Mesa de trabajo "Cibercrimen"

Autor

Agesic

Fecha de creación

08/10/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la séptima mesa de trabajo "**Cibercrimen**" 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 21 de junio se realizó el análisis del pilar “Cibercrimen” de la Estrategia. 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 el Conocimiento. Martín Albornoz, Joaquin Carega, Nicolás Correa, Sebastián Gómez, Sebastián González, Adolfo Nidegger, Bruno Olivera, Natalí Paggiola.

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

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

BROU (Institución pública), Banco de la República Oriental del Uruguay. Antonio Rodríguez, Marcelo Varaldi.

CSIRT (Institución pública), Equipo de Respuesta ante Emergencias Informáticas – Chile. Cristian Bravo.

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

DIPN (Institución pública), Dirección de Investigaciones de la Policía Nacional. Paulo Rocha.

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

GLOBANT (Sector privado), Guillermo García.

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

MI (Institución pública), Ministerio del Interior. Javier Jaureguiberry, Saúl Scanziani.

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

Poder Judicial (Institución pública), Diovanet Olivera.

UCU (Academia), Universidad Católica del Uruguay. Julio Lens, Sandra Silveira.

UM (Academia), Universidad de Montevideo. Martín Pecoy.

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

Resumen del intercambio

A continuación se presenta el informe general de la mesa de trabajo “Cibercrimen” 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 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 “Cibercrimen”.

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 Cibercrimen?

Educación y cultura

Hay una percepción prioritaria de la educación y cultura de la ciberseguridad en general.

Se percibió el tema de la cultura y la educación como transversal a toda la Estrategia, ya que sin ellas no es posible avanzar en ciberseguridad. Se consideró importante que se generen los espacios para que la educación sea transversal. La educación dará sus frutos a largo plazo, por lo que es un tema urgente para enfrentar los desafíos de ciberseguridad futuros, especialmente a medida que las tecnologías sigan creciendo con rapidez.

Se necesitan campañas para que la gente conozca lo que supone la ciberdelincuencia a todo nivel. La ciudadanía debe saber cómo, cuándo y dónde denunciar y que los órganos que deben dar respuesta la provean adecuadamente.

Se remarcó la necesidad de generar una cultura en materia de ciberseguridad para las empresas, ya que la percepción del riesgo no es alta y no hay conciencia hasta después de ocurrido un ciberataque.

Capacitación de todos los actores

Se resaltó la importancia de desarrollar las capacidades de la Estrategia. Se puso especial énfasis en sensibilizar y educar a los decisores para lograr que se destinen recursos a cuestiones de ciberseguridad.

Se reconoció la necesidad de concientización de todos los actores, como por ejemplo los magistrados. También se señaló que los parlamentarios no poseen la educación especializada necesaria para legislar y requieren capacitación además de asesoramiento de expertos.

Es necesaria la educación en las primeras líneas de batalla, es decir, en las comisarías.

La capacitación legal es imprescindible: actualmente no se conoce cómo recoger evidencia y a la hora de proveer evidencia válida se pierde, o se deteriora. La Policía y la Defensa deberían ser los líderes en la cuestión.

Falta capacitación y recursos en las Fiscalías y en el Poder Judicial. Hoy en día los jueces, quienes en definitiva son los que tienen que autorizar los procedimientos, no saben incorporar la evidencia digital.

Definición de niveles estratégicos

Se destacó la importancia de definir diferentes niveles de trabajo: el nivel estratégico, el nivel práctico y el nivel operativo. Además, se añadió que estos niveles deben implementarse a nivel nacional y a nivel internacional, considerando casos de otros países para aprender.

Cooperación internacional

Otro punto relevante teniendo en cuenta que el ciberdelito es internacional es la regulación de la cooperación jurídica internacional, especialmente para el cibercrimen.

Es importante tener en cuenta que el cibercrimen rompe fronteras.

Si bien hay convenios y tratados firmados entre países, al no tener una normativa interna que regule, sucede que cuando piden

cooperación a Uruguay no puede brindarse porque no hay regulación interna que aclare los procedimientos, y viceversa, Uruguay no puede pedir asistencia.

Se sugirió incluir una línea de acción para alinearse con estándares internacionales como NITS, ETSO o ISO (con normas como la ISO 27037 y 27042 que brindan buenas prácticas para el manejo de evidencia digital) en el combate al cibercrimen.

Coordinación y cooperación interna

La coordinación y la cooperación también tuvieron su foco: las actividades deben de estar coordinadas considerando que hay competencias que aplican a más de una temática. Se considera que en este pilar falta una referencia explícita al pilar de "Gobernanza", donde se expresan ideas concretas para definir competencias, responsabilidades y mecanismos de interacción.

Se destacó la necesidad de mejorar la coordinación y cooperación institucional, especialmente con la fiscalía, y se subrayó la importancia de establecer estándares y una organización adecuada, ya que el flujo de información es actualmente inadecuado y las unidades están desorganizadas.

Se resaltó la cooperación entre entes del Estado y otros actores. Se deben de coordinar los esfuerzos de acuerdo a los diferentes niveles mencionados y con actores nacionales e internacionales.

Se subrayó que el ámbito privado puede aportar insumos y material, y es fundamental crear un ámbito de intercambio que fortalezca a todos. El intercambio de información entre los privados y el sector público es imprescindible: se deben implementar canales o plataformas que permitan realmente ese intercambio.

Marco normativo

Se destacó la importancia de desarrollar un debido marco regulatorio para que la Estrategia funcione de forma óptima.

Ante todo, para poder implementar efectivamente la Estrategia, es necesario contar con un marco regulatorio que ampare a los actores involucrados y a la Estrategia en sí misma – es decir, es necesario tipificar. Para tipificar se debe conocer qué es un delito informático, cuál es la realidad de lo que está sucediendo en el entorno digital. No alcanza con importar modelos de otros países, sino que hay que asegurarse de que correspondan a la realidad criminológica del país.

Se señaló que la legislación debe tener en cuenta también los intereses de los ciberdelincuentes para ser efectiva.

Hubo preocupación por la falta de regulación de Internet. Deberían surgir leyes más específicas de ciberseguridad para que no se tengan que utilizar leyes generales de funcionalidad comparativa. También se planteó que debe legislarse el desbloqueo compulsivo de dispositivos electrónicos.

Respecto al proyecto de ley que está en el Parlamento desde agosto de 2021, se señaló que le falta la parte procesal, como la creación del Registro de ciberdelincuentes. Además, se resaltó que cuando salga ya va a haber quedado atrasado.

Recolección y gestión de datos

La información debe estar sistematizada.

Prevención

Se resaltó la necesidad de trabajar en la prevención y poner estándares mínimos como exigencia.

Se comentó que la prevención no solo se da a través de la educación formal, sino que también a través de ciertos actores que ya pasaron por el sistema educativo y no acceden a los recursos y conocimientos. En este contexto, la parte presupuestal cobra gran importancia para llegar a actores que no tienen el mismo acceso a mecanismos de protección y educación. Se destacó a las pymes como este tipo de actores que se encuentran en mayor vulnerabilidad.

Glosario

Se destacó la necesidad de que haya un glosario con definiciones de los distintos términos.

Repeticiones y solapamiento

Se propuso revisar algunas repeticiones que se dan a lo largo de la Estrategia, manifestándose que hay solapamiento entre los pilares. También se subrayó que los temas tratados son muy amplios, y falta bajarlos a tierra.

Protección de los derechos de las personas

Se expresó que la propuesta debe centrarse en proteger los derechos de las personas.

Diversidad de impactos

Es importante tener en cuenta el impacto diferencial que tiene el cibercrimen en distintos sectores de la población: hay estadísticas mundiales que muestran que el cibercrimen incide diferencialmente según el género, la edad y la orientación sexual, entre otras categorías.

Seguimiento y monitoreo

Se entendió fundamental definir el seguimiento y monitoreo de la estrategia y que sea independiente del gobierno, que se le dé continuidad y a su vez que se midan los resultados.

Laboratorio forense, Fiscalía especializada y cadena de custodia

Se sugirió crear una Fiscalía especializada con el objetivo de, entre otros, cuidar adecuadamente la cadena de custodia de la evidencia digital.

La cadena de custodia debe estar incluida en una metodología general forense, dentro de un marco. En la Estrategia se da una propuesta de crear un Laboratorio Forense pero hay que definir cuál es la comunidad que atenderá. Además, exige un grado de inversión y capacitación elevado y, ante todo, implica reconocer la brecha entre la realidad y la posibilidad de concretar. Debe abarcar a todos los actores que toman contacto con indicios o evidencias.

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

En esta parte, se les preguntó a los y las participantes: ¿Qué aspectos específicos de cibercrimen creen que podrían mejorar el abordaje del pilar “Cibercrimen”?

En general, hubo consenso alrededor de los objetivos y líneas de acción del pilar de cibercrimen. Algunos de los aportes específicos son los siguientes:

Precisión de las propuestas

Se felicitó la iniciativa, considerándola un buen punto de partida y una estrategia general amplia que abarca varios pilares importantes. Sin embargo, los comentarios acerca de su grado de precisión y alcance fueron mixtos.

Por un lado, se criticó la superficialidad del contenido, señalando la falta de profundidad en la definición de términos y en la concreción de la estrategia y el marco normativo. Es necesario definir el idioma de la Estrategia, y se requieren precisiones para que se pueda traducir mejor a iniciativas. Se ofreció el ejemplo de la propuesta de creación del Laboratorio Forense, señalando que hay que identificar lo que va a poder atender, y también lo que va a contener. Se tendrá que retrabajar el texto y hacer precisiones.

Por otro lado, se sugirió mantener el pilar en una perspectiva general, ya que ser abarcativo en varias cuestiones específicas es contraproducente a la urgencia del tema. Las especificaciones deben de concretarse más adelante.

También se comentó que se podrían destacar otras dimensiones dentro del enfoque de cibercrimen, como la defensa de los derechos humanos y de la soberanía.

Además, se señaló que se deben identificar correctamente los actores para cada línea de acción. Se destacó la importancia de evaluar el impacto de las exigencias y requisitos en los diferentes actores: es común pensar en base a los problemas de aquellos más grandes como los bancos, sin percibir la realidad de otros actores como las pymes, que no cuentan con las mismas capacidades.

Cibercrimen: ¿pilar o eje transversal?

Hubo una discusión sobre si el cibercrimen debería ser un pilar o un tema transversal. Por un lado, se argumentó que debería ser un pilar debido a la importancia y especificidad del combate del cibercrimen. Actualmente en Uruguay, el marco regulatorio no está definido, por lo que marcar el cibercrimen como pilar enfatiza la urgencia del tema a nivel nacional y la necesidad de crear un marco regulatorio. Además, la educación mostrará resultados a largo plazo, por lo que es razonable tener el cibercrimen como pilar hasta que otros pilares como el de Cultura y Ecosistema cobren mayor fuerza, ya que no se puede esperar que los actores actúen por su propia voluntad. Darle este valor al cibercrimen fomenta la colaboración y la participación de los diferentes actores.

Por otro lado, se defendió que mientras que la inclusión del cibercrimen en la Estrategia es crucial, es un tema muy amplio que la Estrategia no podrá cubrir en su totalidad y tendrá necesariamente que recurrir a otras herramientas. El cibercrimen necesita de normativa, protección de datos, colaboración entre actores, educación, y muchos otros aspectos que lo vuelven un eje transversal a todos los otros pilares de la Estrategia.

Se sostuvo que los elementos constitutivos para la Estrategia son el marco regulatorio, la capacitación y concientización, y la

protección de los derechos, mientras que cibercrimen es un aspecto específico que cruza transversalmente todos los otros temas fundamentales. El debate finalizó en un consenso donde se decidió que actualmente, debido al contexto de Uruguay (específicamente la ausencia de marco regulatorio que integre el cibercrimen), tiene sentido que el cibercrimen se mantenga como un pilar en la Estrategia, ya que le enfatiza la importancia y urgencia del tema. Se espera que para ediciones futuras de la Estrategia Uruguay ya cuente con adelantos en este marco regulatorio sobre cibercrimen, por lo que podría pasar a ser un eje transversal en vez de un pilar.

Formación

La formación para todos y en forma continua es fundamental, y la actualización es clave.

Quienes legislan tienen que mantenerse actualizados. Debe haber un especialista trabajando constantemente con los legisladores, brindando un asesoramiento más dinámico. Es de suma importancia legislar rápido.

Se recalcó que desde la magistratura no se sabe cómo tratar el tema de las nuevas tecnologías. La norma no puede regular todo, pero tiene que dar una pauta. Los funcionarios judiciales necesitan contenido sustantivo y procesal para poder operar.

Aunque existe una oferta educativa en ciberseguridad, falta atraer talento, incluyendo profesionales de otras áreas como el derecho. Se abogó por desarrollar una industria de software seguro en Uruguay y posicionar la industria de ciberseguridad a nivel nacional. Se mencionó la importancia de formar ciberdiplomáticos.

Colaboración

El tema de colaboración con los organismos debería conformar un subtítulo entero aparte, ya que es muy abarcativo. Se propusieron tres líneas de acción para subdividir la cuestión de colaboración:

- una primera línea que establezca acuerdos referidos a lo que son las agencias de cibercrimen, (Interpol, por ejemplo);
- una segunda línea que refiera a la colaboración con el sector privado dado que mucho del apoyo de la investigación de ciberdelitos depende del aporte de este sector (interactuar con Google, con Meta);
- una tercera línea que suele denominarse “comunidad de ciberinteligencia”, que mantenga actualizados los avances y las mediciones (incluyendo incidentes, previsiones y respuestas tanto en lo estatal como en lo privado). Un organismo del tipo del CERTuy podría coordinar la comunidad.

Se deben desarrollar protocolos, siguiendo los marcos de trabajo que ya hay.

Presupuesto

Hay que determinar presupuesto. Se propuso que el financiamiento sea un objetivo en sí mismo dentro de cibercrimen.

Se señaló que el sistema acusatorio debe estar preparado para enfrentar el cibercrimen con suficiente financiación.

Declaración de incidentes

Hay que planificar lineamientos para poder comunicar incidentes.

Hay mucho secretismo en el reporte de incidentes por el impacto que puede tener revelarlos, entonces hay que lograr que se comparta la información al menos parcialmente. Debería haber un plan de comunicación o una ley que disponga plazos obligatorios para declarar vulneraciones y filtraciones. Para ello se requeriría un CSIRT nacional que maneje toda esa información y la haga circular.

Se propuso que el intercambio de información sea un objetivo en sí mismo.

Convenio de Budapest

Con respecto al Convenio de Budapest, se sugirió que debería haber una revisión, debido a que la tecnología cambia velozmente. Sin embargo, más allá de que haya críticas sobre el mismo, se resaltó que está funcionando, por lo que es importante ratificarlo. Se recalcó la necesidad de fortalecerlo mediante recursos y capacitación a la Unidad de Cibercrimen.

Se recomendó no mencionar la adhesión al Convenio en la introducción, sino que implementar los puntos necesarios para adherirse.

Marco normativo

Se destacó que es necesaria la tipificación de ciertos delitos que no pueden faltar, citando como ejemplos los delitos de suplantación de identidad y fraude cibernético. Su subrayó que hay que incorporar en un marco regulatorio la colaboración

internacional y la colaboración intrainstitucional local.

También se propuso que, además de la ley, tendría que existir un Comité Técnico que revise cada seis meses y actualice.

Como aspiración a futuro, se sostuvo que es indispensable llevar adelante una reforma procesal. En ella habría que incorporar la regulación legal de la cadena de custodia de la evidencia digital y abordar las garantías individuales. Se deben prevenir los perjuicios irreparables protocolizando la gestión de la evidencia. Se debe establecer hasta cuándo se conservan las evidencias. Es esencial contemplar también la protección de derechos frente a una agresión sexual. El tratamiento del ciberdelito no debería ser asimilable al tratamiento de los delitos físicos: hay que establecer procedimientos específicos.

Sistema de denuncias

Se debe contemplar la necesidad de establecer un sistema de denuncias, un canal lo más amigable posible (podría ser un 0800 o una aplicación), y que este canal alimente a una Fiscalía especializada que lidere la investigación. A través de esa actividad ésta podrá ir actualizando periódicamente los protocolos de intervención.

Reportes periódicos

Deban realizarse reportes periódicos, tal vez anualmente, que evidencien cuáles son los peligros para poder así actualizar la respuesta a los delitos prevalentes en un momento dado.

Fraude

Se mostró preocupación por delitos de fraude a través de plataformas como Marketplace o Mercado Libre. Además de los altos niveles de captación, es muy difícil de detectar, no existe regulación de fraude específica, no hay protocolos determinados y no hay una cultura de denunciar este tipo de crímenes. A la vez, las denuncias a veces no se concretan. Por este motivo, es crucial la regulación no solo en cuestiones de delitos informáticos, sino también para definir protocolos y procedimientos. El aumento del comercio electrónico aumenta la vulnerabilidad de las personas. Estas vulnerabilidades deben ser tratadas de forma específica a través de verticales.

A la vez, se resalta la necesidad de la educación financiera y de cibercrimen para prevenir este tipo de delitos.

Protección de los derechos de las personas

Se sugirió agregar la frase “con foco a la protección de los derechos de las personas” en algunas líneas de acción de cibercrimen.

Se comentó que en ciertos casos de intercambio de información de algunos delitos se manejan números de teléfono, datos de identidades, y otras cuestiones sensibles. Se debe poner el foco en la protección de la privacidad de la víctima.

Laboratorio forense

Se celebró la iniciativa del laboratorio forense digital. Sin embargo, hay que asegurarse de que se utilice adecuadamente, y hay que definir precisamente sus objetivos y competencias.

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

La segunda mitad 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 en el pilar “Cibercrimen”.

Se recalcó la importancia del cibercrimen como pilar de la Estrategia.

De manera general, se aprobaron los objetivos planteados, y se apoyó su carácter amplio para tratar los diversos temas planteados.

Se subrayaron algunos desafíos:

- Se señaló que hay un desfasaje entre la evolución de la tecnología, los delitos informáticos, y la normativa.
- También se subrayó que se deben mejorar las estrategias de atracción de talento. Se sugirió desarrollar mecanismos para atraer talento de otras profesiones, como por ejemplo el Derecho.
- Se resaltó que en el proyecto de ciberdelitos falta la parte procesal y operativa.

- También falta una política de priorización de los cibercrímenes.

Para atender estas carencias, es importante aprender de las experiencias de otros países.

Por otro lado, se propusieron algunas modificaciones:

Se sugirió que el primer objetivo (“Desarrollo de las capacidades relativas al cibercrimen”) debería enmarcarse en una ley específica de ciberdelito en vez de ser un objetivo general dentro de la Estrategia. Esto se debe a que requiere de varias cuestiones específicas que quizá no puedan abordarse de manera total a través de la Estrategia. En la Estrategia se debería de hacer referencia a la importancia de este objetivo, pero sin abordarlo.

También se propuso añadir el desarrollo y fortalecimiento del marco regulatorio como objetivo para darle la importancia y urgencia que merece. Sin un marco regulatorio es difícil abordar el resto de los objetivos y líneas de acción.

Se comentó que debería de existir algún organismo que tenga las capacidades de ente regulador en materia de cibercrimen, ya que hay esfuerzos de múltiples actores diferentes que capaz no encuentran punto de unión para coordinar y colaborar. En base a esta idea, se propuso un nuevo objetivo: “Identificar una institución que sea un ente coordinador de los esfuerzos de cibercrimen y fomentar su crecimiento”. De crearse este objetivo, habría que analizar la normativa, ya que actualmente AGESIC es el responsable por ley, pero el tema a tratar es demasiado amplio para que AGESIC pueda cumplir este rol en su totalidad.

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

Se sugirieron algunas modificaciones en la redacción, y se plantearon acciones para implementar.

Las modificaciones sugeridas fueron las siguientes:

Introducción al pilar

- En la introducción al pilar, evitar la palabra “inminente” y sustituirla por “impostergable”: “Es impostergable abordar el combate al cibercrimen de forma proactiva y colaborativa.”

Objetivo 1

- En la descripción del objetivo 1, se argumentó que se debería quitar la parte sobre el proceso de adhesión del convenio, y colocarlo como línea de acción. A su vez, se debe identificar lo que falta para la adhesión e implementarlo.
- En la línea de acción i del Objetivo 1, además de “investigación y gestión”, que implica ya combatir el problema del cibercrimen, deberían de también incluirse la “detección y prevención” como capacidades que deben generarse en etapas anteriores.
- En la línea de acción ii del Objetivo 1, se debería agregar: “hacer hincapie en la cooperacion internacional.” Se subrayó que en el convenio de Budapest está prevista la obligatoriedad de la cooperación con los actores privados. Aún se debe resolver eso en Uruguay.
- Respecto a la línea de acción iii del Objetivo 1, se sostuvo que las “carreras de especialización vinculadas a la temática” no es el mejor enfoque, ya que les da mucha prioridad a las carreras cuando hay otros públicos de importancia que también deben de ser capacitados, como los altos cargos y la población.
- Se propuso agregar una cuarta línea de acción sobre alineación con estándares internacionales en la temática (por ejemplo, NIST, ISO, ETSI). Este estándar debe ser coordinado y compatible con los demás países.

Objetivo 2

- En la línea de acción i del Objetivo 2 (“Establecer un laboratorio nacional de forense digital que brinde servicios”), borrar “a la comunidad”. Debe brindar servicios al sistema de justicia, con independencia técnica y protección legal de sus técnicos, y en colaboración con la academia. También se debe establecer una política de priorización de incidentes y delitos.
- Respecto a este laboratorio, se sugirió corregir “forense”, reemplazándolo por “forensia”.
- También se propuso agregar las estrategias de apoyo a las víctimas del cibercrimen como una línea de acción, ya que no se encuentran contempladas. El “apoyo” incluiría la orientación, prevención y apoyo posterior como asesoramiento. Esta idea fue un punto de debate, ya que otras personas participantes consideraron que el apoyo a las víctimas es un aspecto de cultura más que de cibercrimen.
- También se sugirió definir una línea de acción respecto al fortalecimiento de una fiscalía especializada en cibercrimen, añadiéndose que su funcionamiento se verá facilitado y mejorado si se establece por ley. Sin embargo, se advirtió sobre la delicadeza del tema, ya que la amplitud de los posibles ciberdelitos lleva a que el abordaje y trabajo de cada delito sea

muy diferente; por lo tanto, habría que ver si el rol recaería totalmente en un único actor como la fiscalía especializada o en diferentes canales.

Además de las propuestas mencionadas directamente vinculadas a ciertos objetivos y líneas de acción, surgieron las siguientes ideas para integrar y considerar en el pilar sobre cibercrimen.

Laboratorio forense

Se cuestionó su necesidad ya que en Uruguay existen muchos laboratorios muy importantes, pero finalmente se reconoció la importancia de la creación del laboratorio forense como ente unificador. Sin embargo, debe quedar explícito a qué público está dirigido y se deben definir precisamente las cuestiones que atenderá.

Capacitación en el Poder Judicial y en el Poder Legislativo

Se recalcó la necesidad de dotar al Poder Judicial de colaboradores y equipos independientes de la Policía, haciendo hincapié en que a veces la investigación queda en manos poco profesionalizadas. Se subrayó que debería existir un ente regulador con sistemas de control que estén sujetos a revisión.

Se recomendó realizar capacitaciones hacia funcionarios parlamentarios y jurídicos. Se destacó la importancia de llevar los temas de ciberseguridad al Poder Legislativo con las visiones de todos los actores que han participado en estas Mesas de Diálogo.

Necesidad de regulación

Se resaltó la necesidad de regular, es decir:

- Falta una tipificación,
- Falta una ratificación del Convenio de Budapest,
- Falta una clara determinación de cómo vamos a hacer para cooperar internacionalmente y cómo vamos a cooperar inter-institucionalmente en lo local.

Respecto a la regulación de cibercrimen, se comentó que existen distintas categorizaciones. Por ejemplo, la clasificación de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) divide a los ciberdelitos en tres tipos:

- Tradicionales: Delitos que se cometían antes de Internet y que ahora también se cometen a través de Internet, pero la escala en la que se cometen no ha crecido debido al nuevo canal. El fraude es un ejemplo de esto.
- Transicionales: Delitos que se cometían antes de Internet y que ahora también se cometen a través de Internet, pero la escala en la que se cometen sí ha crecido debido al nuevo canal. Los delitos de contenido sexual son ejemplo de esto.
- Digitales: Delitos que no existían antes de Internet, por lo que son digitales propiamente dicho. El phishing es un ejemplo de esto.

Se comentó que se debe comenzar a identificar todo lo que pueda ser definido como “ciberdelito” y luego jerarquizarlo en base al impacto y al riesgo.

Disponibilidad de información

Se discutió mucho acerca de la disponibilidad y el manejo de la información: se debe determinar quién la maneja, para quién, cuándo, y cómo. A partir de eso se podrá determinar la tipificación y proceder a investigaciones.

Necesidad de un campo estadístico

Se necesita un campo estadístico aplicado a esta materia, porque en definitiva antes incluso de tipificar, una adecuada medición de esta criminalidad sería esencial. También es esencial la periodicidad con la cual se brinda la información: se propuso establecer un reporte anual para medir cada agresión y poder reorganizar los esfuerzos según la criminalidad preeminente en cada momento concreto.

Sistematización de las denuncias

También se consideró clave la sistematización de las denuncias: se debe determinar un mecanismo, un canal sencillo para que todos los ciudadanos puedan recibir respuestas. Los asuntos deben tener seguimiento; se les debe brindar la solución y una resolución a su caso.

Creación de una Fiscalía especializada y de un Observatorio de cibercrimen

Se vio necesaria la creación de un Fiscalía especializada. Sería un modo de profesionalizar el tratamiento de estas cuestiones, no solamente en lo inmediato sino a posteriori con el desarrollo de futuras capacidades y resiliencias que el propio Estado debe ir conformando. Se deben ir formando protocolos propios para cada delito, lo que va a ayudar a su vez en investigaciones posteriores.

También se sugirió crear un Observatorio de cibercrimen, incluyendo a la academia.

Tratamiento de la evidencia digital

Respecto al punto del tratamiento de la evidencia digital, la reforma procesal es clave para brindar mecanismos hábiles y garantistas. No existe actualmente una cadena de custodia de la evidencia digital determinada y clara. Esto debe establecerse.

Concientización

No es posible conformar todo este ecosistema sin una adecuada concientización. Esto es clave en todos los ámbitos: en la academia, en los propios órganos del Estado. Se propuso que quizás la Fiscalía especializada o el CSIRT podría cumplir esa función, o se podría implementar un esfuerzo coordinado entre ambos. Todos debemos ser conscientes para poder denunciar, y que esas denuncias a su vez encaminen procedimientos de investigación más ordenados.

Incentivos al sector privado

Se trajo a la mesa la necesidad de encontrar el debido incentivo para el sector privado. En base a esto, se mencionó establecer una certificación en ciberseguridad que sirva como beneficio, u ofrecer exoneraciones impositivas.

También se propuso implementar una exigencia de requisitos mínimos de seguridad en licitaciones públicas de productos y dispositivos tecnológicos.

Finalmente, se recomendó hacer más explícito el enfoque de apuntar a la capacidad de resiliencia frente al cibercrimen.

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

La mayoría de las mesas no llegó a evaluar este punto, pero se subrayó que es necesario hacer un análisis previo de los actores involucrados.

Como posibles actores, se mencionó al Poder Legislativo (para que pueda entender las necesidades y consideraciones técnicas) y, dentro del Poder Ejecutivo, a AGESIC. La industria y la sociedad civil también deberían participar.

Además, se propuso lo siguiente por escrito:

Objetivo 1: los actores serían la academia, Presidencia, los sectores privados, la policía, la Fiscalía, el Poder Judicial, la comunidad legal y el gremio.

Objetivo 2: los actores serían la academia, la educación no formal, Presidencia, el Ministerio de Economía y Finanzas, el Ministerio del Interior, Fiscalía y el Poder Judicial.

Anexo

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

Subgrupo 1

- Moderadora: Natalia Salazar, Agesic.
- Relatora: Marta Susana Manent, ICD.
- Participaron 11 (once) 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

Agesic (Institución pública) - Natalí Paggiola

Expresa que la propuesta debe centrarse en proteger los derechos de las personas. Entiende fundamental definir el seguimiento y monitoreo de la estrategia y que sea independiente del gobierno, que se le dé continuidad y a su vez que se midan los resultados.

Agrega que la cadena de custodia debe estar incluida en una metodología general forense, dentro de un marco. Señala que en la Estrategia se da una propuesta de crear un Laboratorio Forense pero que hay que definir cuáles la comunidad que atenderá.

MI (Institución pública) - Saúl Scanziani

Manifiesta que le costó entender los “Pilares” del borrador porque notó mucho solapamiento. Propone dividir las iniciativas porque supone que en cada pilar habrá especializaciones, y se pregunta cómo generar iniciativas en cada Pilar específico. Considera que se tratan muchos ítems y le suenan muy amplios: habría que bajarlos a tierra.

GLOBANT (Sector privado) - Guillermo García

Menciona como muy importante el tema de la cooperación. Considera que el ámbito privado puede aportar insumos y material. Manifiesta que es fundamental crear un ámbito de intercambio que fortalezca a todos, tanto al sector público como al sector privado. Señala, con respecto a los parlamentarios, que no poseen la educación especializada necesaria para legislar y requieren capacitación además de asesoramiento de expertos. Se necesitan campañas para que la gente conozca lo que supone la ciberdelincuencia a todo nivel. Enfatiza que es necesaria la educación en las primeras líneas de batalla, es decir, en las comisarías donde los policías tienen que comprender la diferencia entre un robo de un objeto físico y un robo o sustracción digital y tener las herramientas para abordar esa situación particular. Considera que, así como a las empresas privadas se les exigen ciertas certificaciones, a los organismos del Estado también debería exigírseles el cumplimiento de ciertos estándares que aseguren cierto grado de seguridad. Por último, opina que desde ciertos sectores privados y también los públicos es necesario generar ámbitos de intercambio de información y conocimientos para solucionar estas falencias.

BID (Institución pública) - Ariel Nowersztern

Comenta que hace más de un año hubo una ronda de consultas con Fiscalía y el Ministerio del Interior, y se concluyó que faltaban capacidades operativas para atender al flujo de casos que llegaran con un cierto nivel de calidad. Para lograr esto, una de las iniciativas que se propuso fue la creación de un Laboratorio Forense. Sin embargo, esto exige un grado de inversión y capacitación elevado y, ante todo, implica reconocer la brecha entre la realidad y la posibilidad de concretar.

Comenta que otro aspecto importantísimo que se debe tener en cuenta en esta sección, si bien también ha sido tratado en otros pilares, es el impacto diferencial que tiene el cibercrimen en distintos sectores de la población: hay estadísticas mundiales que muestran que el cibercrimen incide diferencialmente según el género, la edad y la orientación sexual, entre otras. Debería contemplarse esto en la Estrategia. Por último, enfatiza la importancia de la recolección y gestión de datos. Al plantear la Estrategia, hay que tratar de que sea sistematizada y que mejore lo que ya hay: sin datos será muy difícil lograrlo.

BROU (Institución pública) - Marcelo Varaldi

Manifiesta que los Pilares son muy valiosos, aunque se solapan y habría que ver cómo se vinculan unos con otros. Le parece que presentar el cibercrimen y la ciberdefensa como cuestiones recientemente incorporadas es contraintuitivo y que debería tomarse en cuenta lo preexistente. Ambas deberían ser la vertical porque en definitiva de lo que se está tratando es sobre crimen local e internacional. Hace notar que la mayoría de los ataques son contra las personas. Manifiesta que la capacitación legal es un problema que debería resolverse porque no se conoce cómo recoger evidencia y a la hora de proveer evidencia válida se pierde, o se deteriora. La Policía y la Defensa deberían ser los líderes en la cuestión.

BID (Institución pública) - Ariel Nowersztern

Comenta que una Estrategia Nacional debe tratar de abordar el problema de todas las maneras posibles, pero que esto es un desafío porque hay muchas aristas y visiones según los actores que se involucren. Sostiene que lo bueno de los procesos de co-creación como éste es que permite ver más en profundidad, porque el tema es multidimensional.

UM (Academia) - Martín Pecoy

Coincide con lo manifestado. Comenta que hay áreas que necesitan fortalecimiento. Sostiene que la concientización no se puede llevar a cabo sin una unidad específica que se dedique a difundir para que la población entienda que fue víctima, lo que en muchas oportunidades no ocurre y por ello no se recopilan evidencias y cuando se llega a una causa judicial no hay posibilidad alguna de intervención. Enfatiza que lo previo es: tipificar. Sostiene que no alcanza con importar modelos espectaculares que no se adecuan a la realidad criminológica del país. Entiende que en ese sentido una Fiscalía especializada puede resultar útil y necesaria, y contribuiría a cuidar adecuadamente la cadena de custodia de la evidencia digital. Señala que es deber del Estado tener esto regulado y actualizado en cada una de las instancias. Agrega que los desafíos cambian diariamente y es menester realizar una periódica revisión de las figuras penales y de los procederes en Fiscalía. Resalta que la legislación debe tener en cuenta también los intereses de los ciberdelincuentes para ser efectiva. Opina que cada uno de esos focos son importantes en los distintos momentos de la legislación, tanto en la tipificación como en el seguimiento y eventualmente en la condena.

Con respecto al ecosistema, si bien lo entiende focalizado en esas unidades de gestión especializadas, también reconoce la necesidad de concientización de todo el resto de los actores, como por ejemplo los magistrados. Respecto a la educación, estima que debe haber un plan de divulgación a partir de la ley, porque hay que impulsar una campaña para que la ciudadanía sepa cómo, cuándo y dónde denunciar y que los órganos que deben dar respuesta la provean adecuadamente. Puntualiza que hay un proyecto de ley en el Parlamento desde agosto de 2021, que contiene una tipificación conforme al Convenio de Budapest y contiene también la creación de una campaña de educación. Le falta, sin embargo, la parte procesal, como la creación del Registro de ciberdelincuentes, aunque sí contempla la creación de la Fiscalía especializada. Asimismo, propone que, entre otras medidas procesales, debe legislarse el desbloqueo compulsivo de dispositivos electrónicos, tema que hoy en Uruguay no es posible discutir ya que todavía no se sabe ni siquiera cómo envolver un dispositivo incautado para preservarlo.

BCU (Institución pública) - Daniel Fernández

Manifiesta que coincide con la propuesta como un marco general. Considera que las carencias vienen desde lo normativo, así como también de la educación tanto a nivel usuario como a nivel académico. Indica que, aunque se ha avanzado, falta capacitación y recursos en las Fiscalías y en el Poder Judicial.

Agesic (Institución pública) - Martín Albornoz

Expresa que coincide con todo lo que se ha manifestado y remarca que hay un problema con el Proyecto de ley que se trata desde 2021 puesto que si aún no salió, para cuando salga ya va a haber quedado atrasado. Subraya que lo que está aportando en estas mesas debe ser llevado a la práctica. Sostiene que el intercambio de información entre los privados y los públicos es imprescindible: se deben implementar canales o plataformas que permitan realmente ese intercambio.

Poder Judicial (Institución pública) - Diovanet Olivera

Comparte lo que se ha manifestado. Destaca como uno de los principios de esta propuesta la visión integral para abordar todos los problemas, que tienen que ver con la defensa, con la seguridad, con el cibercrimen, y con la educación. Se deben armonizar las visiones e integrar a todos los actores, incluyendo a la academia y a los operadores judiciales. Le parece de suma importancia la especialización a nivel judicial y de fiscalías para generar capacitación de los operadores judiciales. Reconoce que hoy los jueces no saben incorporar la evidencia digital. El avance tecnológico es vertiginoso y se les hace difícil mantenerse actualizados. Por lo tanto, la capacitación es fundamental. Agrega que, si bien es necesaria la capacitación en la policía y las fiscalías, no se puede dejar afuera de la capacitación a los jueces que en definitiva son los que tienen que autorizar los procedimientos. Señala que para tipificar es necesario conocer qué es un delito informático, cuál es la realidad de lo que está sucediendo en el entorno digital. Agrega que otro punto relevante teniendo en cuenta que el ciberdelito es internacional es la regulación de la cooperación jurídica internacional, especialmente para el cibercrimen, porque si bien hay convenios y tratados firmados entre países, al no tener una normativa interna que regule, sucede que cuando piden cooperación a Uruguay no puede brindarse porque no hay regulación interna que aclare los procedimientos, y viceversa, Uruguay no puede pedir asistencia.

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

Agesic (Institución pública) - Natalí Paggiola

Manifiesta que la formación para todos y en forma continua es fundamental, y la actualización es clave.

MI (Institución pública) - Saúl Scanziani

Sugiere que el tema de colaboración con los organismos debería conformar un subtítulo entero aparte, ya que es muy abarcativo. También recalca que hay que determinar presupuesto. Propone que el financiamiento sea un objetivo en sí mismo dentro de cibercrimen. Propone tres líneas de acción para subdividir la cuestión de colaboración:

- una primera línea que establezca acuerdos referidos a lo que son las agencias de cibercrimen, (Interpol, por ejemplo);
- una segunda línea que refiera a la colaboración con el sector privado dado que mucho del apoyo de la investigación de

ciberdelitos depende del aporte de este sector (interactuar con Google, con Meta);

- una tercera línea que suele denominarse ‘comunidad de ciberinteligencia”, que mantenga actualizados los avances y las mediciones (incluyendo incidentes, previsiones y respuestas tanto en lo estatal como en lo privado). Sugiere que un organismo del tipo del CERTuy debería coordinar la comunidad.

Se deben desarrollar protocolos, siguiendo los marcos de trabajo que ya hay. Menciona que el tema “compliance” es un punto a desarrollar puesto que eso indica en qué hace falta capacitación. Es fundamental priorizar la capacitación.

GLOBANT (Sector privado) - Guillermo García

Sobre la declaración de incidentes, destaca que hay mucho secretismo en el reporte de incidentes por el impacto que puede tener revelarlos, entonces hay que lograr que se comparta la información al menos parcialmente. Esto ocurre sobre todo en el sector privado. Debería haber un plan de comunicación. Comparte el ejemplo de lo que sucede en Chile, donde la ley impone que dentro de las 48 horas de ocurrido un incidente que afecte estructuras críticas hay que dar un informe mínimo y a las 72 horas un informe más profundo. Entiende que es necesario salir del secretismo y hacerse responsable de la vulneración o la filtración que ocurra. Para ello la información tiene que circular, por lo que se requiere un CSIRT nacional que maneje toda esa información.

Considera que quienes legislan tienen que mantenerse actualizados. Debe haber un especialista trabajando constantemente con los legisladores, brindando un asesoramiento más dinámico. Resalta de imperiosa necesidad legislar rápido.

BID (Institución pública) - Ariel Nowersztern

Indica que es necesario definir el idioma de la Estrategia, porque queda muy general, y se requieren precisiones para que se pueda traducir mejor a iniciativas. Ofrece el ejemplo de la propuesta de creación del Laboratorio Forense, señalando que hay que identificar lo que va a poder atender, y también lo que va a contener. Entiende que se va a tener que retrabajar el texto y hacer precisiones.

BROU (Institución pública) - Marcelo Varaldi

Se pregunta si respecto del Convenio de Budapest sigue siendo un objetivo adoptarlo como legislación dentro de la Estrategia Nacional, considerando que tiene que ver con cuestiones de hace 25 años. Entiende que tendría que haber una revisión; la tecnología cambia velozmente y la legislación tendría por ello que ser flexible. Aparte de la ley, tendría que existir un Comité Técnico que revise cada seis meses y actualice.

UM (Academia) - Martín Pecoy

Aporta un esquema de 5 ordinales que son los siguientes:

1. Con respecto al Convenio de Budapest, más allá de que haya críticas sobre el mismo, resalta que es el que hay y está funcionando, por lo que es importante ratificarlo. Menciona que hay también un Tratado en la ONU con un enfoque más actualizado. Ve necesario su fortalecimiento con recursos y capacitación a la Unidad de Cibercrimen.

2. Entiende que es necesaria la tipificación de ciertos delitos que no pueden faltar, citando como ejemplos los delitos de suplantación de identidad y fraude cibernético. Considera que hay que incorporar en un marco regulatorio la colaboración internacional y la colaboración intrainstitucional local.

3. Se debe contemplar la necesidad de establecer un sistema de denuncias, un canal lo más amigable posible (podría ser un 0800 o una aplicación), y que este canal alimente a una Fiscalía especializada que lidere la investigación. A través de esa actividad ésta podrá ir actualizando periódicamente los protocolos de intervención.

4. Propone que deban realizarse reportes periódicos, tal vez anualmente (quizá podría encargarse de esto el CSIRT) que evidencien cuáles son los peligros para poder así actualizar la respuesta a los delitos prevalentes en un momento dado.

5. Como aspiración a futuro, entiende indispensable llevar adelante una reforma procesal. Estima que en ella hay que incorporar la regulación legal de la cadena de custodia de la evidencia digital, cómo conservar y reproducir esta evidencia; abordar las garantías individuales, y abrir el camino para que las fuerzas del orden tengan acceso a la evidencia digital. Se deben prevenir los perjuicios irreparables protocolizando la gestión de dicha evidencia. También se debe establecer hasta cuándo se conservan las evidencias, porque la conservación tiene un costo. Entiende esencial contemplar también la protección de derechos frente a una agresión sexual. Discrepa con el criterio de que el tratamiento del ciberdelito es asimilable al tratamiento de los delitos “analógicos” o físicos y opina que hay que establecer un procedimiento específico.

Agesic (Institución pública) - Martín Albornoz

Propone que el intercambio de información sea un objetivo en sí mismo ya que aporta al monitoreo. También es importante tener en cuenta que el cibercrimen rompe fronteras. Señala que en ciertos casos de intercambio de información de algunos delitos se manejan números de teléfono, datos de identidades, y otras cuestiones sensibles y pregunta qué puede hacerse para proteger la privacidad de la víctima. Al mismo tiempo subraya que debe determinarse lo que se hace con la evidencia. Respecto

a la comunicación de incidentes, plantea que es necesario que se establezca su obligatoriedad. Entiende que hay que planificar lineamientos para poder comunicar incidentes.

Poder Judicial (Institución pública) - Diovanet Olivera

Plantea que desde la magistratura no se sabe cómo tratar el tema de las nuevas tecnologías, y ejemplifica con un caso en el que intervino recientemente donde se había ordenado videovigilancia a una casa con un dron, y tuvo que limitarlo porque entendió que el grado de intrusión que el dron provocaba era asimilable a un allanamiento. Reconoce que la norma no puede regular todo, pero enfatiza el hecho de que da una pauta y que los funcionarios judiciales necesitan contenido sustantivo y procesal para poder operar.

Parte 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

Por falta de tiempo, se salteó puntualizar sobre este eje, considerándose que ya se lo había tratado en la primera ronda. Se recalcó la importancia del cibercrimen como pilar de la Estrategia.

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

Se plantearon actividades y acciones para el pilar “Cibercrimen”, detalladas a continuación según ejes temáticos:

Laboratorio forense

Acerca del laboratorio forense, se consideró que debe quedar explicitado a qué público está dirigido. Se cuestionó su necesidad ya que en Uruguay existen muchos laboratorios muy importantes. Se debe definir precisamente las cuestiones que atendería.

Poder Judicial

Se recalcó la necesidad de dotar al Poder Judicial de colaboradores y equipos independientes de la Policía, haciendo hincapié en que suele haber mucha ingenuidad y no llega a detectarse que hay intereses espurios detrás de ciertos temas cuya investigación queda en manos poco profesionalizadas. Se subrayó que debería existir un ente regulador con sistemas de control que estén sujetos a revisión.

Necesidad de regulación

Se resaltó la necesidad de regular, es decir:

- Falta una tipificación,
- Falta una ratificación del Convenio de Budapest,
- Falta una clara determinación de cómo vamos a hacer para cooperar internacionalmente y cómo vamos a cooperar inter-institucionalmente en lo local.

Disponibilidad de información

Se discutió mucho acerca de la disponibilidad y el manejo de la información: se debe determinar quién la maneja, para quién, cuándo, y cómo. A partir de eso se podrá determinar la tipificación y proceder a investigaciones.

Sistematización de las denuncias

También se consideró clave la sistematización de las denuncias: se debe determinar un mecanismo, un canal sencillo para que todos los ciudadanos puedan recibir respuestas. Los asuntos deben tener seguimiento; se les debe brindar la solución y una resolución a su caso.

Necesidad de un campo estadístico

Se necesita un campo estadístico aplicado a esta materia, porque en definitiva antes incluso de tipificar, una adecuada medición de esta criminalidad sería esencial. También es esencial la periodicidad con la cual se brinda la información: se propuso establecer un reporte anual para medir cada agresión y poder reorganizar los esfuerzos y que el ecosistema se oriente a alguna criminalidad preeminente en cada momento concreto.

Creación de una Fiscalía especializada

Se vio necesaria la creación de la Fiscalía especializada. Sería un modo de profesionalizar el tratamiento de estas cuestiones, no solamente en lo inmediato sino a posteriori con el desarrollo de futuras capacidades y resiliencias que el propio Estado debe ir conformando. Se deben ir formando protocolos propios para cada delito, lo que va a ayudar a su vez en investigaciones posteriores.

Tratamiento de la evidencia digital

Respecto al punto del tratamiento de la evidencia digital, la reforma procesal es clave para brindar mecanismos hábiles y garantistas. No existe actualmente una cadena de custodia de la evidencia digital determinada y clara. Esto debe establecerse.

Concientización

Por último, no es posible conformar todo este ecosistema sin una adecuada concientización. Esto es clave en todos los ámbitos: en la academia, en los propios órganos del Estado. Se propuso que quizás la Fiscalía especializada o el CSIRT podría cumplir esa función, o se podría implementar un esfuerzo coordinado entre ambos. Todos debemos ser conscientes poder denunciar, y que esas denuncias a su vez encaminen procedimientos de investigación más ordenados.

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

En esta mesa no se evaluaron los actores. Sin embargo, la participante Natalí Paggiola (Agesic – institución pública) propuso lo siguiente por escrito:

Objetivo 1: los actores serían la academia, Presidencia, los sectores privados, la policía, la Fiscalía, el Poder Judicial, la comunidad legal y el gremio.

Objetivo 2: los actores serían la academia, la educación no formal, Presidencia, el Ministerio de Economía y Finanzas, el Ministerio del Interior, Fiscalía y el Poder Judicial.

Subgrupo 2

- Moderadora: Fabiana Santellán, Agesic.
- Relatora: Sofía Lopes, 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

URCDP (Institución Pública) - Flavia Baladan

Resalta la importancia de desarrollar las capacidades de la Estrategia, haciendo hincapié en la educación. Cree que las actividades deben de estar coordinadas considerando que hay competencias que aplican a más de una temática.

También destaca que se deben definir diferentes niveles estratégicos de trabajo: el nivel estratégico, el nivel práctico y el nivel operativo.

Nombrando la línea de acción iii del Objetivo 2 del Pilar “Gobernanza y Marco Normativo”, comenta que hay que revisar algunas repeticiones que se dan a lo largo de la Estrategia.

Agesic (Institución pública) - Sebastián González

Se enfoca en la educación como línea de acción transversal a cibercrimen, mediante campañas de concientización de cibercrimen.

Concuerda con la importancia de definir diferentes niveles estratégicos de trabajo. También resalta la importancia de la cooperación entre entes del Estado y otros actores.

UCU (Academia) - Sandra Silveira

Remarca la necesidad de generar una cultura en materia de ciberseguridad para las empresas, ya que la percepción del riesgo no es alta y no hay conciencia hasta después de ocurrido un ciberataque. También está de acuerdo con que se deben definir los tres niveles estratégicos de trabajo.

Opina que, si bien el marco normativo está previsto en la Estrategia, Uruguay se encuentra atrasado en el tema. Este tipo de normativa es una premisa para poder implementar cualquier Estrategia; debe haber una forma de amparar a los actores involucrados y a la Estrategia en sí misma. Resalta la necesidad de trabajar en la prevención y poner estándares mínimos como exigencia.

Agesic (Institución pública) - Nicolás Correa

Ve importante que se generen los espacios para que la educación sea transversal. La educación dará sus frutos a largo plazo, por lo que es un tema urgente para enfrentar los desafíos de ciberseguridad futuros, especialmente porque los problemas relacionados al cibercrimen aumentarán a medida que las tecnologías sigan creciendo con rapidez. Destaca la necesidad de elaborar un glosario.

Además, concuerda con la importancia de definir diferentes niveles estratégicos de trabajo.

BCU (Institución pública) - Isabel Maroñas

Percibe el tema de la cultura y la educación como transversal a toda la Estrategia, ya que sin ellas no es posible avanzar en ciberseguridad. Pone especial énfasis en sensibilizar y educar a los decisores para lograr que se destinen recursos a cuestiones de ciberseguridad.

Concuerda con que se deben definir un nivel estratégico, un nivel práctico y un nivel operativo, y añade que estos niveles deben ser a nivel nacional y a nivel internacional, considerando casos como el de Costa Rica para aprender.

MIEM (Institución pública) - María José Franco

Muestra preocupación por la falta de regulación de Internet. Entiende que la regulación total no es posible y no espera eso, pero sí busca que surjan leyes más específicas de ciberseguridad para que no se tengan que utilizar leyes generales de funcionalidad comparativa.

Comenta que la prevención no solo se da a través de la educación formal, sino que también a través de ciertos actores que ya pasaron por el sistema educativo sin recibir concientización, y ahora no acceden a los recursos ni a los conocimientos. En este contexto, la parte presupuestal cobra gran importancia para llegar a actores que no tienen el mismo acceso a mecanismos de

protección y educación. Destaca las PYMES como este tipo de actores que se encuentran en mayor vulnerabilidad.

Coincide con la necesidad de que haya un glosario con definiciones de los distintos términos.

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

En general, hubo un consenso de que los Objetivos y líneas de acción del pilar de cibercrimen son correctos. Algunos de los aportes específicos son los siguientes:

MIEM (Institución pública) - María José Franco

Percibe como crucial que se identifiquen correctamente los actores para cada línea de acción. Además, apoya mantener el pilar en una perspectiva general, ya que ser abarcativo en varias cuestiones específicas es contraproducente a la urgencia del tema. Las especificaciones deben de concretarse más adelante.

UCU (Academia) - Sandra Silveira

Comenta que se podrían destacar otras dimensiones dentro del enfoque de cibercrimen, como la defensa de los derechos humanos y de la soberanía.

Sin embargo, otros participantes de la mesa le responden que esto ya se encuentra integrado a la Visión y Principios rectores de la ENC, por lo que sería repetitivo.

URCDP (Institución Pública) - Flavia Baladán

Encuentra importante evaluar el impacto de las exigencias y requisitos en los diferentes actores, ya que es común pensar en base a los problemas de aquellos más grandes como los bancos, sin percibir la realidad de otros actores como las pymes, que no cuentan con las mismas capacidades.

Varias personas participantes mostraron preocupación por delitos de fraude a través de plataformas como Marketplace o Mercado Libre. Además de los altos niveles de captación, es muy difícil de detectar, no existe regulación de fraude específica, no hay protocolos determinados y no hay una cultura de denunciar este tipo de crímenes. A la vez, la denuncia a veces no se concreta porque las víctimas no quieren proporcionar los datos personales calificados como evidencia o porque no se encuentra estandarizado qué datos son relevantes como evidencia. Por este motivo, es crucial la regulación no solo en cuestiones de delitos informáticos, sino también para definir protocolos y procedimientos en el marco de lo procesal. A la vez, se resalta la necesidad de la educación financiera y de cibercrimen para prevenir.

MI (Institución pública) - Javier Jaureguiberry

Recuerda que existen muchos aspectos vinculados al cibercrimen que se deben considerar, no solo el fraude.

MIEM (Institución pública) - María José Franco

A raíz de esta preocupación por el fraude, comenta que el aumento del comercio electrónico aumenta la vulnerabilidad de las personas. Estas vulnerabilidades hay que tratarlas de forma específica a través de verticales.

Sostiene que el cibercrimen, en vez de ser un pilar, debería ser un tema transversal. Defiende que mientras que la inclusión del cibercrimen en la Estrategia es crucial, es un tema muy amplio que la Estrategia no podrá cubrir en su totalidad y tendrá necesariamente que recurrir a otras herramientas. El cibercrimen necesita de normativa, protección de datos, colaboración entre actores, educación, y muchos otros aspectos que lo vuelven un eje transversal a todos los otros pilares de la Estrategia. Además, Uruguay se encuentra en un contexto donde está evaluando su adhesión al Convenio de Budapest, que regula el cibercrimen y será una de estas herramientas que fortalecerán el funcionamiento de la Estrategia. Por lo tanto, no le encuentra sentido que sea un pilar propio, y cree que debería de encontrarse en la Estrategia de forma general y transversal; otras herramientas del marco regulatorio uruguayo deberían de encargarse de los detalles del cibercrimen que permitan abarcarlo en su totalidad.

MI (Institución pública) - Javier Jaureguiberry

Manifiesta su desacuerdo con este punto y sostiene que el cibercrimen debe ser un pilar, remarcando la importancia y la especificidad del combate contra el cibercrimen.

UCU (Academia) - Sandra Silveira

Comenta que, actualmente, Uruguay se encuentra en un contexto en el cual el marco regulatorio no está definido, por lo que marcar el cibercrimen como pilar enfatiza la urgencia del tema a nivel nacional y la necesidad de crear un marco regulatorio.

A la vez, comenta que la educación mostrará resultados a largo plazo, por lo que es razonable tener el cibercrimen como pilar hasta que otros pilares como el de Cultura y Ecosistema cobren mayor fuerza, ya que no se puede esperar que los actores actúen por su propia voluntad, sino que se requiere de exigencia con correspondiente apoyo.

URCDP (Institución Pública) - Flavia Baladán

Comparte que darle este valor al cibercrimen fomenta la colaboración y la participación de los diferentes actores.

CSIRT Chile (Institución pública) - Cristian Bravo

Cree que los elementos constitutivos para la Estrategia son el marco regulatorio, la capacitación y concientización, y la protección de los derechos, mientras que cibercrimen es un aspecto específico que cruza transversalmente todos los otros temas fundamentales. Como ya hay un pilar que aborda el marco normativo dentro de la Estrategia y la concientización también está presente de forma transversal, cuestiona el alcance del cibercrimen como pilar. Sin embargo, en consideración del estado actual de Uruguay mencionado en la Mesa, donde aún no hay un marco regulatorio, ve positiva la iniciativa de darle un nivel de pilar al cibercrimen, ya que le daría un nivel prioritario a la regulación del cibercrimen.

Agesic (Institución pública) - Sebastián González

Si bien opina que debería ser un pilar, también comenta que tiene que encontrarse transversalmente en las líneas de acción del pilar de Cultura y Ecosistema.

El debate finalizó en un consenso donde se decidió que actualmente, debido al contexto en el cual Uruguay no cuenta con un marco regulatorio que integre el cibercrimen, tiene sentido que el cibercrimen se mantenga como un pilar en la Estrategia, ya que le enfatiza la importancia y urgencia del tema, potenciando así la regulación del cibercrimen. Se espera que para ediciones futuras de la Estrategia Uruguay ya cuente con adelantos en este marco regulatorio sobre cibercrimen, por lo que el cibercrimen podría pasar a ser un eje transversal en vez de un pilar.

CSIRT Chile (Institución pública) - Cristian Bravo

Sugiere agregar la frase “con foco a la protección de los derechos de las personas” en algunas líneas de acción de cibercrimen. Lo comenta en base al caso de Chile, donde información fue hecha pública sin salvaguardar la privacidad y los derechos de las personas.

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

De manera general, se aprobaron los objetivos planteados, y se apoyó su carácter amplio para tratar los diversos temas planteados.

Se sugirió que el primer objetivo (“Desarrollo de las capacidades relativas al cibercrimen”) debería enmarcarse en una ley específica de ciberdelito en vez de ser un objetivo general dentro de la Estrategia. Esto se debe a que requiere de varias cuestiones específicas que quizá no puedan abordarse de manera total a través de la Estrategia. Sin embargo, en la Estrategia se debería de hacer referencia a la importancia de este objetivo, pero sin abordarlo.

También se propuso añadir el desarrollo y fortalecimiento del marco regulatorio como un objetivo para darle la importancia y urgencia que merece. Sin un marco regulatorio es difícil abordar el resto de los objetivos y líneas de acción.

Se comentó que debería de existir algún organismo que tenga las capacidades de ente regulador en materia de cibercrimen, ya que hay esfuerzos de múltiples actores diferentes que capaz no encuentran punto de unión para coordinar y colaborar. En base a esta idea, se propuso un nuevo objetivo: “Identificar una institución que sea un ente coordinador de los esfuerzos de ciberseguridad y fomentar su crecimiento”. De crearse este objetivo, habría que analizar la normativa, ya que actualmente Agesic es el responsable por ley, pero el tema a tratar es demasiado amplio para que Agesic pueda cumplir este rol en su totalidad.

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

Se hicieron aportes sobre dos líneas de acción:

- Línea de acción i del Objetivo 1: Además de “investigación y gestión”, que implica ya combatir el problema del cibercrimen, deberían de también incluirse la “detección y prevención” como capacidades que deben generarse en etapas anteriores.
- Respecto a la línea de acción iii del Objetivo 1, se sostuvo que las “carreras de especialización vinculadas a la temática” no es el mejor enfoque, ya que les da mucha prioridad a las carreras cuando hay otros públicos de importancia que también deben de ser capacitados, como los altos cargos y la población, que deberían de contar con la educación necesaria para poder identificar cuestiones de cibercrimen como fraude o phishing.
- También se propuso agregar las estrategias de apoyo a las víctimas del cibercrimen como una línea de acción, ya que no se encuentran contempladas. El “apoyo” incluiría la orientación, prevención y apoyo posterior como asesoramiento. Esta idea fue un punto de debate, ya que otras personas participantes consideraron que el apoyo a las víctimas es más un

aspecto de cultura que de cibercrimen.

- También se sugirió definir una línea de acción en apoyo al fortalecimiento de una fiscalía especializada en cibercrimen, añadiéndose que si el establecimiento de una fiscalía especializada en cibercrimen se da por ley, su funcionamiento se verá facilitado y mejorado. Sin embargo, se advirtió sobre la delicadeza del tema, ya que la amplitud de los posibles ciberdelitos, que pueden ir desde extorsión por fraude hasta delitos por contenido sexual, llevan a que el abordaje y trabajo de cada delito sea muy diferente; por lo tanto, habría que ver si el rol recaería totalmente en un único actor como la fiscalía especializada o en diferentes canales.

Se destacó la importancia de la creación del laboratorio forense como ente unificador.

Además de las propuestas mencionadas directamente vinculadas a ciertos objetivos y líneas de acción, surgieron las siguientes ideas para integrar y considerar en Cibercrimen.

Respecto a la regulación de cibercrimen, se comentó que existen distintas categorizaciones. Por ejemplo, la clasificación de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) divide a los ciberdelitos en tres tipos:

- Tradicionales: Delitos que se cometían antes de Internet y que ahora también se cometen a través de Internet, pero la escala en la que se cometen no ha crecido debido al nuevo canal. El fraude es un ejemplo de esto.
- Transicionales: Delitos que se cometían antes de Internet y que ahora también se cometen a través de Internet, pero la escala en la que se cometen sí ha crecido debido al nuevo canal. Los delitos de contenido sexual son ejemplo de esto.
- Digitales: Delitos que no existían antes de Internet, por lo que son digitales propiamente dicho. El phishing es un ejemplo de esto.

Se comentó que se debe comenzar a identificar todo lo que pueda ser definido como “ciberdelito” y luego jerarquizarlo en base al impacto y al riesgo. Por ejemplo, si es un riesgo al país, riesgo a empresa o riesgo a la persona.

También se destacó la colaboración y coordinación como aspectos fundamentales debido a la cantidad de actores involucrados.

Se recomendó hacer más explícito el enfoque de apuntar a la capacidad de resiliencia frente al cibercrimen.

Se hizo hincapié en establecer garantías dentro de la regulación procesal para que haya un equilibrio.

Además, se trajo a la mesa la necesidad de encontrar el debido incentivo para el sector privado. En base a esto, se comentó sobre la certificación de la ciberseguridad en EE.UU. como un estándar que funciona como beneficio, y se mencionó ofrecer exoneraciones impositivas como beneficio.

Finalmente, todos destacaron la importancia de llevar los temas de ciberseguridad al Poder Legislativo con las visiones de todos los actores que han participado de estas Mesas de Diálogo.

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

No se llegó a trabajar este punto.

Subgrupo 3

- Moderadora: Mariana Ferraro, Agesic.
- Relatora: Mauro Parada, ICD.
- Participaron 8 (ocho) personas de 6 (seis) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Agesic (Institución pública) - Adolfo Nidegger

Destaca la necesidad de mejorar la coordinación y cooperación institucional, especialmente con la fiscalía, y subraya la importancia de establecer estándares y una organización adecuada, ya que el flujo de información es actualmente inadecuado y las unidades están desorganizadas. También enfatiza la crucial necesidad de abordar la financiación. Sugiere incluir una línea de acción para alinearse con estándares internacionales como NITS y ETSO en el combate al cibercrimen, y señala que el sistema acusatorio debe estar preparado para enfrentar el cibercrimen con suficiente financiación. Adicionalmente, enfatiza la importancia de atacar a delincuentes de alto perfil y menciona que el Poder Legislativo debería estar involucrado en este proceso.

BROU (Sector privado) - Antonio Rodŕiguez

Resalta la importancia de la cooperación entre instituciones y observa un desfase entre el conocimiento tecnológico de los usuarios y los productos que deben usar, como los celulares, promovidos por las industrias. Señala que los usuarios no dimensionan adecuadamente los riesgos de los productos tecnológicos e identifica un problema en el tiempo que lleva desde la denuncia hasta la intervención policial, especialmente en casos de estafa.

FGN (Institución pública) - Ricardo Lackner

Critica la falta de claridad en el sistema político sobre los delitos cibernéticos y la omisión de debates cruciales sobre temas procesales y licencias de software. Sugiere cambiar "inminente" por "imprescindible" en la redacción, y enfatiza que no se puede seguir improvisando en el debate sobre cibercrimen. Apoya la creación de un laboratorio nacional de forense digital independiente y resalta la necesidad de una obligación de denunciar incidentes graves. Insiste en definir claramente los delitos informáticos y lamenta la falta de legislación adecuada en materia de ciberseguridad. Además, subraya la importancia de usar los recursos eficientemente y propone adoptar un modelo de especialización en crímenes cibernéticos similar al de otros países.

UCU (Academia) - Julio Lens

Felicita el borrador, considerándolo un buen punto de partida y una estrategia general amplia que abarca varios pilares importantes. Sin embargo, critica la superficialidad del contenido, señalando la falta de profundidad en la definición de términos y en la concreción de la estrategia y el marco normativo. Enfatiza que no hay políticas públicas sin costos y subraya la importancia del financiamiento adecuado. Destaca la necesidad de contar con peritos informáticos, ya que muchos delitos tradicionales se cometen a través de medios informáticos, y ambos tipos de delitos deben legislarse en paralelo. Además, resalta la importancia de la cooperación internacional, mencionando problemas prácticos como la falta de incautación de dispositivos electrónicos durante detenciones.

LACNIC (Sociedad civil) - Graciela Martínez

Subraya la importancia de diferenciar entre la comunicación entre organizaciones y la gestión de evidencia, y aboga por una estrategia clara y sencilla con proyectos e indicadores específicos y presupuesto adecuado. Destaca la necesidad de cooperación internacional y capacitación en ciberseguridad para abogados y el sistema judicial, señalando atrasos en procesos judiciales y la falta de peritos informáticos. Expresa preocupación por el aumento de incidentes cibernéticos y sugiere enfocarse en abordar el cibercrimen proactivamente. Recomienda no mencionar la adhesión al Convenio de Budapest en la introducción, sino implementar los puntos necesarios para adherirse. Propone aprovechar la experiencia internacional; enfatiza la importancia de la educación y cultura en la estrategia, y resalta que el Estado debe exigir requisitos mínimos de seguridad en sus licitaciones para evitar problemas de malware.

Agesic (Institución pública) - Joaquín Carega

Menciona que algunos incidentes no se denuncian a la policía porque no se consideran delitos. Señala la incertidumbre sobre si ciertos incidentes serán judicializables debido a la falta de claridad sobre su naturaleza delictiva y los responsables, además de la ausencia de una cadena de custodia rigurosa. Destaca que, en ocasiones, se interviene en incidentes que finalmente no son manejados por la policía. Propone extender la línea de acción para que el proyecto de adhesión al Convenio de Budapest sea más exhaustivo.

CUTI (Sector privado) - Ana Lucero

Señala la necesidad de una definición precisa de infraestructuras críticas para entender la relevancia de cada entidad. Destaca

que, aunque existe una oferta educativa en ciberseguridad, falta atraer talento, incluyendo profesionales de otras áreas como el derecho. Aboga por desarrollar una industria de software seguro en Uruguay y posicionar la industria de ciberseguridad a nivel nacional. Menciona la importancia de formar ciberdiplomáticos y la participación de CUTI en la ley de cibercrimen, expresando preocupaciones sobre la redacción de ciertos artículos. Pregunta cómo el ciudadano común podrá acceder al laboratorio forense digital y teme que, por falta de cultura en el ámbito, el laboratorio no se utilice adecuadamente.

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 validados, con algunas observaciones:

- Como desafío, se señaló que hay un desfasaje entre la evolución de la tecnología, los delitos informáticos, y la normativa.
- También se subrayó que se deben mejorar las estrategias de atracción de talento. Se sugirió desarrollar mecanismos para atraer talento de otras profesiones, como por ejemplo el Derecho.
- Se resaltó que al proyecto de ciberdelitos le falta la parte procesal y operativa.
- También falta una política de priorización de los cibercrímenes.
- Para atender estas carencias, es importante aprender de las experiencias de otros países.

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

Se sugirieron algunas modificaciones en la redacción, y se plantearon nuevas líneas de acción.

Las modificaciones sugeridas fueron las siguientes:

- En la introducción al pilar, evitar la palabra “inminente” y sustituirla por “impostergable”: “Es impostergable abordar el combate al cibercrimen de forma proactiva y colaborativa.”
- En la descripción del objetivo 1, se argumentó que se debería quitar la parte sobre el proceso de adhesión del convenio, y colocarlo como línea de acción. A su vez, se debe identificar lo que falta para la adhesión e implementarlo.
- Agregar una cuarta línea de acción sobre alineación con estándares internacionales en la temática (por ejemplo, NIST, ISO, ETSI) en el Objetivo 1. Este estándar debe ser coordinado y compatible con los demás países.
- En la línea de acción ii del Objetivo 1 (“Definir y establecer la forma de colaboración activa entre todos los organismos gubernamentales, autoridades locales, el sector privado y organizaciones internacionales para intercambiar información y recursos en la lucha contra el cibercrimen”), agregar: “hacer hincapie en la cooperacion internacional.” Se subrayó que en el convenio de Budapest está prevista la obligatoriedad de la cooperación de los actores privados. Hay que ver cómo se resolvería esto en Uruguay.
- En la línea de acción i del Objetivo 2 (“Establecer un laboratorio nacional de forense digital que brinde servicios”), borrar “a la comunidad”. Debe brindar servicios al sistema de justicia, con independencia técnica y protección legal de sus técnicos, y en colaboración con la academia. También se debe establecer una política de priorización de incidentes y delitos.
- Respecto a este laboratorio, se sugirió corregir “forense”, reemplazándolo por “forensia”.
- Crear un Observatorio de cibercrimen, incluyendo a la academia.
- Implementar una exigencia de requisitos mínimos de seguridad en licitaciones públicas de productos y dispositivos tecnológicos.
- Armar un esquema de diferenciación entre delito informático y delito que se realiza a través de la informática.
- Realizar capacitaciones hacia funcionarios parlamentarios y jurídicos.

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

Los actores mencionados fueron:

- Fiscalía
- Poder legislativo (para que puedan entender las necesidades y consideraciones técnicas)

- Poder ejecutivo / Agesic
- Academia, industria y sociedad civil.

Sin embargo, se subrayó que es necesario hacer un análisis previo de los actores involucrados.