Consulta Pública: Segunda Estrategia Nacional de Ciberseguridad

Introducción.

La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional, sienta los principios rectores y desarrolla los objetivos centrales que permitirán fijar las previsiones nacionales en materia de protección del ciberespacio. Tiene como finalidad brindar un contexto seguro para su aprovechamiento por parte de las personas y organizaciones públicas y privadas, desarrollando, de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo e institucional acorde.

A partir del desarrollo de la Estrategia Nacional de Ciberseguridad, elaborada por el COMITÉ DE CIBERSEGURIDAD creado por el Decreto N° 577 del 28 de julio de 2017, modificado por el Decreto N° 480/2019, es necesario continuar desplegando acciones para el uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar la seguridad y el progreso de nuestra Nación.

Estas acciones se llevarán a cabo sobre la base de la coordinación y cooperación entre la Administración Pública Nacional, otros poderes nacionales, las administraciones y poderes de las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, municipales, el sector privado, las organizaciones no gubernamentales y las entidades académicas.

La irrupción de las Tecnologías de la Información y las Comunicaciones (TIC), junto a su continua evolución, ha significado un cambio de paradigma y punto de inflexión en la historia. Muchos de los aspectos de nuestra vida cotidiana se encuentran atravesados por este fenómeno, en tanto las personas encuentranen la tecnología un nuevo mundo interconectado donde desarrollar los aspectos más básicos circunstancia que se ha visto magnificada a partir de la irrupción del COVID-19, a raíz de lo cual, el teletrabajo y la educación a distancia se convirtieron en parte de la cotidianeidad.

Asimismo, las organizaciones se han redefinido en torno a estos avances, con independencia de su tamaño, el sector al que pertenecen, su ubicación geográfica o su objeto. Estas tecnologías han impactado notablemente en las estructuras económicas y en las relaciones humanas, erigiéndose como un medio imprescindible para el desarrollo.

La realidad exhibe que servicios esenciales para la vida de las personas y para la economía, como la energía, el agua, el transporte, las comunicaciones, la educación, la salud, el comercio y los servicios financieros, entre otros, tienen en la actualidad una fuerte dependencia de las redes informáticas.

Adicionalmente, la vigencia de las tecnologías de procesamiento masivo de datos (big data), la computación en la nube (cloud computing), Internet de las cosas (Internet of things IoT), el desarrollo de 5G y los avances en la inteligencia artificial, tanto así como la utilización de redes sociales y plataformas para la comunicación interpersonal, resulta determinante para los Estados incorporar la problemática dela ciberseguridad a la agenda gubernamental.

Es necesario trabajar para que los beneficios de estas innovaciones se distribuyan con justicia, equidad y con pleno respeto de los derechos humanos. Sin embargo, este horizonte también nos muestra amenazas y potenciales daños a los derechos de las personas y las organizaciones.

La Resolución N° A/RES/66/290 aprobada por la Asamblea General de las Naciones Unidas (ONU) establece que la seguridad humana “exige respuestas centradas en las personas, exhaustivas, adaptadasa cada contexto y orientadas a la prevención que refuercen la protección y el empoderamiento de todas las personas y todas las comunidades”. En este sentido, la ciberseguridad es un concepto amplio que va más allá de la seguridad informática, por lo cual debe centrar sus esfuerzos en prevenir actos disvaliosos que afecten los derechos de las personas, entre ellos su libertad, integridad física, privacidad de sus datosy propiedad privada.

Dicho esto, la ciberseguridad es abordada en la presente Estrategia como el conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las personas y las organizaciones, frente a amenazas, incidentes y delitos, entre otros, que utilicen como medio y/o fin un dispositivo informático.

También las acciones en el ciberespacio inciden en la actividad de las administraciones gubernamentales permitiéndoles transparentar y comunicar sus acciones de gobierno. En el mismo sentido, son sensibles a incidentes informáticos que pueden afectar su normal desenvolvimiento.

A su vez, aspectos como la paz y la soberanía de las naciones se ven interpeladas por las TIC. En ese marco,la acción del Estado cobra sentido a través del desarrollo de una Estrategia de Ciberdefensa, como elemento transversal al resto de los dominios de las Fuerzas Armadas, con su participación en el ciberespacio atendiendo las normativas vigentes y el Sistema de Defensa Nacional. En este sentido, se ratifica el espíritu de no proliferación de conflictos armados y desmilitarización del ciberespacio.

El ciberespacio exhibe dificultades relacionadas con la atribución de responsabilidad, las vulnerabilidades de las infraestructuras críticas de información, las grandes asimetrías que se manifiestan entre los países a partir de la globalización y las cuestiones vinculadas con el ejercicio de la soberanía, entre otras. En ese sentido, el ciberespacio representa un dominio soportado por infraestructuras físicas y sistemas de comunicación sobre el cual resulta desafiante, pero no por ello menos necesario, el ejercicio de la soberanía.

En el ámbito de las Naciones Unidas, la comunidad internacional se encuentra trabajando para lograr y profundizar consensos sobre lo que constituye el comportamiento responsable del Estado en el ciberespacio, con el objetivo común de mantener su carácter abierto, libre, estable, seguro y pacífico. En este marco, la REPÚBLICA ARGENTINA promoverá en todos los foros en los que participe, el uso pacífico del ciberespacio y apoyará toda iniciativa que tenga por fin la instauración de valores como la Justicia, el respeto al Derecho Internacional, el equilibrio y la reducción de la brecha digital entre las naciones, impulsando el diálogo y la cooperación. En este sentido, el ciberespacio debe constituirse en un dominio en el que impere la paz, impidiendo el desarrollo de posibles conflictos armados, o aquellos que puedan poner en riesgo la seguridad de la Nación y de su población.

Cabe señalar que en la REPÚBLICA ARGENTINA, la legislación establece una marcada diferenciación entre Seguridad Interior y Defensa Nacional, señalando claramente que el uso de recurso militar puedeemplearse en forma subsidiaria en tareas de seguridad interior únicamente en casos excepcionales, es decir, cuando este sistema resulte insuficiente a los fines de mantener el orden.

Esta intervención solo puede darse en situaciones de extrema gravedad donde peligra *“la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional”,* conforme lo establecido en la Ley de Seguridad Interior N 24.059.

La REPÚBLICA ARGENTINA, atendiendo los fenómenos de la recolección y procesamiento masivo de datos personales de las personas que llevan adelante las plataformas digitales, ha de adoptar medidas idóneas que promuevan la protección de los derechos de sus ciudadanos en este sentido en el ciberespacio.

Ante esta realidad que, con luces y sombras, muestra los enormes beneficios actuales y futuros que el ciberespacio brinda a la sociedad y las graves amenazas y riesgos para las personas y organizaciones de nuestro país, la presente Estrategia Nacional de Ciberseguridad promueve una serie de objetivos centrales, sustentados por principios rectores, que conducirán al desarrollo de planes, políticas y accionesconcretas para beneficio de la Nación.

Principios Rectores de la Ciberseguridad.

La Estrategia Nacional de Ciberseguridad se sustenta e inspira en los siguientes Principios Rectores:

PAZ Y SEGURIDAD EN EL CIBERESPACIO: Las acciones tendientes a brindar ciberseguridad al Estado y a la sociedad en su conjunto deben contemplar el principio de mantenimiento de la paz y la seguridad promovido en los Tratados Internacionales de los que la REPÚBLICA ARGENTINA es parte.

RESPETO POR LOS DERECHOS HUMANOS, LOS DERECHOS Y LIBERTADES INDIVIDUALES: La protección en materia de ciberseguridad debe contemplar el respeto por los derechos y libertades individuales consagrados en la CONSTITUCIÓN NACIONAL y en los Tratados Internacionales de los cuales la REPÚBLICA ARGENTINA es parte.

CONSTRUCCIÓN DE CAPACIDADES Y FORTALECIMIENTO FEDERAL: En materia de ciberseguridad el Estado Nacional debe promover políticas públicas que tengan por objeto construir capacidades de detección, prevención y respuesta a incidentes cibernéticos, en coordinación con los estados provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las competencias y recursos involucrados.

COOPERACIÓN INTERNACIONAL: El carácter transfronterizo de las amenazas requiere de la cooperación global y regional. El Estado Nacional debe articular acciones con otros actores internacionales y en particular, promover acuerdos regionales en América del Sur, generando todas las posibles sinergias, con el fin de minimizar los riesgos y mejorar los índices de resiliencia.

RESPETO POR LA SOBERANÍA NACIONAL: El carácter global de la red no implica la renuncia a los aspectos soberanos ineludibles como nación ni afecta la vigencia de las leyes nacionales que protegen los derechos y libertades de los ciudadanos argentinos y extranjeros en nuestro territorio. Este principio debe aplicar a las empresas proveedoras de Internet que brindan servicios en la REPÚBLICA ARGENTINA.

CULTURA DE CIBERSEGURIDAD Y RESPONSABILIDAD COMPARTIDA: La masividad y capilaridad del fenómeno digital conlleva la necesidad de que el Estado Nacional, en coordinación con los gobiernos provinciales, los municipios, la Ciudad Autónoma de Buenos Aires, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de sus competencias, promueva el desarrollo de una cultura de ciberseguridad que sea capaz de aumentar los niveles de concientización sobre el uso seguro y responsable del ciberespacio. Para esto es necesario fortalecer la cooperación y trabajo mancomunado con todos los sectores para procurar que las inversiones óptimas, que garanticen la seguridad de la información en sus organizaciones.

FORTALECIMIENTO DEL DESARROLLO SOCIOECONÓMICO: Atento que la ciberseguridad es indispensable para potenciar las posibilidades que brinda el ciberespacio para el desarrollo económico y social de la Nación, el Estado Nacional procurará establecer los instrumentos necesarios para propender un entorno ciberseguro.

Objetivos de la Estrategia Nacional de Ciberseguridad.

La presente Estrategia Nacional de Ciberseguridad se centra en los siguientes objetivos prioritarios:

Objetivo 1. Concientización, Capacitación y Educación en el uso responsable del ciberespacio y promoción para la formación de especialistas en Ciberseguridad.

La concientización, capacitación y educación estarán dirigidas al desarrollo de iniciativas y planes, cuyo objetivo es la generación de recursos humanos especializados en ciberseguridad.

Para ello será necesario:

- Crear un plan programático de concientización de alcance nacional sobre la seguridad en el ciberespacio, abarcativo de la sociedad en su conjunto.
- Incrementar las actividades de formación en materia de ciberseguridad y concientización en el uso responsable de las TIC en el ámbito educativo, en todo nivel.
- Desarrollar ejercicios técnicos en ciberseguridad, tanto a nivel gubernamental como en articulación con los sectores privado y civil.
- Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes y todo aquello que afecte a los derechos y libertades de los ciudadanos.
- Desarrollar iniciativas que fomenten la capacitación en materia de ciberseguridad con perspectiva de género en colaboración con el sector académico y sector privado, articulando, a su vez, una estrategia para la inserción de más profesionales en el sector público.

Objetivo 2. Desarrollo del marco normativo.

Generar, adecuar y actualizar los marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.

Para ello será necesario:

- Actualizar el marco jurídico tomando en cuenta las necesidades locales y los principios comunes mínimos con la comunidad internacional; en línea con las normas técnicas y las buenas prácticas reconocidas internacionalmente.
- Propender al desarrollo de un marco normativo que considere los roles y responsabilidades de los proveedores de servicios y productos tecnológicos.
- Propender al desarrollo de un marco normativo aplicable a las entidades y/o organizaciones responsables del manejo de infraestructuras críticas, infraestructuras críticas de información, su operación, comunicación y resguardo.

Objetivo 3. Fortalecimiento de capacidades de prevención, detección y respuesta.

Fortalecer las capacidades de prevención, detección y respuesta frente al uso del ciberespacio con fines ilícitos o indebidos.

Para ello será necesario:

- Ampliar y mejorar las capacidades de detección y análisis de amenazas para una defensa y protección más eficaz de los activos digitales.
- Ampliar y mejorar las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos críticos nacionales, contemplando asimismo los ataques a la ciudadanía.
- Optimizar y promover las capacidades de los organismos y fuerzas de seguridad con competencia en la investigación y persecución de la delincuencia, el crimen organizado y el terrorismo en el ciberespacio.
- Garantizar la coordinación, cooperación y el intercambio de información entre el gobierno nacional y los gobiernos provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las competencias de cada uno y los recursos involucrados.

Objetivo 4. Protección y recuperación de los sistemas de información del Sector Público.

Adoptar las medidas necesarias para que los sistemas de información que utiliza el Sector Público, en todos sus poderes y jurisdicciones, posean un adecuado nivel de seguridad y recuperación.

Para ello será necesario:

- Diseñar e implementar las políticas públicas necesarias para fortalecer la seguridad y resiliencia de los sistemas de información del Sector Público, incluyendo los mecanismos de control para la aplicación de las Políticas de Seguridad de la Información.
- Trabajar coordinadamente con los responsables de seguridad informática de los Entes Reguladores y otros organismos de la Administración Pública Nacional, las administraciones provinciales, de la Ciudad Autónoma de Buenos Aires y de los municipios, en los cuales se hayan identificado sistemas de información críticos.
- Garantizar el proceso de jerarquización y fortalecimiento de los recursos humanos encargados de la seguridad de los sistemas informáticos del Estado Nacional, asistiendo a aquellas jurisdicciones, gobiernos provinciales y/o municipales que requieran el apoyo del Gobierno nacional al respecto.

Objetivo 5. Fomento de la industria de la ciberseguridad.

Promover el desarrollo de la industria nacional en los sectores vinculados a la ciberseguridad.

Para ello será necesario:

- Impulsar el desarrollo de la industria de ciberseguridad nacional.
- Fomentar y potenciar capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a diferentes amenazas, promoviendo actividades de investigación, desarrollo e innovación (I+D+i), tanto en el sector

académico, organizaciones de la sociedad civil, como en entidades del sector público y privado.

Objetivo 6. Cooperación Internacional.

Contribuir a elevar las condiciones de ciberseguridad en el ámbito internacional, de manera de promover la paz y seguridad internacional.

Para ello será necesario:

- Promover el desarrollo de acuerdos a nivel bilateral, regional e internacional que contribuyan a mantener un ciberespacio abierto, libre, pacífico y seguro.
- Fortalecer la presencia de la REPÚBLICA ARGENTINA en todos los organismos internacionales, en materia de ciberseguridad.
- Promover el avance de la institucionalización del tratamiento de la ciberseguridad y el comportamiento responsable de los Estados en el ciberespacio en el ámbito de Naciones Unidas, en un formato abierto, participativo, flexible y de carácter permanente.
- Promover la participación de diversos sectores y actores en los procesos internacionales vinculados a ciberseguridad, sin perjuicio de las funciones asignadas al estado, de modo que se trate de un esfuerzo multisectorial.
- Fortalecer las instancias de coordinación interministerial, bajo la articulación del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, para el desarrollo y adecuación de la política exterior argentina en materia de ciberseguridad en los diversos foros y procesos regionales y globales, mediante la ciberdiplomacia.

Objetivo 7. Protección de las Infraestructuras Críticas Nacionales.

Promover el desarrollo de estrategias, políticas y medidas de acción para la protección de infraestructuras críticas nacionales, operación y comunicación.

Para ello será necesario:

- Promover la definición e identificación de las infraestructuras críticas del país, de información, operación y comunicación.
- Fortalecimiento de la articulación público-privada en resguardo de las infraestructuras críticas del país, en el marco de las respectivas responsabilidades de cada organización.
- Fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas cibernéticas.
- Promover esfuerzos coordinados dentro de las redes industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos.

- Favorecer una mayor inversión de las organizaciones en recursos orientados a la protección de sus infraestructuras.

Objetivo 8. Fortalecimiento del sistema institucional para el abordaje de la problemática de la ciberseguridad a nivel federal.

Instrumentar políticas públicas desde el gobierno nacional para asistir en la generación de instancias institucionales de abordaje de la problemática a nivel provincial en los Poderes Ejecutivo, Legislativo y Judicial.

Para ello será necesario:

- Generar espacios de concientización y articulación con los Poderes Legislativos y Judiciales, nacionales y provinciales; para abordar la importancia de contar con oficinas de gobierno provinciales para el abordaje de la problemática de la ciberseguridad a nivel jurisdiccional, fiscalías especializadas de delitos informáticos.
- Favorecer la creación de centros de respuesta de emergencias informáticas (CERTS o CSIRT) provinciales.
- Favorecer instancias de intercambio de información entre los representantes de los Poderes Legislativos Provinciales para la formulación de normativa vinculada a la ciberseguridad.

Anexo - Definiciones

Capacitación: proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso responsable del ciberespacio, así como para el diseño, implementación, creación y despliegue de tecnologías, servicios y buenas prácticas para brindar seguridad en el ciberespacio.

Ciberdefensa: Capacidades militares que se desarrollan para actuar en la dimensión ciberespacial en los ambientes operacionales terrestre, naval y aéreo; a efectos de anticipar, prevenir y rechazar ciberataques provenientes de agresiones externas de Estados, contribuyendo a garantizar las operaciones del Instrumento Militar asociadas a la misión principal, poniendo énfasis en contar con capacidades de vigilancia y control del ciberespacio de interés de la Defensa Nacional.

Ciberespacio: Entorno global compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones y la dimensión lógica creada a partir de uso de los mismos, que tiene como características esenciales, su dimensión transfronteriza, sin perjuicio de la soberanía de los Estados, su masividad y su vertiginosa y constante evolución.

Ciberdiplomacia: Uso de los métodos y las prácticas de la diplomacia aplicadas a los asuntos del ciberespacio y de la gobernanza digital.

Ciberseguridad: Conjunto de políticas, estrategias y acciones orientadas a elevar los niveles de seguridad de las personas físicas y jurídicas frente a incidentes y delitos que utilicen como medio y/o fin un dispositivo informático.

Concientización: proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del ciberespacio y junto a ello, la adopción de hábitos basados en las mejores prácticas.

Delito informático: Conducta tipificada penalmente que se comete mediante dispositivos electrónicos o contra un sistema electrónico u informático, u ocurre mediante redes informáticas o en el entorno digital.

Evento cibernético: Ocurrencia observable en un sistema de información. Los eventos cibernéticos podrían indicar que se está produciendo un incidente de seguridad informática**.**

Incidente informático o incidente de seguridad informática: Evento cibernético que: i. pone en peligro la ciberseguridad de un sistema de información o la información que el sistema procesa, almacena o transmite; o ii. infringe las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, sea o no producto de una actividad maliciosa.

Infraestructuras Críticas: aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Infraestructuras Críticas de Información: las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas.

Seguridad informática: Preservación de la confidencialidad, la integridad y la disponibilidad de la información y/o de los sistemas de información a través del medio cibernético. Asimismo, pueden estar involucradas otras propiedades, tales como la autenticidad, la trazabilidad, el no repudio y la confiabilidad.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-133944871-APN-SSTI#JGM

CIUDAD DE BUENOS AIRES
Martes 13 de Diciembre de 2022

Referencia: Anexo I - Segunda Estrategia Nacional de Ciberseguridad

---

El documento fue importado por el sistema GEDO con un total de 10 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.12.13 13:48:06 -03:00

Agustina BRIZIO
Subsecretaria
Subsecretaría de Tecnologías de la Información
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2022.12.13 13:48:07 -03:00