Segunda Estrategia Nacional de Ciberseguridad

Informe resultante del proceso de Consulta Pública

Introducción

El 6 de enero del corriente, por medio de la Resolución N° 1 del 2 de enero de 2023 de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS, se declaró la apertura del procedimiento de consulta pública respecto de la SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD incluida como Anexo IF-2022- 133944871- APN- SSTI#JGM. En la misma norma, se encomendó a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, impulsar los actos administrativos y demás acciones necesarias para la implementación de la SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.

El documento puesto a consideración de la ciudadanía mediante el proceso de elaboración participativa de normas, fue confeccionado por el Grupo de Trabajo del Comité de Ciberseguridad creado a tal fin. Este grupo está conformado por representantes de los Ministerios de Defensa; Seguridad; Relaciones Exteriores, Comercio Internacional y Culto y Justicia y Derechos Humanos y las Secretarías de Innovación Pública y Asuntos Estratégicos. Participaron también, en calidad de invitados, funcionarios de la Sindicatura General de la Nación, el Banco Central de la República Argentina, ARSAT, la Administración Federal de Ingresos Públicos, la Agencia de Acceso a la Información Pública, la Secretaría Legal y Técnica y la Agencia Federal de Información.

Una vez finalizada la versión preliminar del documento, la misma fue puesta a consideración del Comité de Ciberseguridad, el cual la aprobó en la reunión realizada el 7 de noviembre de 2022, donde también se decidió someter el texto a una consulta pública de carácter no vinculante, con el objetivo de participar y contar con la perspectiva de todas las partes interesadas. El proceso abierto por la Resolución N° 1/2023 fue cerrado el 17 de febrero del corriente. A partir de dicho proceso se recibieron 18 aportes: tres (3) propuestas provenientes del Sector Público, cuatro (4) del Sector Privado, siete (7) de la sociedad civil, una (1) del sector académico, dos (2) de organismos y entidades internacionales y una (1) de la comunidad técnica.

Análisis de las propuestas recibidas

En función de los distintos tipos de aportes recibidos, se abordaron distintas estrategias para el tratamiento de las presentaciones. En los casos en que los aportantes efectuaron sugerencias textuales sobre alguno de los puntos del texto preliminar puesto a consulta, las mismas fueron revisadas y, en algunos casos, incorporadas. En otros casos, las presentaciones constan de aportes no textuales, producto de lo cual se efectuó una valoración de los puntos sugeridos, receptando las agregaciones en los casos que se estimó pertinente.

A continuación se realizará una síntesis de los aspectos más destacados de las sugerencias, observaciones y comentarios recibidos al texto preliminar de la Segunda Estrategia Nacional de Ciberseguridad.

A tales fines, se mostrará el resumen de la información dividida por categoría de aportante en base a las presentaciones realizadas por las distintas partes interesadas:

1. **Sector Público**

2. **Sector Privado**
3. **Academia**
4. **Sociedad civil**
5. **Organismos y entidades internacionales**
6. **Comunidad técnica**

1. Presentaciones provenientes del Sector Público

1.1 Se formuló una propuesta concreta de modificación del texto de la estrategia vinculada entre otros aspectos, a la necesidad de una arquitectura institucional de carácter federal sobre la que se base el marco normativo; la creación de maestrías y doctorados en ciberseguridad; la generación de becas o acuerdos laborales que habiliten el cursado intensivo; la capacitación en todos los niveles; el diseño y construcción de una red de centros de datos regionales que permite entre otras funciones, el resguardo de la información crítica; la innovación y la mención específica a determinados estándares internacionales reconocidos.

Por otro lado, se resaltó la importancia de focalizarse en el respeto por los derechos de la ciudadanía, con un enfoque centrado en la prevención.

Asimismo, se resaltó la importancia de establecer marcos de ciberseguridad para definir ámbitos de coordinación y un marco organizativo de ejecución acordes con las políticas públicas y de la Estrategia Nacional de ciberseguridad; el fortalecimiento institucional a través de la creación de un organismo con competencias en la materia; la consideración de aspectos relativos a la protección de datos personales como principio rector; la creación de una institución que estudie, analice e investigue los distintos aspectos de la ciberseguridad para la capacitación, emisión de normativa y asesoramiento al Poder ejecutivo; el fortalecimiento de los procesos de gestión de incidentes y de vulnerabilidades y la promoción de la investigación en materia de ciberseguridad.

1.2 Otra de las propuestas sugirió la inclusión de un principio que reconozca la necesidad de proteger a personas que se encuentren en situaciones de vulnerabilidad en razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales y la modificación del texto del principio “Construcción de capacidades y fortalecimiento federal” para incluir al sector privado. Además, en cuanto a los objetivos, recomendó el desarrollo de un marco normativo aplicable a las entidades y/u organizaciones responsables de la operación y protección de las infraestructuras críticas de información y la promoción de un sistema de intercambio de información con alertas tempranas a nivel internacional.

1.3 La tercer propuesta recibida propuso entre otros aspectos, incluir entre los principios la protección de datos y privacidad; la adopción de un marco de medición para la planificación e implementación de acciones, la creación de una institución que estudie, analice e investigue aspectos tales como la capacitación, la emisión de regulaciones y normativa y el asesoramiento al Poder Ejecutivo y la identificación de áreas de conocimientos faltantes. Sugiere asimismo, el fomento de la investigación en la materia y la adopción de marcos de ciberseguridad reconocidos en la materia, tanto para la gestión de incidentes como de vulnerabilidades.

2. Presentaciones provenientes del Sector Privado

2.1 Una de las propuestas recibidas recomienda enfáticamente la importancia de reservar al ámbito nacional el poder de compra de la industria local por parte del mercado gubernamental por razones de ciberseguridad y ciberdefensa.

Se señala además, que no se menciona explícitamente la identidad digital en la versión de la Estrategia bajo análisis, si bien se podría encontrar contemplada en algunos de los objetivos. En este sentido se expresa preocupación en cuanto a que gobiernos subnacionales validen la identidad digital del ciudadano a través de plataformas globales ajenas a supervisión nacional.

También se recalca que es necesario mejorar la remuneración de los funcionarios públicos dedicados a las actividades y servicios informáticos para su retención.

2.2 Otra de las propuestas señala que respecto a la incorporación de Soberanía entre los Principios Rectores, no debería interferir con el flujo libre y global de información, por la posible afectación en los derechos humanos.

En materia de desarrollo normativo, indica que toda iniciativa debe ser compatible con la protección de los derechos a la libertad de expresión y al acceso a la información.

Destaca la necesidad de promover el desarrollo de CERTs y CSIRTs y la necesidad de promover la investigación e inversión privadas en el desarrollo de la industria de la ciberseguridad.

En relación a la protección de las Infraestructuras Críticas (IC), destaca que las políticas públicas y regulaciones que a implementarse no deben implicar un avance sobre la propiedad privada, recomendándose poner el acento en la infraestructura estatal, dejando el sector privado para una etapa posterior.

2.3 En otra de las propuestas, se alienta al gobierno en la adopción de estándares internacionales reconocidos.

Con respecto a infraestructura crítica de información, se resalta la relevancia en la distinción entre (i) infraestructura de tecnología de la información como una de las verticales de infraestructura crítica (tal como energía, etc.); y (ii) los reguladores específicos de la industria regulando a los proveedores de nube y servicios de tecnología de la información como proveedores de servicios externos críticos para garantizar la resiliencia de su industria.

Para que la regulación sea efectiva, destaca que es importante comprender estos dos enfoques diferentes para un buen diseño de su alcance y para las partes interesadas, dado que al mezclar estos dos enfoques en uno solo se podrían crear algunos desafíos para la implementación de la regulación específica vinculados a su efectividad.

2.4 Otra de las propuestas pone esencialmente el foco en el rol y los intereses del sector privado, sin que esto implique que no se encuentren ya abordados aspectos sustanciales dentro de la Estrategia. En sus consideraciones, se alude a la necesidad de considerar a la Estrategia como un documento vivo que involucra múltiples actores y por ello requiere de una fuerte institucionalidad.

Considera que es necesario clarificar y especificar el alcance que se le da al principio de soberanía nacional, por sus posibles implicancias para el sector privado y entiende que la

promoción de la industria nacional de la ciberseguridad debería hacerse en el marco de lo que establecen los estándares internacionales en la materia.

En cuanto al glosario, se objetan las definiciones de Infraestructuras Críticas e Infraestructuras Críticas de Información, que deberían limitarse a los servicios esenciales para el funcionamiento del Estado. Alude a la necesidad de un marco normativo específico en cuanto a los procesos de designación de IC en el sector privado, preservando el derecho a las empresas a cuestionar esta designación; sugiriendo que este mecanismo de designación debería estar mencionado en el texto de la Estrategia. Asimismo se resalta que la definición de incidente informático sería demasiado amplia, afirmando que la misma debería aplicarse sólo a los casos que impliquen actividad maliciosa.

Por su parte, se sugiere que la Estrategia promueva el uso de tecnologías innovadoras como por ejemplo los servicios de nube.

Asimismo, se propone utilizar para la ciberseguridad un enfoque basado en riesgos, que tenga como fin la construcción de capacidades de detección, prevención, respuesta y recuperación a incidentes cibernéticos, con un enfoque federal.

Se sugiere además la mención explícita a determinados marcos reconocidos internacionalmente y la adopción de estrategias de ciber resiliencia para infraestructuras críticas, formulándose algunas observaciones sobre los términos incorporados en el glosario.

En algunas de las presentaciones se incluyen documentos vinculados al software libre y la industria del software en Argentina.

3. Presentación proveniente del sector académico

Dicha presentación destaca la importancia de focalizarse específicamente en la concientización de los sectores de la sociedad que tienen acceso limitado o nulo a Internet o a computadoras en sus domicilios, escuelas y/o puestos de trabajo. También resalta que cualquier campaña para mejorar la ciberseguridad debe partir de las personas e incluir a las organizaciones de la sociedad civil, movimientos sociales, cooperativas, PyMEs y organismos públicos (comprendiendo en su alcance al sistema educativo y de investigación y desarrollo de nuestro país), así como empresas, particularmente argentinas.

Asimismo, se señala que para concientizar a niños, niñas y adolescentes es necesario promover la inserción del tema en la currícula de escuelas primarias y secundarias y en Universidades y que para formar profesionales en ciberseguridad es necesario promover vocaciones desde edades tempranas, mediante distintas actividades.

Finalmente, recomienda la generación de material actualizado y de calidad en español y la promoción de la investigación de nuevas amenazas y vulnerabilidades.

4. Presentaciones provenientes de la sociedad civil

4.1 En una de las propuestas, se solicita que la participación de los sectores interesados generada a partir de la Consulta Pública impulsada, continúe en las etapas de implementación de la Estrategia Nacional y los planes de trabajo que se lleven adelante.

En esta propuesta, además, se formula una advertencia respecto a una posible expansión de la vigilancia estatal, que afectaría los derechos de las personas, en particular la libertad de

expresión y la privacidad. Considera la Protección de los Datos Personales como una cuestión central de la seguridad digital, lo cual incluye el debido derecho al acceso a la información respecto a las medidas de protección de los datos personales.

Se afirma además, que es necesario establecer parámetros de transparencia y de rendición cuentas, que permitan verificar los avances alcanzados y el cumplimiento de las metas propuestas, resaltando la necesidad de auditorías de los sistemas informáticos.

Asimismo, se cuestiona la definición de Ciberseguridad abordada, en tanto la vincula directamente con Cibercrimen. En este sentido, propone el reemplazo del término Ciberseguridad por el de "Seguridad Digital".

Sugiere además el uso de técnicas de cifrado en las comunicaciones y para el resguardo de datos, como un principio fundamental a incluir en la nueva versión de la Estrategia, y la incorporación de evaluaciones de impacto anteriores a la implementación de medidas concretas de seguridad digital.

Recomienda además, la incorporación de la perspectiva de género, especialmente en el Objetivo relativo a la "Concientización, Capacitación y Educación".

4.2 Otra de las propuestas señala la necesidad de promover la seguridad desde el diseño como principio y durante todo el ciclo de vida; la protección de los datos personales y la privacidad de todas las personas; la incursión de la seguridad de la información y la protección de datos en los planes de educación de todos los niveles de formación; así como el fortalecimiento de las capacidades del CERT nacional y la promoción de la creación de CSIRT sectoriales.

Adicionalmente, sugiere la eliminación de la referencia al delito en la definición de ciberseguridad y la orientación del objetivo 3 al fortalecimiento de las capacidades de prevención, detección y respuesta ante incidentes de seguridad informática o ciberseguridad, en la misma línea.

4.3 Otra propuesta celebra con beneplácito la publicación de la Segunda Estrategia Nacional de Ciberseguridad, la cual se encuentra inspirada en las mejores prácticas, recomendando articular un modelo de coordinación tanto en los aspectos de prevención como de detección, alertas y respuestas de toda el tejido gubernamental nacional y subnacional.

Sugiere además, fortalecer la iniciativa de fomento de la industria nacional en ciberseguridad, tanto en infraestructuras como en el software, insistiendo en las buenas prácticas relacionadas con el uso de software de fuente abierta.

En cuanto a la identificación y protección de las infraestructuras críticas de información (objetivo 7 de la versión sometida a consulta), enfatiza la necesidad del trabajo coordinado público-privado.

4.4 Otro de los aportes cuestiona en su integralidad el texto de la Estrategia Nacional sometido a consulta, extendiendo sus objeciones al proceso de consulta, considerándolo inadecuado. Además, cuestiona los Principios Rectores de la versión preliminar de la Segunda Estrategia Nacional de Ciberseguridad, por considerarlos una ampliación de los principios expuestos en la primera versión de la Estrategia, manifestando su disconformidad con la incorporación del principio de "Respeto a la soberanía nacional" por considerar que no posee claridad suficiente.

4.5 Asimismo, entre los aportes recibidos, uno de los proponentes ha analizado el contexto actual de la ciberseguridad, señalando los diversos riesgos que amenazan tanto a entidades como a personas, citando la opinión de varios expertos, incluyendo varios gráficos e infografías explicativas. Se sugiere que podrían ser citados en la redacción ciertos documentos emanados de organismos internacionales reconocidos. Asimismo, se menciona que la falta de recursos dedicados al fortalecimiento de la capacidad en ciberseguridad y la escasez de conocimientos especializados y experiencia práctica podrían afectar los avances de la referida Estrategia, registrándose el mismo problema en otros países de la región.

También se destacan los problemas asociados a la falta de recursos humanos calificados y el logro de una cultura de ciberseguridad, señalando que estos puntos han sido tratados tanto en la Estrategia vigente como en la que se propone para su reemplazo. Se sugiere además, la revisión de la diferenciación entre Seguridad Interior y Defensa Nacional y expone algunos puntos que deberían considerarse.

4.6 Asimismo, uno de los aportes recomienda la creación y capacitación de un cuerpo o red de ciber diplomáticos; así como la adopción de estándares y requisitos de provisión de material informático, que involucre por ejemplo, la seguridad por defecto (desde el diseño) y control de cambios exhaustivo; la introducción de métricas; la retención del talento; y la profundización de la coordinación a nivel regional.

4.7 Otro de los aportes sugiere tener en cuenta diferentes tecnologías como la fibra óptica y los sistemas de telemetría y destaca la importancia de la capacitación.

También se referencia la necesidad de promover el impulso a las carreras de grado y posgrado en ciberseguridad y la creación de un catálogo de infraestructuras críticas.

Finalmente, se han formulado comentarios específicos vinculados a referenciar las tecnologías de la Operación que caracterizan a los entornos industriales; las vulnerabilidades y amenazas, el monitoreo, la vigilancia y la resiliencia.

5. Presentaciones provenientes de organismos y entidades internacionales

4.1 En este caso, una de las propuestas recibidas ofrece guías y modelos para redactar una nueva estrategia sobre la base de los criterios y parámetros que esa Organización considera apropiados.

Respecto a la estructura de la versión de la Estrategia Nacional bajo análisis, entre los puntos a destacar, se recomienda contemplar el financiamiento ya que todas las acciones deben estar presupuestadas; la unificación del glosario de términos y la incorporación de las cuestiones vinculadas al monitoreo y evaluación.

Con relación al contenido del documento, recomienda la inserción de nuevas temáticas, la consideración del tema relativo a la igualdad de género, diversidad e inclusión social, la promoción del desarrollo de la fuerza laboral, la apertura a tecnologías emergentes como la inteligencia artificial, el machine learning, el internet de las cosas, 5G, el blockchain, el Big Data y la computación cuántica, la seguridad en la nube, en el diseño y por defecto.

4.2 Finalmente, otra de las propuestas sugiere incorporar en el objetivo de fortalecimiento de capacidades de prevención, detección y respuesta, el análisis de vulnerabilidades, la ampliación

y mejora de las capacidades de detección y respuesta ante la fuga de información y ante amenazas al uso de servicios de cómputo públicos, y la construcción de capacidades para la detección del tráfico saliente del país hacia infraestructuras controlada por cibercriminales. Además, entiende oportuno que se incorpore a la comunidad internacional en el apartado del mismo objetivo, correspondiente a la coordinación, cooperación e intercambio de información con el gobierno.

6. Presentación proveniente de la comunidad técnica

La única propuesta en este caso, celebra el trabajo realizado para la elaboración de la Segunda Estrategia Nacional de Ciberseguridad, destacando que refleja las mejores prácticas en la materia. Incluye además, distintos ajustes a su texto, entre entre los que pueden citarse: la realización de acciones coordinadas, tanto preventivas como detectivas y de respuesta, con todo el sector gubernamental nacional y subnacional; la promoción y el uso de recursos públicos y privados para fortalecer la provisión a través de la industria nacional de infraestructura y software, especialmente el de fuente abierta; y la necesidad de retener el recurso humano calificado y de impulsar la protección de las infraestructuras críticas de información.