Mesa de trabajo "Gobernanza y Marco normativo"

Autor

Agesic

Fecha de creación

20/09/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la segunda mesa de trabajo "**Gobernanza y Marco normativo**" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad del 17 de junio al 21 de junio del 2024.

Participaron representantes de: sector público, sector privado, academia, sociedad civil y organismos internacionales.

Introducción

En el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay, la semana del 17 al 21 de junio de 2024 se realizaron ocho mesas de diálogo para recoger 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 que permitan cocrear la ENC. En este espacio se dialogó acerca del alcance de la Estrategia, los principios, objetivos y acciones específicas a impulsar.

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

Este documento presenta en forma sintética los intercambios en esta mesa.

Participantes

Agesic (Institución pública), Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento. Jimena Hernández, Adrián Marrero, Mauricio Papaleo, Fabiana Santillán, Gonzalo Sosa.

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

AMEPP (Institución pública), Agencia de Monitoreo y Evaluación de Políticas Públicas. Jonnathan Silva.

ANCAP (Institución pública), Administración Nacional de Combustibles, Alcohol y Portland. María Nela Moreno, Lucía Pose.

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

BBVA (Sector privado), Banco Bilbao Vizcaya Argentaria S.A. Leandro Secco.

BCU (Institución pública), Banco Central del Uruguay. Daniel Fernández, Isabel Maroñas.

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

CEIBAL (Institución pública), Conectividad Educativa de Informática Básica para el Aprendizaje en Línea. Isabel Fernández, Diego Russo.

CERTuy (Institución pública), Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Bruno Olivera.

CLAEH (Academia), Centro Latinoamericano de Economía Humana. Graciela Cami.

CSIRT (Institución pública), Equipo de Respuesta ante Incidentes de Seguridad Informática de Chile. Cristian Bravo.

DENTONS (Sector privado), Estudio Jurídico. Mariela Ruanova.

Dinatel (Institución pública), Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual. María José Franco.

Ferrere Abogados (Sector privado), Martín Pesce.

FGN (Institución pública), Fiscalía General de la Nación. Ricardo Legner.

LIDECO (Sociedad civil), Liga de Defensa Comercial. Nicolás Antunez.

MIEM (Institución pública), Ministerio de Industria, Energía y Minería. Agustina Pérez Comenale, Sofía Delgado, Sebastián López.

OEA (Institución pública), Organización de Estados Americanos. Alexander Crowther, David Moreno.

Parlamento (Institución pública), Darío Burstin.

Presidencia de la República (Institución pública), Ariel Collazo.

UAIP (Institución pública), Unidad de Acceso a la Información Pública. Mariel Lorenzo.

UCU (Academia), Universidad Católica del Uruguay. Julio Lens, Agustina Santos.

UDELAR (Academia), María Viega.

URCDP (Institución pública), Unidad Reguladora de Datos Personales. Flavia Baladan.

URUDATA (Sector privado), José Callero.

Resumen del intercambio

A continuación, se presenta el informe general de la mesa de trabajo “Marco normativo 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 una de las rondas de participación tenía foco en un eje específico de la ENC, en la mayoría de los casos la discusión se vio enriquecida excediendo la temática propuesta.

Parte 1. Ronda de intercambio sobre el borrador

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

Parte A. Aportes generales sobre la propuesta borrador

En esta primera parte, la pregunta disparadora fue: ¿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 Marco normativo de la ciberseguridad?

Se valoró la propuesta y se consideró que abarca todas las temáticas y cubre todos los puntos. Sin embargo, también se comentó que aún está a nivel general, y que se deben prever debates y cuestionamientos. Para esto se enfatizó la importancia de involucrar al sector privado, permitiéndole aportar a la ENC y anticipar posibles críticas.

En efecto, se sostuvo que los actores involucrados van más allá de aquellos que tienen un vínculo estricto con la materia, y es importante que todos se sientan colaboradores legítimos para la ENC durante todo el proceso de creación. Las Mesas de diálogo son espacios muy importantes como instancia de colaboración entre diferentes actores para la apropiación de la ENC.

Se coincidió en que hay un buen punto de partida en Uruguay, pero aún quedan deficiencias y vulnerabilidades. La regulación es laxa, ya que establece obligaciones, pero no existen sanciones asociadas a la misma. Se debe establecer una línea de base que describa la situación actual, reforzar el marco legal y complementarlo con otras instancias. Un marco legal sólido también tendría que definir las potestades regulatorias de cada institución.

También se afirmó que los pilares de la estrategia están definidos de manera demasiado estanca; deberían ser más generales y centrarse en la generación de confianza y de capacidades. Se puso énfasis en la dificultad de generar confianza cuando los objetivos son abordados por diferentes entidades, y en la importancia de una coordinación efectiva y centralizada (se sugirió que Agesic podría ser la entidad encargada, con capacidad de hacer cumplir y recursos). Se recomendó definir objetivos transversales con líneas de acción más concretas y detalladas, y ampliar la descripción de los objetivos de gestión para incluir una visión estratégica clara.

Para prevenir en ciberseguridad, se requieren herramientas tecnológicas, marcos normativos y educación. Se subrayó que es deber del Estado capacitar, tanto a las personas que integran el sistema jurídico como a los usuarios en general. Se señaló que falta formación, y las autoridades deben comprender que se trata de una política pública. Además, los usuarios deben conocer la normativa vigente y saber adónde acudir en caso de incidentes. Esto es parte de crear una cultura en torno al tema.

En resumen, se celebró la ENC como un instrumento que da autonomía al fenómeno del cibercrimen, pero se resaltó que falta determinar cuestiones conceptuales más claramente y cooperar más entre los actores y los dispositivos, lo que actualmente se menciona de forma genérica pero no de forma específica. Se debe pensar en cómo llevar al documento de la ENC a la práctica considerando aspectos como recursos humanos y presupuesto, y estableciendo un plan estratégico con los pasos necesarios para alcanzar el resultado deseado.

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

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

Durante el desarrollo, los y las participantes propusieron una serie de mejoras:

Ordenar la normativa actual

Uruguay ya cuenta con leyes, decretos regulatorios y otras normativas de relevancia para el tema de ciberseguridad. Se debería identificar y compilar esta normativa para no repetir o hacer una norma que entre en conflicto con otra. Para eso, ante todo, es necesario determinar una línea de base de la estrategia, que incluya la institucionalidad existente y el nivel de madurez en ciberseguridad del país.

Pilares y confianza

Se sugirió que los pilares de la estrategia deberían enfocarse más en generar confianza y capacidades, en lugar de ser tan estancos.

Cooperación y coordinación

Se resaltó que se debe especificar más sobre la cooperación y la coordinación entre los actores y los instrumentos, que actualmente es muy general. Definir mecanismos de coordinación y fortalecer los procedimientos de comunicación existentes.

Además, se habló de la importancia de involucrar a actores judiciales y fiscales en el desarrollo del marco normativo.

Distribución de roles y responsabilidades

Se destacó la necesidad de dejar claros los roles en los niveles de estrategia, táctico y operativo, y la necesidad de dotar a los responsables de poderes suficientes que les permita ejercer esa autoridad, así como posibles potestades sancionatorias.

Inclusión del sector privado

Se enfatizó en la necesidad de interactuar con el sector privado, establecer reglas de cooperación público/privado, y establecer en esas reglas también qué se le pide al sector privado y cuándo. Esto debe incluir recursos humanos y financieros, y mecanismos rápidamente activables de colaboración.

También se destacó que se deben identificar incentivos claros para la inclusión del sector privado, y que este adopte una postura preventiva y proactiva. Surgió la propuesta de un fondo de indemnización y de incentivos tributarios para que sea atractivo para el sector privado y potencie la inversión extranjera.

Definición de conceptos y creación de glosario

Se puso énfasis en la necesidad de definir temas conceptuales de forma más clara y específica, para que se comprenda qué implica cada término en una definición única y para asegurar la competencia de las herramientas en las cuestiones adecuadas. Se subrayó la importancia de utilizar un lenguaje claro y comprensible, y se sugirió revisar términos como "datos informáticos" y "sólido" en el contexto jurídico.

Se propuso crear un glosario para aclarar los términos y hacer el documento accesible para todas las personas.

Ampliación de la normativa

Se recomendó ampliar el marco normativo, considerando tipificar en materia de cibercrimen añadiendo normas de ciberseguridad para cuestiones procesales y ciberdelitos, con las que Uruguay no cuenta. Se consideran fallidas y estancadas las normas y discusiones sobre la regulación actuales. Además, se enfatizó la necesidad de actualizar y ampliar el marco normativo de ciberseguridad para incluir conceptos como la supraterritorialidad.

Sin embargo, también se recalcó el riesgo de la hiperregulación, que puede ser una barrera, limitar la innovación y la competitividad. Desarrollar estrategias a conciencia.

Se sugirió basar la legislación en estándares más que en reglas, ya que éstos son más abiertos.

Acompañamiento del marco normativo

Se expresó la necesidad de acompañar la normativa con herramientas de calidad para hacer investigaciones en las fiscalías.

Para las investigaciones policiales es de suma importancia encontrar un balance entre reducir los daños de los ciberataques y salvaguardar la evidencia que puede llevar al autor del crimen. Esto genera una tensión entre la protección de datos personales y la investigación que no se encuentra regulada. El debido proceso requiere de normas procesales y la enseñanza de los equipos.

Capacitación y formación

Se resaltó que la capacitación es fundamental para todos los actores, desde todo el sistema judicial hasta los usuarios.

Además, se propuso brindar conocimiento de ciberseguridad al sector privado, con un enfoque en la prevención. Se propuso certificar a las empresas privadas que brindan servicios al sector público para tener confianza a la hora de las contrataciones.

Se enunció que se debe concientizar sobre los daños que pueden provocar las falencias en seguridad. Si no se estandarizan las exigencias en seguridad, no se puede auditar y controlar.

Educación y cultura

Se sostuvo que el Estado debe brindar enseñanza sobre el uso responsable de las tecnologías a los y las estudiantes, e incluirla en el currículo educativo. No puede existir una sanción por el cibercrimen sin educación y cultura que permita entender el problema.

También debe haber una estrategia de comunicación clara para llegar a toda la población.

Fiscalización proactiva

La fiscalización debe ser contemplada en el documento. Actualmente, la fiscalización surge de la demanda a partir de un incidente. Se debería pasar a una fiscalización más proactiva.

Además, actualmente existen obligaciones sin cumplimiento. El desafío, más allá de desarrollar una normativa, es estratégico: es hacer cumplir con un nivel de madurez inicial.

Se hizo énfasis en el incentivo en vez de la penalización.

También se propuso crear una auditoría, e integrar esta iniciativa como un subcapítulo.

Se planteó determinar un umbral mínimo para cada sector. Una vez definido ese umbral, determinar cómo hacer para alcanzarlo, y recién ahí prever una sanción eventual cuando haya apartamiento.

Sistema de escalas

Debería introducirse un sistema de escalas para distintos niveles de necesidades en ciberseguridad.

Marco regulatorio certificable

La Estrategia debería ser un marco regulatorio certificable.

Organismo de ciberseguridad

Se planteó la posibilidad de crear un organismo o agencia de ciberseguridad que respalde la normativa, impulse la ciberseguridad y desarrolle la institucionalidad. Se entiende que Agesic lleva adelante una labor formidable en esta materia actualmente, pero se reconoce que tiene otras tareas también y la ciberseguridad no es su único foco. Se requiere una entidad centralizada, sea Agesic u otra, para coordinar las acciones de ciberseguridad y cumplimiento.

Además, se resaltó la importancia de que todos los organismos estatales incluyan la ciberseguridad en su planificación y que se definan claramente las normas y regulaciones necesarias.

Asignación de recursos

Se deben identificar y asegurar los recursos necesarios como prioridad, para que la ENC no quede en la teoría.

Es necesario dar visibilidad a los costos de los incidentes de ciberseguridad.

Política de Estado

La Estrategia deber ser una política de Estado, de manera que se asegure la continuidad y la capacidad de los diferentes actores para seguirla de forma adecuada.

Medidas de prevención

Bajo la idea de que es mejor prevenir, la ciberseguridad tiene que funcionar como un seguro. Para esto es necesario que se conozca la importancia del tema y generar una estrategia desde la academia.

Cibercrimen y comunicación de incidentes

Se hizo énfasis en la importancia de no avergonzarse de los incidentes de ciberseguridad y comunicar estos problemas abiertamente.

Consideración de los aspectos procesales

Las normativas actuales no consideran los aspectos procesales, lo que dificulta la práctica de la normativa y el acceso a la justicia. Debería tenerse en cuenta para el marco regulatorio.

Consideración de las prácticas internacionales

Se resaltó la importancia de observar lo que ocurre en otros países para definir si la estrategia nacional está en consonancia con prácticas internacionales.

Cambios en la redacción

En cuanto a la redacción, se sugirió que para integrar la ciberseguridad como un objetivo de gestión, se deben considerar ajustes presupuestarios y administrativos específicos, prefiriendo el término "marco administrativo" sobre "marco regulatorio".

También se propuso cambiar el término "ciudadanía" por "personas" para un enfoque más inclusivo y claro.

Temas invocados que se deben incluir en el marco regulatorio

Conservación de datos.

Recolección, cadena de custodia y presentación de la evidencia digital.

Se señalaron deficiencias en sectores específicos como la salud y el sector bancario, que necesitan más avances, especialmente en temas de ciberseguridad y fraude con tarjetas de crédito.

Finalmente, se plantearon dudas acerca de la necesidad de una ley marco y lo que abarcaría. Se invocó la idea de incluir una línea de acción detallada que explique cómo poner en marcha y medir los objetivos de gestión, con una guía de implementación específica.

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

La segunda parte del intercambio 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 respecto al marco normativo en el pilar “Gobernanza y Marco normativo”.

En líneas generales fueron validados los objetivos, pero se señaló que es difícil estar en desacuerdo con ellos ya que son muy amplios. En esa línea, se recalcó la necesidad de definirlos y sus acciones asociadas claramente, y de establecer una visión estratégica coherente. Se propuso ampliar los objetivos con distintos aportes detallados en la Parte B, debido a la transversalidad del tema y la diversidad de aspectos que abarca.

Los objetivos planteados están validados con algunas consideraciones a los mismos:

- El marco legal, además de ser sólido y coherente como se indica en la ENC, debe ser claro, adaptarse a los cambios, incluir grises y ser transversal;
- Necesidad de establecer roles y responsabilidades;
- Énfasis en que el marco normativo debe basarse en estándares más que en reglas;
- Debería incluirse la gestión de riesgo;
- También debería incluirse la concientización y educación dentro del marco normativo, sea en los objetivos o en la hoja de ruta.
- Se recomendó, en el primer objetivo (“Establecer la gobernanza nacional de ciberseguridad”), agregar una visión más estratégica de lo que se busca, y alinear todas las líneas de acción establecidas en gobernanza, marco regulatorio y en objetivos de gestión, debajo de esa visión integral de gobernanza e institucionalidad.

Se sostuvo que hay que considerar si es importante impulsar una ley marco. Es clave establecer criterios mediante normativas y generar instrumentos para los controles y la gobernanza. Sin embargo, hay que buscar consenso y generar una cultura del cumplimiento, para lo que es necesario pensar en programas de mejoramiento en la gestión y construir instrumentos complementarios a la normativa. Se mencionó que en materia de cibercrimen existe un proyecto que tiene avance de aprobación legislativa, pero que hay que adoptar algo más integral.

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

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

Varios de los aportes de la primera ronda fueron reiterados en los subgrupos en la segunda ronda.

Al igual que en la primera ronda, se hizo hincapié en la necesidad de establecer una línea de base, redefinir roles y responsabilidades, y establecer mecanismos de coordinación. Se destacó la necesidad de recopilar, ordenar y sistematizar toda la normativa vigente sobre ciberseguridad que hay en Uruguay tanto para justificar la importancia como para ver qué hace falta. También se reiteró que se debe crear un glosario en el que se definan los diferentes conceptos de ciberseguridad dentro de la ENC con criterios racionales para facilitar la comprensión. Surgió nuevamente la duda de si alcanza con aprobar una ley de tipificación de ciberdelito, y se sostuvo que también harían falta otras instancias.

Se volvió a mencionar la importancia de que la ENC sea un marco certificable para que pueda utilizarse como estándar de buenas prácticas en ciberseguridad. Se enfatizó la necesidad de flexibilidad, para asegurar que el marco legal sea sólido pero adaptable a los diferentes actores, temas y sectores.

Se reiteró la importancia del involucramiento del sector privado, y de establecer incentivos y mecanismos para que éste sepa lo que tiene que hacer y lo cumpla. Se propuso especificar los requisitos mínimos de seguridad que tienen que cumplir las empresas, a efectos de establecer los estándares mínimos que se aplicarán en el área pública y en el sector privado.

Además, se volvió a plantear la posibilidad de designar responsables por sector. Se sugirió, por otro lado, que una vez designados los responsables, cada sector y cada inciso gestione sus modos de cumplimentar. Se sostuvo que deben generarse regulaciones específicas para diferentes niveles de necesidad en ciberseguridad.

Se reforzó la necesidad de incorporar la cooperación internacional.

Además, se ahondó en cuestiones que habían sido previamente mencionadas, y se propusieron nuevas acciones y actividades:

Análisis de impacto regulatorio

Se recomendó hacer un análisis de impacto regulatorio.

Cultura de la ciberseguridad

Se identificó el problema de la falta de técnicos y de recursos humanos, y se destacó la necesidad de desarrollar una política agresiva de construcción de la cultura de ciberseguridad con enfoques diferentes para los distintos actores:

- Para el sector privado se sugirieron cursos de capacitación adaptables sectorialmente, que incluyan un respaldo de capacitación especial a las startups y las pymes.
- Para el sector público se recomendó la capacitación de funcionarios públicos con reglas más prescriptivas.
- Para la población en general se propuso la capacitación mediante la incorporación de temas de ciberseguridad a la educación formal y acuerdos con instituciones educativas.

Participación de múltiples actores

Se debe contemplar la participación de múltiples actores. Se necesita un marco normativo dirigido a actores privados y públicos, y que considere la diversidad de contextos de acuerdo con los sectores y los grados de madurez. Según la situación de los actores, es importante pensar en generar incentivos económicos, específicamente tributarios.

También se debe generar un proceso de elaboración normativa que involucre a la diversidad de partes involucradas incluyendo una consulta pública y debida rendición de cuentas.

Organismo de ciberseguridad

Hace falta un órgano que tenga potestades propias para actuar rápidamente con carácter de una agencia reguladora, que le pueda dar agilidad. A su vez, debería ser un servicio autónomo, para tener menos incidencia del poder político con presupuesto propio. Esto no quita que puedan seguir existiendo los comités asesor y operativo.

También se planteó la posibilidad de crear un Observatorio Nacional de Ciberseguridad.

Acceso a la justicia

Garantizar el acceso a la justicia en las distintas dimensiones, no solo en el área penal. Se consideró necesaria una mayor cooperación en los procesos y sumar al sistema existente competencias más específicas en vez de crear otro organismo nuevo.

Hay varios aspectos de la justicia por mejorar. Se consideró que podría haber una unidad de retroalimentación que trate este

tipo de temas, que sirva de nivel anterior al judicial.

Coordinación y gobernanza

Institucionalizar la coordinación y la gobernanza, que debe incluir a los distintos instrumentos jurídicos que existen dentro de la temática de la ciberseguridad.

Presupuesto

Para que las medidas sean viables, es necesario tener recursos. Se debe prever un presupuesto de acuerdo a la propuesta de la ENC.

Hubo diferentes ideas sobre cómo financiar la ENC. Como alternativa a los impuestos, que no son atractivos para la población, se propuso la imposición de sanciones (por ejemplo, multas) si no se cumplen con ciertos estándares mínimos.

Además, la financiación debe adaptarse a los diferentes actores. Para el sector privado podrían considerarse incentivos o exoneraciones tributarias, por ejemplo.

Se destacó la necesidad de invertir, ya que de lo contario será más caro solucionar incidentes.

También se propuso que para obtener recursos se podría aportar información real que muestre los costos de reparar un incidente. Se habló de la creación de un Observatorio para hacer un estudio estadístico de los riesgos, planteando que una manera de hacer visible la necesidad de cumplir es transformando la vulnerabilidad en costos (tanto materiales como de reputación) y visibilizando riesgos.

Fiscalización, cumplimiento de normas y auditoría

Actualmente, el comité de gestión no cumple con potestad para fiscalizar varias temáticas de la ENC. Se debe definir quién es competente para facilitar la fiscalización y cuestiones jurídicas y judiciales. Mientras que algunos participantes ven como un problema que la fiscalización la lleve adelante un organismo público, otros no lo perciben así.

Se debatieron las posibilidades de control y sanción, enfatizando las dificultades ligadas al cumplimiento en el sector público y la importancia de generar mecanismos efectivos.

Se propuso que la ciberseguridad en cada estructura sea parte de sus planes estratégicos.

Se señaló que hoy en día, aquellas organizaciones que forman parte de los servicios críticos del país, públicas o privadas, están obligadas a cumplir criterios estándares de ciberseguridad según la Ley 20.212, enfatizando que falta el decreto que reglamente quién tiene que cumplir qué.

Se sugirió aprovechar la experticia de Agesic, que está preparando un marco de ciberseguridad con el que audita a las entidades públicas, en vez de pagar la auditoría a terceras partes. Se podría establecer una auditoría interna, pero requeriría recursos porque hoy en día Agesic no tiene los medios. Se propuso también estudiar la viabilidad y pertinencia de que las auditorías dentro de la Administración Central sean realizadas por la AIN. Sería un camino que llevaría a una norma para penalizar.

Transparencia

Se subrayó la necesidad de tener una transparencia activa, aunque se reconoce que es un tema delicado ya que no se le puede exigir a todos los actores. Se cuestionó si se podría interferir en el ámbito privado para lograr transparencia considerando que es un tema de interés nacional.

Fortalecimiento del CERTuy

Es importante fortalecer al CERTuy y otros sectores relacionados.

Gestión de datos

Se planteó la necesidad de gestionar los datos, ya que existe la información pero faltan los recursos para procesarla.

Se propuso armar un plan de formación y un protocolo para recoger información. Se indicó que en ciberseguridad todos tendrán que asumir un mínimo de involucramiento, y que es un requisito la intervención del Estado.

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

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

Se consideró pertinente priorizar las siguientes acciones:

- Definir los mecanismos de coordinación estableciendo una gobernanza clara que incluya actores y responsabilidades, normas y recursos necesarios.
- Definir los sectores críticos y sus roles.
- Proponer un marco legal y normativo adecuado y actualizado, incluyendo la privacidad y el acceso a la información.
- Desarrollar líneas de acción prácticas y detalladas para la implementación efectiva del marco normativo.

Para ello, será necesario

- Hacer un relevamiento de la normativa de la institución a corto plazo: realizar un mapeo, definir la nueva institucionalidad, determinar la brecha a cubrir, y fortalecer los mecanismos que ya existen para optimizar recursos. También se recomendó focalizarse en las regulaciones existentes que no se cumplen, y determinar cómo proceder en estos casos.
- Establecer la ciberseguridad como objetivo de gestión, teniendo en cuenta que es un bien organizacional, y trabajar el concepto de cómo se mide la ciberseguridad como objetivo de gestión dentro de las organizaciones, estableciendo estándares mínimos a cumplir y un marco administrativo de cómo se lleva adelante, qué se mide y cómo.
- Elaborar un glosario con los conceptos importantes: conceptos como marco sólido e informático, resiliencia, supraterritorialidad, ciberespacio, entre otros.
- Ser más agresivo con la estrategia de concientización (por ejemplo, visibilizar los problemas de seguridad aprovechando la información y datos existentes); prever la necesidad de formación técnica para todo el sistema de justicia y de generar herramientas y mecanismos más flexibles.
- Destinar recursos.

En cuanto a los actores, se subrayó que además del sector público y del privado, deberían estar involucrados los colegios de abogados y escribanos, así como la academia.

Las acciones se ven viables en un plazo de cinco años, pero el tema clave que surgió mucho es el del presupuesto. Son acciones que se pueden abrir en sub-acciones y realizar al menos algunas. Para ello sería importante contar con indicadores que permitan evaluar los avances.

Respecto al orden de las acciones, se mencionó que se debería priorizar a la primera línea de acción (“Definir los niveles, organizaciones y responsabilidades para la gobernanza a nivel Estratégico, Operativo y Sectorial”) del primer objetivo.

Anexo

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

Subgrupo 1

- Moderadora: Tania da Rosa, Agesic.
- Relatora: Sofía Lopes e Isabel Álvarez, ICD
- Participaron 10 (diez) personas de 10 (diez) 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

Dinatel (Institución pública) - María José Franco

Valora la iniciativa de la ENC y las Mesas de diálogo como una instancia de colaboración y creación con multiplicidad de actores de diferentes sectores y ámbitos. Recordó que las personas no son los únicos usuarios afectados por la ENC, sino que también todos los actores del sector público, sector privado, sociedad civil y academia partícipes de la creación de la ENC. Los actores involucrados van más allá de aquellos que tienen un vínculo estricto con la materia, y es importante que todos se sientan colaboradores legítimos para la ENC durante todo el proceso de creación, haciendo énfasis en el sector privado.

ANCAP (Institución pública) - Lucía Pose

Compartió la idea de que las Mesas de diálogo son cruciales como instancia de colaboración entre diferentes actores para la apropiación de la ENC, ya que serán parte de los afectados por la ENC.

LIDECO (Sociedad civil) - Nicolás Antunez

Cree difícil la regulación de la ciberseguridad sin un incidente a la seguridad de la información que despierte un interés nacional.

FGN (Institución pública) - Ricardo Legner

Hizo una evaluación del estado actual de la ciberseguridad en Uruguay, donde encuentra deficiencias y vulnerabilidades. Desde su experiencia en Fiscalía, reportó que han habido accidentes de gravedad que no han trascendido a la atención pública, lo que puede afectar la salud de otras investigaciones.

CEIBAL (Institución pública) - Diego Russo

Alertó sobre los grandes incentivos que tienen los cibercriminales en el contexto de la redituabilidad del crimen organizado. El Estado tiene el deber de capacitar sobre la ciberseguridad y la ciberdelincuencia, brindando una enseñanza sobre el uso responsable de las tecnologías a los estudiantes.

ANP (Institución pública) - Marcos Cocchiararo

Prefirió enfocarse en cuestiones más técnicas en sus comentarios, por lo que no participó de esta primera ronda de diálogo. Luego destacó cuestiones del marco regulatorio, hablando de la importancia de la inversión en ciberseguridad como medida de prevención y de la creación de una estrategia desde la perspectiva académica para la formación educativa.

UCU (Academia) - Agustina Santos

Valora la ENC y la divide en tres dimensiones al visualizarla: normativa, intervención social y fiscalización. Respecto a la normativa, celebró la ENC como un instrumento que da autonomía al fenómeno del cibercrimen, ya que comúnmente se recurre a equivalencias funcionales con otros instrumentos a cuestiones en el ordenamiento vinculadas a la tecnología, en vez de crear herramientas específicas. Sin embargo, hay que determinar cuestiones conceptuales más claramente y cooperar más entre los actores y los dispositivos, que actualmente se menciona de forma genérica pero no de forma específica. En cuanto a la intervención social, se debe introducir la política de la gobernanza en la intervención social de manera más específica. Finalmente, la fiscalización viene más de la demanda de un incidente, por lo que se debe pasar a una actitud más proactiva.

URCDP (Institución pública) - Flavia Baladán

Ve importante no solo pensar en el documento de la ENC de forma teórica, sino que también en cómo llevarlo a la práctica considerando cuestiones como recursos humanos y presupuesto, y estableciendo un plan estratégico con los pasos necesarios para alcanzar el resultado deseado. Uruguay ya cuenta con instituciones e instrumentos que facilitan el camino de la Estrategia, como la Ley de Protección de Datos y órganos de control; sin embargo, hay que trabajar más en la coordinación con las competencias de estos organismos.

BBVA (Sector privado) - Leandro Secco

Celebró iniciativas como las Mesas de diálogo porque involucra la voz del sector privado, permitiéndole aportar a la ENC y

conocer con antelación sus posibles efectos. También valora que esta instancia esté ocurriendo en año electoral, ya que indica la intención de que la ENC sea una política pública de Estado. La ENC debe incluir incentivos para el sector privado, que piensa en términos de rentabilidad, como un fondo de indemnidad.

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

La discusión se dio de manera que los participantes fueron añadiendo aportes de manera conjunta, por lo que están organizados por tema en vez de por autor.

Entre las recomendaciones elaboradas, figuran:

Inclusión del sector privado

Identificar incentivos claros para la inclusión del sector privado, que piensa en clave de rentabilidad, para que adopten una postura preventiva y proactiva. Surgió la propuesta de un fondo de indemnización y de incentivos tributarios para que sea atractivo para el sector privado y potencie la inversión extranjera.

Definición de conceptos

Definir cuestiones conceptuales de forma más clara y específica, para que se comprenda qué implica cada término en una definición única y para asegurar la competencia de las herramientas en las cuestiones adecuadas y no el uso de instrumentos de funcionalidad equivalente.

Cooperación y coordinación

Especificar más sobre la cooperación y la coordinación entre los actores y los instrumentos, que actualmente es muy general.

Intervención social

Introducir la política de la gobernanza en la intervención social de forma más específica.

Fiscalización proactiva

Actualmente, la fiscalización viene de la demanda de un incidente. Hay que pasar a una fiscalización más proactiva.

Ampliación de la normativa

Ampliar el marco normativo, considerando añadir normas de ciberseguridad para cuestiones procesales y ciberdelitos, con las que Uruguay no cuenta. Se consideran fallidas y estancadas las normas y discusiones sobre la regulación actuales.

Organismo de ciberseguridad

Crear un organismo o agencia de ciberseguridad que respalde la normativa, impulse la ciberseguridad y desarrolle la institucionalidad. Se entiende que AGESIC lleva adelante una labor formidable en esta materia actualmente, pero se reconoce que tiene otras tareas también y la ciberseguridad no es su único foco.

Educación y cultura

Brindar por parte del Estado una enseñanza sobre el uso responsable de las tecnologías a los estudiantes. Muchos ciberdelitos son cometidos por menores de edad, por lo que generar una cultura sobre el cibercrimen para potenciar la prevención e incorporar los valores es crucial, en el contexto en el cual las tecnologías han avanzado más rápido que la cultura de ciberseguridad hasta el momento. No puede existir la sanción por el cibercrimen sin una educación y cultura que dé a entender el problema.

Brindar conocimiento de ciberseguridad al sector privado, con un enfoque en la prevención. Se sugiere canalizarlo a través de las Cámaras Empresariales para otorgar estrategias de prevención acordes al sector y al tamaño de las empresas.

Ordenar la normativa actual

Uruguay ya cuenta con leyes, decretos regulatorios y otras normativas de relevancia para el tema de ciberseguridad. Se debería identificar y compilar esta normativa para no repetir o hacer una norma que entre en conflicto con otra.

Consideración de la competencia policial

Para las investigaciones policiales es crucial encontrar un balance entre reducir los daños de los ciberataques y salvaguardar la

evidencia que puede llevar al autor del crimen. Esto genera una tensión entre la protección de datos personales y la investigación que no se encuentra regulada. El debido proceso requiere de normas procesales y la enseñanza de los equipos.

Asignación de recursos

Destacar la asignación de recursos, la cual es crucial para que la Estrategia sea una política de Estado que asegure la continuidad y la capacidad de los diferentes actores para seguir la Estrategia de forma adecuada. Por este motivo, la iniciativa debería partir desde Presidencia, porque es quien tiene los recursos.

Marco regulatorio certificable

Hacer que la Estrategia sea un marco regulatorio certificable.

Medidas de prevención

Bajo la idea de que es mejor prevenir, la ciberseguridad tiene que funcionar como un seguro. Para esto es necesario que se conozca la importancia del tema y generar una estrategia desde la academia.

Consideración de los aspectos procesales

Las normativas actuales no consideran los aspectos procesales, lo que dificulta la práctica de la normativa y el acceso a la justicia. Debería tenerse en cuenta para el marco regulatorio.

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

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

En general se encontraron muy de acuerdo con lo planteado dentro del pilar. Se propuso ampliar el objetivo con diferentes aportes detallados en la Parte B, debido a la transversalidad del tema y la diversidad de aspectos que abarca.

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

Cultura de la ciberseguridad

Desarrollar una cultura de ciberseguridad como política agresiva con enfoques diferentes para los distintos actores:

Para el sector privado se sugirieron cursos de capacitación adaptables sectorialmente, que incluyan un respaldo de capacitación especial a las startups y las pymes.

Para el sector público se recomendó la capacitación de funcionarios públicos con reglas más prescriptivas.

Para la población en general se propuso la capacitación mediante la incorporación de temas de ciberseguridad a la educación formal.

Participación de múltiples actores

Contemplar la participación de múltiples actores que no sean solo las personas. Se necesita un marco normativo que apunte a actores privados y públicos, y que considere la diversidad de contextos de acuerdo con los sectores y los grados de madurez. Según la situación de los actores, es importante pensar en generar incentivos económicos, específicamente tributarios.

Acceso a la justicia

Garantizar el acceso a la justicia en las distintas dimensiones, no solo en el área penal. Actualmente, hay una unidad de cibercrimen pero no abarca la justicia. Se consideró necesaria una mayor cooperación en los procesos y sumar al sistema existente competencias más específicas en vez de crear otro organismo nuevo.

Hay varios aspectos de la justicia por mejorar. Por ejemplo, la primera acción podría ser un reclamo en la plataforma misma y luego la vía judicial. Se consideró que podría haber una unidad de feedback que trate este tipo de temas, que sirva de nivel anterior al judicial.

Coordinación y gobernanza

Institucionalizar la coordinación y la gobernanza, donde se definan los roles y responsabilidades de los actores de forma clara.

Además, la coordinación debe ser entre los diferentes actores incluyendo los distintos instrumentos jurídicos que existen dentro

de la temática de la ciberseguridad.

Cooperación internacional

Incorporar la cooperación internacional.

Trazabilidad y dominabilidad digitales

Contar con trazabilidad y dominabilidad digitales. Este enfoque surgió desde una propuesta sobre garantizar la soberanía digital del país, pero termina siendo descartada debido a que ya hay regulación sobre esto y no necesariamente asegura la seguridad territorial. Como de todas formas se consideró crucial tener contingencias, se decidió la incorporación de la trazabilidad y dominabilidad digitales.

Presupuesto

Prever un presupuesto de acuerdo a la propuesta de la ENC.

Hubo diferentes ideas sobre cómo financiar la ENC. Por un lado, se propuso generar un impuesto a los celulares a una tasa razonable para financiar la ciberseguridad y la investigación de delitos cibernéticos. Sin embargo, esta idea fue rechazada por la mayoría de la mesa porque medidas como los impuestos no son atractivas para la población y otros actores, lo que disminuye las chances de que se implemente la ENC. Por otro lado, como alternativa a los impuestos, se propuso la imposición de sanciones si no se cumplen con ciertos estándares mínimos, como una multa si una contraseña es 12345, por ejemplo.

Además, la financiación debe adaptarse a los diferentes actores. Para el sector privado podrían considerarse incentivos o exoneraciones tributarias, por ejemplo.

Fiscalización

Actualmente, el comité de gestión no cumple con potestad para fiscalizar varias temáticas de la ENC. Se debe definir quién es competente para facilitar la fiscalización y cuestiones jurídicas y judiciales. Mientras que algunos participantes ven como un problema que la fiscalización la lleve adelante un organismo público, otros no lo perciben así.

Estándares

Hacer que la ENC sea un marco certificable para que pueda utilizarse como estándar de buenas prácticas en ciberseguridad. La competencia correspondería a AGESIC.

Transparencia

Tener una transparencia activa, aunque se reconoce que es un tema delicado ya que no se le puede exigir a todos los actores. Se cuestionó si se podría interferir en el ámbito privado para lograr transparencia considerando que es un tema de interés nacional.

Ordenar la normativa actual

Recopilar, ordenar y sistematizar toda la normativa vigente sobre ciberseguridad que hay en Uruguay tanto para justificar la importancia como para ver qué hace falta.

Glosario

Definir los diferentes conceptos de ciberseguridad dentro de la ENC con criterios racionales para facilitar la comprensión.

Flexibilidad

Asegurar que el marco legal sea sólido pero adaptable a los diferentes actores, temas y sectores.

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

Los análisis, las acciones priorizadas y los actores vinculados identificados por los participantes se discutieron en conjunto con la Parte B, por lo que se encuentran plasmados allí.

Subgrupo 2

- Moderadora: Ninoschka Dante, Agesic
- Relatora: Marta Susana Manent, ICD
- Participaron 10 (diez) 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

DENTONS (Sector privado) - Mariela Ruanova

Considera que la propuesta abarca todas las temáticas y cubre todos los puntos. Le parece que la educación es muy importante y que los usuarios y las empresas (privadas, sobre todo) tienen clara la normativa con respecto a la protección de datos. Indica que es importante reforzar el área de sistemas de pagos, por la vulneración de datos y por el riesgo.

MIEM (Institución pública) - Agustina Pérez Comenale

Propone separar los “grises”. Comenta que hay áreas que necesitan regulaciones específicas, y que debería introducirse un sistema de escalas para distintos niveles de necesidades en materia de ciberseguridad. Considera que es difícil enmarcar todo en la misma línea.

UCU (Academia) - Julio Lens

Comenta que la estrategia tiene niveles de profundidad modestos, que es muy superficial. Cree que a este nivel de mención de los temas no hay disputas sino una expresión de deseos. Estima que como punto de arranque es maravilloso, pero luego los privados tendrán temas de cuestionamiento como por ejemplo si los datos, todos, deben ser reportados. Considera que, en materia penal, además de la adhesión al Convenio de Budapest, hay que ampliar una enorme cantidad de figuras y normas.

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

Agesic (Institución pública) – Jimena Hernández

Celebra la iniciativa de la estrategia desde el punto de vista legal. Es urgente establecer reglas más claras y le preocupa que no se ha interactuado con los privados. Entiende que, en materia de cibercrimen, es necesario tipificar. Resalta que hay un proyecto, el cual es perfectible. Precisa que la normativa no sirve si no se acompaña con las herramientas necesarias de calidad para hacer las investigaciones en las fiscalías y considera que ese es otro desafío. Plantea la necesidad de establecer reglas de cooperación público/privada y establecer en esas reglas también qué se le pide al privado y cuándo.

Hace hincapié en que es importante concientizar sobre los daños que pueden provocar las falencias en seguridad, estandarizar qué se exige como nivel de seguridad, y luego auditar y controlar. Entiende que el control preventivo es prioritario, antes de la auditoría. Propone sumarle una guía pública para controlar las acciones frente al incumplimiento y las modalidades de sanción frente a otro organismo estatal. Además, menciona los inconvenientes asociados al publicar los niveles bajos de ciberseguridad de un organismo, interrogando qué mecanismos serían los más apropiados.

Reconoce que se sabe que hay que fiscalizar, pero no se cumple, aún de sector público a sector público, y menciona lo presupuestario como un escollo a superar. Manifiesta que es necesario cuantificar y dar visibilidad a los costos de “tapar el agujero y que no entre más agua”, además de lo que después hay que gastar en forense, y que hay que poner sobre la mesa lo que se gasta en general. También menciona que hay algunos ítems regulatorios más dispersos y que debería ser más sectorial.

AIN – Rodrigo Pagliaro - (Institución pública)

Sostiene que lo fundamental es desarrollar la formación, las capacitaciones.

AMEPP (Institución pública) – Jonnathan Silva

Percibe el documento como un paso base, abarcativo, que va a ir instrumentándose. Señala que ya hay un marco normativo y existen decretos. Efectivamente, está la obligación pero no el cumplimiento. Esto se agilizaría definiendo un responsable de ciberseguridad. Considera que más allá de desarrollar un marco normativo abarcativo, el desafío es más estratégico: es hacerlo cumplir con un nivel de madurez inicial. La estrategia tiene que ser más estática que el dinamismo de la política: debe ser más bien una estrategia de Estado.

ANCAP (Institución pública) - María Nela Moreno

Comenta que no cambiaría ninguno de los pilares. Entiende la importancia de que estén claros los roles. Propone poder

certificar a las empresas privadas que brindan servicios al sector público para tener confianza a la hora de las contrataciones. Estima que es muy importante el desarrollo de las capacidades, y que acompañe la sociedad; en especial, los abogados. Refiere que ha habido situaciones donde ante la comisión de un delito no se encuentra respaldo porque la evidencia no quedó bien recogida. Considera que debe haber capacitación y que es algo que está lejos de la situación actual. Indica que es muy necesario definir un marco y que luego exista un mecanismo de control, por eso insiste en la certificación.

Entiende que el control del cumplimiento efectivo y la fiscalización pública que acompañe estos procesos no se ve contemplada en el documento. Propone la creación de un Regulador que ayude y que también se arme un cronograma de ayuda y mejora.

CSIRT (Institución pública) – Cristian Bravo

Comparte la experiencia en su país, Chile, y resalta que el interés del privado es distinto del público. Cuenta que a fin de asegurar el cumplimiento y saber quién tiene que hacerse cargo llegaron a instaurar que el responsable final en un servicio público es el director, entonces la mayor parte de la penalización va a sueldo o a suspensión del director. Reconoce que es controversial, pero funciona muy bien. También, en lo que es incentivos en vez de castigos, refiere que hubo un Programa de Mejoramiento de la Gestión y el sueldo dependía del cumplimiento de objetivos con porcentajes sobre cumplimiento. También insistió en que es necesario separar el “qué” del “cómo”. Opina que no se va a definir el cómo en este momento, y enfatiza que una vez que uno define el “qué”, no hay infinitas maneras del “cómo” sino que finalmente hay dos o tres modos.

DENTONS – (Sector privado) Mariela Ruanova

Propone ver cómo incentivar en vez de cómo penalizar. Sugiere como ejemplo incentivar con un beneficio fiscal al sector privado. Señala que existe un programa de mejora de la gestión, pero hay que unirlo con ciberseguridad. Considera que hay normas que tendrían que ser del sector privado en sí, específicamente, en algunas líneas más allá de la interacción con lo público.

MIEM – (Institución pública) Agustina Pérez Comenale

Estima que además de buenas prácticas, es necesario agregar el aspecto de auditoría como subcapítulo. Considera que incentivar es positivo y que ayude también difundir, porque en general se cree que lo que se destina a ciberseguridad es un costo hundido.

MIEM (Institución pública) Sebastián López

Plantea dudas: ¿Cómo se va a encarar la parte normativa? Si es una ley marco, ¿qué abarcará? porque lo penal va por otro lado. Indica que la ley marco va a necesitar leyes especiales, que serían las más importantes.

UCU – (Academia) Julio Lens

Propone dejar el tema de la sanción y la fiscalización para cuando esté claro qué tiene que cumplir cada actor. Señala la necesidad de determinar un umbral mínimo para cada sector, incluyendo al sector privado, que hoy en día no está muy involucrado. Una vez definido ese umbral, hay que determinar cómo hacer para alcanzarlo, y recién ahí prever una sanción eventual cuando haya apartamiento.

Toma el ejemplo del mecanismo de prevención de lavado, que en ciertos aspectos no fue provechoso pero dio buenas enseñanzas desde el punto de vista de la necesidad de dialogar con todas las partes. La estrategia no puede elaborarse desde una posición de confrontación.

Finalmente, subrayó que es un buen momento para establecer las bases para generar una cultura de cumplimiento.

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

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

En líneas generales fueron validados los objetivos, y se señaló que es difícil estar en desacuerdo con ellos. Los desacuerdos, se sostuvo, aparecerán a la hora de interpretarlos e implementarlos. Se subrayó que el marco regulatorio debe incluir grises, se transversal, y hacer referencia a la gobernanza, al cibercrimen, a las infraestructuras críticas, etc.

Se mencionó que en materia de cibercrimen existe un proyecto que tiene avance de aprobación legislativa, pero que tiene que adoptarse algo más integral. Además, lo que no hace este proyecto es revisar el Código Penal. Se indicó que se ha intentado aprobar una reforma al Código Penal varias veces, aún sin éxito. Sin embargo, desde un punto de vista técnico, el Código Penal es muy limitante porque hace imposible tomar ciertas acciones directas ante un ciberdelito.

Se sostuvo que hay que considerar si es importante impulsar una ley marco. Es clave establecer criterios mediante normativas y generar instrumentos para los controles y la gobernanza. Sin embargo, hay que buscar consenso y generar una cultura del cumplimiento, para lo que es necesario pensar en programas de mejoramiento en la gestión y construir instrumentos que vayan por fuera de lo normativo.

También se recomendó incluir la educación en ciberseguridad en las empresas en algún punto, sea en los objetivos o en una hoja de ruta.

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

Se planteó que es crucial gestionar los datos, ya que existe la información pero faltan los recursos para procesarla. Hay que invertir porque de lo contario será más caro solucionar incidentes. A partir de la información existente, es necesario analizar en qué escalón estamos para poder ascender, crecer.

Surgió la duda de si alcanza con aprobar una ley de tipificación de ciberdelito, y se sostuvo que también harían falta otras instancias. Por ejemplo, es necesario capacitar al policía que está en primera línea y darle las herramientas para la preservación de la evidencia digital.

Se debatieron las posibilidades de control y sanción, enfatizando las dificultades ligadas al cumplimiento en el sector público y la importancia de generar mecanismos efectivos.

Se propuso que la ciberseguridad en cada estructura sea parte de sus planes estratégicos.

Se señaló que hoy en día, aquellas organizaciones que forman parte de los servicios críticos del país, públicas o privadas, están obligadas a cumplir criterios estándares de ciberseguridad según la Ley 20.212, enfatizando que falta el decreto que reglamente quién tiene que cumplir qué.

Se sugirió aprovechar la experticia de Agesic, que está preparando un marco de ciberseguridad con el que audita a las entidades públicas, en vez de pagar la auditoría a terceras partes. Se podría establecer una auditoría interna, pero requeriría recursos porque hoy en día Agesic no tiene los medios. Se propuso también estudiar la viabilidad y pertinencia de que las auditorías dentro de la Administración Central sean realizadas por la AIN con un paréntesis gigante que implica el tema presupuestario. Sería un camino que llevaría a una norma para penalizar.

Además, se hizo hincapié en la necesidad de designar responsables por sector. Se sugirió, por otro lado, que una vez designados los responsables, cada sector y cada inciso gestione sus modos de cumplimentar. Si no hay voluntad de cumplir desde adentro, se resaltó, será muy difícil hacer cumplir desde afuera.

Se trajo a consideración la problemática de que actualmente muchas empresas del ámbito privado no saben lo que tienen que hacer y para cuándo - sobre todo aquellas que brindan servicios en áreas críticas. Se reconoció que es vital que lo sepan, pero no es posible en ese contexto garantizarlo solamente con multas. Se sugirió ofrecer algún beneficio para incentivar el cumplimiento. En todo caso, hubo consenso acerca de la importancia de involucrar al sector privado. Se planteó la necesidad de fortalecer específicamente el sector de sistemas de pagos.

Se propuso especificar los requisitos mínimos de seguridad que tienen que cumplir las empresas, a efectos de establecer los estándares mínimos que se aplicarán en el área pública y el sector privado.

Para que las medidas sean viables, es necesario tener recursos. Para obtenerlos se podría aportar información real que muestre los costos de reparar un incidente. Se propuso la creación de un Observatorio para hacer un estudio estadístico de los riesgos, planteando que una manera de hacer visible la necesidad de cumplir es transformando la vulnerabilidad en costos (tanto materiales como de reputación). Se habló de visibilización de los riesgos como parte de la sensibilización. Lo reputacional, se subrayó, también entra en el área de la concientización.

Se propuso armar un plan de formación y un protocolo para recoger información. Se indicó que en ciberseguridad todos tendrán que asumir un mínimo de involucramiento, y que el Estado va a tener que invertir.

Se sostuvo que deben generarse regulaciones específicas para diferentes niveles.

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

Se consideró muy importante ver el estado actual de la ciberseguridad mediante mapeos y revisión de normativas. Se sostuvo que hay que realizar un análisis del contenido de la ley marco y de su aptitud para lograr los objetivos. También se recomendó focalizarse en las regulaciones existentes que no se cumplen, y determinar qué hacer en estos casos.

Se planteó la necesidad de:

- Establecer estándares mínimos a cumplir;
- Cooperación;
- Definir los sectores críticos y sus roles;
- Examinar la cuestión de financiamiento de las estructuras nuevas;

- Hacer énfasis en la responsabilidad de los funcionarios;
- Incluir el tema de ciberseguridad en cada estructura;
- Ser más agresivo con la estrategia de concientización (por ejemplo, visibilizar los problemas de seguridad aprovechando la información y datos existentes);
- Prever la necesidad de formación técnica para todo el sistema de justicia y de generar herramientas y mecanismos más flexibles.

Subgrupo 3

- Moderadora: Natalia Salazar, Agesic.
- Relatora: Daniel Miranda, ICD
- Participaron 8 (ocho) personas de 7 (siete) 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

CLAEH (Academia) - Graciela Cami

Comenta que desde la Asociación de Escribanos están trabajando en la seguridad con respecto a la firma electrónica. Se debe hacer un trabajo de evangelización porque hay sectores más reacios, aunque están trabajando desde que salió la ley en 2009 e igualmente se ven los logros. Falta formación. Desde la Universidad CLAEH se concientiza sobre la importancia del tema. Las autoridades deben comprender que se trata de una política pública.

Ferrere Abogados (Sector privado) - Martín Pesce

Comenta que Uruguay tiene un buen punto de partida, tiene legislación avanzada en ciberseguridad, así como en protección de datos. Existe el marco de ciberseguridad de Agesic, por lo que en términos generales hay un buen punto de partida. Por lo menos así se percibe desde el sector privado.

Agesic (Institución pública) - Adrián Marrero

Sostiene que Uruguay tiene una posición que ha venido trabajando a lo largo de los años y se ha posicionado a nivel regional con un nivel muy maduro. Desde el área de seguridad, todavía se ven algunas dificultades en la regulación que es un poco laxa. Hay obligaciones, pero no hay sanciones. Cada organismo es distinto y tiene dificultades distintas, pero falta el impulso. Deberían verse sanciones frente al incumplimiento.

BCU (Institución pública) - Isabel Maroñas

En líneas generales está de acuerdo con el borrador. Los temas que resalta como más importantes son la necesidad de dejar claro los roles en los niveles de estrategia, táctico y operativo, y la necesidad de dotar a los responsables de poderes suficientes que les permita ejercer esa autoridad, así como posibles potestades sancionatorias. Sobre todo, destaca la necesidad de que todo esté acompañado de dotación de recursos para que no quede en letra muerta.

Un tema más específico del marco regulatorio es que el tema de cibercrimen es importante. Se debe reforzar el tema procesal y de la recolección de pruebas, ya que siempre hay dudas sobre la cadena de custodia y sobre qué es aceptable para la justicia. Aún hay mucho para acordar en esta temática.

Presidencia de la República (Institución pública) - Ariel Collazo

Argumenta que específicamente uno de los puntos más importantes es lograr el concepto de lo que se necesita para regularizar el tema de ciberseguridad y que todas las personas comprendan la importancia. Para esto es necesario tener un marco bien definido, tanto en el sector público como en el privado. Hay que tener claro las problemáticas que van a plantearse y crear una cultura en torno al tema. Se debe exigir a los organismos públicos y también a los proveedores. Hay que regular eso. Es necesario lograr que los niños desde la base conozcan todos los riesgos. En la parte privada el tema de seguridad es percibido como algo delicado. Falta mucha concientización sobre el hecho que la seguridad es una problemática de todos; hay que estar entrenando permanentemente a las personas. A veces el concepto del respaldo está tan diluido que tiende a perderse. Se necesitan personas comprometidas con el proceso.

Agesic (Institución pública) - Mauricio Papaleo

Coincide con que hay un buen punto de partida, pero le falta. Se debe complementar ese marco legal, con todo lo que va a implicar en la policía, la justicia, escribanos, abogados, etc. Pero hay que normar más fuerte los incidentes que se deben reportar y tiene que existir la figura del responsable de seguridad y sus responsabilidades definidas. Si hubo un problema y hubo una negligencia por parte del responsable, tiene que haber un marco legal que aporte sanciones. El responsable de su ejecución es un tema para ampliar. En ese marco legal debe estar incluida la concientización y la educación, en la escuela primaria, secundaria, etc. Todo esto debe estar definido en un marco legal.

Parlamento (Institución pública) -Darío Burstin

Afirma que el “contexto cambiante”, el dinamismo, puede ser un problema. Las potestades regulatorias a veces no son claras. Expresa dudas acerca de las potestades regulatorias y sancionatorias de la URSEC. Un marco solido debería definir las potestades regulatorias de cada institución para no tener que ir al parlamento ante cada necesidad. Debería haber un organismo con potestades regulatorias propias.

BID (Institución pública) - Ariel Nowersztern

Sostiene que cada pilar necesitaría contar con antecedentes, con una visión para ese aspecto y después las líneas de acción deberían cubrir la brecha entre la situación y la visión. Lo ve como un proceso de gestión, que identifica la brecha, prioriza, trabaja y mantiene un monitoreo del mundo cambiante. La estrategia podría establecer en qué se va a trabajar.

OEA (Institución pública) - Alexander Crowther

Enuncia que un tema importante es la concientización. Se podría desarrollar una campaña de información para legisladores, porque se necesita un marco legal y recursos. También se debe desarrollar la educación frente al crimen, ya que cada persona con acceso a internet es una vulnerabilidad. Una campaña de educación de los jóvenes garantizaría el éxito a largo plazo. Ejemplifica con el programa “salto del tigre” en Estonia, que empieza en el kínder. La ciber-educación va a prevenir el 80 por ciento de nuestros problemas. Se debe invertir en educación.

Ferrere Abogados (Sector privado) - Martín Pesce

Señala que las herramientas para prevenir en ciberseguridad son las tecnológicas, los marcos normativos y la educación, y sostiene que el 70% de los problemas en ciberseguridad se dan por fallas del factor humano. Por lo tanto, la educación es clave por la relevancia del factor humano.

Agesic (Institución pública) - Adrián Marrero

Argumenta que la concientización se puede integrar en el sector público y privado porque todo va a tener un impacto financiero, pero hay que tener en cuenta que si un ciudadano tiene un problema, debe saber dónde reportarlo, y disponer de herramientas legales a las que recurrir. Como usuario final, debo saber cuáles son las acciones posibles. Hay que habilitar herramientas para incidentes de seguridad para la ciudadanía, que debe ser concientizada desde la juventud. Los jóvenes son nativos digitales pero ignorantes en ciberseguridad y en las medidas que hay que tomar para exigirla. Deben crearse canales de comunicación claros para que la ciudadanía pueda reportar un incidente.

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

Parlamento (Institución pública) -Darío Burstin

Asegura que el documento tiene el nivel de abstracción que debe tener a esta altura del proceso. Pero se preguntaría el alcance, por ejemplo, de la conservación de datos. Hay organismos donde la información no se conserva, como aquellos en los que se elimina la casilla de una persona cuando deja de trabajar ahí. Plantea si la conservación de datos debería estar vinculada a esto, o si es otra cosa (BID - Ariel Nowersztern responde que la obligación de borrar datos puede ser también un tema de ciberseguridad).

Ferrere Abogados (Sector privado) - Martín Pesce

Explica que los datos deben ser eliminados cuando su conservación no cumple a los fines con los que se crearon. La conservación de la información tiene que ver con las responsabilidades legales. La conservación de datos tiene que ver con la ciberseguridad.

BCU (Institución pública) - Isabel Maroñas

Comenta que en el sector financiero hay una obligación de la conservación de ciertos datos por 5 años, pero depende de los marcos regulatorios de cada organismo.

Presidencia de la República (Institución pública) - Ariel Collazo

Afirma que la conservación depende de la trascendencia de la información, ya que conservar la información también implica un costo. Si no hay una regulación específica no se conserva la información sin razón. Por eso los marcos regulatorios son tan importantes: obligan a que se hagan ciertas cosas.

Agesic (Institución pública) - Adrián Marrero

Sostiene que debe estar regulado el tema del borrado.

OEA (Institución pública) - Alexander Crowther

Comenta que en ciertos países donde se está haciendo cosas importantes, se destruyen archivos, lo que hace que sea difícil escribir la historia de los procesos o de los hechos. Todo existe en archivos digitales y casi nada en formato papel; hay que tener cuidado con este tema para preservar la historia.

CLAEH (Academia) - Graciela Cami

Explica que hay bastante regulación en algunos temas, como el de identificación digital, pero igual faltaría un poco más de

penetración. Además, se deberían establecer reglas claras en cuento a la recolección, cadena de custodia y presentación de la evidencia digital. También habría que incluir obligatoriamente en la currícula todo el tema de formación en ciberseguridad.

Además, faltaría un mecanismo articulador que permita actuar rápidamente.

BCU (Institución pública) - Isabel Maroñas

Cuenta que en el banco central se trabaja en educación financiera en algunos centros educativos, pero recién ahora se logró un convenio con CODICEN (Consejo Directivo Central de la Administración Nacional de Educación Pública) para incorporarla a la currícula. Ahora hay que operativizarlo.

Agesic (Institución pública) - Mauricio Papaleo

Subraya que el marco legal debería ser claro sobre cómo comunicar todos estos temas a nivel general. Desde Agesic se avanza, pero no se llega a toda la población. También se debe mejorar la colaboración entre el sector público y el privado, armar algo más colaborativo con recursos humanos y financieros. A veces hay una muralla de leyes que lo impide.

Añade que no hay organización que por sí sola pueda superar un incidente. Enfatiza en la importancia de armar una sinergia y colaborar sin complicaciones de por medio. Debería haber una forma de activar esos mecanismos rápidamente.

Ferrere Abogados (Sector privado) - Martín Pesce

Sostiene que las regulaciones que se están discutiendo tienen que aportar valor que se base en principios que puedan soportar el paso del tiempo. Hay que tener cuidado con la sobrerregulación, porque puede ser una barrera, limitar la innovación y la competitividad. La híper-regulación puede que nos ponga en una situación más compleja.

Pide que no se convierta solo en una “checklist”, sino que se desarrollen estrategias a conciencia.

Parlamento (Institución pública) - Darío Burstin

Indica que tal vez la legislación debería ser más basada en estándares que en reglas. Los estándares son reglas más abiertas. El control puede ser más difícil. La claridad del marco legal es fundamental.

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 planteados están validados con algunas consideraciones a los mismos:

- El marco legal, además de ser sólido y coherente como se indica en la ENC, debe ser claro y debe adaptarse a los cambios;
- Necesidad de establecer roles y responsabilidades;
- Énfasis en que el marco normativo debe basarse en estándares más que en reglas;
- Debería incluirse la gestión de riesgo;
- También debería incluirse la concientización y educación dentro del marco normativo.

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

Las personas participantes plantearon ciertas actividades para desarrollar:

Hace falta un órgano que tenga potestades propias para poder actuar rápidamente con carácter de una agencia reguladora, que le pueda dar agilidad y a su vez, sea un servicio autónomo, cuya ventaja es tener menos incidencia del poder político con presupuesto propio. Se pone como ejemplo la Agencia de Chile. Esto no quita que puedan seguir existiendo los comités asesor y operativo.

Sería importante la creación de un Observatorio de Ciberseguridad.

Generar un proceso de elaboración normativa que involucre a la diversidad de partes involucradas incluyendo una consulta pública y debida rendición de cuentas.

Hacer un análisis de impacto regulatorio.

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

Se subrayó que deberían estar involucrados los colegios de abogados y escribanos, así como la academia.

Se planteó la duda de que, más allá de que actualmente existe un comité asesor y un comité de gestión, y que Agesic coordina a los dos comités, se debería empoderar a algún órgano más. Deberían estar involucrados los colegios y las cátedras y ser liderado por Agesic.

Las acciones se ven viables en un plazo de 5 años, el tema es presupuestal. Son acciones que se pueden abrir en sub-acciones y realizar al menos algunas. Para ello sería importante contar con indicadores.

En cuanto al orden de las acciones se menciona que se debería priorizar a la primera línea de acción (“Definir los niveles, organizaciones y responsabilidades para la gobernanza a nivel Estratégico, Operativo y Sectorial”) del primer objetivo.

Subgrupo 4

- Moderadora: Nancy Ibarra, Agesic.
- Relatora: Marcelo Castillo y Mauro Parada, ICD
- Participaron 10 (diez) personas de 8 (ocho) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

En esta primera ronda se discutió acerca del pilar “Gobernanza y marco normativo” tal como planteado en la propuesta borrador.

URUDATA (Institución privada)- José Callero

Destacó que los pilares de la estrategia están definidos de manera demasiado estanca, sugiriendo que deberían ser más generales, centrándose en temas como la generación de confianza y de capacidades, y sobre esos conceptos avanzar. Señaló la dificultad de generar confianza cuando los objetivos son abordados por diferentes entidades, y recomendó definir objetivos transversales con líneas de acción más claras y específicas. Subrayó la necesidad de una base que describa la situación actual para saber qué se necesita para alcanzar los objetivos propuestos. Sugirió que las líneas de acción deberían ser más concretas y detalladas, alineadas con un "norte estratégico", y propuso ampliar la descripción de los objetivos de gestión para incluir una visión estratégica clara.

BCU (Institución pública) - Daniel Fernández

Expresó que existe un protocolo y un departamento especializado, pero destacó la falta de aplicación y de competencias jurisdiccionales, señalando que esto debe ser abordado a través del sistema judicial. Subrayó que, en muchos casos de fraude, el delincuente es alguien cercano a la víctima, lo que complica la situación. Comentó que todas las compañías trabajan con un porcentaje de fraude previsto y equilibran la inversión en ciberseguridad con los costos del fraude. Enfatizó la importancia de una coordinación efectiva y centralizada, sugiriendo que Agesic debería ser la entidad encargada, con capacidad de hacer cumplir y suficientes recursos. Además, mencionó las dificultades legales, como el secreto bancario, que complican la colaboración entre bancos.

CEIBAL (Institución pública) - Isabel Fernández

Consideró importante observar lo que ocurre en otros países para definir si la estrategia nacional está en consonancia con prácticas internacionales. Sugirió realizar un relevamiento para determinar el punto de partida y el nivel de madurez en ciberseguridad del país. También destacó la importancia de identificar y asegurar los recursos necesarios, ya que a veces los órganos regulatorios carecen de los recursos para funcionar adecuadamente, como en el caso de las sanciones. Finalmente, enfatizó que deberían existir mecanismos y medidas concretas para cumplir con los objetivos de gestión, incluyendo la prevención y el manejo de crisis.

UAIP (Institución pública) - Mariel Lorenzo

Propuso la inclusión de un glosario para aclarar términos y hacer el documento accesible para todos. Expresó dudas sobre la capacidad del Estado uruguayo de abordar adecuadamente la supraterritorialidad en ciberseguridad y cuestionó el entendimiento de la ciberseguridad como objetivo de gestión. Consideró que la seguridad debe ser un objetivo en sí misma, bien definido y medible, y que las líneas de acción deberían enfocarse en cómo implementar este marco administrativo. Además, subrayó la importancia de utilizar un lenguaje claro y comprensible, y sugirió revisar términos como "datos informáticos" y "sólido" en el contexto jurídico. También resaltó la necesidad de considerar la privacidad y la transparencia de la información, y cuestionó la pertinencia de términos como "ciberresiliencia". También, destacó que es esencial que todos los organismos estatales incluyan la ciberseguridad en su planificación y que se definan claramente las normas y regulaciones necesarias.

Agesic (Institución pública) - Gonzalo Sosa

Comentó sobre la reciente Ley 20.212, la cual establece una nueva estructura en seguridad e información, incluyendo nuevas obligaciones para organismos públicos, la creación de la Dirección de Ciberseguridad y un registro nacional de incidentes de seguridad. También mencionó que hay muchas disposiciones que aún están pendientes de reglamentación y que actualmente existen documentos disgregados. Sugirió que el marco normativo debería estar bien definido y separado de las líneas de acción para no condicionarlas, además de aclarar el alcance y a quiénes impacta el marco. También destacó la necesidad de unificar y clarificar los términos relacionados con el marco legal y regulatorio.

BID (Institución pública) - María Inés Vázquez

Señaló la necesidad de actualizar y ampliar el marco normativo de ciberseguridad para incluir conceptos como la supraterritorialidad, que actualmente no están bien representados en los pilares del documento. Además, subrayó la importancia de involucrar a actores judiciales y fiscales en el desarrollo del marco normativo, ya que son fundamentales para la aplicación de las regulaciones relacionadas con cibercrimen y ciberdelitos. También sugirió que para integrar la ciberseguridad

como un objetivo de gestión, se deben considerar ajustes presupuestarios y administrativos específicos, prefiriendo el término "marco administrativo" sobre "marco regulatorio". Además, destacó la mayor rapidez del sector privado en implementar medidas de seguridad y propuso que la gobernanza debería ser el objetivo principal, compuesto por actores, recursos y mecanismos claros, posiblemente gestionado por un organismo organizacional dedicado. Finalmente, recomendó incluir una línea de acción detallada que explique cómo poner en marcha y medir los objetivos de gestión, con una guía de implementación específica.

UDELAR (Academia) - María José Viega

Destacó que Uruguay ha avanzado en la institucionalización y creación de un marco jurídico para la ciberseguridad, con entidades como la Dirección de Ciberseguridad de Agesic, el Ministerio de Defensa, y Antel, entre otros. Sin embargo, señaló la necesidad de mejorar en áreas críticas como la salud y la implementación de criptografía, donde la firma electrónica avanzada no se utiliza ampliamente. También mencionó la importancia de la guía de ciberseguridad sectorial, que no está suficientemente integrada en la estrategia general. Resaltó la urgencia de abordar los ciberdelitos, la falta de adhesión al Convenio de Budapest, y la necesidad de crear efectivamente el comando conjunto de ciberdefensa, como establecido en el decreto 271/020. Además, insistió en la importancia de definir mecanismos de coordinación y fortalecer los procedimientos de comunicación existentes, especialmente en el contexto del CERTuy. Subrayó que la línea de base de la estrategia debería incluir la institucionalidad existente, aunque reconoció el problema global de falta de técnicos especializados en ciberseguridad.

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

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

Se recalcó la necesidad de definir claramente los objetivos y las acciones asociadas, estableciendo una visión estratégica coherente.

También se recomendó, en el objetivo de “Establecer la gobernanza nacional de ciberseguridad (...)”, agregar una visión más estratégica de lo que se quiere, y alinear todas las líneas de acción establecidas en gobernanza, marco regulatorio y en objetivos de gestión, debajo de esa visión integral de gobernanza e institucionalidad.

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

Se recomendaron varias acciones:

- Línea de base y roles: Realizar un relevamiento para establecer una línea de base, redefinir roles y responsabilidades, y establecer mecanismos de coordinación.
- Fortalecimiento del CERTuy: Es importante fortalecer al CERTuy y otros sectores relacionados.
- Recursos y capacitación: Identificación de la falta de técnicos y recursos humanos, con propuestas de acuerdos con instituciones educativas para la capacitación.

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

En la Ronda 2 se consideró pertinente priorizar las siguientes acciones:

- Definir los mecanismos de coordinación estableciendo una gobernanza clara que incluya actores, normas y recursos necesarios.
- Proponer un marco legal y normativo adecuado y actualizado, incluyendo la privacidad y el acceso a la información.
- Desarrollar líneas de acción prácticas y detalladas para la implementación efectiva del marco normativo.

Para ello, será necesario

- Hacer un relevamiento de la normativa de la institución a corto plazo: compilarla, elaborar una definición de la nueva institucionalidad, determinar la brecha a cubrir, y fortalecer los mecanismos que ya existen para optimizar recursos.
- Establecer la ciberseguridad como objetivo de gestión, teniendo en cuenta que es un bien organizacional, y estableciendo organizaciones tanto públicas como privadas, y trabajar el concepto de cómo se mide la ciberseguridad como objetivo de gestión dentro de las organizaciones, estableciendo un marco administrativo de cómo se lleva adelante, qué se mide y cómo.
- Elaborar un glosario con los conceptos importantes, como “marco sólido”, “resiliencia”, “supraterritorialidad”, “ciberespacio”, entre otros.
- Destinar recursos.