República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Informe

Número: IF-2023-81810563-APN-SSTI#JGM

CIUDAD DE BUENOS AIRES
Viernes 14 de Julio de 2023

Referencia: EX-2023-81004342- -APN-SSTI#JGM - Anexo I

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA

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 Nacional 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 encuentran en la tecnología un nuevo mundo interconectado donde desarrollar los aspectos más básicos; circunstancia que se ha visto magnificada luego de la pandemia del COVID, 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), las tecnologías de la operación, 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, hacen determinante que los Estados incorporen la problemática de la 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, adaptadas a 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, integridad y disponibilidad de sus datos, y propiedad privada.

La ciberseguridad es abordada en la presente Estrategia como el conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las infraestructuras de las TIC, que podrían, según el caso, ser potencialmente vulnerables ante amenazas y/o incidentes. De este modo, se tiene como objetivo prevenir acciones que afecten la administración del Estado, las organizaciones, los servicios esenciales y, en consecuencia, a las personas.

Las acciones en el ciberespacio inciden también en la actividad de las administraciones gubernamentales: permiten transparentar, comunicar sus acciones y aperturar datos y gestiones de gobierno. Esto hace que sean también sensibles a incidentes informáticos que pueden afectar su normal desenvolvimiento.

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. 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. 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 el término ciberdefensa refiere al área de Capacidad militar que se desarrolla para actuar en la dimensión ciberespacial de 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 su misión principal según Ley de Defensa Nacional y Decreto Reglamentario, poniendo énfasis en contar con capacidades de monitoreo y control del ciberespacio de interés para la Defensa Nacional.

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 beneficios actuales y futuros que el ciberespacio brinda a la sociedad y, también, las 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 acciones concretas para beneficio de la Nación.

A continuación, se enumeran una serie de principios rectores de esta Estrategia Nacional de Ciberseguridad y ocho objetivos que marcan el rumbo a seguir.

Principios Rectores de la Ciberseguridad.

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

1. 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.

2. RESPETO POR LOS DERECHOS HUMANOS Y LIBERTADES FUNDAMENTALES: La protección en materia de ciberseguridad debe garantizar el respeto por los derechos humanos y las libertades fundamentales.

3. CONSTRUCCIÓN DE CAPACIDADES Y FORTALECIMIENTO FEDERAL: En materia de ciberseguridad el Estado Nacional debe promover políticas públicas basadas en riesgos, que tengan por objeto construir capacidades de detección, prevención, monitoreo, resiliencia, respuesta y recuperación a incidentes cibernéticos, de forma articulada entre el Sector Público Nacional y 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.

3. COOPERACIÓN INTERNACIONAL: El carácter transfronterizo de las amenazas requiere de la cooperación global y regional. El Estado Nacional, de considerarlo oportuno, podrá articular acciones con otros actores internacionales. La promoción de acuerdos a nivel global, regional y subregional, en

particular con los países de América Latina y Caribe, contribuirá a generar todas las posibles sinergias, con el fin de minimizar los riesgos y mejorar los índices de resiliencia.

4. 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 fomentar las inversiones necesarias, que garanticen la seguridad de la información en sus organizaciones reconociendo que la misma es una responsabilidad compartida entre todas las partes.

6. 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.

7. SEGURIDAD EN EL CIBERESPACIO PARA PERSONAS EN SITUACIÓN DE VULNERABILIDAD O HISTÓRICAMENTE DISCRIMINADAS: Las políticas públicas y medidas que se desarrollen para la creación de un entorno digital seguro, deben prestar especial atención y garantizar la protección de personas que se encuentren en situación de vulnerabilidad y/o que hayan sido históricamente discriminadas.

8. PERSPECTIVA DE GÉNERO Y DERECHOS HUMANOS: El desarrollo de todas las actividades orientadas a la concreción de los Objetivos de la presente Estrategia y el Plan de Acción a desarrollarse en consecuencia, deberán contar con una perspectiva de género y teniendo como eje transversal la promoción y protección de los derechos humanos.

Objetivos de la Estrategia Nacional de Ciberseguridad.

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

Objetivo 1. 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 y 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 con los representantes de los Poderes Legislativos Provinciales para que, en conjunto y de manera armónica, se procure la formulación de normativa vinculada a la ciberseguridad.

Objetivo 2. 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.

- Fomentar la articulación público-privada en resguardo de las infraestructuras críticas, 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 de datos 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 3. 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, incluyendo todos sus poderes y organismos, posean un adecuado nivel de seguridad y recuperación.

Para ello será necesario:

- Diseñar e implementar las políticas públicas basadas en mejores prácticas internacionales 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 la profesionalización y jerarquización de los recursos humanos encargados de la respuesta ante incidentes informáticos del Estado Nacional, especialmente a aquellos del Gobierno Nacional que asisten a gobiernos provinciales y/o municipales ante requerimientos de apoyo.

- Fomentar la implementación de estándares, normas internacionales y la ejecución de auditorías que permitan fortalecer los sistemas de información del Sector Público Nacional.

- Promover la seguridad desde el diseño y en todas las fases de la implementación y adopción de proyectos tecnológicos del Sector Público Nacional, garantizando estándares adecuados para la protección de datos personales y de seguridad de la información.

Objetivo 4. Fortalecimiento de capacidades de prevención, detección y respuesta.

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

Para ello será necesario:

- Ampliar y mejorar las capacidades de detección y análisis de vulnerabilidades, compromisos en red, contactos con infraestructura adversaria y amenazas para una defensa y protección más eficaz de los activos digitales.

- Ampliar y mejorar las capacidades de detección, monitoreo 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. En cuanto a la lucha contra el terrorismo en todas sus formas, la Argentina privilegia su tratamiento en el marco de los foros multilaterales, a nivel global, en el ámbito de las Naciones Unidas; regional, en el marco del Comité Interamericano contra el Terrorismo (CICTE) de la OEA; y subregional, en el Foro Especializado en Terrorismo (FET) del MERCOSUR y Estados Asociados, entre otros.

- Promover el uso innovador de tecnologías emergentes, con el fin de fortalecer las capacidades de prevención, detección, respuesta y recuperación sobre las mismas.

- 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, comunidad técnica y la sociedad civil y la comunidad internacional, con una adecuada articulación de las competencias de cada uno y los recursos involucrados, conforme a la legislación nacional y tratados internacionales aplicables.

- Construir capacidades de monitoreo a nivel país que permita la detección del tráfico saliente del país hacia infraestructura controlada por cibercriminales, lo cual permite identificar los tipos de amenazas que las entidades públicas y privadas pueden estar enfrentando en el país y definir estrategias de protección eficaces.

- Ampliar, acelerar y mejorar las capacidades de detección y respuesta ante eventos de fugas de información que perjudiquen la privacidad de los ciudadanos y/o organizaciones.

- Ampliar y mejorar las capacidades de detección y respuesta ante amenazas asociadas al uso de servicios de infraestructura y servicios de cómputo públicos.

Objetivo 5. Concientización, Capacitación, Educación y promoción para la formación de especialistas en ciberseguridad.

La concientización, capacitación y educación estarán dirigidas al desarrollo de iniciativas y planes, con el fin de

comunicar los riesgos que conlleva el uso de las tecnologías, impulsar la adopción de medidas y hábitos basados en reglas del buen arte y generar 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 el sector privado y la sociedad.
- Fortalecer la capacitación en técnicas de prevención, detección, recuperación, 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.
- Implementar medidas a favor de la inserción y retención de especialistas de ciberseguridad en el Sector Público Nacional.
- Articular con el sector académico la inserción de la ciberseguridad en las currículas, junto con actividades específicas que aumenten las vocaciones en la materia.

Objetivo 6. Desarrollo del marco normativo.

Generar, adecuar, actualizar y adoptar 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:

- Impulsar la revisión continua y actualización del marco normativo aplicable a la materia tomando en cuenta las necesidades nacionales y en línea con las normas y reglas del buen arte internacionales.
- Propender al desarrollo e implementación de estándares y marcos regulatorios reconocidos internacionalmente y basados en riesgo y consenso, que consideren los roles y responsabilidades de los proveedores de servicios y productos tecnológicos, incluyendo ISO/IEC 27110 y 27103 o el marco de Ciberseguridad del NIST, entre otros.
- Propender al desarrollo de un marco normativo aplicable a las entidades y/o organizaciones responsables de la operación y protección de las infraestructuras críticas e infraestructuras críticas de información.

Objetivo 7. 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.

- Promover a nivel internacional un sistema de intercambio de información entre los equipos de respuesta a incidentes, con alertas tempranas con el fin de desarrollar un enfoque coordinado en la lucha contra las amenazas cibernéticas, conforme a la legislación nacional y tratados internacionales aplicables.

- Promover la adopción de estrategias de ciber resiliencia que permitan llevar adelante planes relacionados con inclusión digital, sustentabilidad y mejora de las capacidades de protección. La ciber resiliencia no deberá enfocarse únicamente en la mitigación de riesgos y vulnerabilidades o incidentes, sino también en su prevención, en la seguridad de la red, y en su conexión con otras redes internas y externas, siempre asegurando la continuidad de los servicios esenciales.

- Procurar una correcta identificación y evaluación de riesgos e impacto de las infraestructuras críticas de información contando, además, con planes de contingencia para asegurar la continuidad operativa de sus servicios.

Objetivo 8. 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.

- Articular con el sector privado, la comunidad académica, la sociedad civil y comunidad técnica estrategias de fortalecimiento de la industria de bienes y servicios nacionales de ciberseguridad.

- Fomentar y potenciar capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a diferentes amenazas sin perjuicio de la experiencia de usuario en el acceso a los servicios TIC, 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.

Digitally signed by Gestion Documental Electronica
Date: 2023.07.14 16:55:01 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2023.07.14 16:55:14 -03:00