ANEXO I

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA

Introducción.

La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional con el consenso del conjunto de la sociedad en forma multidisciplinaria y multisectorial, sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio. Su finalidad es 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 acorde.

A partir del desarrollo de la Estrategia Nacional de Ciberseguridad, a cargo del COMITÉ DE CIBERSEGURIDAD creado por el Decreto N° 577 del 28 de julio de 2017, se desplegarán las acciones para el uso seguro del Ciberespacio en nuestro país, 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, y municipales, el sector privado, las organizaciones no gubernamentales y las entidades académicas. Todo ello se hará efectivo en el marco del respeto a los principios recogidos en la CONSTITUCIÓN NACIONAL y a las disposiciones de los tratados y acuerdos internacionales a los que la REPÚBLICA ARGENTINA ha adherido.

La irrupción de las nuevas Tecnologías de la Información y las Comunicaciones ha significado un punto de inflexión en la historia. Todos los aspectos de la vida humana están atravesados por este fenómeno. Hoy las personas se comunican, se expresan, se educan, crean, comercian, investigan y desarrollan gran parte de su vida social y laboral en el Ciberespacio.

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 incrementado notablemente la eficiencia de las estructuras económicas, al punto tal que ya no es posible prescindir de ellas, ni concebir el futuro sin su creciente presencia.

Este fenómeno tiene enormes implicancias en cuanto a las posibilidades que brinda para el desarrollo humano, el progreso económico y los avances científicos. El horizonte que se abre hacia el futuro, es el de una promesa extraordinaria de progreso y bienestar. A manera de ejemplo, los últimos desarrollos en materia de “Internet de las cosas” permitirán alcanzar niveles de bienestar impensables hasta hace pocos años. Por ello es necesario trabajar para que los beneficios de estas innovaciones se distribuyan con justicia y equilibrio. Sin embargo, este horizonte también nos muestra graves amenazas y efectivos daños a los derechos de las personas y las organizaciones, en especial en lo referido a la privacidad de sus datos personales, así como también, riesgos potencialmente devastadores para la paz y la seguridad internacionales.

El Ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones, tiene entre otras, como características

esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución.

Como toda construcción humana, esta revolución tecnológica no es perfecta, contiene errores y debilidades y conlleva vulnerabilidades que es necesario reconocer. Uno de los prerrequisitos esenciales para que el Ciberespacio se despliegue en toda su potencialidad en beneficio de la humanidad, es alcanzar niveles razonables de seguridad y confiabilidad.

Nos encontramos frente a un cambio de paradigma, a partir del cual se han trasladado al entorno virtual una gran cantidad de actividades. 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 y los servicios financieros, entre otros, tienen en la actualidad una fuerte dependencia de las redes informáticas. Su protección es extremadamente compleja, entre otras razones, porque implica la coordinación de esfuerzos de múltiples actores públicos y privados.

Por otra parte, el uso de las Tecnologías de la Información y las Comunicaciones para el relacionamiento entre las personas, la interacción del Estado con el ciudadano o el surgimiento de la economía digital, entre otras actividades, ha contribuido al crecimiento exponencial del uso del Ciberespacio, aumentando consecuentemente los riesgos a los que se encuentran expuestas las personas y las organizaciones. Es necesario reconocer esta realidad y asumir su complejidad, como primer paso indispensable para enfrentar las dificultades y problemas y hallar las soluciones adecuadas.

La realidad nos muestra que en el Ciberespacio existen, entre otras, dificultades originadas en aspectos relacionados con la atribución de responsabilidad, las vulnerabilidades de las infraestructuras críticas, las grandes asimetrías que se manifiestan entre los países a partir de la globalización y las cuestiones vinculadas con el ejercicio de la soberanía. Este último concepto en particular, entendido como el ejercicio supremo del poder del Estado, está necesariamente vinculado a lo territorial. Sin embargo, Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía, poniendo a prueba el concepto antes mencionado e instaurando un nuevo paradigma que es necesario entender.

El escenario internacional presenta fuertes antagonismos y tensiones. Un número importante de países está haciendo un uso militar creciente del Ciberespacio, generando inestabilidad y desconfianza entre las naciones y temores en las sociedades. 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 disminución 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, sustrayéndolo de posibles conflictos armados.

Otra característica esencial de este proceso revolucionario, es su naturaleza global. Si bien la “brecha digital” entre países desarrollados y países en desarrollo es, en algunos casos, abismal, podemos afirmar que no hay región de la tierra que no esté, en alguna medida, alcanzada por estas transformaciones.

Atento el fuerte crecimiento de las empresas multinacionales que basan su negocio en la colección y el procesamiento de datos personales y que muchas veces tienen su sede y/o el despliegue de sus actividades en otras jurisdicciones, encontrándose por lo tanto sometidas a legislaciones foráneas, es necesario que la REPÚBLICA ARGENTINA tome debida nota de este fenómeno, a los fines de adoptar las medidas idóneas para proteger la privacidad de los datos de las personas y organizaciones de nuestro país.

Una paradoja que acompaña la masividad del uso del Ciberespacio es que, a mayor desarrollo, mayor es la vulnerabilidad. En efecto, a medida que una sociedad avanza y mayor es la cantidad de personas y organizaciones públicas y privadas que se conectan a las redes, mayores son los riesgos y desafíos. Sin perjuicio de ello, hoy el progreso y el bienestar en todos los campos, están indisolublemente ligados al desarrollo digital, cuya expansión es imposible de detener.

La naturaleza dual del Ciberespacio, cuyos componentes pueden ser utilizados tanto en beneficio como en perjuicio de las personas y las organizaciones, implica que puede caracterizarse lisa y llanamente a algunos de estos componentes como armas disponibles para la comisión de todo tipo de daños, e inclusive para la agresión contra Estados.

Enfrentar los desafíos que se presentan requiere articular adecuadas capacidades de prevención, detección, análisis, investigación, recuperación, defensa y respuesta, que constituyen elementos esenciales para alcanzar todos los beneficios que el uso seguro del Ciberespacio ofrece a nuestra Nación. Este fenómeno adquiere particular importancia en lo referido a las infraestructuras críticas de información.

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 acciones concretas para beneficio de la Nación.

Principios Rectores de la Ciberseguridad.

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

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

- LIDERAZGO, CONSTRUCCIÓN DE CAPACIDADES Y FORTALECIMIENTO FEDERAL: En materia de ciberseguridad el Estado Nacional debe asumir el liderazgo y 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.

- INTEGRACIÓN INTERNACIONAL: El carácter transfronterizo de las amenazas requiere de la cooperación global y regional. El Estado Nacional debe unir sus fuerzas con otros actores internacionales generando todas las posibles sinergias, con el fin de resolver esta problemática.

- CULTURA DE CIBERSEGURIDAD Y RESPONSABILIDAD COMPARTIDA: La masividad y capilaridad del fenómeno digital conlleva a la necesidad de que las organizaciones públicas y privadas, académicas, la sociedad civil y la ciudadanía, deban asumir las correspondientes responsabilidades para garantizar un Ciberespacio seguro. El Estado Nacional debe promover la generación de una cultura de ciberseguridad.

- FORTALECIMIENTO DEL DESARROLLO SOCIOECONÓMICO: Atento que la ciberseguridad es indispensable para potenciar las posibilidades que brinda el Ciberespacio para el progreso económico y social de la Nación, el Estado Nacional debe establecer los instrumentos necesarios para alcanzar un entorno ciberseguro.

Objetivos de la Estrategia Nacional de Ciberseguridad.

Objetivo 1) Concientización del uso seguro del Ciberespacio.

En el marco del presente documento, es el 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.

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.

• Fortalecer y articular con los sectores privados y las organizaciones civiles la promoción de contenidos de concientización.

• Incrementar las actividades de concientización en el ámbito educativo.

Objetivo 2) Capacitación y educación en el uso seguro del Ciberespacio.

En el marco del presente documento, es entendido como el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio.

Para ello será necesario:

• Promover la formación de profesionales, técnicos e investigadores.

• Desarrollar talleres y ejercicios, tanto gubernamentales como con los sectores privados y el sector civil.

• Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes.

• Incrementar las actividades transversales de formación en el sector académico.

Objetivo 3) Desarrollo del marco normativo.

Adecuar y generar las normas jurídicas, 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 la necesidad de principios comunes mínimos con la comunidad internacional.

• Actualizar el marco normativo técnico en línea con las normas técnicas y las buenas prácticas reconocidas internacionalmente.

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

Fortalecer las capacidades de prevención, detección y respuesta frente al uso del Ciberespacio con fines ilegales.

Para ello será necesario:

• Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas 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 de carácter nacional.

• 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 Estado Nacional y 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.

Objetivo 5) Protección y recuperación de los sistemas de información del Sector Público.

Garantizar que los sistemas de información que utiliza el Sector Público, incluyendo sus organismos descentralizados, posean un adecuado nivel de seguridad y recuperación.

Para ello será necesario:

• Desarrollar las políticas públicas necesarias para garantizar 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 y descentralizados, las administraciones provinciales, de la CIUDAD AUTÓNOMA DE BUENOS AIRES, de los municipios y el sector privado, en los cuales se hayan identificado sistemas de información críticos.

• Impulsar la realización de auditorías y la generación de métricas, que permitan evaluar la mejora constante de los niveles de seguridad de los sistemas y la capacidad de resiliencia de los mismos.

• Continuar el proceso de jerarquización y fortalecimiento de los recursos humanos encargados de la seguridad de los sistemas informáticos del Estado Nacional.

Objetivo 6) 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 las capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a las diferentes amenazas, fomentando las actividades de investigación, desarrollo e innovación (I+D+i) tanto a nivel público como privado.

Objetivo 7) Cooperación Internacional.

Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Para ello será necesario:

• Promover el desarrollo de acuerdos a nivel regional e internacional que contribuyan a la generación de un Ciberespacio pacífico y seguro.

• Fortalecer la presencia de la REPÚBLICA ARGENTINA en todos los organismos internacionales, en materia de ciberseguridad.

• Mantener una participación activa en todos los ámbitos académicos y técnicos internacionales en lo que se trabaje la temática.

Objetivo 8) Protección de las Infraestructuras Críticas Nacionales de Información.

Fortalecimiento de la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país.

Para ello será necesario:

• Promover la definición, identificación y protección de las infraestructuras críticas nacionales de la información.

• Articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques, a partir de los recursos y responsabilidades de cada organización.

• Fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas.

• Promover esfuerzos coordinados dentro de las redes industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos.

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Anexo

Número: IF-2019-49036224-APN-SGM#JGM

CIUDAD DE BUENOS AIRES
Viernes 24 de Mayo de 2019

Referencia: EX-2018-54284663-APN-DGDA#JGM. Estrategia Nacional de Ciberseguridad. Anexo I.

El documento fue importado por el sistema GEDO con un total de 9 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.05.24 15:29:58 -03'00'

Andrés Horacio Ibarra
Secretario de Gobierno
Secretaría de Gobierno de Modernización
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.05.24 15:29:58 -03'00'