Mesa de trabajo “Infraestructuras de información crítica”

Autor

Agesic

Fecha de creación

20/09/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la tercer mesa de trabajo "**Infraestructuras de información crítica**" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad del 17 de junio al 21 de junio del 2024.

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

Introducción

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

En la jornada del 18 de junio se realizó el análisis del pilar “Infraestructuras de información crítica” de la Estrategia. En este informe se detallan las propuestas y aportes compilados en las mesas de diálogo, y se presenta en forma sintética los intercambios que se dieron en esta mesa.

Participantes

Agesic (Institución pública), Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Jesús Alfonso, Joaquín Cabrera, Martín Cherro, Nicolas Correa, Sebastián Gómez, Ismael González, Eduardo Mascolo, Maximiliano Maneiro, Natalí Paggiola, Pablo Pajon, Mauricio Papaleo, Federico Beux.

ANCAP (Institución pública), Administración Nacional de Combustibles, Alcohol y Portland. Osvaldo Barrios, Patricia Márquez, Daniel Pérez.

ANTEL (Institución pública), Administración Nacional de Telecomunicaciones. Carlos Piana, Alejandro Reyna.

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

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

CERTuy (Institución pública), Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Jesús Alfonso, Víctor Blanco.

Ciberdefensa (Institución pública), Unidad de Ciberdefensa del Ejército. Pedro Gómez.

CORREO URUGUAYO (Institución pública), Javier Lago, Andrea Machado.

CSIRT CHILE (Institución pública), Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas. Cristian Bravo.

CTM (Institución pública), Comisión Técnica Mixta de Salto Grande. Álvaro Llama, Alejandro Reyes.

DGI (Institución pública), Dirección General Impositiva. Julio Montañez, Guillermo Torneyes.

DINACIA (Institución pública), Dirección Nacional de Aviación Civil e Infraestructura Aeronáutica. Gonzalo Lima.

DNA (Institución pública), Dirección Nacional de Aduanas. Santiago Madura, Darío Perla, Matías Prieto, Álvaro Salvarini.

DNIC (Institución pública), Dirección Nacional de Identificación Civil de la República Oriental del Uruguay. Cinthia Los Santos, Guillermo Lungo.

FORTINET (Sector privado), Gaston Sancassano.

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

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

MATRIZ (Sector privado), Daniel Pérez.

MDN (Institución pública), Ministerio de Defensa Nacional. Claudio López.

MGAP (Institución pública), Ministerio de Ganadería, Agricultura y Pesca del Uruguay. Marcos Chavez, Andrés Rodríguez.

MI (Institución pública), Ministerio del Interior. Javier Jaurguiberry.

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

Movistar (Sector privado), Carolina Matos, Facundo Payseé.

Presidencia (Institución pública), Ignacio Durán.

Scotiabank (Sector privado), Mercedes Gatti.

SIEE (Institución pública), Secretaría de Inteligencia Estratégica de Estado. Jorge Alliaume, Robert Figueroa.

Teledata (Sector privado), Alejandro Pereyra.

URSEC (Institución pública), Unidad Reguladora de Servicios de Comunicaciones. Luis González, Fernando Hernández, Agustín Hill, Mauro Ríos, Nelson Rodriguez.

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

VaFirma (Sector privado), Martin Fernández.

Resumen del intercambio

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

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

Parte 1. Ronda de intercambio sobre el borrador

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

Parte A. Aportes generales sobre la propuesta borrador

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

Se plantearon diversos aspectos relevantes.

Ubicación de la Estrategia en la Agenda Uruguay Digital 2025

Se sostuvo que no se debe circunscribir el tema de infraestructura critica atendiendo solamente al Objetivo X de la Agenda Uruguay Digital 2025 (“Ciberseguridad”), sino incluirlo en el Objetivo IX, Línea de acción 42: “Desarrollar redes resilientes mediante el análisis de la infraestructura crítica de telecomunicaciones, que aseguren la disponibilidad de los servicios.” Además, se discutió ampliar la definición a “comunicaciones” en vez de “telecomunicaciones”

Alcance de la ENC

Surgieron debates acerca del alcance de la ENC, en particular sobre si debiera ser un documento con mayor detalle o más general. Algunos sostuvieron que debería tener un enfoque general, macro y holístico porque definir cuestiones de forma específica lo vuelve estructurado e inflexible y el área de las tecnologías está en constante cambio y actualización. Además, un alcance general de la ENC no impide que se puedan definir indicadores y objetivos generales. Por otro lado, se cuestionó si se está preparado para un abordaje general una vez se definan las infraestructuras críticas, ya que no hay tareas previas en la definición del marco teórico ni claridad sobre el estado de las instituciones involucradas. Aunque la estrategia se lea de manera amplia, al definirse las infraestructuras críticas quizá no quede claro cómo abordar las instituciones específicas.

Se propuso una estructura con niveles: un nivel general que establezca cuestiones como el glosario y también una estructura de guía para que los actores sepan qué hacer a nivel de prevención, redacción, recuperación y defensa. Luego, especificar y desplegar estas cuestiones dentro de cada pilar. Dentro de los pilares, hay que agregar cuestiones como un glosario, principios básicos, requisitos mínimos, procesos de auditoría y funcionamiento activo de los procesos. También se deben definir los roles dentro de las líneas de acción, que especifiquen las responsabilidades de cada actor.

Necesidad de un marco regulatorio claro

Se planteó la necesidad de una ley que instrumente la estrategia, así como de un marco regulatorio más fuerte. Se propuso utilizar normas y marcos existentes como inspiración, y agregar varias regulaciones:

- Ciberdiplomacia: Conseguir tratados con países avanzados para mantener estándares de seguridad similares a los de las naciones seguras.
- Cultura y ecosistema: Incorporar una línea de acción para explorar nuevos mecanismos de financiación estatales que mejoren la ciberresiliencia en empresas y el Estado.
- Implementar una ley de ciberseguridad que contemple la criticidad de asegurar la infraestructura crítica. El concepto de seguridad debe estar incorporado desde el diseño.

Se comentó en cuanto al pilar de cibercrimen, que hay una gran carencia en la parte jurídica que debe ser abordada para completar la política y para que este tema que involucra múltiples organismos tanto públicos como privados pueda ser llevado adelante, ya que escapa a las propias funciones de AGESIC, siendo como es en todos los países, una estrategia de Estado.

Glosario y definición de las IIC

Se hizo hincapié en la necesidad de un glosario de términos para establecer definiciones en común que avalen de qué se esté hablando y no queden dudas. Muchos de los términos son muy generales y se usan indistintamente, cuando no son lo mismo. Es necesario tener un glosario común para marcar términos como ciberdefensa, ciberataque, y resiliencia, entre otros.

Además, se reiteró mucho la necesidad de definir las infraestructuras de información crítica. Se cuestionó el término “infraestructuras de información crítica”, y se planteó reemplazarlo por “infraestructuras críticas” para incluir a las infraestructuras “físicas”.

También se propuso ampliar este pilar, definiendo mejor las infraestructuras críticas y prefiriendo el término "sistemas de información crítica". En todo caso, se sostuvo que es necesario esquematizar y clarificar esta parte, especificando cuáles son las infraestructuras críticas en Uruguay y cuáles son los sistemas de información crítica que dependen de ellas.

Estas especificaciones son cruciales para asignar roles y decretar situaciones de emergencia que le permitan a los diferentes actores responsables saber cuándo deben responder. Las definiciones necesitan legitimidad de carácter de ley para que funcionen como una garantía legal antes las acciones y las consecuencias.

Inclusión de infraestructuras físicas

Respecto a la inclusión de las infraestructuras físicas, se señaló que el enfoque del borrador de la “Estrategia Nacional de Ciberseguridad de Uruguay” basa su desarrollo directamente sobre todos los aspectos que suceden en el ciberespacio, sin tener en cuenta que éste funciona dado la existencia de las infraestructuras físicas de comunicaciones, las cuales dependen a su vez de otras infraestructuras físicas esenciales. Por lo tanto, cualquier incidente de carácter físico / operativo que interrumpa el normal funcionamiento de estas infraestructuras nombradas (de comunicaciones y de abastecimiento de recursos para su funcionamiento), provocaría un colapso en cascada del ciberespacio.

Que no esté determinado, desarrollado y priorizado cada eslabón en esta “cadena”, en conjunción con los planes de acción y previsión frente a afectaciones de los mismos, hace que cualquier plan o estrategia de ciberseguridad, por mejor planificada y desarrollada que esté, quede obsoleta por el más insignificante acontecimiento. La Estrategia Nacional debe tener un enfoque integral y no limitarse solamente a sistemas informáticos.

Inventario de las IIC

Con el fin de definir e identificar a las infraestructuras de información crítica, se propuso realizar un inventario de éstas, lo que incluye identificar activos críticos y medir la criticidad de las infraestructuras en base a la criticidad de los activos. Se debe tener claro el estado actual mediante auditorías, identificar plenamente los incidentes, lograr ciertas certificaciones, y generar un programa de capacitación y concientización en ciberseguridad.

También se deben clasificar las IIC para establecer medidas de protección. Hay que tener criterios claros para definir lo que es una estructura crítica. Se sugirió que quizá la responsabilidad de definirlas podría trasladarse a cada uno de los responsables de los distintos organismos públicos o empresas privadas para que las pudieran identificar.

Se deben incluir específicamente las estructuras críticas que están relacionadas con países limítrofes, y tener en cuenta sus desafíos.

A partir de este inventario, se podrá desarrollar un BCP o estrategias de recuperación ante desastres.

Definición de actores, roles y responsabilidades, coordinación

Se recalcó la importancia de identificar los actores, definir sus roles, y especificar sur responsabilidades. Se propuso un modelo de gobernanza con responsabilidades definidas, priorizando la adopción de criterios mínimos y la creación de estándares y auditorías.

Se destacó la importancia del sector privado, y se hizo hincapié en que al incluir una mezcla de entidades privadas y públicas, debe haber mecanismos de coordinación en la relación público-privada para que sea efectiva.

Es una estrategia difícil de concretar, lo que impone la necesidad de definir quién liderará la estrategia desde el Estado. Aunque AGESIC ha iniciado el proceso y ha establecido ciertos pilares, la estrategia es demasiado grande para que AGESIC la gestione sola. Se requieren recursos jurídicos, económicos y de empoderamiento para atraer y vincular al sector privado, que a menudo carece de la capacidad financiera para implementar medidas de ciberseguridad por sí mismo. AGESIC debe proporcionar recursos, consultorías y capacidad a organismos para ayudarlos a implementar la estrategia.

También se mencionó que debe haber un responsable en cada organismo, así como centros de referencia y de respuesta.

Se remarcó que aún falta coordinación. Es necesario generar protocolos de comunicación entre los sectores de infraestructuras críticas.

Capacitación e intercambio

Es vital unir al sector, por la sinergia que se puede generar desde las capacitaciones hasta la respuesta a incidentes, al tener un común accionar entre todos. Se propuso crear un entorno común de trabajo, haciendo énfasis en la necesidad de capacitación y de intercambio. También se elogió la iniciativa de generar instancias como ésta, de diálogo entre distintos actores.

Se requiere estandarización y protocolos de comunicación. Se enfatizó que el eslabón más débil de la cadena es el humano, por lo que las capacitaciones y el trabajo en equipo son muy importantes.

Gestión de riesgos, mecanismos de prevención

Falta gestión de riesgos, planes de contingencia, manejo de incidentes, mecanismos de prevención. No está definida la matriz de riesgo, hace falta un procedimiento estandarizado.

Se comentó que el mecanismo de detección y respuestas es complicado por el tema de las pruebas.

Debe haber un Plan B y respaldos en caso de incidentes.

Fortalecimiento del monitoreo

Se deben establecer indicadores de avance y fortalecer el monitoreo.

Política de Estado, enfoque internacional

Se sostuvo que se debería agregar más información internacional en la Estrategia para quienes no están familiarizados con el tema, así como datos del Estado.

Además, para gestionar las infraestructuras, se deben adoptar programas reconocidos internacionalmente que garanticen madurez organizacional.

Esta Estrategia debería ser una política de Estado.

Trabajar en conjunto IT, OT, y software

Se detectó una disociación total entre IT y OT (tecnología de la información y tecnología operativa) que hay que subsanar. Se planteó que a nivel de diseño es importante tomar tres aspectos: IT, OT y software, en especial el desarrollo de software seguro. Se deben crear certificaciones o ir al aprendizaje en las facultades para poder incorporar la ciberseguridad en eso.

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 creen que podrían mejorarse o añadirse en el pilar “Infraestructuras de información crítica”?

Se plantearon una diversidad de aspectos a considerar y añadir en este pilar.

Presupuesto

Habría que calcular un presupuesto y un estimado de recursos humanos. Es muy importante incorporar la parte de innovación e inversión, y que sea más fácil conseguir los recursos.

Se mencionó que el presupuesto tiene que estar dentro de los planes estratégicos de las empresas públicas y privadas, porque sino no se invertirá en eso. El presupuesto no es ajeno: se necesitan recursos para todo. Hay que pensar en el sector privado como un ámbito con múltiples actores donde puede que no todos tengan la capacidad económica para financiar lo propuesto por el pilar, lo que debilitaría toda la cadena de protección de las IIC. El presupuesto debería ser concebido a nivel nacional, pero también en especial consideración del sector privado y otros actores que podrían debilitar la cadena de protección de las IIC.

Hay que priorizar la asignación de recursos y trabajar mucho en mejorar lo que hay en vez de generar iniciativas nuevas.

Hubo visiones opuestas: también se opinó que el presupuesto debe basarse en un plan de acción más detallado, y no es el momento de hacerlo. Actualmente se debe de apuntar a que la ENC y el pilar tengan un enfoque general, macro y holístico.

Prevención

Se marcó la importancia de la prevención y la relevancia de tener mecanismos de medición de impacto. Hay que hacer pruebas de qué pasa si se corta un servicio, saber quién lo puede arreglar, quién tiene ese conocimiento. Se deben implementar mecanismos de reportes porque no está contemplada la prevención.

Es importante identificar vulnerabilidades y que se vea el panorama internacional. Se debe establecer un criterio mínimo que todos tienen que cumplir. Se recalcó la necesidad de medir. Se dudó, sin embargo, si enfrentar en detalle la necesidad de prevención en la estrategia.

Plan de acción para el manejo de crisis

Habría que tener un plan de acción general para el manejo de crisis y generar una metodología de catálogo de infraestructuras críticas.

Comunicación y capacitación

También es importante fomentar el intercambio de las amenazas. En las organizaciones críticas, debe ser obligatoria la capacitación en ciberseguridad. Se recalcó la importancia de la coordinación.

Actualización constante

Los sistemas industriales están interconectados y se conciben para que duren 20 años. Es un trabajo continuo que requiere actualización constante.

Gobernanza de las infraestructuras críticas

Se debe priorizar la infraestructura crítica.

Es necesario definir una gobernanza clara de las infraestructuras críticas. Debería ser controlado por un órgano independiente. Hay riesgos que afectan a muchos sectores. Se propuso agregar el objetivo de identificar las infraestructuras críticas y priorizarlas, ya que lo que no se conoce no se puede atacar. Es necesario identificar responsables y referentes de las infraestructuras.

Se debe fortalecer el rol de los reguladores de cada sector. Se deberá potenciar la participación de los reguladores. AGESIC o un ente aparte debería lograr regular y generar planes de contingencia.

Se debe jerarquizar: se propuso llevar el área de tecnología a la altura de otras gerencias.

Roles

En el pilar se deben detallar roles claros, el alcance del tamaño de las infraestructuras y las amenazas para Uruguay; en base a estas cuestiones, definir luego qué son las infraestructuras críticas.

Se planteó la necesidad de un referente de ciberseguridad distinto de TI, pero no hubo consenso. Por un lado, se estimó que debería venir de afuera, y por otro lado, se consideró que es natural que el responsable encargado de ciberseguridad nazca en TI y que crear una gerencia específica requeriría una asignación presupuestaria.

Definición de las IIC

No hubo consenso sobre si debería de definirse qué son las infraestructuras críticas o no dentro del pilar. Se remarcó la necesidad de definir un criterio común, y se propuso determinar los sectores afectados o involucrados en las infraestructuras críticas, en vez de definir las infraestructuras críticas en sí mismas.

Dependencia entre infraestructuras críticas

Se debe establecer la dependencia entre las infraestructuras críticas y la relación que tienen, porque no es suficiente seguir buenas prácticas que hagan que el nivel de madurez en una infraestructura crítica sea muy valorable y presentable, si quien la abastece de energía, por ejemplo, no lo hace.

Transversalidad

Se cuestionó si “Infraestructuras de la información crítica” debería ser un pilar, ya que es transversal a todos los otros pilares. Es crucial que la ENC contemple las infraestructuras de la información crítica como un eje transversal.

Marco normativo

Varios participantes de la mesa hicieron referencia a que es necesaria una ley de infraestructuras críticas para que el alcance llegue a los diferentes actores de forma transversal, ya que sin obligatoriedad no se podrá involucrar efectivamente al sector privado. Es importante la legislación para que no haya matices en cuanto al ámbito de las infraestructuras críticas.

También se sostuvo que existe un marco normativo, y el mayor problema es el incumplimiento del mismo. Para mejorar el

cumplimiento se debe concientizar y educar.

Capacitación y educación

Para fortalecer y subir los niveles de madurez en las infraestructuras críticas, se debe generar mejor capacidad en la educación a todos los niveles.

Se propuso un plan de concientización para públicos y privados: se podría tener un equipo de delegados liderado por AGESIC, y no requeriría mucho presupuesto.

Gestión de riesgos

Se trajo a la mesa la necesidad de la gestión de riesgo acompañada a las infraestructuras críticas. Cuando se define el riesgo de un activo, se define que este activo tiene un dueño responsable. Hay que encontrar qué medidas de control se deberán tomar para mitigar el riesgo, con su adecuada gestión de riesgo.

Infraestructuras críticas físicas

En las infraestructuras críticas físicas es importante el tema de control de acceso. Se planteó la necesidad de simulacros y de planes de recuperación de acceso.

Interior del país y descentralización

Se enfatizó la importancia de que este pilar llegue al interior del país también, ya que muchas veces no llega este tema, pero es fundamental. Esto incluye, también, a las infraestructuras transfronterizas.

Se debe de incluir el rol de los gobiernos departamentales y explicitar las infraestructuras críticas que les corresponden si las tienen.

Sector privado

Varios participantes hicieron mención del sector privado como un actor que debe estar involucrado, pero se enfatizó que no será fácil su participación. Más allá de la necesidad de regulación, se deben pensar incentivos para el sector privado. Hay que asegurar que sea una prioridad empresarial destinar los recursos a este ámbito. El sector privado destina recursos a la protección de las IIC cuando hay una percepción de riesgo alta, que no siempre ocurre y es un problema.

Además, se subrayó la necesidad de colaboración dentro del sector privado para la gestión y protección de las IIC.

En cuanto a las IIC pertenecientes al sector privado pero de importancia nacional, varios participantes opinaron que debe de haber un responsable o referente más allá del privado.

En resumen, se debe concretizar un enfoque integral, tal como sostenido en la Estrategia.

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

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

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

En esta parte las personas participantes discutieron acerca de los objetivos planteados en el pilar “Infraestructuras de información crítica”.

Los integrantes de la mesa validaron los objetivos planteados, con algunos aportes detallados a continuación.

Denominación del pilar

Más allá de los objetivos, no todos están de acuerdo con que las infraestructuras críticas sean solo de información, ya que, para muchos, “información” implica que la dimensión física queda por fuera cuando no debería. Además, todas las infraestructuras críticas no necesariamente almacenan información, sino que muchas sustentan la circulación de información entre los diferentes actores y sectores. También se argumentó que hay que abarcar todas las infraestructuras críticas en general, no solo las de información, ya que si una infraestructura crítica se ve perjudicada, las consecuencias las sufrirá todo el sistema. Por estos motivos, se propuso eliminar “información” de la denominación.

Otros opinaron que la palabra “infraestructura” acota a la dimensión física, por lo que los servicios se verían excluidos cuando no deberían; de esta forma, debería de incorporarse “servicios” a la denominación del pilar para que pase a ser

“Infraestructuras y servicios de la información crítica”.

También hubo participantes que compartieron que no le encuentran problemas a la denominación actual del pilar porque perciben que la infraestructura engloba tanto la dimensión física como a los servicios.

Preámbulo del pilar

El preámbulo del pilar menciona “consecuencias devastadoras”. Se destacó la necesidad de definir qué son las consecuencias devastadoras y cuál es el alcance por las cuales se miden.

Nuevo objetivo: definición, identificación y clasificación de las IIC

Se reiteró en varias mesas que uno de los nuevos objetivos debe ser llegar a una definición, identificación y clasificación de las IIC. Es importante, para esto, identificar cuáles son los activos críticos de esas IIC.

Con este fin, se debe asignar el rol de identificar las IIC. Una vez establecidos estos puntos, se podrá priorizar las IIC y generar capacidades para que esas priorizaciones tengan una adaptabilidad ágil y flexible para responder a los cambios y a las amenazas.

Nuevo objetivo: prevenir

Se propuso agregar un objetivo: el de prevenir. Dentro de ese objetivo podría estar también la Seguridad por Diseño, ya que su falta es una debilidad actualmente. Por otro lado, también se propuso incluirlo como línea de acción dentro de los objetivos, y algunos participantes consideraron que no era necesario, ya que está contemplado de manera más amplia en la ENC.

Nuevo objetivo: considerar la dependencia entre las IIC

Se debe considerar la dependencia entre las IIC, y establecer protocolos de acción si cae una. Es necesario tener un “Plan B” de soporte en caso de incidentes.

Modificaciones al objetivo 1: “Proteger las IIC”

- En la descripción del objetivo 1, se establece que las IIC “deberán estar preparadas para detectar y gestionar de forma correcta los incidentes de ciberseguridad”. Se sugiere incluir la prevención, que debe contemplar el monitoreo de las tendencias de ciberataque (mantenerse actualizado sobre las últimas vulnerabilidades y amenazas de seguridad para poder tomar medidas preventivas adecuadas); generar una base de conocimientos e identificación de vulnerabilidades; generar mecanismos de comunicación e instancia de intercambio.
- Respecto a la línea de acción iv del objetivo 1 (“Proteger las IIC”), se propuso modificar la redacción: “Desarrollar ejercicios conjuntos entre varias IIC para el desarrollo de las habilidades y garantizar que los canales de comunicación funcionan.”
- Se propuso agregar una línea de acción a este objetivo que sea: “Implementar y fortalecer las capacidades nacionales de ciberdefensa”. Debe incluir los sistemas de monitoreo necesarios para proteger las IIC.
- También se sugirió agregar una línea de acción que sea: “Definir una gestión de riesgos para las IIC con sus correspondientes responsables.”

Modificaciones al objetivo 2: “Fortalecer la resiliencia de las IIC”

- Respecto a la primera línea de acción de este objetivo (“Establecer los planes de recuperación de las IIC”), varios participantes “recuperación” implica que ya hubo un incidente, por lo que vieron necesario incluir también la prevención. Surgieron dos ideas principales de cómo concretar esto: incluir “prevención” de forma explícita dentro de esta línea de acción a modo de fomentar la cultura de prevención; o incluir otra línea de acción u objetivo sobre gestión de riesgo que incluya la prevención.
- En cuanto a la línea de acción iv (“Generar y/o adoptar los estándares y las auditorías a tales fines”), se percibió que “los estándares y las auditorías” era muy genérico, especialmente considerando que ya hay un Marco de Ciberseguridad en Uruguay que puede funcionar como estándar. Como el Marco de Ciberseguridad no es tan abarcativo para considerar todas las cuestiones del pilar y de la ENC y se encuentra más enfocado al Gobierno Central, se propuso primero adaptar el Marco de Ciberseguridad para que se alinea a los temas de la ENC y luego adoptarlo a la ENC. De esta forma, la nueva redacción de esta línea de acción sería: “Adaptar y adoptar el Marco de Ciberseguridad a tales fines.”
- Se cuestionó la necesidad de incluir la línea de acción v (“Desarrollar una nueva infraestructura de Claves Públicas Nacional contemplando tendencias internacionales y algoritmos criptográficos post cuánticos”) en el objetivo 2. Se planteó que es demasiado técnica y no es aplicable para esta primera Estrategia, sino que debería definirse en un nivel ulterior.

- En cuanto a la resiliencia, se destacó que se debe definir el término con más precisión y se subrayó que hay que tener en consideración la necesidad de la interdependencia y colaboración, no solo intra/local sino internacional. Se subrayó la complejidad de casos como Salto Grande que, además de ser infraestructura crítica, es internacional.

Presupuesto

Se debatió si el garantizar presupuesto para alcanzar el logro de los objetivos es o no una línea de acción, pero no se llegó a un consenso.

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

Las personas participantes aportaron actividades y acciones para el pilar “Infraestructuras de información crítica”.

Las acciones propuestas por los y las participantes son:

- Lo primero es definir qué infraestructura se va a considerar para luego ver elaborar un plan de acción. Se debe generar una metodología que permita la identificación y elaboración de un inventario/catálogo de infraestructuras críticas, porque van cambiando y se deben actualizar.
- También se debe identificar las dependencias entre ellas y su impacto, tanto a nivel nacional como internacional.
- Una vez identificada una criticidad, el monitoreo debería ser obligatorio y reportar a un lugar centralizado, a definir. Incrementar las capacidades de monitoreo en una primera etapa sería lograr que las 15 IIC públicas tengan un monitoreo real y robusto y no meramente nominal. Se debe una línea base de infraestructuras, y debe generar la capacidad para que el riesgo y el impacto se estén midiendo constantemente.
- Definir organismos rectores, para que gestionen e identifiquen las IIC. Se necesita una línea de acción para priorizar las estructuras y definir criterios mínimos de ciberseguridad. Identificar claramente las responsabilidades y tareas a nivel privado y público.
- Establecer una figura coordinadora para que se lleven a cabo las mejoras en las respuestas de incidentes y monitoreos. Es muy importante la auditoría y monitoreo constante de amenazas críticas, así como el monitoreo del cumplimiento de las líneas de acción y de su impacto.
- Respecto al monitoreo, también se sugirió jerarquizarlo: hoy AGESIC es responsable de concentrar ese monitoreo, pero si se generan las capacidades que se plantean en la línea de acción ii del Objetivo (generar equipos especializados a nivel sectorial), se deberían establecer monitoreos dentro de cada organismo, de cada organización.
- Debe haber intercambios en estos monitoreos.
- Se deben identificar responsables de cada organismo en IIC.
- Generar una base de conocimiento compartida. Se debería compartir los conocimientos recolectados por ese monitoreo continuo en una comunidad técnica para que todos se enriquezcan. Se propuso incluir una línea de acción que establezca la necesidad de compartir el aprendizaje, y que haya una instancia de recolección de la información en las distintas infraestructuras críticas identificadas. A partir de esa base de conocimiento se puede ir madurando y evolucionando.
- Establecer capacitaciones obligatorias en seguridad de la información para todos los involucrados.
- Desarrollar programas que "democraticen" de alguna manera el acceso a las soluciones de seguridad, ya que las realidades económicas de los organismos es muy dispar.
- Asegurar el involucramiento de operarios a nivel industrial en cuestiones relacionadas a la ciberseguridad, a través de concientización y capacitación tanto de estos como de los altos mandos. Por ejemplo, se podrían implementar simulacros de ciberseguridad para lograr la sensibilización y conciencia sobre los riesgos a nivel industrial.
- Crear equipos multidisciplinarios especializados en ciberseguridad.
- Establecer el compromiso de gestión y liderazgo en todos los niveles.
- Establecer un criterio mínimo en ciberseguridad, un marco, que contemple los procedimientos y garantice auditorías y lineamientos, tanto en el ámbito público como en el privado.
- Elaborar un plan de acción para el manejo de crisis.
- Debido a la interdependencia de las IIC, se deben realizar ejercicios en conjunto.
- Medirse para mejorar, evaluarlo en los proyectos de impacto.

- Garantizar que la adquisición de insumos de tecnología cumpla los requerimientos adecuados (no comprar por precio).
- Explicar dentro de un glosario las definiciones importantes como infraestructura crítica, sistemas de información, OT, TI, entre otros.

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

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

Respecto al objetivo 1 (“Proteger las IIC”), se mencionó que deberían estar involucrados el Ministerio de Defensa, el Ministerio de Educación y Cultura, un representante de cada IIC, uno de cada área pública y privada, de la academia, AGESIC, y un regulador.

Respecto al objetivo 2 (“Fortalecer la resiliencia de las IIC”), se debería tener en cuenta al Ministerio de Economía y Finanzas, al Ministerio de Relaciones Exteriores, al Ministerio de Defensa y Secretaría de Inteligencia del Estado, a Fiscalía, al Poder Judicial, a AGESIC, y a representantes de cada IIC.

Otros actores mencionados fueron el Ministerio del Interior, el Ministerio de Industria, Energía y Minería, URSEA (Unidad Reguladora de Servicios de Energía y Agua), URSEC (Unidad Reguladora de Servicios de Comunicaciones), y organismos públicos y privados. Se tiene que definir cómo el país encarará el tema de infraestructuras críticas, no solo para situaciones nacionales, sino para la realización de eventos internacionales, donde la infraestructura debe ser tenida en cuenta.

En cuanto a la priorización, lo primero es asegurar la estructura organizativa (se debe establecer una jerarquía dentro de los actores), y un inventario/catálogo de las IIC. Se debe empezar definiendo exactamente lo que son las IIC, y quién tiene el rol de identificarlas.

Anexos

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

Subgrupo 1

- Moderadora: Maria Noel Hernández, Agesic.
- Relatora: Isabel Álvarez, ICD.
- Participaron 13 (trece) 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:

DNIC (Institución pública) - Guillermo Lungo

Destaca la poca resiliencia ante cualquier desastre. No hay planes de acción ni gestión de riesgos. Está de acuerdo con algunos puntos, pero dice que no hay ciclos de contingencia y hay procesos críticos que no se contemplan.

MGAP (Institución pública) - Marcos Chávez

Sostiene que hay un estadio anterior de preparación para tener una planificación y estrategia más concreta y armada. Habría que tener gestión de riesgos, manejo de incidentes y no salir a apagar incendios. Ve aspectos positivos pero se necesitan mejoras.

SIEE (Institución pública) - Robert Figueroa

Destaca la necesidad de un marco regulatorio más claro. Remarca la importancia de sumar al sector privado.

ANTEL (Institución pública) - Carlos Piana

Resalta que falta camino. No está tan claro cuál es la infraestructura crítica en Uruguay – habría que cuestionarse qué es grave y definirlo bien.

DNIC (Institución pública) - Cinthia Los Santos

Argumenta que no está bien definida la matriz de riesgo y que hace falta un procedimiento estandarizado.

DNA (Institución pública) - Santiago Madura

Nota que, si bien están todos impulsando lo mismo, falta coordinación. No existe contingencia y no hay planes elaborados. ¿Cómo sabemos cuando hay un ciberataque? Es importante definir lo que es crítico. Hay otras entidades que deben ser considerados.

VaFirma (Sector privado) - Martín Fernández

Aprueba el borrador, y le gusta la idea de la capacitación. Pide el fortalecimiento del monitoreo. Está de acuerdo en cuanto a la necesidad de mecanismos de prevención. Destaca que habría que ver la cobertura de los planes y especificar el fortalecimiento en la identificación digital de mecanismos remotos, que avanza en la región pero está mas estancado en Uruguay.

Agesic (Institución pública) - Nicolás Correa

Hace hincapié en la identificación de infraestructuras críticas y en la importancia de la cooperacion.

MI (Institución pública) - Javier Jaurguiberry

Sostiene que la importancia del texto radica en la importancia de proteger las infraestructuras.

Agesic (institución pública) - Natalí Paggiola

Asegura que es relevante dejar como pilar las infraestructuras críticas de telecomunicación. Es muy importante la cooperación y la comunicación.

URSEC (Institución pública) - Nelson Rodríguez

En Uruguay no existe un reconocimiento de las infraestructuras críticas. La realidad depende de una situación externa que quizás no está vista como crítica pero que en el momento puede llegar a hacerlo. La energía, el agua, y la salud tienen que estar siempre. Hay que dimensionar los centros de referencia en cuanto a la salud. Si no existe la coordinación y un lugar adonde llamar, no se puede responder correctamente.

Agesic (Institución pública) - Pablo Pajon

Comenta que estas instancias son muy importantes porque crean conciencia. Hay que compartir lo que hay e identificar lo que falta. Sostiene que nunca estamos 100% preparados para enfrentar problemas. Es un trabajo continuo, y esta iniciativa es un paso adelante.

Agesic (Institución pública) - Eduardo Mascolo

Manifiesta su acuerdo en términos generales. Comenta que el mecanismo de detección y respuestas es complicado. No es tan fácil hacer pruebas. Remarca que para las pymes hay muchas cosas que son inviables. Las TIC o proveedores de soluciones deberían certificar que lo que están vendiendo cumple con ciertos estándares. Las certificaciones son muy importantes.

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

Agesic (institución pública) - Natalí Paggiola

Habría que calcular un presupuesto y un estimado de recursos humanos. También se deben implementar mecanismos de reportes porque no ve que se contemple la prevención. Es importante identificar vulnerabilidades y que se vea el panorama internacional. Habría que tener un plan de acción general para el manejo de crisis.

Además, comenta que los sistemas industriales están conectados y se hacen para que duren 20 años. Sostiene que se debe elaborar un plan de acción para el manejo de crisis y generar una metodología de catálogo de infraestructuras críticas. También es importante fomentar el intercambio de las amenazas. Entiende que en las organizaciones críticas, debe ser obligatoria la capacitación en ciberseguridad. Hay que estar actualizados.

Agesic (Institución pública) - Eduardo Mascolo

Comenta que las realidades son muy diferentes y es difícil de unificar. La coordinación le parece muy importante. Es una tarea que no termina nunca, porque requiere actualización constante.

URSEC (Institución pública) - Nelson Rodríguez

Habla de priorizar la infraestructura crítica y determinar el presupuesto.

MI (Institución pública) - Javier Jaurguiberry

Es necesario definir una gobernanza clara de las infraestructuras críticas. Hoy el órgano que tiene más conocimiento de infraestructura crítica no es quien debe controlar esto. Debería ser un órgano independiente. Hay riesgos que afectan a muchos sectores. Propone agregar el objetivo de identificar las infraestructuras críticas y priorizarlas, ya que lo que no se conoce no se puede atacar. Es necesario identificar responsables y referentes de las infraestructuras. También sugiere establecer un criterio mínimo que todos tienen que cumplir, establecer un marco regulatorio y generar presupuesto.

Agesic (Institución pública) - Nicolás Correa

Hace hincapié en que se debe fortalecer el rol de los reguladores de cada sector. Se deberá potenciar la participación de los reguladores.

VaFirma (Sector privado) - Martin Fernández

Hace énfasis en el presupuesto y en las pymes. Hay que priorizar la asignación de recursos y trabajar mucho en mejorar lo que hay en vez de generar iniciativas nuevas. Destaca la necesidad de medir.

DNA (Institución pública) - Santiago Madura

Remarca que es un trabajo continuo. Agesic o un ente aparte debería lograr regular y generar planes de contingencia. Se deben plantear requisitos mínimos.

DNIC (Institución pública) - Cinthia Los Santos

Marca la importancia de la prevención y la relevancia de tener mecanismos de medición de impacto. Hay que hacer pruebas de qué pasa si se corta un servicio, saber quién lo puede arreglar, quién tiene ese conocimiento.

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

Todos los integrantes de la mesa validaron los objetivos planteados, con algunos aportes detallados a continuación.

En la descripción del objetivo 1 (“Proteger las IIC”), se establece que las IIC “deberán estar preparadas para detectar y gestionar de forma correcta los incidentes de ciberseguridad”. Se sugiere incluir la prevención, que debe contemplar el monitoreo de las tendencias de ciberataque (mantenerse actualizado sobre las últimas vulnerabilidades y amenazas de

seguridad para poder tomar medidas preventivas adecuadas); generar una base de conocimientos e identificación de vulnerabilidades; generar mecanismos de comunicación e instancia de intercambio.

Se sugirieron algunas modificaciones en las líneas de acción.

Respecto a la línea de acción iv del objetivo 1 (“Proteger las IIC”), se propuso modificar la redacción: “Desarrollar ejercicios conjuntos entre varias IIC para el desarrollo de las habilidades y garantizar que los canales de comunicación funcionan.”

Se cuestionó la necesidad de incluir la línea de acción v (“Desarrollar una nueva infraestructura de Claves Públicas Nacional contemplando tendencias internacionales y algoritmos criptográficos post cuánticos”) en el objetivo 2 (“Fortalecer la resiliencia de las IIC”).

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

Los y las participantes realizaron aportes sobre actividades y acciones que se deberían realizar en el marco del objetivo 1 (“Proteger las IIC”):

- Lo primero es definir qué infraestructura se va a considerar para luego ver elaborar un plan de acción. Se debe generar una metodología que permita la identificación y elaboración de un inventario/catálogo de infraestructuras críticas, porque van cambiando y se deben actualizar.
- Definir organismos rectores, para que gestionen e identifiquen las IIC. Se necesita una línea de acción para priorizar las estructuras y definir criterios mínimos de ciberseguridad.
- Establecer una figura coordinadora para que se lleven a cabo las mejoras en las respuestas de incidentes y monitoreos.
- Identificar responsables de cada organismo en IIC.
- Generar una base de conocimiento compartida.
- Establecer capacitaciones obligatorias en seguridad de la información para todos los involucrados.
- Establecer el compromiso de gestión y liderazgo en todos los niveles.
- Establecer un criterio mínimo en ciberseguridad, un marco, que contemple los procedimientos y garantice auditorías y lineamientos.
- Elaborar un plan de acción para el manejo de crisis.
- Medirse para mejorar, evaluarlo en los proyectos de impacto.
- Respecto a línea de acción i (“Incrementar y fortalecer las capacidades de monitoreo y detección de las IIC”), debe haber intercambios en estos monitoreos.

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

Respecto al objetivo 1 (“Proteger las IIC”), se mencionó que deberían estar involucrados el Ministerio de Defensa, el Ministerio de Educación y Cultura, un representante de cada IIC, uno de cada área pública y privada, de la academia, Agesic, y un regulador.

Respecto al objetivo 2 (“Fortalecer la resiliencia de las IIC”), se debería tener en cuenta al Ministerio de Economía y Finanzas, al Ministerio de Relaciones Exteriores, al Ministerio de Defensa y Secretaría de Inteligencia del Estado, a Fiscalía, al Poder Judicial, a Agesic, y a representantes de cada IIC.

En cuanto a la priorización, lo primero es asegurar la estructura organizativa (se debe establecer una jerarquía dentro de los actores) y un inventario/catálogo de las IIC.

Debería de haber un presupuesto para arreglar las consecuencias de un incidente: se deben determinar esos fondos.

Subgrupo 2

- Moderadora: Arianne Palau, Agesic.
- Relatora: Marta Susana Manent, ICD.
- Participaron 14 (catorce) personas de 11 (once) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

DNA (Institución pública) - Matías Prieto

Cree que la propuesta recoge los principios básicos, y que todas las dimensiones están contempladas. Considera que tiene una buena estructura.

DNA (Institución pública) - Álvaro Salvarini

Le parece que es muy importante incorporar la parte de innovación e inversión, y que sea más fácil conseguir los recursos.

MDN (Institución pública) - Claudio López

Hace una analogía entre agresiones contra el cuerpo humano, los niveles de penetración de esas agresiones y las respuestas para restaurar la salud y las agresiones a las infraestructuras de la información críticas, los niveles de agresión y las capas de protección. Sintetiza el núcleo de la temática en pensar cómo defender a los “órganos vitales” del Estado que son las IIC.

AGESIC (Institución pública) - Federico Peux

Señala que hay que tener criterios claros para definir lo que es una estructura crítica y que eso se podría de alguna forma trasladar a cada uno de los responsables de los distintos organismos públicos o empresas privadas para que las pudieran identificar.

URSEC (Institución pública) - Mauro Ríos

Plantea que la infraestructura de informción crítica adquiere valor por los activos de información que contiene, por lo que es prioritario identificarlos, así como evaluar su criticidad tanto a nivel nacional como en cada organismo y empresa. Además, resalta la importancia de analizar la criticidad desde una perspectiva nacional.

El interviniente fue claro en señalar que, si la infraestructura de información crítica falla, debe existir un plan alternativo (Plan B), compuesto por una segunda línea de instituciones públicas y privadas, que brinden resiliencia y permitan mantener operativos los servicios clave del país. Propone que debe haber un Plan A y un Plan B: ¿qué sucede si no es posible proteger una infraestructura crítica? ¿Quiénes actuarán como respaldo? En caso de falla, el Plan B deberá garantizar la continuidad de los servicios esenciales mediante la participación de instituciones de respaldo.

Además, considera que es fundamental no solo proteger la infraestructura crítica, sino también invertir en concientización y capacitación, ya que el factor humano es crucial en este proceso.

Por otro lado, señala que el presupuesto destinado a las áreas tecnológicas es imprescindible y debe ser aumentado. Sin embargo, antes de eso, destaca un problema previo: en la Administración Pública, estas áreas suelen estar en niveles jerárquicos bajos, muchas veces como dependencias ad-hoc. Propone que se jerarquicen a niveles intermedios, como jefaturas o gerencias, lo que facilitaría la gestión de recursos y la solicitud de presupuesto. Con una estructura formal y jerarquizada, estas áreas podrían incluso ser consideradas para líneas presupuestarias dentro del Presupuesto Nacional.

CTM (Institución pública) - Alejandro Reyes

Le parece muy completa la ENC, ya que tiene en cuenta todos los aspectos desde la gobernanza y puntos legales, hasta la parte cultural, la difusión, la concientización. Se toma en consideración no solamente la parte técnica de los organismos, sino que abarca al público general y la educación. Cree que es vital el unir el sector, por la sinergia que se puede generar desde las capacitaciones hasta la respuesta a incidentes, al tener un común accionar entre todos.

Correo uruguayo (Institución pública) - Javier Lago

Manifiesta acuerdo a nivel general. Enfatiza que el eslabón más débil de la cadena es el humano. Entonces le parece que las capacitaciones y el trabajo en equipo son muy importantes.

SIEE (Institución pública) - Jorge Alliaume

Expresa que los objetivos y las líneas de acción están muy bien definidos. También concuerda y le parece fundamental resaltar

que casi todo termina en el factor humano.

AGESIC (Institución pública) - Sebastián Gómez

Manifiesta que está 100% de acuerdo con el documento, y totalmente de acuerdo con que hay que identificar las estructuras críticas, incluyendo las que están relacionadas con países limítrofes. Plantea la generación de protocolos de comunicación entre los sectores de infraestructuras críticas.

ANCAP (Institución pública) - Patricia Márquez

Está completamente de acuerdo con el abordaje. Propone reforzar la parte técnica de prevención, porque así se evita que se llegue al órgano vital ya que hay un diseño que lo hace más difícil. En vez de esperar a defender ese órgano o tratar de que se recupere más rápido, conviene dificultar el acceso al órgano vital.

Teledata (Sector privado) - Alejandro Pereyra

Considera que el borrador está muy bien, abarca bastantes puntos importantes. Detecta una disociación total entre IT y OT (tecnología de la información y tecnología operativa) que hay que subsanar. Plantea que a nivel de diseño es importante tomar tres aspectos: IT, OT y software, en especial el desarrollo de software seguro. Se deben crear certificaciones o ir al aprendizaje en las facultades para poder incorporar la ciberseguridad en eso. Le preocupa el tema presupuesto. Cree que el presupuesto tiene que estar dentro de los planes estratégicos de las empresas públicas y privadas, porque si el nivel de ciberseguridad no está en el presupuesto, podrán hacerse muchos marcos, pero no se va a invertir en eso, tanto sea en recursos humanos como en tecnología. Por último, también la coordinación entre público y privado le parece importante.

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

CTM (Institución pública) - Alejandro Reyes

Una duda que plantea es si está bien hablar de infraestructura de información crítica o de infraestructura crítica. En el caso de la hidroeléctrica es más infraestructura crítica, que de información. Otro tema que no ha visto mencionado es que en las infraestructuras críticas físicas es importante el tema de control de acceso. Plantea la necesidad de simulacros y de planes de recuperación de acceso. Por otro lado, estima que es natural que el responsable encargado de ciberseguridad nazca en TI y que crear una gerencia específica requiere una asignación presupuestaria.

URSEC (Institución pública) - Mauro Ríos

Expresa que el presupuesto para las áreas de tecnologías es imprescindible y debe ser aumentado. Pero existe un problema anterior y es que en la Administración Pública estas áreas existen en diversos niveles jerárquicos, en muchos casos sumergidos a dependencias casi *ad hoc*. Se debería jerarquizarlas al nivel de áreas medias como Jefaturas o Gerencias. Al estar en un mejor estatus jerárquico, se hace más accesible solicitar o reclamar presupuesto. Estando estas áreas de tecnología en una estructura formal y jerarquizadas, incluso pueden ser objeto de líneas presupuestales en el Presupuesto Nacional.

También refiere que, aunque existe un marco normativo para los procesos de adquisiciones de tecnología en la Administración Pública, el mayor problema es el incumplimiento del mismo. Específicamente cuando se trata de los procesos de adquisiciones de tecnología en la Administración Pública, donde en tecnología muchas veces se adquiere por precio, una práctica común, pero en desconocimiento de la posibilidad de adquirir por conveniencia según lo establece el propio TOCAF. En tecnologîa, y más hablando de infraestructura crîtica, adquirir barato no es lo recomendable. Debe adquirirse lo conveniente.

Una práctica común es que muchas veces la tecnología se adquiere por precio, pero en desconocimiento de la posibilidad de adquirir por conveniencia según lo establece el propio TOCAF. En tecnología, y más hablando de infraestructura crítica, adquirir barato no es lo recomendable. Debe adquirirse lo conveniente. Enfatiza que lo que haría falta para mejorar el cumplimiento es concientizar y educar, más allá de las carreras universitarias.

AGESIC (Institución pública) - Federico Peux

Entiende que la parte educativa se tiene que dar a todos los niveles - no solamente a nivel de la Facultad, cuando ya hay una orientación hacia la parte tecnológica. Hay un eslabón débil en la cadena, así que por más que podamos fortalecer y subir los niveles de madurez de lo que tiene que ver con infraestructuras críticas, hay un factor humano que es importante. En una empresa siempre hay gente con orientación técnica y otra que no, y todos pueden fallar. Por lo tanto, es esencial generar una mejor capacidad en la parte educativa. Considera fundamental tener los criterios para que puedan los organismos y las entidades públicas y privadas establecer si pertenecen a una infraestructura crítica o no. También se debe establecer la dependencia entre esas infraestructuras críticas y la relación que tienen, porque no es suficiente seguir buenas prácticas que hagan que el nivel de madurez en una infraestructura crítica sea muy valorable y presentable, si quien abastece de energía no lo hace. No es solamente identificar las IIC sino también la relación entre las distintas infraestructuras críticas, la dependencia que hay en cada una de ellas y además en este marco ofrecer niveles de madurez para poder ir mejorando.

MDN (Institución pública) - Claudio López

Con respecto a la diferencia entre infraestructura crítica e infraestructura de información crítica, explica que la infraestructura de información crítica es un sistema de información de una infraestructura crítica. No existe una infraestructura de información crítica que no pertenezca a una infraestructura crítica del país, está contenida dentro de una infraestructura crítica y va más allá. Considera que poner el presupuesto por delante es poner la carreta por delante de los bueyes. En cambio, plantea que primero hay que tener identificado quién es el responsable de ciberseguridad en una infraestructura crítica, ya que, incluso, está establecido por ley que tiene que haber un responsable. Cuando exista, se le podrá asignar un presupuesto. Este encargado, opina, no tiene que venir de TI sino que tiene que estar opuesto a esa situación, tiene que verla desde afuera.

ANCAP (Institución pública) - Patricia Márquez

Considera que tal vez cuando el nivel cultural y de concientización sea generalizado, se pueda tener el responsable de ciberseguridad afuera y estar más como un órgano supervisor o de mejora continua. Pero antes, conviene que esté adentro y agarre las cosas desde el principio.

Teledata (Sector privado) - Alejandro Pereyra

Con relación al tema presupuesto explica que si se quiere generar un área de ciberseguridad o TI se debe considerar tanto inversiones como recursos humanos, que es un gasto. Entonces hay que plantear un plan de negocios para que ese gasto se convierta en inversión. El presupuesto pasa a ser un actor bastante importante para el que toma las decisiones.

DNA (Institución pública) - Álvaro Salvarini

Comparte que la Estrategia es integral, como lo dice el documento, y la infraestructura crítica tiene que estar en esa integralidad, por lo que el presupuesto no es ajeno: se necesita plata para todo. Haciendo foco en la resiliencia, considera que cuando se habla de Plan A y Plan B, el plan B a la tecnología es más tecnología. Resume diciendo que el enfoque tiene que ser integral como dice el documento, tiene que atender riesgo y tiene que prever más tecnología para la tecnología primaria, para tener procesos operativos que funcionen en situaciones de desastres y que permitan volver a estar en condiciones normales o cuasi normales en plazos razonables.

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 de manera general, pero se hicieron algunos aportes:

- Se propuso agregar un objetivo: el de prevenir.
- Dentro de ese objetivo podría estar también la Seguridad por Diseño, que es una debilidad que se tiene actualmente, ya que no lo tenemos o se tiene únicamente por acciones específicas.
- Hay dos objetivos previos a Fortalecer y Proteger que son: identificar las IIC y saber quién y dónde las identifica; e identificar cuáles son los activos críticos de esas IIC.
- Una vez establecidos esos puntos, se podrá priorizar las IIC y generar capacidades para que esas priorizaciones tengan una adaptabilidad ágil y flexible para responder a los cambios y a las amenazas.
- Será materia a discutir si el garantizar presupuesto para alcanzar el logro de los objetivos es o no una línea de acción.
- También se planteó agregar como objetivo “considerar la dependencia entre las IIC”, y establecer protocolos de acción si cae una. Es necesario tener un “Plan B” de soporte por si una IIC cae.
- Una vez identificada una criticidad, el monitoreo debería ser obligatorio y reportar a un lugar centralizado, a definir. Incrementar las capacidades de monitoreo en una primera etapa sería lograr que las 15 IIC públicas tengan un monitoreo real y robusto y no meramente nominal.
- Se debería compartir los conocimientos recolectados por ese monitoreo continuo en una comunidad técnica para que todos se enriquezcan. Se propuso incluir una línea de acción que establezca la necesidad de compartir el aprendizaje, y que haya una instancia de recolección de la información en las distintas infraestructuras críticas identificadas. A partir de esa base de conocimiento se puede ir madurando y evolucionando.
- Establecer auditorías periódicas para constatar el cumplimiento de los monitoreos y dar ayuda.
- Garantizar que la adquisición de insumos de tecnología cumpla los requerimientos adecuados (no comprar por precio).
- Dentro de la resiliencia, tener en consideración la necesidad de la interdependencia y colaboración, no solo intra/local sino internacional. Se subrayó la complejidad de casos como Salto Grande que, además de ser infraestructura crítica, es internacional.
- También se planteó que la línea de acción v es demasiado técnica al referirse a los algoritmos criptográficos post

cuánticos: no es aplicable para esta primera Estrategia, sino que debería definirse en un nivel ulterior.

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

Las acciones propuestas por los y las participantes son:

- Identificar lo que es la infraestructura crítica,
- las dependencias entre ellas,
- el impacto que tienen,
- no sólo la infraestructura y la dependencia a nivel nacional sino también en colaboración con lo internacional.
- Además, después de identificar esa línea base de infraestructuras, se debe generar la capacidad para que ese riesgo y ese impacto se estén midiendo constantemente.
- Que se pueda cambiar de forma ágil y dinámica lo que se considera una estructura crítica y en qué momento, ya que pueden cambiar las prioridades y por lo tanto la criticidad de las infraestructuras.
- Es muy importante la auditoría y monitoreo constante de amenazas críticas, así como el monitoreo del cumplimiento de las líneas de acción y de su impacto.
- Respecto al monitoreo, también se sugirió jerarquizarlo: hoy AGESIC es responsable de concentrar ese monitoreo, pero si se generan las capacidades que se plantean en la línea de acción ii del Objetivo (generar equipos especializados a nivel sectorial), se deberían establecer monitoreos dentro de cada organismo, de cada organización.
- Debido a la interdependencia de las IIC, se deben realizar ejercicios en conjunto.

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

No se llegó a analizar este punto.

Subgrupo 3

- Moderadora: Ninoschka Dante, Agesic.
- Relatora: Sofía López, ICD.
- Participaron 12 (doce) personas de 12 (doce) 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:

A continuación se detallan los aportes generales de los y las participantes, en base a los ejes temáticos que se discutieron.

Glosario

Diferentes participantes de la mesa enfatizaron la necesidad de un glosario de términos para establecer definiciones en común que avalen de qué se esté hablando y no queden dudas. Muchos de los términos son muy generales y se usan indistintamente, cuando no son lo mismo. Es necesario tener un glosario común para marcar términos como ciberdefensa, ciberataque, entre otros.

Alcance

Los participantes de la mesa no lograron llegar a un acuerdo sobre el alcance de la ENC, en particular sobre si debería ser un documento con mayor detalle o más general.

Presidencia (Institución pública) - Ignacio Durán

Opinó que actualmente se debe de apuntar a que la ENC y el pilar de IIC tengan un enfoque general, macro y holístico. Definir cuestiones de forma específica lo vuelve muy estructurado e inflexible, lo cual puede afectar la adaptación de la ENC a los diferentes actores. Además, el área de las tecnologías de la información está en constante cambio y actualización, por lo que se correría el riesgo de que la ENC deje de ser relevante rápidamente si se detalla mucho. Propuso que los detalles se encuentren en líneas de acción dentro de un documento diferente.

IM (Institución pública) - María Eugenia Corti

Argumentó que un alcance general de la ENC no impide que se puedan definir indicadores y objetivos generales.

AGESIC (Institución pública) - Martín Cherro

En el marco de los rápidos cambios tecnológicos, agregó que la ENC debe de estar en mejora y revisión continua. Se deben establecer indicadores de avance.

Estructura de la ENC

Movistar (Sector privado) - Carolina Matos

Opinó que la ENC debería de tener una estructura de acuerdo a niveles. En primer lugar, que se establezcan a nivel general cuestiones como el glosario y también una estructura de guía para que los actores sepan qué hacer a nivel de prevención, redacción, recuperación y defensa. Luego, especificar y desplegar estas cuestiones dentro de cada pilar. Dentro de los pilares, hay que agregar cuestiones como un glosario, principios básicos, requisitos mínimos, procesos de auditoría y funcionamiento activo de los procesos. También enfatizó en que se definan los roles dentro de las líneas de acción, que especifiquen las responsabilidades de cada actor.

Definición de roles

Movistar (Sector privado) - Carolina Matos

Enfatizó la necesidad de que se definan los roles dentro de las líneas de acción de cada pilar, que especifiquen las responsabilidades de cada actor.

MIEM (Institución pública) - María José Franco

Llamó a que se identifiquen los actores relevantes para cada pilar de la ENC, definiendo sus responsabilidades y cometidos.

La ENC como política pública de Estado

LACNIC (Sociedad civil) - Graciela Martínez

Comentó que el mayor desafío es que la ENC sea una política de Estado en la práctica. Muchos países que tenían este tipo de borradores de ENC siguen con el borrador porque se enfrentan a conflictos a la hora de definir quién debería de llevar la delantera y marcar indicadores trascendentes a los diferentes gobiernos.

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

Ciberdefensa (Institución pública) - Pedro Gómez

Sostiene que hay tres cuestiones de glosario a considerar de suma importancia: identificar y definir las infraestructuras críticas; diferenciar entre los conceptos “ciberseguridad” y “ciberdefensa”; decidir si utilizar “infraestructuras de la información crítica” o “infraestructuras críticas de la información”. Desde la Unidad de Ciberdefensa del Ejército, evalúan que estas especificaciones son cruciales para asignar roles y decretar situaciones de emergencia que le permitan a los diferentes actores responsables saber cuándo deben responder. Las definiciones necesitan legitimidad de carácter de ley para que funcionen como una garantía legal antes las acciones y las consecuencias.

También comparte que es importante asignar roles y definir las situaciones de emergencia que le permitan a los diferentes actores responsables saber cuándo deben responder.

IM (Institución pública) - María Eugenia Corti

Argumenta que en el pilar se deben detallar roles claros, el alcance del tamaño de las infraestructuras y las amenazas para Uruguay; en base a estas cuestiones, definir luego qué son las infraestructuras críticas. A la vez, debe de otorgarse un rol para definirlo.

URSEC (Institución pública) - Luis González

Propone determinar los sectores afectados o involucrados en las infraestructuras críticas, en vez de definir las infraestructuras críticas en sí mismas.

LACNIC (Sociedad civil) - Graciela Martínez

Opina que una vez concretada la ENC, la misma se debe utilizar para definir las infraestructuras críticas.

AGESIC (Institución pública) - Martín Cherro

Considera crucial la definición de roles y responsabilidades para luego armar los proyectos dentro del pilar en base a eso.

ANTEL (Institución pública) - Alejandro Reyna

Consideró que tiene que haber un criterio común que determine qué es crítico, con una visión holística a nivel nacional, no solo en perspectiva de cierto sector.

IM (Institución pública) - María Eugenia Corti

Cuestionó si Infraestructuras de la información crítica debería ser un pilar, ya que le parece transversal a todos los otros pilares.

ANTEL (Institución pública) - Alejandro Reyna

Encuentra crucial que la ENC contemple las infraestructuras de la información crítica como un eje transversal. Considera que para que el alcance llegue a los diferentes actores de forma transversal debería de ser una ley, ya que sino el alcance no involucraría al sector privado porque no hay obligatoriedad.

LACNIC (Sociedad civil) - Graciela Martínez

Trajo a la mesa la necesidad de la gestión de riesgo acompañada a las infraestructuras críticas. Cuando se define el riesgo de un activo, se define que este activo tiene un dueño responsable. Hay que encontrar qué medidas de control se deberán tomar para mitigar el riesgo, con su adecuada gestión de riesgo.

CTM (Institución pública) - Álvaro Llama; CERTuy (Institución pública) - Víctor Blanco

Enfatizaron en que este pilar llegue al interior del país también, ya que muchas veces no llega este tema pero es fundamental.

IM (Institución pública) - María Eugenia Corti

Dijo que debe de incluirse el rol de los gobiernos departamentales y explicitar las infraestructuras críticas que les corresponden si las tienen.

CTM (Institución pública) - Álvaro Llama

Cree importante la legislación para que no haya matices en cuanto al ámbito de las infraestructuras críticas.

MIEM (Institución pública) - María José Franco

Percibe la regulación como un paso necesario para involucrar al sector privado. La legislación deberá ser legitimada por todos los actores involucrados para que pueda apropiarse, por lo que funcionará como garantía para que el sector privado cumpla con sus cometidos. Comenta que debe encontrarse definido el rol que va a tener el sector privado. Cree importante que se identifiquen los diferentes actores y se les asigne responsabilidades y cometidos de acuerdo al pilar.

ANTEL (Institución pública) - Alejandro Reyna

Considera que el alcance de ley es la única forma de asegurar la participación del sector privado, ya que habría obligatoriedad. Hace hincapié en la importancia de la participación del sector privado.

URSEC (Institución pública) - Luis González

Manifiesta su acuerdo con la necesidad de regulación para involucrar al sector privado.

CERTuy (Institución pública) - Víctor Blanco

También concuerda, y agrega que se deberá pensar en incentivos para que el sector privado acceda también.

MIEM (Institución pública) - María José Franco

En relación al presupuesto, dice que hay que pensar en el sector privado como un ámbito con múltiples actores donde puede que no todos tengan la capacidad económica para financiar lo propuesto por el pilar, lo que debilitaría toda la cadena de protección de las IIC.

Llama a pensar en términos de presupuesto a nivel nacional, pero también en especial consideración del sector privado y otros actores que podrían debilitar la cadena de protección de las IIC debido a falta de capacidad económica para financiar lo propuesto por el pilar.

ANTEL (Institución pública) - Alejandro Reyna

Agrega que la cuestión con los privados es que si no tienen el presupuesto, directamente mueren, por lo que hay que buscar incentivos para el sector. Sin embargo, subraya que las entidades públicas también pueden no tener el presupuesto y recursos necesarios.

Movistar (Sector privado) - Carolina Matos

Añade que incluso dentro de la parte del sector privado con los recursos necesarios para proteger las IIC, hay que asegurar que sea una prioridad empresarial destinar los recursos a este ámbito. El sector privado destina recursos a la protección de las IIC cuando hay una percepción de riesgo alta, que no siempre ocurre y es un problema.

Además, subraya la necesidad de colaboración dentro del sector privado para la gestión y protección de las IIC.

En cuanto a las IIC pertenecientes al sector privado pero de importancia nacional, varios participantes de la mesa opinan que debe de haber un responsable o referente más allá del privado.

Presidencia (Institución pública) - Ignacio Durán

Opina que concretar un presupuesto debe basarse en un plan de acción más detallado, que no es el momento de hacerlo. Actualmente se debe de apuntar a que la ENC y el pilar tengan un enfoque general, macro y holístico.

MIEM (Institución pública) - María José Franco

Sostiene que el pilar debe estar enfocado más a la resolución, pero hay que también fomentar la cultura de la prevención. Duda de si ponerlo en detalle, pero hay que pensar en las diferentes verticales y ver dentro de ellas cuál podría ser la prevención adecuada. Habló de la certificación como un posible mecanismo.

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

Denominación del pilar

Más allá de los objetivos, la primera apreciación de la mesa se relacionó a la denominación del pilar.

No todos están de acuerdo que las infraestructuras críticas sean solo de información, ya que, para muchos, “información” implica que la dimensión física queda por fuera cuando no debería, ya que los ciberataques pueden requerir una respuesta física o tener impacto físico. Además, todas las infraestructuras críticas no necesariamente almacenan información, sino que muchas sustentan la circulación de información entre los diferentes actores y sectores. También se argumentó que hay que abarcar todas las infraestructuras críticas en general, no solo las de información, ya que si una infraestructura crítica se ve perjudicada, las consecuencias las sufrirá todo el sistema, incluyendo todo tipo de infraestructuras críticas sean o no de la información. Por estos motivos, se propuso eliminar “información” de la denominación.

Otros opinaron que la palabra “infraestructura” acota a la dimensión física, por lo que los servicios se verían excluidos cuando no deberían; de esta forma, debería de incorporarse “servicios” a la denominación del pilar para que pase a ser “Infraestructuras y servicios de la información crítica”.

También hubo participantes que compartieron que no le encuentran problemas a la denominación actual del pilar porque perciben que la infraestructura engloba tanto la dimensión física como a los servicios.

Alcance

Se encontró prioritario definir el alcance del pilar para las IIC. Se deben definir criterios claros para poder decidir cuáles son las IIC. Para ello surgieron las ideas de considerar los sectores involucrados, los niveles de riesgo, los intereses nacionales y las prioridades de la ENC.

A la vez, encuentran fundamental que el alcance se vea fortalecido por un marco legal.

Definición, identificación y clasificación de las IIC

Se llegó a un consenso en la mesa que uno de los nuevos objetivos debe ser llegar a una definición, identificación y clasificación de las IIC. Es importante que no sea solo para las IIC que almacenan la información, ya que las infraestructuras críticas pueden transportar y procesar información.

Detallar sobre las “consecuencias devastadoras”

El preámbulo del pilar menciona “consecuencias devastadoras”. Vieron necesario definir qué son las consecuencias devastadoras y cuál es el alcance por las cuales se miden.

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

Nueva línea de acción sobre ciberdefensa al primer objetivo

Se propuso agregar una línea de acción a este objetivo que sea: “Implementar y fortalecer las capacidades nacionales de ciberdefensa”. Debe incluir los sistemas de monitoreo necesarios para proteger las IIC.

Nueva línea de acción sobre gestión de riesgos al primer objetivo

Se sugirió agregar una línea de acción que sea: “Definir una gestión de riesgos para las IIC con sus correspondientes responsables.”

Nueva línea de acción sobre presupuesto al primer objetivo

Se sugirió agregar una nueva línea de acción sobre presupuesto que sea: “Generar los mecanismos de financiamiento que aseguren la seguridad de las IIC y de sus líneas de acción”.

No todos estuvieron de acuerdo en agregar esta línea de acción. Mientras que algunos opinaron que cada pilar de la ENC debe definir su propio presupuesto, otros consideraron que el presupuesto debería de ser más general y transversal a todos los pilares.

Además, en cuanto a la redacción de esta nueva línea de acción, hubo inconclusión sobre la palabra “generar”. Algunos compartieron que para ellos “generar” sonaba a que se impondrán impuestos, lo cual no es la idea. Otras ideas fueron “dotar” o “brindar” pero para muchos estas opciones implican que el Estado siempre otorgará los recursos necesarios y que los diferentes actores no deben nunca invertir sus propios recursos para la protección de las IIC.

Línea de acción I del segundo objetivo: “Establecer los planes de recuperación de las IIC.”

La mayoría de los participantes opinaron que “recuperación” implica que ya pasó el proceso, por lo que vieron necesario incluir también la prevención. Surgieron dos ideas principales de cómo concretar esto:

Incluir “prevención” de forma explícita dentro de esta línea de acción a modo de fomentar la cultura de prevención, ya que sería

la base.

Incluir otra línea de acción u objetivo sobre gestión de riesgo que incluya la prevención.

Otra parte de los participantes no vieron necesario incluir la prevención, ya que lo ven incorporado dentro de la ENC como parte de sus objetivos macro.

Línea de acción IV del segundo objetivo: "Generar y/o adoptar los estándares y las auditorías a tales fines."

En la mesa se percibió que "los estándares y las auditorías" era muy genérico, especialmente considerando que ya hay un Marco de Ciberseguridad en Uruguay que puede funcionar como estándar. Como el Marco de Ciberseguridad no es tan abarcativo para considerar todas las cuestiones del pilar y de la ENC y se encuentra más enfocado al Gobierno Central, se propuso primero adaptar el Marco de Ciberseguridad para que se alinea a los temas de la ENC y luego adoptarlo a la ENC. De esta forma, la nueva redacción de esta línea de acción sería: "Adaptar y adoptar el Marco de Ciberseguridad a tales fines."

Línea de acción V del segundo objetivo: "Desarrollar una nueva Infraestructura de Claves Públicas Nacional contemplando tendencias internacionales y algoritmos criptográficos post cuánticos."

Los participantes de la mesa consideraron que "algoritmos criptográficos post cuánticos" es una apreciación muy técnica que debe cambiarse. Hubo diferentes propuestas sobre qué hacer.

Por un lado, se propuso sustituirlo a un concepto más genérico como "últimas tecnologías".

Por otro lado, se sostuvo que debería de eliminarse y no sustituirse porque está comprendido en el resto de las líneas de acción. También fue considerado como un plan de acción que no debería estar incluido dentro del pilar.

También se propuso eliminar la línea de acción por completo y sustituirla por: "Crear un mecanismo y observatorio del desarrollo de las tecnologías".

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

No se llegó a trabajar este punto.

Subgrupo 4

- Moderadora: Noelia Rodriguez, Agesic.
- Relatora: Mauro Parada y Sabrina Piffaretti, ICD.
- Participaron 20 (veinte) personas de 15 (quince) 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

DGI (Institución pública) - Guillermo Dornreyes

Sobre la propuesta borrador dice que el enfoque está bien pero que hay mucho para trabajar. Menciona que la realidad del Uruguay es dispar respecto a IIC y es difícil llegar a un acuerdo entre todos ya que cada actor tiene diferentes dificultades.

URSEC (Institución pública) - Fernando Hernández

Plantea que hay que integrar a todos los interesados y generar un entorno común de trabajo. Explica que, si bien se habla de resiliencia y de infraestructuras críticas en el país en el documento, no se definen y ello sería lo primero a solucionar porque sino se da lugar a diferentes interpretaciones. Pone al ejemplo de Brasil, que formó un grupo por ley donde se identificaron las infraestructuras y cómo repercutía el error de una en el resto; por ello, propone identificar las infraestructuras.

Resalta que la definición de infraestructura crítica debe incluirse en el marco normativo. No hay definiciones, incluyendo fundamentalmente la de infraestructura crîtica, lo que da lugar a diferentes interpretaciones. Debe incluirse en el marco normativo. A su juicio, falta un marco normativo (leyes, decretos, resoluciones) para que este tema, que involucra a múltiples organismos, públicos y privados, pueda avanzar, escapa a AGESIC, siendo como es en todos los países una estrategia de Estado. No se tiene un marco normativo (Leyes, Decretos, Resoluciones) que haga que este tema que involucra múltiples organismos tanto públicos como privados pueda ser llevado adelante, ya que escapa a las propias funciones de AGESIC, siendo como es en todos los paîses, una estrategia de Estado. Deben intervenir coordinadamente Secretaria de inteligencia del Estado, SINAE, Fiscalîa, Poder Judicial, MDN, MI, MIEM, MEC, MRREE, AGESIC, URSEA, URSEC, organismos públicos y privados ya que se tiene que definir como paîs el encare del tema de infraestructuras crîticas, no solo para situaciones nacionales, sino para la realización de eventos internacionales, donde

Finalmente sostiene que no circunscribir el tema de infraestructura critica atendiendo solamente el Objetivo X Ciberseguridad de la AUD2025, sino incluir el Objetivo IX Lînea de acción 42 Desarrollar redes resilientes mediante el análisis de la infraestructura crîtica de telecomunicaciones, que aseguren la disponibilidad de los servicios. Ya que es uno de los sectores con infraestructura crîtica que es transversal al resto. Incluso en la mesa de trabajo se discutió ampliar la definición a “comunicaciones” en vez de “telecomunicaciones”, teniendo el antecedente cercano del rol que desempeñaron los servicios postales y de logîstica durante la pandemia de COVID-19.

URSEC (Institución pública) - Agustín Hill

Explica que hablar de infraestructura de información crítica no es tan adecuado y se debería ir a algo más específico. Propone modificar y aclarar cómo se lo llama, y aggiornarlo a perspectivas internacionales que sirvan como modelo.

MGAP (Institución pública) - Andres Rodriguez

El documento le parece muy genérico y amplio, lo cual deja dudas sobre dónde empezar. Cuestiona si se está preparado para un abordaje general una vez se definan las infraestructuras críticas, ya que no hay tareas previas en la definición del marco teórico ni claridad sobre el estado de las instituciones involucradas. Le preocupa que, aunque la estrategia se lea de manera amplia, al definirse las infraestructuras críticas, no quede claro cómo abordar las instituciones específicas. También menciona que la estrategia incluye una mezcla de entidades privadas y públicas, y se pregunta cómo se coordinará esa relación público-privada para que sea efectiva. Considera que la estrategia es adecuada, pero necesita desglosarse más porque actualmente es demasiado genérica.

CERTuy (Institución pública) - Jesús Alfonso

Destaca pilares 2, 3 y 4 (cibercrimen, infraestructuras de información crítica y ciberdefensa) del borrador. Sin embargo, el 3 relativo a las IIC lo cree genérico.

Cree que faltan dos cosas: adoptar un enfoque sistemático para la gestión de la seguridad de la información, que incluye identificación de activos críticos, su urbanización en estructura segura y clasificación para medidas de protección.

También cree que para gestionar las infraestructuras, se deben adoptar programas reconocidos internacionalmente que garanticen madurez organizacional. Habla de los actores: ISACA, COMPTIA Y SANS que son estándares de esos aspectos.

ANCAP (Institución pública) - Osvaldo Barrios

Está de acuerdo con la estrategia propuesta, pero considera esencial involucrar ciertos aspectos: prefiere hablar de servicios más que de infraestructuras. Le parece interesante seguir los lineamientos de la ITU sobre criterios mínimos de seguridad para infraestructuras críticas debido a las complejidades actuales. Cree fundamental establecer un estado mínimo de base que las empresas que operan con infraestructura crítica deben alcanzar.

También, destaca la importancia de la concientización sobre ciberseguridad para los trabajadores de la industria y otras empresas estatales, sugiriendo la necesidad de un programa de concientización y un marco de gobernanza de ciberseguridad que involucre el marco industrial dentro de la estrategia de ciberseguridad de la empresa. Menciona que en ANCAP están viviendo una transformación en TI, pero el sector industrial no está involucrado, lo que requiere sinergia para evitar esfuerzos aislados.

Propone adoptar criterios mínimos, un modelo de gobernanza con responsabilidades definidas, y priorizar la creación de estándares y auditorías. También sugiere tener claro el estado actual mediante auditorías, identificar plenamente los incidentes, lograr ciertas certificaciones, y generar un programa de capacitación y concientización en ciberseguridad.

Finalmente, señala que AGESIC debe implementar esto asegurando que haya una contraparte responsable en cada organismo, especialmente en sectores donde la ciberseguridad no es su core de negocio, como en salud.

MATRIZ (Sector privado) - Daniel Pérez

Manifiesta su acuerdo y propone inventariar las infraestructuras. Plantea la problemática de la capacitación de personal de infraestructura en el lado de ciberseguridad. La capacitación en industria debería ser un pilar: se debe concientizar al personal en la importancia de la ciberseguridad, porque que no logran verlo. También, plantea la adopción de un marco adaptado a la OT (tecnología operativa) o a la ciberseguridad industrial.

FORTINET (Sector privado) - Gastón Sancassano

Desde su posición, observa que los ambientes industriales se ven muy afectados porque antes estaban aislados y ahora se han unido a IT. La seguridad en OT no está al nivel de IT, y en la unión de estas dos redes, OT tiene problemas similares a IT. Propone hacer un listado de infraestructuras críticas, resaltando que OT está muy presente y enfrenta problemas de seguridad.

Sugiere nivelar la seguridad en todos los ambientes industriales, ya que están relegados en este aspecto debido a que antes la industria era cerrada y solo se accedía físicamente. Con la conectividad actual, surge la problemática de seguridad, especialmente con sistemas operativos obsoletos y la falta de experticia. También menciona que la gente no se anima a actualizar los sistemas, generando obsolescencia, y subraya la necesidad de concientización desde los altos mandos para promover la seguridad.

MOVISTAR (Sector privado) - Facundo Payseé

Sugiere utilizar normas y marcos existentes como inspiración, mencionando específicamente la reciente ley marco de seguridad de Chile y la política chilena de ciberseguridad 2023-2028. Propone analizar el principio de "seguridades del diseño", que asegura que todo el sistema, desde su inicio, protege la privacidad y la seguridad de la información. Como ejemplo, menciona ciertos manuales de uso del Instituto Federal de Comunicaciones que incluyen códigos de seguridad.

Propone agregar dos regulaciones:

Ciberdiplomacia: conseguir tratados con países avanzados para mantener estándares de seguridad similares a los de las naciones seguras.

Cultura y ecosistema: incorporar una línea de acción para explorar nuevos mecanismos de financiación estatales que mejoren la ciberresiliencia en empresas y el Estado.

AGESIC (Institución pública) - Ismael González

Opina que la estrategia es muy de alto nivel y difícil de concretar. Destaca la necesidad de definir quién liderará la estrategia desde el Estado. Aunque AGESIC ha iniciado el proceso y ha establecido ciertos pilares, la estrategia es demasiado grande para que AGESIC la gestione sola. Se requieren recursos jurídicos, económicos y de empoderamiento para atraer y vincular al sector privado, que a menudo carece de la capacidad financiera para implementar medidas de ciberseguridad por sí mismo.

Menciona que la ciberseguridad tiene muchas partes, lo que dificulta que organismos pequeños, como los de salud, adopten un plan de ciberseguridad. Propone que AGESIC debe adoptar una postura paternalista hacia estos organismos, proporcionando recursos, consultorías y capacidad para ayudarlos a implementar la estrategia.

Sugiere que se debe definir claramente quién en el Estado será responsable de esta estrategia, dotándolos de recursos financieros y jurídicos para tomar las infraestructuras críticas y adoptarlas. Además, resalta la necesidad de tener la autoridad para supervisar y controlar al sector privado en términos de ciberseguridad, asegurando que cumplan con las normas y no pongan en riesgo a los clientes.

AGESIC (Institución pública) - Maximiliano Barreiro

Sugiere agregar más información internacional en la estrategia para aquellos que no están familiarizados con el tema. Propone incluir el uso de datos del Estado. Cree que sería útil definir mejor el concepto de resiliencia, ya que es algo nuevo y necesita desarrollo.
En cuanto al capítulo de cibercrimen y ciberdelito, menciona que hay una gran carencia en la parte jurídica que debe ser abordada para completar la política. Reconoce que las infraestructuras críticas están soportadas por sistemas de información y destaca que el software está tomando más control de estas infraestructuras, lo que aumenta la vulnerabilidad.
Propone ampliar este capítulo, definiendo mejor las infraestructuras críticas y prefiriendo el término "sistemas de información crítica". Cree que es necesario esquematizar y clarificar esta parte, especificando cuáles son las infraestructuras críticas en Uruguay y cuáles son los sistemas de información crítica que dependen de ellas.

CORREO URUGUAYO (Institución pública) - Andrea Machado

El borrador le parece genérico. Cree que hay que definir la infraestructura crítica, ver a qué se refiere. También plantea que hoy en día no existe una ley de seguridad y eso falta. Considera importante que haya una ley que instrumente la estrategia.

UTE (Institución pública) – Evelyn Anton

Transmite que distribuyó la estrategia a diferentes sectores en UTE y la mayor preocupación fue de aquellos sectores vinculados a operaciones e infraestructura "física", talleres por ejemplo, que no se sintieron reflejados en el concepto de infraestructura crítica.

BPS (Institución pública) - Álvaro Arias

Plantea la necesidad de tener un inventario de Infraestructuras críticas, con niveles de criticidad y planes de acción acorde a ellos.

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

A partir de los aportes anteriores, se identificaron los aportes específicos sobre el pilar “Infraestructuras de información crítica”:

- Necesidad de hacer un relevamiento;
- Importancia de elaborar un plan de abordaje a nivel nacional;
- Necesidad de coordinación de expertos privados y públicos para armar un marco, con definiciones claras de los conceptos que se tratan;
- Establecimiento de cierto nivel de obligatoriedad aplicando auditorías;
- Definición de a quiénes alcanza.

URSEC (Institución pública) - Agustín Hill

Propone además mejor coordinación y destaca la importancia de que todos tenemos que entender la misma definición. Es necesario que el marco incluya definiciones nacionales del concepto.

CORREO URUGUAYO (Institución pública) - Andrea Machado

Considera que el marco de ciberseguridad de AGESIC se debe poder hacer genérico al menos a nivel público, y establecer cierto nivel de obligatoriedad.

CERTuy (Institución pública) - Jesús Alfonso

Propone un plan de concientización para públicos y privados: tener un equipo de delegados liderado por AGESIC para ver por ejemplo temas de phishing que a veces son los vectores de ataque. Menciona que esto no requiere mucho presupuesto.

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

En la Ronda 2 se identificaron ciertos aportes estratégicos y acciones importantes:

- Explicar dentro de un glosario las definiciones importantes como infraestructura crítica, sistemas de información, OT, TI, entre otros.
- Identificar claramente las responsabilidades y tareas a nivel privado y público.
- Realizar un inventario de infraestructuras críticas a nivel nacional, así como de los actores críticos de estas y las empresas que manejan infraestructuras críticas.
- Asegurar el involucramiento de operarios a nivel industrial en cuestiones relacionadas a la ciberseguridad, a través de

concientización y capacitación tanto de estos como de los altos mandos. Por ejemplo, se podrían implementar simulacros de ciberseguridad para lograr la sensibilización y conciencia sobre los riesgos a nivel industrial.

- Crear equipos multidisciplinarios especializados en ciberseguridad.
- Adaptar los criterios mínimos de ciberseguridad a nivel nacional en ámbitos públicos y privados.

Se formalizó, y se hizo énfasis, en la siguiente propuesta:

La línea de acción a desarrollar es que se debe determinar el alcance y definición de la infraestructura crítica, y que incluya la noción de OT. En el marco deben figurar definiciones conceptuales más amplias o más claras y explícitas respecto al concepto de Infraestructura crítica, y deben abarcar la OT: se debe definir qué involucra, cuál su alcance, no solamente incluyendo a las TI clásicas.

Respecto a los actores, se sostuvo que deben intervenir coordinadamente la Secretaria de inteligencia del Estado, SINAE (Sistema Nacional de Emergencias), Fiscalía, Poder Judicial, MDN (Ministerio de Defensa Nacional), MI (Ministerio del Interior), MIEM (Ministerio de Industria, Energía y Minería), MEC (Ministerio de Educación y Cultura), MRREE (Ministerio de Relaciones Exteriores), AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento), URSEA (Unidad Reguladora de Servicios de Energía y Agua), URSEC (Unidad Reguladora de Servicios de Comunicaciones), y organismos públicos y privados. Se tiene que definir cómo el país encarará el tema de infraestructuras críticas, no solo para situaciones nacionales, sino para la realización de eventos internacionales, donde la infraestructura debe ser tenida en cuenta (por ejemplo, el Mundial 2030).