tema de la educación debería ser transversal.

En cuanto a los usuarios finales, se debe educar a la ciudadanía en su conjunto para que haga presión y exija la ciberseguridad. Esto requiere capacitación docente. Se debe desarrollar la educación formal e informal. Se sugirió poner el foco en distintos públicos, dividiéndolos en sectores. Se consideró importante abordar con la formación a todas las franjas etarias, incluyendo a la franja del medio de la población a la que no se puede llegar por los sistemas educativos.

Coordinación y cooperación

Se sostuvo que hace falta una sección “Gobernanza del Ecosistema y Marco jurídico”: debería haber una estructura formal y organizada que lidere para que no sean acciones puntuales.

Se señaló la necesidad de darle forma concreta a la coordinación de esfuerzos entre distintos sectores. Se deben generar interacciones en el sistema para que formen un círculo virtuoso. Se resaltó la importancia de formar grupos de trabajo para compartir experiencias, y de armar redes de colaboración.

Incentivos para el cumplimiento

Se habló de la posibilidad de multa, ya que cumplir debe ser más barato que incumplir. Sobre todo, se indicó que se debe fomentar y generar incentivos para las pymes. El Estado debe proporcionar herramientas de apoyo, formación y seguimiento, en especial para las pymes. Se propuso exigir certificaciones a las empresas en los pliegos de compras para armar una cadena de cumplimiento, sosteniendo que falta plasmar los requerimientos para asegurar la cadena de proveedores y que todos

cumplan con determinados controles en la estrategia.

Se afirmó que debe haber planes de incentivo, entrenamientos y guías para que las pymes puedan acceder a servicios de ciberseguridad. La concienciación y los cursos son muy importantes: se sugirió generar campañas de concientización en lugar de obligaciones estrictas, cursos específicos sobre seguridad digital, y centros de asesoramiento para pymes. Además, se propuso ofrecer subsidios, incentivos y reducciones de impuestos para fomentar estas prácticas, resaltando la necesidad de inversión en este ámbito. Se debe concientizar a las empresas sobre su responsabilidad ante los ciberataques.

Se sugirió que CERTuy o AGESIC asesoren a los compradores sobre cómo adquirir software seguro, estableciendo estándares claros de requisitos a cumplir.

Legislación

La legislación existe, pero se debe divulgar ya que se desconoce. Hace falta colaboración con abogados.

Jerarquización y asignación de roles

Se resaltó la necesidad de jerarquizar los roles y que haya consecuencias cuando ocurren incidentes. Se mencionó la posibilidad de crear una superintendencia, asimilándola a lo que es la superintendencia del Banco Central para el sector financiero.

También se hizo hincapié en que faltan responsables de ciberseguridad: debe implementarse un referente, y se debe cumplir. Además, los políticos deberían tener interlocutores idóneos.

Se expresó preocupación por la disponibilidad de personal para los cuatro CSIRTs planificados y se sugirió que, en lugar de centrarse en la implementación específica de estos, es más efectivo definir un nivel de seguridad a alcanzar y proporcionar un lineamiento general que guíe a cada entidad hacia ese objetivo.

Heterogeneidad en el ecosistema

Se mencionó que hay una gran heterogeneidad en el ecosistema, por lo que se deberían

definir métodos para compartir y comunicar información. AGESIC debería asistir a las organizaciones con menos grado de madurez en el tema. ANII tendría que tener una estrategia institucional que apoye a estos aspectos y que no sea de un área específica de TI, sino de la institución entera.

Monitoreo y respuesta

Se sostuvo que se deben impulsar equipos de monitoreo y respuesta tanto a nivel público como privado.

Se estableció la necesidad de establecer métricas claras para medir el éxito o fracaso de cada línea de acción, y comenzar por fortalecer la seguridad en empresas de desarrollo.

También se propuso crear más centros de respuestas.

Cooperación internacional

Se resaltó la necesidad de cooperación internacional y de monitorear el panorama internacional. Se propuso hablar de ecosistema internacional en vez de nacional: consistiría en trabajar en las fortalezas nacionales y pedir apoyo internacional.

Sector privado

Debería ser un objetivo estratégico aprovechar al sector privado. Se debe especificar cómo se incentivará su participación.

Categorización de ciberataques

Se planteó la necesidad de categorizar las consecuencias de los ciberataques según el impacto que tienen en las organizaciones y en la sociedad en general.

Reorganización de objetivos

Se planteó que el objetivo 4 (“Mejorar la ciberseguridad de las MiPymes”) no debería conformar un objetivo en sí mismo. Se propuso abordar la estrategia de ciberseguridad organizando las acciones por sectores en lugar de por tamaño de empresa, priorizando aquellos sectores con mayores riesgos y vulnerabilidades conocidas, como el sector de la salud. A estos efectos, se hizo énfasis en que se debe definir cuáles son los sectores críticos y tenerlos bien identificados.

Respecto al objetivo 5 (“Fortalecer el ecosistema de Firma Identificación digital para fortalecer el gobierno digital”), también se planteó que no debería ser un objetivo por sí mismos. Sin embargo, se hizo hincapié en la necesidad de simplificar este proceso.

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

En esta parte las personas participantes discutieron acerca de los objetivos planteados en el capítulo relativo al ecosistema e industria de la ciberseguridad del pilar “Ecosistema y cultura”.

Los objetivos fueron generalmente validados.

Se señaló que lo más importante es que la seguridad sea una responsabilidad proactiva a nivel estratégico, que abarque todo.

También se recomendó definir qué es el ecosistema que pretendemos atender. Se sugirió que se trataba de los profesionales – las personas, los equipos – dedicados a la ciberseguridad. Se enfatizó la visión de que Uruguay cuente con un ecosistema vibrante, al frente del conocimiento, que atienda las necesidades del país. Los objetivos serían mantener o impulsar elementos del ecosistema para lograr esa visión. Actualmente faltan profesionales de ciberseguridad: hay que tener líneas de trabajo para generar más profesionales. También se debe fortalecer la interconectividad en el ecosistema, tanto mediante canales formales como mediante “hubs de conocimiento” más informales. Un ecosistema fuerte es un elemento clave para que el país logre altas capacidades en ciberseguridad.

Se enfatizó la necesidad de un marco normativo fuerte y transparente, de concientización y capacitación, y se subrayó la importancia de desarrollar un plan de acción unificado.

Se propuso agregar como objetivo la necesidad de identificar sectores especialmente sensibles para empezar (por ejemplo, la salud) y enmarcarlos dentro del pilar “Ecosistema y cultura”.

Se emitieron ciertas observaciones respecto a cada objetivo, detalladas a continuación.

Objetivo 1: “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”

- El fortalecimiento contemplado no debe ser solamente técnico: los equipos en las empresas públicas también deben ser fortalecidos en el sentido que su opinión debe contar en la toma de decisiones de la empresa.
- La segunda línea de acción de este objetivo, “Generar y establecer una serie de ejercicios anuales específicos para los equipos,” es demasiado específica.
- Se propuso agregar una cuarta línea de acción que consista en elaborar un plan de acción general que unifique a todos.
- Se sugirió que el intercambio podría incluir a otros países de la región.

Objetivo 2: “Impulsar el desarrollo de una industria del software seguro”

- Se propone titular al objetivo “Impulsar el desarrollo, la adquisición y el uso del desarrollo de software seguro.”
- Se considera importante no solo enfocarse en formación, sino también en analizar cómo la empresa está asegurada frente a un ataque. Eso requeriría un monitoreo.

Objetivo 3: “Posicionar la industria de ciberseguridad nacional”

- La primera línea de acción (“Incentivar la industria nacional de ciberseguridad”) es demasiada abstracta. Sería necesario ampliarla y concretizarla un poco más. Además, se debe definir cómo se va a medir algo tan poco concreto.
- Respecto a su línea de acción i, “Incentivar la industria nacional de ciberseguridad”, se sostuvo que el esfuerzo también debe venir del lado de la empresa. Por lo tanto, es necesario incentivar no solamente al sector público, sino también al privado: se debe generar un esfuerzo de control para las empresas que brindan servicios.
- Además, se señaló que hoy existen incentivos para las pymes, pero no hay incentivos específicamente para empresas de ciberseguridad. Se hizo una distinción entre las empresas de ciberseguridad y las empresas que tienen datos de los ciudadanos, y se debatió acerca de la necesidad de agregar un objetivo respecto a los mecanismos de reconocimiento.
- Respecto a la segunda línea de acción, “Promover los mecanismos y ámbitos para la participación academia-público-

privada", se plantearon las dificultades asociadas a la ley de ciberdelito que se está por aprobar, que no contiene mecanismos de aceptación para las herramientas de hacking ético. Se pidió generar una salvaguarda para la seguridad ofensiva, asimilada al "porte de arma".

- En la línea de acción iii ("promover la investigación y desarrollo en ciberseguridad"), se propuso reemplazar "promover" por "posicionar".

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

- Se plantearon dudas acerca de la necesidad de posicionar a las pymes como uno de los objetivos, cuando hay otra cantidad de cosas también importantes que deberían ser incluidas.

Objetivo 5: "Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital"

- Se plantearon dudas acerca de lo que significa la identificación digital.
- Se discutió acerca de si este objetivo debería entrar en la estrategia de ciberseguridad, y si debería constituir un objetivo. También se cuestionó su inclusión en el pilar "Ecosistema y cultura".
- Se agregó que se debería marcar la necesidad de mejorar la identificación. Se propuso delegar todo en AGESIC y que sea obligatorio en los trámites.
- Se subrayó que hay que impulsar la firma digital y electrónica, y debe ser aceptada por todas las oficinas del Estado. Se debe seguir ampliando y se deben generar mecanismos de reconocimiento a nivel internacional.

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

Las personas participantes aportaron actividades y acciones para el pilar "Ecosistema y cultura, detallados según cada objetivo.

Objetivo 1: "Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta"

Acciones propuestas:

- Incluir a la sociedad civil, que no aparece en la descripción del objetivo: se habla solamente del ámbito público, privado, y la academia.
- Darle una figura jurídica al tema de la ciberseguridad, a través de la creación de una agencia nacional de ciberseguridad. En ese sentido hay que ver la institucionalidad que se le quiere dar, que le permita tener presupuesto y que se le otorgue poder entre para hacer la vigilancia y control de los organismos. Se plantea que el rol de AGESIC – que se debe definir más claramente - podría ser más de regulador, de órgano rector.
- Hacer tres niveles de capacitación: un nivel para la población que aún está en el sistema educativo, otro para la gente que ya ha pasado por el sistema educativo o que está fuera de la educación, y el tercero para los tomadores de decisiones. Sería importante que haya un bloque de ciberseguridad en las carreras de relaciones internacionales, y cursos para las personas en la administración pública.
- Establecer obligaciones legales claras o implementar un sistema de incentivos y sanciones para garantizar el cumplimiento de las normativas de ciberseguridad.
- Definir métodos específicos para medir el éxito y la efectividad de las iniciativas de ciberseguridad.
- Desarrollar estándares y guías claras para la creación y operación de CSIRTs.
- Asegurar la disponibilidad de recursos humanos capacitados y recursos materiales suficientes para su implementación y operación.
- Considerar la creación de un CSIRT ciudadano para fomentar la cultura de ciberseguridad y desarrollar perfiles técnicos adecuados.
- Fomentar la coordinación entre los diferentes CSIRTs y otros organismos para asegurar una comunicación efectiva.
- Definir estrategias claras y sostenibles para la continuidad de las iniciativas de ciberseguridad.
- Definir qué organismos deberían tener un SOC (se mencionó a UTE, ANCAP y OSE) y unir los SOCs para que compartan información, sobre todo los indicadores de compromiso.
- Agregar un servicio de Ciberinformación que registre los ciberincidentes que ocurren en el país.

- Ante todo, se debe cambiar la mentalidad para que se comparta la información, que se haga un régimen colaborativo. Quizá sea necesario un marco jurídico que lo efectivice.
- Se deben considerar las especificidades de los sectores.

Objetivo 2: "Impulsar el desarrollo de una industria del software seguro"

Acciones propuestas:

- Promover el cumplimiento de normativas y estándares verificables como los de OWASP.
- Implementar mecanismos para la evaluación y certificación de software seguro, incluyendo beneficios comerciales para quienes cumplan con estos criterios.
- Crear incentivos económicos, como subsidios y reducciones de impuestos, para promover el desarrollo y adquisición de software seguro.
- Establecer programas de formación y guías prácticas para desarrolladores y empresas sobre cómo implementar y mantener software seguro.
- Asegurar que las compras del Estado se realicen solo a proveedores que cumplan con los estándares de software seguro, incentivando al mercado a mejorar sus prácticas.
- Crear una agencia que supervise y eduque en temas de seguridad del software.
- Definir los criterios para identificar a un software seguro y establecer criterios de riesgos.
- Generar las capacidades para exigirlo. Generar incentivos, o crear una certificación de software seguro. Proveer los recursos para que las empresas, pagando, se hagan de las herramientas que se necesitan.

Objetivo 3: "Posicionar la industria de ciberseguridad nacional"

Acciones propuestas:

- Apuntar al conocimiento especializado y garantizar que la investigación acompañe. No sólo se trata de promover la investigación (aunque la ANII debería tener proyectos que promuevan la investigación en ciberseguridad), también hay que evaluar cómo se está investigando.
- Hacer un relevamiento de qué hay en la región y qué hace falta para buscar complementariedad. Estudiar los servicios que existen en el sector privado, para buscar nichos vacíos.
- Fortalecer el programa de becas existente para hacer cursos de posgrado en ciberseguridad.
- Crear un listado de empresas que cumplan los requisitos o estándares mínimos, que vaya más allá del carrito de compras del Estado.

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

Acciones propuestas:

- Desarrollar programas que ofrezcan a las pymes acceso a servicios de ciberseguridad a través de proveedores calificados. Establecer planes de incentivo, entrenamiento y guías específicas para pymes en ciberseguridad. Implementar campañas de concientización y capacitación sobre ciberseguridad para pymes. Ofrecer cursos prácticos sobre temas específicos como respaldos de datos y seguridad en redes sociales.
- Categorizar las pymes según el riesgo y el impacto de un ciberataque para priorizar las medidas de seguridad.
- Fomentar la implementación de buenas prácticas de ciberseguridad en sectores críticos y en la cadena de suministro.
- Se mencionó que las MiPymes tienen poco presupuesto y en general quieren contratar un servicio. Lo que habría que buscar en estas líneas de acción es desarrollar un servicio de asesoramiento para complementar. Por ejemplo, se podría desarrollar un servicio en el que las MiPymes pagan una suma módica por mes y reciben herramientas, computadoras, servicios de autentificación, etc. También se pueden ofrecer consultorías para obtener madurez. Podría ser Antel con un programa para pymes, u ofrecer computadores como CEIBAL.

Objetivo 5: "Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital"

Acciones propuestas:

- Regular el uso de sellos de competencia en firmas electrónicas avanzadas para garantizar la autenticidad y competencia de los firmantes.
- Asegurar que las firmas electrónicas avanzadas sean ampliamente aceptadas y reconocidas legalmente. Simplificar los mecanismos.
- Exigir el cumplimiento de la normativa existente que permite el uso de firmas electrónicas en documentos legales.
- Implementar mecanismos de fiscalización para asegurar que las firmas electrónicas sean utilizadas y aceptadas correctamente en todas las instancias legales y comerciales.

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

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

Respecto a la priorización: Se recalcó la necesidad de empezar por la formación y capacitación para enfrentar el problema de la falta de recursos humanos y de profesionales técnicos capacitados.

Se manifestó que, como no se puede atacar todo al mismo tiempo, se debería empezar identificando a los sectores prioritarios para priorizar los esfuerzos. También se subrayó la importancia de seguir generando estas instancias que faciliten los intercambios.

Se recalcó que para lograr los objetivos se necesitan recursos, y que hay que establecer responsabilidades claras. También es muy importante pensar en cómo incentivar la industria nacional de ciberseguridad.

Se debe establecer un plan de acción claro y ejecutable.

Las personas participantes de la mesa enumeraron a los distintos actores vinculados según cada objetivo.

Objetivo 1: “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”

Además del sector público y del privado, se resaltó que se requiere una figura coordinadora y se destacó que los reguladores son jugadores importantes. Para generar este tipo de reglamentación hay que meter a los reguladores de cada uno de los sectores (Banco Central, URSEA, JUNASA, así como prestadores de salud, etc.)

Objetivo 2: “Impulsar el desarrollo de una industria del software seguro”

Además del sector público, del sector privado y de la academia, se hace hincapié en las entidades que deben estar involucradas de Presidencia: ARCE (Agencia Reguladora de Compras Estatales), AGESIC, OPP (Oficina de Planeamiento y Presupuesto de la República). También se debe involucrar a las comunidades en ciberseguridad como OWASP (“Open Worldwide Application Security Project”), y a referentes como CUTI (Cámara Uruguaya de Tecnologías de la Información).

Objetivo 3: “Posicionar la industria de ciberseguridad nacional”

Además del sector público y del privado, se subrayó la necesidad de que la ANII brinde apoyo, y de que la academia para que no se trate de formación sólo a nivel de posgrado.

También deben estar involucradas las comunidades internacionales.

Objetivo 4: “Mejorar la ciberseguridad de las MiPymes”

Coo actores, se mencionó al Ministerio de Trabajo, al Ministerio de Educación, al Ministerio de Industría, Energía y Minería, a Datacenter, a ANDE (Agencia Nacional de Desarrollo), ANTEL, y a gremiales de pymes.

En todos los objetivos se destacó la importancia de que AGESIC cumpla un rol vital de coordinación y que prevea herramientas y asistencia.

Anexo

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

- Subgrupo 1
- Subgrupo 2
- Subgrupo 3
- Subgrupo 4

Subgrupo 1

- Moderadora: Natalia Salazar, Agesic.
- Relatora: Olivia Domínguez, ICD.
- Participaron 12 (doce) 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

Las Partes A y B se desarrollaron en conjunto. En general los participantes estuvieron de acuerdo con los objetivos planteados, pero agregaron ciertas consideraciones respecto a las líneas de acción:

DGI (Institución pública) - Carlos Vidal

Elogió la iniciativa, pero resaltó que la estrategia requiere fondos, lo cual no es mencionado en ninguna parte del documento. Es complicado poner en balance la seguridad o la seguridad de datos, el almacenamiento o equipo de seguridad, y en el documento el punto más débil es que no se habla.

Subraya que se debe tramar conciencia, trabajar mucho en los usuarios finales que son el punto más débil, y después trabajar en la infraestructura.

Plantea que mucho de lo que se incorpora en la estrategia corresponde a un gasto y no a una inversión (hablando de ejecución presupuestal) y eso podría jugar en contra.

BCU (Institución pública) - María Isabel Maroñas

Comenta que el tema de la financiación ha sido un denominador común en todas las mesas. Otro tema reiterado ha sido la necesidad de coordinación y de darle una forma concreta a esa coordinación entre esfuerzos en distintos sectores (público, privado, academia). Menciona que se consideró desagregar la cooperación en distintas capas (estratégica, operativa). Además, como se ha repetido a lo largo de las jornadas, piensa que el pilar de cultura fue transversal y debe atravesar a todos los demás. Hay que trabajar en eso, poner el foco en distintos públicos, sensibilizar a toda la población, así como a los decisores que no necesariamente están capacitados. Si no se logra llegar a ellos, no habrá recursos. Enfatiza que si bien la capacitación de los usuarios es importante, los incidentes muchas veces tienen como protagonistas centrales a personas que son de ciberseguridad (cisadmin). Por lo tanto, hay que trabajar en la capacitación de gente que está directamente vinculada en la protección de la información y en la ciberseguridad.

ASSE (Institución pública) - Gerardo Otero

Coincide con que la iniciativa de llevar adelante una estrategia como esta es muy importante, y destaca que es muy importante que sea tangible para los decisores. Sostiene que el punto difícil es el tema del usuario final, que es una vulnerabilidad y no es realista pensar que se podrá llegar a todos los sectores y a todas las personas. Por lo tanto, se deben poner barreras y tomar medidas para que los usuarios finales representen un riesgo contenido.

ASSE (Institución pública) - Adriana Peluffo

Toma el ejemplo de Europa, donde se multa a las empresas privadas cuando no tienen los análisis correspondientes necesarios a la hora de poner un software en funcionamiento. Ya existe una ley aprobada, por lo que si las empresas no cumplen con los requisitos de análisis de riesgo y de impacto, el gobierno debería multarlas y las multas recaudadas deberían ser invertidas en ciberseguridad.

Además, sostiene que el gobierno debe hablar con las gerencias para darle importancia a la ciberseguridad, ya que es un área que no puede estar sin recursos humanos y económicos.

Respecto a la educación, afirma que deberían existir carreras en ciberseguridad para reforzar las capacidades. Mientras que en otros países como Argentina hay licenciaturas en ciberseguridad, en Uruguay no existen. También se podría dar oportunidades de pasantías en organismos a los estudiantes, ya que pueden representar un recurso.

QoxIT (Sector privado) - Pablo Alzuri

Manifiesta que es pesimista respecto al objetivo de ciberseguridad como gestión. Duda de si es factible, si hay incentivo real. Sostiene que ante todo, se debe educar a la ciudadanía para que exija la ciberseguridad. Ya existe una ley, lo que demuestra que esto no alcanza en términos de exigencia. El punto más importante es concientizar: no solo enseñarles a las personas a no caer en phishing, sino concientizarlas de que los datos les pertenecen, no son de las empresas, y éstas tienen el deber de cuidarlos. Eso es lo que debe exigir la población. Hoy en día, nadie se cambia de sociedad porque no le cuidan los datos, y por esa razón no hay financiamiento.

Es importante, en este sentido, que haya capacitación docente: educar a los educadores es vital para lograr que la ciudadanía exija. No se va a lograr este cambio a través de sanciones. Si en Europa la multa funciona, señala que es porque hay un nivel de conciencia mayor.

CGN (Institución pública) - Guillermo Freire

Concuerda con que el tema de los recursos es importancias. Es imposible exigir que las pequeñas empresas implementen. En lugar de multar, se debería fomentar, dar beneficios para motivar a las empresas pequeñas a tener cumplimiento.

A nivel de la legislación también es complicado, ya que se desconoce, y más en las pequeñas empresas. Incluso en los organismos públicos que tienen abogados se desconoce la legislación en la materia. Por lo tanto se debería simplificar la legislación, divulgarla de otra manera, y fomentar la creación de guías que faciliten su entendimiento y adherencia.

También subraya que el tema de riesgos es uno de los pilares, pero no se sabe gestionar los riesgos a pesar de que AGESIC definió una metodología basada en la NIST. Sin embargo, sostiene que no termina de bajarse a tierra y no es fácil de aplicar.

Además, cuando se habla de ciberseguridad se le asigna responsabilidad a las personas técnicas, y el resto de las personas del organismo se lavan las manos. Hay que concientizar de que todos tienen cierto rol que cumplir en la protección de la información y deben asumirlo.

Se deben simplificar los mecanismos y procedimientos: por ejemplo, hoy hay tantos sistemas de autentificación de usuario y cambio de clave que termina siendo contraproducente.

ASSE (Institución pública) - Stella Rossi

Recuerda que las leyes existen: con la promulgación de la Ley 18.331, Uruguay fue pionero. Desde el punto de vista legal, el tema está afianzado. Respecto a la facilitación de la comprensión legal no pasa por la creación de manuelas ni por facilitar el lenguaje, sino que debe haber un comité interdisciplinario. No alcanza con que el técnico aplique un manual, sino que el abogado debe estar a su lado.

Por otro lado, señala que AGESIC no es una reguladora independiente como debería ser, sino que a diferencia de los órganos que aplican sanciones en Europa, depende del Poder Ejecutivo. En Europa las empresas invierten porque es más cara la multa que puede aplicar la agencia. En Uruguay, por lo contrario, se cae en la inoperancia porque no hay poder coercitivo.

Estima que los técnicos deben saber transmitir, y no esperar que el usuario final entienda los aspectos técnicos y específicos de la ciberseguridad.

ANII (Institución pública) - Fabio Bonanno

Reitera la importancia de los fondos y del desarrollo de la educación formal como la informal. Subraya la necesidad de incentivar: la seguridad tiene que ser un todo y hay muchas empresas que no tienen las capacidades necesarias. Por lo tanto, el Estado tiene que fomentar herramientas de apoyo, sobre todo para las pymes.

Datasec (Sector privado) - Carlos Serra.

Concuerda con que el tema de recursos es esencial y agrega que esto es una consecuencia, no una causa. Considera que la Estrategia debería obligar, tener sanciones, porque de lo contrario no va a avanzar. Sostiene que el concepto de ciberseguridad es relativamente nuevo, y hay que gestionar un cambio. El problema es, ante todo, cultural.

En el sector público, aún falta. Por ejemplo, a veces ocurren incidentes y no tienen consecuencias. Según la propuesta, AGESIC va a auditar y tener función de percibimiento. Si esto toma estado público es distinto. Se debe empezar por la conciencia de la consecuencia de que los datos sean filtrados, y generar preocupación por la responsabilidad de los datos, que tienen un valor como otras cosas.

La segunda línea de defensa es jerarquizar al CISO, lo que existe a nivel financiero. Podría crearse, a estos efectos, una superintendencia. Si se jerarquizan los roles y hay consecuencias deberían aparecer recursos.

Señala que actualmente, en muchos organismos se encuentran agujeros pero éstos quedan en un informe y no tienen consecuencia. Al año siguiente se hacen las mismas observaciones. Hay que definir motores.

Respecto al sector privado, no hay poder coercitivo. Señala que un 14% de las empresas privadas no tiene antivirus. Propone exigir certificaciones a las empresas en los pliegos de compras para armar una cadena de cumplimiento.

El problema, sostiene, no se arregla solamente mediante la capacitación (si bien también es necesaria). Faltan los incentivos, sean positivos o negativos.

CGN (Institución pública) - Guillermo Freire

Concuerda con la importancia de los recursos, y añade que hay heterogeneidad en todo el ecosistema. Recalca que se deben definir los métodos para compartir y comunicar información. Comenta que desde la CGN se hicieron varios esfuerzos con

AGESIC para cooperar e intercambiar información de ciberseguridad con organismos públicos antes de que AGESIC se centralizara. Subraya las dificultades asociadas a este tipo de esfuerzos: hay disparidad en los organismos públicos. Desde el punto de vista técnico, hay mucho por trabajar. Hay que darles la misma cantidad de recursos a todos para equiparar, desde un lugar central. La construcción de un ecosistema no será posible, subraya, sin recursos económicos y humanos.

IM (Institución pública) - Luis Garcimartín

Concuerda con que la normativa no tiene efecto sin penalización, y que las regulaciones son fundamentales. Piensa que podría implementarse una multa. Comenta que en la IM crearon un comité de seguridad, y regularmente se hace un informe que contiene los problemas grandes y es enviado a la dirección. Subraya que es fundamental porque es una forma de transferir el riesgo.

Manifiesta que también hay una falta grande de responsables de ciberseguridad, a nivel público y privado. Se suele mandar a las personas que trabajan en TI como responsables, pero no tienen tiempo para la ciberseguridad. Debería haber un referente contratado específicamente, que pase lista de lo que se debe hacer a las empresas que manejan datos de ciudadanos, y que por lo tanto tienen que protegerlos. Por ahí se les debería exigir que tengan un responsable de ciberseguridad.

BID (Institución pública) - Ariel Nowersztern

Ya que surgió muy destacadamente el tema de recursos, señala que AGESIC invierte hace años millones de dólares por año en tema de ciberseguridad, y está previsto que esto siga en los años que viene. Hay programas multianuales, hay recursos y muchos van al ecosistema: se estableció un laboratorio, se otorgaron becas, se creó un marco de ciberseguridad para que las empresas y las instituciones lo utilicen, se generó un currículo de ciberseguridad para entrenar profesionales.

Plantea un interrogante: ¿si una empresa del sector privado no quiere ciberseguridad, hasta dónde interviene el gobierno? El Estado puede proporcionar información y conocimiento, facilitar la disponibilidad de profesionales y de proveedores de ciberseguridad, tener un estándar accesible y herramientas de autoevaluación, pero si la empresa no es crítica y su falla causa más daño a ella misma, no hay necesidad de imponer regulaciones.

Subraya que se está invirtiendo en ecosistema pero hay que hacerlo de manera específica, con un plan, mostrando los beneficios. La ENC es esencial para generar una hoja de ruta y una base para priorizar las inversiones. El tema es más cómo utilizar y cómo asignar los recursos existentes.

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

Los objetivos fueron generalmente validados.

Se señaló que lo más importante es que la seguridad sea una responsabilidad proactiva a nivel estratégico, que abarque todo.

También se recomendó definir qué es el ecosistema que pretendemos atender. Se sugirió que se trataba de los profesionales – las personas, los equipos – dedicados a la ciberseguridad. Se enfatizó la visión de que Uruguay cuente con un ecosistema vibrante, al frente del conocimiento, que atienda las necesidades del país. Los objetivos serían mantener o impulsar elementos del ecosistema para lograr esa visión. Actualmente faltan profesionales de ciberseguridad: hay que tener líneas de trabajo para generar más profesionales. También se debe fortalecer la interconectividad en el ecosistema, tanto mediante canales formales como mediante “hubs de conocimiento” más informales. Un ecosistema fuerte es un elemento clave para que el país logre altas capacidades en ciberseguridad. Es una de las patas de la mesa y hay que incluirlo.

Además, se planteó que en el objetivo “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”, el fortalecimiento contemplado no debe ser solamente técnico: los equipos en las empresas públicas también deben ser fortalecidos en el sentido que su opinión debe contar en la toma de decisiones de la empresa.

Se planteó que la segunda línea de acción de este objetivo, “Generar y establecer una serie de ejercicios anuales específicos para los equipos,” es demasiado específica. Efectivamente se deben generar mecanismos para revalidad y certificar, pero eso ya es bajar un escalón. Hay que poner plazos realistas, medidas realistas y no perder de vista que hay un cambio cultural de por medio que hay que lograr.

Se propuso agregar como objetivo la necesidad de identificar sectores especialmente sensibles para empezar (por ejemplo, la salud) y enmarcarlos dentro del pilar de ecosistema. Se debe establecer una distinción para aquellos sectores que distorsionan al país si caen. Estos sectores no necesariamente coinciden con las infraestructuras críticas (por ejemplo, pueden incluir a las pymes, que son vulnerables por la cantidad de personas que pueden verse afectadas).

Respecto al objetivo relativo a la firma e identificación digital, se afirmó que se debe seguir ampliando y se deben generar mecanismos de reconocimiento a nivel internacional. Es importante que sea reconocido en otros países para generar confianza.

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

A lo largo de la discusión se hizo hincapié en algunas cuestiones específicas.

Se hizo especial referencia al objetivo “Posicionar la industria de ciberseguridad nacional.” Respecto a su línea de acción i, “Incentivar la industria nacional de ciberseguridad”, se discutió cómo pedir niveles de seguridad, y se sostuvo que el esfuerzo también debe venir del lado de la empresa. Por lo tanto, es necesario incentivar no solamente al sector público, sino también al privado: se debe generar un esfuerzo de control para las empresas que brindan servicios. Se propuso crear un listado de empresas que cumplan los requisitos o estándares mínimos, que vaya más allá del carrito de compras del Estado.

Además, se señaló que hoy existen incentivos para las pymes, pero no hay incentivos específicamente para empresas de ciberseguridad. Se hizo una distinción entre las empresas de ciberseguridad y las empresas que tienen datos de los ciudadanos, y se debatió acerca de la necesidad de agregar un objetivo respecto a los mecanismos de reconocimiento.

Respecto a la segunda línea de acción, “Promover los mecanismos y ámbitos para la participación academia-público-privada”, se plantearon las dificultades asociadas a la ley de ciberdelito que se está por aprobar, que no contiene mecanismos de aceptación para las herramientas de hacking ético. Se expresó temor a que se frene la investigación y el desarrollo por temor a ser penalizado, y se pidió homologarlo y generar una salvaguarda para la seguridad ofensiva, asimilada al “porte de arma”.

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

Se manifestó que, como no se puede atacar todo al mismo tiempo, se debería empezar identificando a los sectores prioritarios para priorizar los esfuerzos. También se subrayó la importancia de seguir generando estas instancias que faciliten los intercambios.

Se recalcó que para lograr los objetivos se necesitan recursos, y que hay que establecer responsabilidades claras. También es muy importante pensar en cómo incentivar la industria nacional de ciberseguridad.

Se debe establecer un plan de acción claro y ejecutable.

Subgrupo 2

- Moderadora: Clara Michelini, Agesic.
- Relatora: Marcelo Castillo, ICD.
- Participaron 14 (catorce) personas de 12 (doce) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Las Partes A y B se desarrollaron en conjunto.

CERTuy (Institución pública) – Natalí Paggiola

Subraya que es importante incluir a la cultura como ecosistema con un enfoque en la ciudadanía. Entiende que debe haber una estructura organizativa. Observa en general información mezclada, por ejemplo, hay línea de acción de formación en ciberdelitos, en vez que esté en este pilar. Por ejemplo, hay una línea de acción de formación en ciberdelitos, en vez de que esté en este pilar. Debería haber un presupuesto adecuado para que la ENC sea duradera.

Galileo Latam (Sector privado) - Mauro Flores

Comenta que le cuesta ver en el documento la interacción en el ecosistema, no ve cómo cada uno de los pilares aportan para generar un círculo virtuoso. También sostiene que el componente técnico debería ser más alto: no tenemos profesionales técnicos con capacidades para el desarrollo de aplicaciones y para la validación de seguridades. Es algo que se tiene enfocar de manera importante.

Señala que a veces cuando se convoca a los políticos envían a los secretarios, lo que demuestra que no se tiene un interlocutor idóneo. De la misma forma que tienen asesores especializados en otros temas, deberían tenerlos en ciberseguridad.

BPS (Institución pública) - Álvaro Arias

Coincide con que se nota la falta de mano de obra de nivel técnico. Faltan buenos arquitectos de seguridad y faltan buenos gestores en ciberseguridad. Afirma que se debe apostar por ese lado. Respecto al pilar “Ecosistema y cultura”, está flaco el fomento de la cultura de los tomadores de decisión que son quienes aprueban los presupuestos.

Pero no se trata solo de presupuesto, sino también de visión estratégica. La ENC no debería depender de una mirada de corto plazo de un período de gobierno.

Ministerio del Interior (Institución pública) - Javier Jaureguiberry

Señala que hay una pata que falta que es la de “Gobernanza del Ecosistema y Marco jurídico”. Debería haber una estructura formal y organizada que lidere para que no sean acciones puntuales. Coincide con lo que se decía de impulsar los recursos humanos capacitados y tener una buena oferta educativa.

UTE (Institución pública) - Alejandro Álvarez

Duda de cómo serían los flujos de trabajo entre organismos. Comenta que ya hubo un intento de armar mesas de trabajo con otras empresas públicas y no se logró por cuestiones de confidencialidad. Manifiesta su acuerdo con la idea de concientización de las jerarquías en temas de ciberseguridad. El año pasado se planteó un SOC cooperativo, pero no terminó saliendo. No se tiene idea del impacto que pueden tener estos temas.

EY Uruguay (Sector privado) - José Luis Vera

Concuerda con que los temas mencionados son los más considerables. Su principal preocupación tiene que ver con la separación entre lo técnico y lo político. Se está planteando una estrategia a 6 años con objetivos y necesidad de monitoreo, pero hay muchos elementos que dependen del sistema político - y se viene un nuevo gobierno. Dentro de estos objetivos no se incluye un presupuesto como para medir el desempeño de las verticales. Es algo a incorporar de alguna forma.

URSEC (Institución pública) - Fernando Hernández

Responde que todo se dispara una vez que haya un marco normativo fuerte que refleje el ecosistema, una vez que todos los organismos sepan qué rol van a tener y qué papel van a jugar.

SECIU – UDELAR (Academia) - Javier Valena

Concuerda con que se requiere mayor interacción entre los distintos sectores del ecosistema, y con que es importante que se resalte lo presupuestal. Comenta que en el ámbito de la Universidad cuentan con la aprobación para formar un CSIRT académico, pero está demorando mucho por falta de recursos y falta de conciencia de las autoridades para que se pueda dar.

Agesic (Institución pública) - Maite Rodríguez

Manifiesta que de forma general está de acuerdo con los objetivos y los lineamientos planteados. Señala que hay objetivos en otros pilares que son transversales: gobernanza, normativa – tocan en todo y capaz que por eso no lo dice en este específico.

Indica que falta concientización de los cargos que toman las decisiones.

Agesic (Institución pública) - Mateo Cabrera

Está de acuerdo en líneas generales con los lineamientos de arriba, y con que la ENC debe ser una política de Estado y no de un gobierno u otro. Resalta la importancia de mejorar las compras y las licitaciones y trabajar con el sector privado para enfrentar el problema de raíz.

ANII (Institución pública) - Mauricio Rinaldi

Muestra su preocupación por los recursos humanos y la preparación, y sostiene que se debe tener claro el flujo entre los actores. Además, subraya que hay distintas organizaciones que tienen distintos grados de madurez en este tema, por lo que Agesic debería asistir a las menos maduras. ANII tendría que tener una estrategia institucional que apoye a estos aspectos y que no sea de un área específica de TI sino de la institución entera.

LIDECO (Sociedad civil) - Bernardo Quesada

Reafirma la importancia de formar grupos de trabajo. Comenta que Agesic había formado grupos con LIDECO que se cortaron por falta de recursos. Hay que retomarlo para compartir experiencias y conocimientos. Habría que organizar sensibilizaciones con los políticos, con los decisores: los que conocen de este tema deberían sensibilizar a quienes toman las decisiones.

Apoya lo que se dijo acerca de que las organizaciones tienen niveles diferenciales de aprendizaje, y Agesic debería apoyar a las rezagadas. Además, se debe sensibilizar al usuario final.

Galileo Latam (Sector privado) - Mauro Flores

Hay un tema importante que es de la percepción del riesgo: hoy en día los tomadores no tienen percepción del riesgo en estos temas y en base a eso no toman las decisiones que se deberían tomar. En la actualidad muchos de los procesos judiciales implican cuestiones tecnológicas, pero como país no tenemos las capacidades, por ejemplo, para hacer un análisis forense siguiendo reglamentaciones internacionales. Hay una falta de entendimiento.

Agesic (Institución pública) - Estefanía Almeyda

Agradece la iniciativa del documento. Le preocupa que la población y los estudiantes de la maestría que está haciendo no estén motivados por estudiar o meterse en temas de ciberseguridad. En el marco de la academia, señala que no tuvo ninguna materia, ni un taller sobre ciberseguridad, y por lo tanto no tuvo la oportunidad de acercarse al tema y darse cuenta de si le interesa o no. No hay materias en la currícula: cuando alguien se ve motivado a especializarse en el tema es a nivel de posgrado. Sostiene que desde Agesic se ofrecen capacitaciones, y que al menos la gente que está en la Administración Pública debe estar capacitada en Ciberseguridad.

Además, señala que siempre se cuestiona a los que toman decisiones, a la falta de presupuesto, y cree que lo que se puede hacer es proponer y mostrar los objetivos que se persiguen, para no quedarse sólo en la cultura de cuestionar. Sugiere proponer lo que se quiere hacer en materia de ciberseguridad y que los decisores gestionen el presupuesto.

EY Uruguay (Sector privado) - José Luis Vera

Sostiene que está faltando en la discusión la seguridad en la cadena de suministros. Comenta que en EY Uruguay trabajan en auditorías y a veces pasa que hay clientes que tienen contratados servicios de almacenamiento y se debe terminar auditando a los proveedores. Le parece que falta aplicar este aspecto en la estrategia y plasmar los requerimientos para asegurar la cadena de proveedores y que todos cumplan con determinados controles.

Galileo Latam (Sector privado) - Mauro Flores

Señala que el problema de las auditorías es que se focaliza mucho en los procesos, pero no en la eficiencia. Está de acuerdo con lo que se menciona de las auditorías, pero también hay que complementarlas con la medición de la eficiencia y la eficacia.

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

Durante la segunda ronda, los participantes discutieron acerca de los objetivos planteados en el pilar "Cultura y Ecosistema". Se sugirió crear un plan de acción general que unifique a todos los actores del ecosistema, así como un servicio de ciberinformación que registre los incidentes cibernéticos que ocurren en el país. También se mencionó la importancia de establecer redes colaborativas entre los SOC (Centros de Operaciones de Ciberseguridad) para compartir información y compartir indicadores de compromiso.

Se identificaron varios aspectos clave para abordar eficientemente los retos y desafíos en el ecosistema y la industria de la ciberseguridad. Algunos de los más resaltados se resumen a continuación.

Necesidad de un marco normativo fuerte y transparente

Se marcó la necesidad de que se fije un marco normativo fuerte y transparente que refleje el ecosistema en ciberseguridad y establezca responsabilidades claras para los diferentes actores públicos y privados.

Se propuso crear un reglamento que establezca responsabilidades claras para las empresas, organizaciones y particulares que manejan datos personales y confidenciales.

Se sugirió crear un sistema de sanciones efectivas para las empresas y organizaciones que incumplen las normas de ciberseguridad. A la vez, definir un proceso claro y transparente para reportar incidentes cibernéticos y compartir información sobre riesgos y vulnerabilidades.

Concientización, capacitación, formación y educación en ciberseguridad

Se remarcó la importancia de capacitar a los tomadores de decisiones y profesionales técnicos en ciberseguridad. Se sugirió crear programas de formación en ciberseguridad para los tomadores de decisiones y profesionales técnicos, especialmente en áreas como la gestión de riesgos, seguridad de la información y respaldo de datos.

Se dijo que hay que mejorar la conciencia y la formación en ciberseguridad entre los jóvenes y los estudiantes. Se mencionó la importancia de incluir educación en ciberseguridad en el currículum escolar, desde la educación primaria hasta la universidad. En ese sentido, se propuso crear materiales educativos y recursos para padres y educadores sobre cómo enseñar a los niños sobre ciberseguridad.

También se planteó crear un certificado o diploma en ciberseguridad que acredite la competencia y habilidades en este campo.

Se sugirió crear campañas publicitarias y educativas para concienciar a los ciudadanos sobre la importancia de la ciberseguridad y acerca de cómo protegerse contra ataques cibernéticos.

Desarrollo de un plan de acción unificado

Se remarcó la importancia de desarrollar un plan de acción que unifique a los diferentes actores del ecosistema y promueva la colaboración y el intercambio de información. En ese sentido, se sugirió crear un plan que incluya al gobierno, empresas, organizaciones civiles y academia.

Se propuso crear un comité interinstitucional que coordine esfuerzos y recursos para implementar el plan de acción.

Se mencionó la importancia de establecer indicadores clave de rendimiento para medir el progreso del plan de acción.

Redes colaborativas entre SOC

Se propuso crear un sistema de alerta temprana para detectar e informar incidentes cibernéticos importantes.

Se mencionó la importancia de establecer protocolos claros para compartir información confidencial entre los SOC (Centros de Operaciones de Ciberseguridad). Se sugirió crear una red colaborativa entre los SOC para compartir información e indicadores de compromiso.

Medición

Se espera que la propuesta de ENC contenga lineamientos y que los objetivos sean SMART para luego medirlos. Es difícil ver cómo se van a medir ciertas líneas de acción como las relativas a “incentivar”.

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

Durante la segunda parte de la segunda ronda, los y las participantes examinaron cada objetivo planteado en el pilar “Cultura y Ecosistema” y se discutieron actividades y acciones que deberían desarrollarse para llevarlos a cabo.

Objetivo 1: “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”

- Se hizo hincapié en la necesidad de unir los SOCs para que compartan información, sobre todo los indicadores de compromiso.
- Se propuso agregar una cuarta línea de acción que sea elaborar un plan de acción general que unifique a todos. Se destacó la necesidad de formar redes colaborativas para defenderse contra un mismo vector de ataque.

- También se sugirió agregar un servicio de Ciberinformación que registre los ciberincidentes que ocurren en el país.
- Esto comprende definir qué organismos deberían tener un SOC (se mencionó a UTE, ANCAP y OSE)
- Se resaltó que ante todo, se debe cambiar la mentalidad para que se comparta la información, que se haga un régimen colaborativo. Tiene que haber una normativa – capaz para que sea obligatorio es necesario un marco jurídico que lo efectivice. En la normativa tiene que decir que debe ser obligatorio compartir, se debe definir qué, cómo y quién tiene que compartir los datos en ciberseguridad -al menos entre SOCs.
- Sin embargo, también se deben considerar las especificidades de los sectores. Por ejemplo, no se puede violar el secreto bancario.
- Se sugirió que el intercambio podría incluir a otros países de la región.

Objetivo 2: "Impulsar el desarrollo de una industria del software seguro"

- Se destacó la necesidad de definir los criterios para identificar a un software seguro. Hay que definir precisamente qué tienen que cumplir las empresas para que tengan parámetros a los que ajustar sus acciones y comportamientos y cuando presenten sus softwares den cuenta de esos procesos seguros. También se deben establecer criterios de riesgos. No es necesario que todos los involucrados en los procesos sepan mucho de seguridad sino de cómo manejarse con los procedimientos fijados en base a criterios claros que hay que cumplir.
- Se discutió acerca de cómo generar las capacidades para exigirlo. Se sugirió generar incentivos, o crear una certificación de software seguro. También se habló de establecer una normativa que estipule un plazo de certificación de software seguro que luego impida, si no se cumple, presentarse a compras públicas o licitaciones. Agesic debería proveer los recursos para que las empresas, pagando, se hagan de las herramientas que se necesitan. Por la tienda virtual, los que estén habilitados como desarrolladores deberían tener softwares seguros.

Objetivo 3: "Posicionar la industria de ciberseguridad nacional"

- Hay que apuntar al conocimiento especializado y garantizar que la investigación acompañe. No sólo se trata de promover la investigación (aunque la ANII debería tener proyectos que promuevan la investigación en ciberseguridad), también hay que evaluar cómo se está investigando. Habría que generar un instituto en Ciberseguridad. Es importante generar las capacidades, motivar a la gente y ayudar a las empresas.
- En la línea de acción III ("promover la investigación y desarrollo en ciberseguridad"), se propuso reemplazar "promover" por "posicionar".
- Es necesario hacer un relevamiento de qué hay en la región y qué hace falta para buscar complementariedad. También habría que hacer un estudio de los servicios que existen en el sector privado, para buscar nichos vacíos. Hay que hacer un relevamiento que haga sentido según las necesidades y capacidades nacionales.
- Capaz se podría fortalecer el programa de becas existente para hacer cursos de posgrado en ciberseguridad.

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

- Se mencionó que las MiPymes tienen poco presupuesto y en general quieren contratar un servicio. Lo que habría que buscar en estas líneas de acción es desarrollar un servicio de asesoramiento para complementar. Por ejemplo, se podría desarrollar un servicio en el que las MiPymes pagan una suma módica por mes y reciben herramientas, computadoras, servicios de autentificación, etc. También se pueden ofrecer consultorías para obtener madurez. Podría ser Antel con un programa para pymes, u ofrecer computadores como CEIBAL. Sin embargo, se señaló que la falta de capacidades y de especialistas en ciberseguridad podría ser un problema.
- Existen caminos (por ejemplo, por el Ministerio de Industria, Energía y Minería a través de la Dirección de MyPymes), pero hay que ver qué normativa establece responsabilidades.

Objetivo 5: "Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital"

- Se discutió acerca de si este objetivo debería entrar en la estrategia de ciberseguridad, y si debería constituir un objetivo. También se cuestionó su inclusión en el pilar "Ecosistema y cultura".
- Se agregó que se debería marcar la necesidad de mejorar la identificación. Se propuso delegar todo en Agesic y que sea obligatorio en los trámites.
- Se subrayó que hay que impulsar la firma digital y electrónica, y debe ser aceptada por todas las oficinas del Estado.

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

Las personas participantes de la mesa enumeraron a los distintos actores vinculados según cada objetivo.

Objetivo 1: "Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta"

Además del sector público y del privado, se resaltó que se requiere una figura coordinadora y se destacó que los reguladores son jugadores importantes. Para generar este tipo de reglamentación hay que meter a los reguladores de cada uno de los sectores (Banco Central, URSEA, JUNASA, así como prestadores de salud, etc.)

Objetivo 2: "Impulsar el desarrollo de una industria del software seguro"

Además del sector público, del sector privado y de la academia, se hace hincapié en las entidades que deben estar involucradas de Presidencia: ARCE (Agencia Reguladora de Compras Estatales), AGESIC, OPP (Oficina de Planeamiento y Presupuesto de la República). También se debe involucrar a las comunidades en ciberseguridad como OWASP ("Open Worldwide Application Security Project"), y a referentes como CUTI (Cámara Uruguaya de Tecnologías de la Información).

Objetivo 3: "Posicionar la industria de ciberseguridad nacional"

Además del sector público y del privado, se subrayó la necesidad de que la ANII brinde apoyo, y de que la academia para que no se trate de formación sólo a nivel de posgrado.

También deben estar involucradas las comunidades internacionales.

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

Como actores, se mencionó al Ministerio de Trabajo, al Ministerio de Educación, al Ministerio de Industría, Energía y Minería, a Datacenter, a ANDE (Agencia Nacional de Desarrollo), ANTEL, y a gremiales de pymes.

En todos los objetivos se destacó la importancia de que Agesic cumpla un rol vital de coordinación y que prevea herramientas y asistencia.

Se destacó que faltan muchas habilidades blandas. No se puede abarcar todo al mismo tiempo, por lo que es necesario empezar definiendo prioridades.

Subgrupo 3

- Moderadora: María Noel Hernandez, Agesic.
- Relatora: Daniel Miranda, ICD.
- Participaron 14 (catorce) personas de 13 (trece) 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

En esta primera parte, los y las participantes aportaron tanto sobre aspectos generales del borrador como sobre aspectos específicos del pilar “Ecosistema y cultura”.

SECIU - UDELAR (Academia) - Sergio Ramírez

Resaltó dos aspectos: primero, el tema de la formación en ciberseguridad le parece esencial debido a la alta escasez de personal en esa área. Habría que buscar una línea de acción que sea efectiva y rápida en el tema de educación. El segundo aspecto es el de la cooperación, colaboración y coordinación entre todos los actores en el país: habría que formalizar esa cooperación para que sea más efectiva.

Tilsor (Sector privado) - Rodrigo Martínez

Concuerda con que la falta de capacidades es lo que más duele en el área de ciberseguridad. De los cinco objetivos, el tema de la inclusión de la industria de la ciberseguridad en las estrategias lo considera muy importante. En relación al fortalecimiento de equipos de monitoreo y respuestas en las cibergestiones, es importante incluir a las personas, pero también a la MiPymes. Se debe conformar un espacio para ayudarlas y compartir buenas prácticas en materia de ciberseguridad. Otro tema es el fortalecimiento y creación del sector público: hay que fortalecerlo y darle más gobernanzas, más acceso, con un rol más de coordinación general, donde haya alguien que lidere.

Agesic (Institución pública) - Claudio Martínez

Coincide con la importancia de la educación para incentivar la industria nacional: sostiene que falta gente formada y es captada por el mercado extranjero. Es necesario que el incentivo esté enfocado en retener a los especialistas en ciberseguridad, en cómo hacer para lograr una buena remuneración en el sector público y crear doctorados o posgrados en el país.

Atos Uruguay (Sector privado) - Joaquín Pérez

Coincide con el tema de educación, y pone énfasis en el tema de los posgrados. También es necesario mejorar los centros de respuestas; Agesic no tiene capacidad para atender todo lo que abarca. Sería necesario crear más centros de respuestas, porque entiende que se está llegando a su capacidad máxima. Se une a la necesidad de atender personas, porque un ciudadano no tiene donde atenderse frente a un ataque o incidente.

CUTI (Sector privado) - Ana Lucero

Está de acuerdo con los objetivos planteados en el documento, y subraya que es necesario impulsar el desarrollo de software seguro, donde se debe seguir desarrollando el rol de CUTI. En relación con el tema de compra de equipamiento seguro, está de acuerdo con implementarlo para todos los sectores.

Respecto al segundo objetivo (“Impulsar el desarrollo de una industria de software seguro”), comenta que en la CUTI, el 80% son MiPymes. Entiende que si bien este punto está enfocado a un desarrollo seguro, hay que tener en cuenta cómo es el ecosistema.

Respecto al tema de la firma digital, está de acuerdo con mejorar el desarrollo digital, y resalta que el Estado debe sumar varias políticas para que se pueda llevar a todo el entorno.

Dinatel (Institución pública) - Virginia Alonso

Afirma que habría que incorporar la cooperación internacional y estar atentos al panorama tecnológico para ver cuáles son los nuevos desafíos. Si bien en este momento de la ciberseguridad se está elaborando una estrategia a nivel general, considera que debería haber políticas sectoriales.

Agesic (Institución pública) - Claudio Martínez

Es necesario cambiar la currícula de formación desde la educación media en adelante, ya que falta mucho en ese nivel y es muy grave: hay generaciones que no tienen las herramientas para involucrarse en el mercado laboral. La seguridad es un conjunto, y la seguridad de la información es un problema.

Con relación a la coordinación de los actores en el ecosistema uruguayo, es necesario que existan reguladores del mismo.

En cuanto a la información, hay observatorios de tecnologías por todos lados, pero falta compartir la información. Es muy difícil lograr que el sector privado comparta información, pero en materia de ciberseguridad debería ser común. Se deben auditar las infraestructuras críticas, y se debe encontrar maneras de manejarlo con las empresas privadas.

La academia no incorpora iniciativas porque faltan profesionales. Otro de los problemas que tenemos es la legislación en Uruguay, ya que demoran mucho en desarrollarse leyes.

URSEC (Institución pública) - Nelson Rodríguez

Piensa que no habrá un verdadero impulso hasta que no suceda un ataque grande, lo que podría ser muy grave para la ciberseguridad debido al tamaño del país. Sin embargo, valora mucho esta instancia y sostiene que la estrategia debería ser una política de Estado.

Respecto al tema de comparto de información, es complejo porque el sector privado va a otra velocidad y las políticas de Estado muchas veces van en otra dirección.

En cuanto al tema de la educación, debería ser transversal.

Teledata (Sector privado) - Alejandro Pereyra

Con relación a los objetivos, le parece que el que es relativo a las MiPymes (“Mejorar la ciberseguridad de las MiPymes”) debería estar como línea de acción en vez de como objetivo general.

También le parece que en lugar de ecosistema nacional, se debería hablar de ecosistema internacional, ya que las empresas venden a nivel internacional. Sostiene que sería bueno pensar fuera de la caja. Trabajar en las fortalezas nacionales y pedir apoyo en lo internacional trayendo gente que nos apoye en el sistema del monitoreo es parte de esa colaboración internacional.

Además, subraya que en el marco del ecosistema se debe aprovechar mucho al privado: eso debería ser el objetivo estratégico.

Finalmente, subraya que se necesitan recursos financieros. Sin presupuesto no va a funcionar: debería figurar en el documento.

Fortinet (Sector privado) - Gastón Sancassano

Coincide con la necesidad de capacitación y estudio y considera que hay que trabajar mucho en el tema de monitoreo y respuesta. Agregaría que se deben impulsar equipos de monitoreo y respuestas tanto a nivel público como privado. Respecto al tema de educación, señala la dificultad de llegar a los sectores de mayor edad.

Patria Investments (Sector privado) - Leonardo Martins

Menciona que en Santander armaron una red de colaboración para coordinar sobre lo sucedido y las acciones a llevar a cabo cuando tenían un incidente. La colaboración es clave. Resalta que “el lema en ciberseguridad debe ser que no competimos, sino que colaboramos”. Además destaca que Santander tiene la obligación de reportar las incidencias al BCU.

En cuanto a la formación de profesionales, es clave y es urgente la formación en las escuelas.

En cuanto a las pymes, menciona que en Santander se generó un servicio para las pymes en cinco pilares, y sostiene que sería bueno implementar un servicio parecido a nivel nacional para hacer la formación y el acompañamiento a la pymes.

ANCAP (Institución pública) - Andrea Parada

En el documento se diferencia claramente entre cultura y capacidad. Sin embargo, sería importante continuar trabajando en el tema competencias. La ciberseguridad es transversal a toda la tecnología, por lo tanto debería ser transversal a todas las carreras, para que se tome como algo natural. Se requiere que los docentes den esos conocimientos desde el principio. Es necesario trabajar desde las escuelas sobre la percepción del riesgo. Los padres dan tecnología a sus hijos, sin tener en cuenta el riesgo para minimizarlo y sin difundir los peligros asociados.

En cuanto al ecosistema y la colaboración, es esencial trabajar en colaboración en todos los ámbitos, en base a que todos tenemos un enemigo común, por eso debemos fortalecer nuestra capacidad.

MRREE (Institución pública) - Daniel Pesce

Comparte lo que se ha dicho de falta de capacitación. Es importante la capacitación en las primeras líneas de la educación, donde es fundamental. Sin embargo, subraya que la masa de población que está en el medio, que queda sin ser absorbida por los centros educativos, también es un problema importante. Es necesario por lo tanto llegar desde otro lado y generar una capacitación a nivel general como lo están haciendo los bancos en avisar por ejemplo sobre los fraudes cibernéticos.

Comparte lo que se ha venido mencionando: es necesario dividir el tema en temáticas verticales, ya que ayudaría en los niveles de intervención.

También concuerda con que respecto al tema de la globalización, se debe contar con una mirada como Estado. Por ejemplo, ahora nuestros activos están en la nube. En Europa hicieron su propia nube. Tal vez sería bueno aprender de eso y analizar su viabilidad. Debemos tener mucho cuidado en concientizar a los desarrolladores, pero también tenemos que pensar en la cadena de suministros para que lo que nos entregan esté evaluado en ciberseguridad.

Más generalmente, se plantearon algunas observaciones respecto a los objetivos establecidos en la propuesta borrador.

Los y las participantes consideraron que sería importante agregar en los objetivos un enfoque internacional para pensar un ecosistema internacional en vez de solo nacional.

También se hizo hincapié en que falta en todo el documento una línea de acción previa que es conseguir financiamiento y recursos humanos. Es fundamental para pensar proyectos que sean efectivamente realizables.

Además, en el documento las líneas de acción están desarrolladas de forma muy genéricas y a veces no quedan claros los alcances, el impacto y los involucrados.

Respecto a las infraestructuras críticas, se considera que tal vez en lugar de hablar de infraestructura crítica sea mejor hablar de servicios críticos. En cuanto a su definición, se considera que será política porque son los tomadores de decisión que deciden el riesgo que quieren asumir. Además, se destaca que las infraestructuras críticas son dinámicas e irán variando rápidamente con el correr de los años. Se debe ir evaluando y ajustándola.

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

- Se definió el tema de formación como prioritario para abordar la ciberseguridad en todos los niveles, y para ir formando esa fuerza laboral que se necesita.
- Se considera importante abordar con la formación todas las franjas etarias, pero en particular la franja del medio de la población a la que no se puede llegar por los sistemas educativos.
- Otro aspecto a potenciar es la coordinación entre todos los actores públicos, privados, academia, organizaciones sociales, etc.
- Es importante definir cuál es el sector crítico para tenerlo bien identificado.
- Es necesario contar con una visión de seguridad de la información en forma integral para las industrias y las empresas.
- Es necesario, importante y urgente la designación de presupuestos y recursos que no es menor.

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

Los objetivos fueron en gran medida validados. A continuación se detallan los comentarios, aportes y propuestas hechos sobre cada uno de ellos.

Objetivo 1: "Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta"

El objetivo se da como validado, con los siguientes aportes:

- Se considera importante incluir a sociedad civil que no aparece en la descripción del objetivo: se habla del ámbito público, privado, la academia, pero no de sociedad civil.
- Se plantea que es necesario darle una figura jurídica al tema de la ciberseguridad, a través de la creación de una agencia nacional de ciberseguridad. En ese sentido hay que ver la institucionalidad que se le quiere dar, que le permita tener presupuesto y que se le otorgue poder entre otras cosas para hacer la vigilancia y control de los organismos. Se plantea que el rol de Agesic podría ser más de regulador, de órgano rector. Se resalta que se debe definir más claramente el rol de Agesic.
- Se proponer hacer tres niveles de capacitación: un nivel para la población que aún está en el sistema educativo, otro para la gente que ya ha pasado por el sistema educativo o que está fuera de la educación, y el tercero para los tomadores de decisiones. Hay una escuela de gobierno, pero no se da un curso de ciberseguridad. Sería importante que haya un bloque de ciberseguridad en las carreras de relaciones internacionales.

Objetivo 2: "Impulsar el desarrollo de una industria del software seguro"

El objetivo se da como validado, con los siguientes aportes:

- Hay una dualidad en lo planteado en el título del objetivo, donde se impulsa solamente el desarrollo. Sería bueno que se considere que también somos consumidores de software. Se propone titular al objetivo “Impulsar el desarrollo, la adquisición y el uso del desarrollo de software seguro.”
- En relación con el software seguro, se plantean dudas sobre el concepto. Es difícil determinar si un software es seguro. Además surge la pregunta sobre lo que significa garantizar compras seguras del Estado.
- Se considera importante no solo enfocarse en formación, sino también en analizar cómo la empresa está asegurada frente a un ataque. Eso requeriría un monitoreo.

Objetivo 3: “Posicionar la industria de ciberseguridad nacional”

El objetivo se da como validado, con los siguientes aportes:

- La primera línea de acción (“Incentivar la industria nacional de ciberseguridad”) es demasiada abstracta. Sería necesario ampliarla y concretizarla un poco más.

Objetivo 4: “Mejorar la ciberseguridad de las MiPymes”

- Se plantean dudas acerca de la necesidad de posicionar a las pymes como uno de los objetivos, cuando hay otra cantidad de cosas también importantes que deberían ser incluidas.

Objetivo 5: “Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital”

- Se plantean dudas acerca de lo que significa la identificación digital.

Subgrupo 4

- Moderadora: Noelia Rodríguez, Agesic.
- Relatora: Marta Manent, Mauro Parada, ICD.
- Participaron 10 (diez) personas de 7 (siete) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Se salteó la parte A de la primera ronda para comentar los objetivos específicos del pilar “Ecosistema y Cultura”. Los aportes se encuentran organizados según cada objetivo.

Objetivo 1: “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”

Grant Thornton (Sector privado) - Ignacio Lagomarsino

Comparte su preocupación sobre la falta de medidas específicas y señala que Uruguay ya tiene organismos nacionales similares a los propuestos. Considera innecesario gastar en nuevas herramientas cuando ya existen, y sugiere que el Estado debe asignar recursos humanos para utilizarlas. Destaca la necesidad de que las pymes tengan acceso a servicios de ciberseguridad de calidad. Elogia al Banco Central por sus regulaciones y resalta la importancia de la educación en la estrategia de ciberseguridad. Subraya que la estrategia nacional debe establecer objetivos específicos para todas las organizaciones del Estado, en lugar de simplemente imponer la creación de un SOC, que puede ser costoso para muchas empresas.

IM (Institución pública) - Fernando Rodríguez

Apoya la creación de la red pero enfatiza que no debe hacerse solo por el hecho de crearla. Destaca la importancia de la coordinación y la comunicación efectiva, enfatizando que el contenido y propósito deben estar claramente definidos y bien integrados. Cuestiona la necesidad de que cada sector tenga su propio CSIRT y sugiere la posibilidad de tener una estructura general con coordinación centralizada.

URUDATA (Sector privado) - José Callero

Critica que la descripción de objetivos es genérica y no indica claramente el propósito final, haciendo que las líneas de acción parezcan aplicables a cualquier país. Valora la especificidad de la línea sobre la creación de un CSIRT ciudadano. Señala la necesidad de incluir una línea de acción sobre la sostenibilidad de las iniciativas para asegurar su continuidad a lo largo del tiempo. Sugiere que, dado que ya existen CSIRTs, el plan debe considerar lo que ya está en marcha. Plantea que el rol de los CSIRTs debe ser la coordinación entre todos, y cuestiona la inclusión de aspectos normativos como líneas de acción, considerándolos más como herramientas para alcanzar objetivos.

MIEM (Institución pública) - María José Franco

Expresa dudas sobre cómo funcionarán los CSIRTs en distintos sectores, considerando que algunos tendrán más riesgo que otros. Se cuestiona la comunicación entre los CSIRTs y la población general, y si habrá espacios para canalizar denuncias. Además de los recursos humanos y materiales, le preocupa la disponibilidad de recursos para las diferentes verticales. Visualizar la implementación de estas estructuras en otros sectores le parece complicado. Propone la idea de un CSIRT ciudadano para fomentar capacidades en cultura y perfil técnico.

URSEC (Institución pública) - Agustín Hill

Busca comprender la finalidad de los ejercicios planteados en la línea 2, cuáles serían, y bajo qué línea estratégica.

OWASP (Sociedad civil) - Gerardo Canedo

Enfatiza que es fundamental establecer una obligación legal o un sistema de beneficios y castigos para asegurar el cumplimiento del monitoreo de seguridad, ya que las personas tienden a no verlo necesario hasta que enfrentan problemas. Además, resalta la falta de claridad sobre quién aplicará estas normas y el nivel punitivo correspondiente, subrayando que cumplir debe ser más económico que incumplir. Expresa preocupación por la disponibilidad de personal para los cuatro CSIRTs planificados y sugiere que, en lugar de centrarse en la implementación específica de estos, es más efectivo definir un nivel de seguridad a alcanzar y proporcionar un lineamiento general que guíe a cada entidad hacia ese objetivo.

Agesic (Institución pública) - Adolfo Nidegger

Comenta que le gustaría agregarle la parte de estandarización, porque plantea que las soluciones deben realizarse de forma integral. A su vez, plantea una clasificación de infraestructuras críticas para sectores públicos y privados, donde se categorice el nivel de criticidad del mismo.

MIEM (Institución pública) - Gabriel Artucio

Expresa dudas sobre la estandarización, destacando la dificultad de aplicarla en ambientes y organismos heterogéneos. Cuestiona cómo medir efectivamente con estándares en contextos tan diversos. Además, considera poco práctico establecer la obligatoriedad de tener un CSIRT en todos los ámbitos y sugiere evaluar en qué áreas sería adecuado implementarlos e integrarlos.

Agesic (Institución pública) - Fabiana Santellán

Sugiere incluir antecedentes sobre ciberseguridad en Uruguay, ya que algunos decisores carecen de esta información. Propone separar la cultura y la industria como pilares independientes debido a su importancia. También considera necesario establecer un nuevo SOC o CSIRT, pero advierte que debe hacerse con una visión estratégica y no simplemente por crear estructuras nuevas.

Objetivo 2: "Impulsar el desarrollo de una industria del software seguro"

Grant Thornton (Sector privado) - Ignacio Lagomarsino

Plantea la cuestión de quién financiará la implementación de software seguro, sugiriendo que se deben ofrecer incentivos para mejorar la seguridad del software. Considera que si el Estado exige software seguro sin antes incentivar su desarrollo, no habrá proveedores disponibles. Propone establecer un *roadmap* que categorice a las empresas para que mejoren su seguridad y sean competitivas, junto con una agencia que supervise estos requisitos y promueva la educación en el tema.

URUDATA (Sector privado) - José Callero

Sugiere que el CERTuy o Agesic deberían asesorar a los compradores sobre cómo adquirir software seguro, estableciendo estándares claros de requisitos a cumplir. Propone que la línea de acción se refiera directamente a "establecer los lineamientos para la compra de software seguro", sin especificar, para abarcar todos los tipos de software.

OWASP (Sociedad civil) - Gerardo Canedo

Destaca la importancia del *compliance*, señalando que en Uruguay falta un enfoque real en este aspecto. Critica la práctica de afirmar cumplimiento con estándares como *OWASP Top 10* sin realizar análisis o verificaciones. Propone que además de sancionar, se debería ofrecer incentivos o ventajas comerciales para aquellos que cumplan con criterios de seguridad verificables. Además, considera que el *compliance* debería verse como una ventaja competitiva, no solo como un gasto.

Objetivo 3: "Posicionar la industria de ciberseguridad nacional"

Grant Thornton (Sector privado) - Ignacio Lagomarsino

Señala que el documento menciona la necesidad de cooperación entre sectores, pero sin un respaldo concreto, parece ficticia. Argumenta que el sector privado no cooperará a menos que el Estado promueva incentivos, roles, metas y un marco claro de trabajo que beneficie a ambos sectores. Aunque la estrategia enfatiza la importancia del sector privado, no especifica cómo se incentivará su participación.

URUDATA (Sector privado) - José Callero

Sugiere que la descripción del objetivo incluya un contexto u objetivo estratégico claro, en lugar de términos vagos como "pujante". Insiste en que se debe hablar de manera más concreta y específica, con líneas de acción precisas. Se necesita una visión estratégica que marque claramente hacia dónde se quiere ir y qué se busca lograr.

Agesic (Institución pública) - Alejandro Arancio

Agregaría "innovación" donde dice "investigación y desarrollo" en la línea de acción iii.

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

Grant Thornton (Sector privado) - Ignacio Lagomarsino

Destaca que, aunque existen proveedores de ciberseguridad, las pymes no pueden pagar por estos servicios debido a los altos costos. Esto afecta negativamente su seguridad. Propone que debe haber planes de incentivo, entrenamientos y guías para que las pymes puedan acceder a servicios de ciberseguridad. Considera importantes los incentivos, la concienciación y los cursos, sugiriendo campañas de concientización en lugar de obligaciones estrictas.

Intentencia de Montevideo (Institución pública) - Fernando Rodríguez

Sugiere que, al igual que el Plan Ceibal proporcionó computadoras a cada niño, las pymes deberían tener garantizado el acceso a la ciberseguridad como un derecho. Propone que se ofrezca una capa de servicios de ciberseguridad a las pymes a través de proveedores especializados.

URUDATA (Sector privado) - José Callero

Destaca la necesidad de categorizar las consecuencias de los ciberataques según el impacto que tienen en las organizaciones y en la sociedad en general. Subraya la importancia de concientizar a las empresas sobre sus responsabilidades en la prevención de ciberataques y menciona que en muchos países europeos se sanciona la falta de medidas preventivas más que el ciberataque en sí mismo.

MIEM (Institución pública) - María José Franco

Señala que las pymes son incentivadas hacia lo digital y el uso de medios de pago electrónicos, pero carecen de la capacidad financiera para adoptar estas tecnologías de manera segura. Destaca la necesidad de trabajar en este aspecto para que las pymes puedan acceder a los recursos necesarios para su digitalización segura.

Agesic (Institución pública) - Adolfo Nidegger

Propone abordar la estrategia de ciberseguridad organizando las acciones por sectores en lugar de por tamaño de empresa, priorizando aquellos sectores con mayores riesgos y vulnerabilidades conocidas, como el sector de la salud. Sugiere también una atención especial a la tercerización de servicios, dado que muchos ataques a grandes empresas comienzan en proveedores más pequeños. Destaca la necesidad de establecer métricas claras para medir el éxito o fracaso de cada línea de acción, y enfatiza comenzar por fortalecer la seguridad en empresas de desarrollo.

Agesic (Institución pública) - Fabiana Santellán

Propone la creación de centros de asesoramiento para pymes en temas de ciberseguridad, así como cursos específicos sobre seguridad digital. Además, sugiere que se ofrezcan subsidios, incentivos y reducciones de impuestos para fomentar estas prácticas, resaltando la necesidad de inversión en este ámbito.

Objetivo 5: “Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital”

OWASP (Sociedad civil) - Gerardo Canedo

Expresa preocupación sobre la aceptación de estas firmas en la práctica.

Grant Thornton (Sector privado) - Ignacio Lagomarsino

Plantea dudas sobre la validez jurídica y la resolución de disputas en casos que involucran contratos firmados electrónicamente. Se resalta la necesidad de fiscalizar y asegurar el cumplimiento de la ley en cuanto al uso de firmas electrónicas.

Agesic (Institución pública) - Adolfo Nidegger

Menciona la necesidad de regular los sellos de competencia para las firmas electrónicas avanzadas, como los utilizados por profesionales como escribanos y abogados.

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

Esta ronda también se organizó en torno a los objetivos del pilar. Se detallan los aportes estratégicos y las priorizaciones según cada uno.

Objetivo 1: “Impulsar el fortalecimiento y la creación de equipos de monitoreo y respuesta”

- Desarrollar estándares y guías claras para la creación y operación de CSIRTs.
- Definir métodos específicos para medir el éxito y la efectividad de las iniciativas de ciberseguridad.
- Establecer obligaciones legales claras o implementar un sistema de incentivos y sanciones para garantizar el cumplimiento de las normativas de ciberseguridad.
- Asegurar la disponibilidad de recursos humanos capacitados y recursos materiales suficientes para la implementación y operación de CSIRTs.
- Considerar la creación de un CSIRT ciudadano para fomentar la cultura de ciberseguridad y desarrollar perfiles técnicos adecuados.
- Definir estrategias claras y sostenibles para la continuidad de las iniciativas de ciberseguridad.
- Fomentar la coordinación entre los diferentes CSIRTs y otros organismos para asegurar una comunicación efectiva.

Objetivo 2: “Impulsar el desarrollo de una industria del software seguro”

- Promover el cumplimiento de normativas y estándares verificables como los de OWASP.
- Implementar mecanismos para la evaluación y certificación de software seguro, incluyendo beneficios comerciales para quienes cumplan con estos criterios.
- Crear incentivos económicos, como subsidios y reducciones de impuestos, para promover el desarrollo y adquisición de software seguro.
- Establecer programas de formación y guías prácticas para desarrolladores y empresas sobre cómo implementar y mantener software seguro.
- Asegurar que las compras del Estado se realicen solo a proveedores que cumplan con los estándares de software seguro, incentivando al mercado a mejorar sus prácticas.
- Crear una agencia que supervise y eduque en temas de seguridad del software.

Objetivo 4: "Mejorar la ciberseguridad de las MiPymes"

- Desarrollar programas que ofrezcan a las pymes acceso a servicios de ciberseguridad a través de proveedores calificados.
- Establecer planes de incentivo, entrenamiento y guías específicas para pymes en ciberseguridad.
- Implementar campañas de concientización y capacitación sobre ciberseguridad para pymes.
- Ofrecer cursos prácticos sobre temas específicos como respaldos de datos y seguridad en redes sociales.
- Categorizar las pymes según el riesgo y el impacto de un ciberataque para priorizar las medidas de seguridad.
- Fomentar la implementación de buenas prácticas de ciberseguridad en sectores críticos y en la cadena de suministro.

Objetivo 5: "Fortalecer el ecosistema de Firma e Identificación digital para fortalecer el gobierno digital"

- Regular el uso de sellos de competencia en firmas electrónicas avanzadas para garantizar la autenticidad y competencia de los firmantes.
- Asegurar que las firmas electrónicas avanzadas sean ampliamente aceptadas y reconocidas legalmente.
- Exigir el cumplimiento de la normativa existente que permite el uso de firmas electrónicas en documentos legales.
- Implementar mecanismos de fiscalización para asegurar que las firmas electrónicas sean utilizadas y aceptadas correctamente en todas las instancias legales y comerciales.