Anexo

Número: IF-2021-22386693-GDEBA-SSGDMJGM

LA PLATA, BUENOS AIRES
Lunes 30 de Agosto de 2021

Referencia: Estrategia de Ciberseguridad 2021 - 2024.

ANEXO ÚNICO

ESTRATEGIA DE CIBERSEGURIDAD 2021 - 2024

1. INTRODUCCIÓN

En plena era de transformaciones y de incertidumbres, se debe proveer un horizonte sólido en materia de ciberseguridad, dado su carácter transversal, acorde a los nuevos tiempos y amenazas. Dicha definición debe ser capaz de atender los distintos retos y hacerlo desde una visión de cooperación público-privada y con el apoyo de una ciudadanía consciente de la realidad cambiante y comprometida con las soluciones propuestas.

La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, y su vulnerabilidad es uno de los principales riesgos para nuestro desarrollo como sociedad.

La ciberseguridad es un objetivo prioritario en las agendas de los diferentes gobiernos con el fin de garantizar niveles aceptables, basándose en que la confianza es un elemento fundamental.

Resulta necesario contribuir a la generación de un ciberespacio seguro y fiable, desde un enfoque multidisciplinario, abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podríamos enfrentar, incluyendo nuevas y emergentes.

El recurso humano es un factor crítico y necesario. Existe una diferencia significativa entre el número de puestos de trabajo requeridos con especialización en ciberseguridad, y las personas disponibles con el nivel de conocimiento adecuado.

La seguridad de las redes, y sistemas de información, requieren potenciar las medidas de prevención, identificación, protección, detección, respuesta y recuperación, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Las ciberamenazas son cada vez más sofisticadas y complejas, abarcan un amplio abanico de acciones y se caracterizan por su diversidad, tanto en lo que respecta a capacidades como a motivaciones. Asimismo, el ciberespacio es un ámbito sin fronteras ni demarcaciones jurisdiccionales claras, de débil regulación, donde resulta difícil la trazabilidad y la atribución territorial de las presuntas acciones delictivas.

La cibercriminalidad, por su parte, es un problema de primer orden que afecta a toda la ciudadanía, representando una de las amenazas más extendidas, y generalizadas, que se materializa de forma continua y que victimiza a miles de organizaciones y la ciudadanía. Las noticias falsas, así como los ataques contra los datos personales con el fin último de cometer ciertos delitos, robar credenciales, suplantación de identidad, y contra los procesos democráticos, entre otros, hacen necesario la definición de protocolos específicos en la materia.

Es por ello que, resulta necesaria la definición de una Estrategia de Ciberseguridad Provincial, que establezca el propósito, los principios rectores, sus objetivos, y líneas de acción, la cual permitirá establecer diferentes actividades tendientes a la protección de los activos de información.

2. PROPÓSITO Y PRINCIPIOS

En el marco de la aprobación del Plan Integral de Ciberseguridad, la presente estrategia define los lineamientos de la Provincia de Buenos Aires en la materia con relación al periodo 2021-2024, cuyo objetivo radica en contar con niveles adecuados de protección basados en la confidencialidad, integridad, disponibilidad y la privacidad de la información. Se hará énfasis en la necesidad de prevenir, identificar, proteger, detectar, responder y recuperarse frente a la potencial ocurrencia de incidentes cibernéticos, con vistas a reducir el nivel de riesgo a niveles aceptables, definidos previamente, promoviendo la ciberresiliencia. Es además un punto de inflexión en el pensamiento estratégico provincial, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

La Provincia de Buenos Aires precisa garantizar un uso seguro y responsable de las infraestructuras tecnológicas, los sistemas de información y las comunicaciones, a través del fortalecimiento de las capacidades de gestión de la ciberseguridad, potenciando y adoptando medidas específicas para contribuir a la generación de un ciberespacio seguro y fiable.

3. PRINCIPIOS RECTORES

La estrategia Provincial de Ciberseguridad, se sustenta y se inspira en los siguientes principios rectores:

1. Gestión de Riesgos y ciberresiliencia

La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras tecnológicas. El estado provincial debe asegurar niveles razonables de protección de aquellos activos de información que se consideren esenciales, mejorando la defensa contra las ciberamenazas y garantizando la toma de decisiones basada en la gestión del riesgo.

2. Coordinación

La respuesta frente a un incidente de ciberseguridad será efectiva, eficiente y se verá reforzada siempre que sea coordinada. Se debe generar una adecuada preparación y articulación de acciones entre todos los involucrados y posibilitar una gestión centralizada, lo que permite mantener una visión completa del escenario de la amenaza y posibilitará el empleo de los recursos disponibles de forma más rápida y eficiente.

3. Anticipación

Se debe priorizar las acciones preventivas sobre las reactivas. Es imprescindible disponer de la información de forma rápida y efectiva, lo más cercano al tiempo real, lo cual permitirá alcanzar una adecuada comprensión del escenario. Dicho factor resulta imprescindible para minimizar los tiempos de respuesta, y es un diferencial para reducir los impactos de las ciberamenazas.

4. Eficiencia

La ciberseguridad precisa del empleo de herramientas específicas, en algunos casos con alto costo derivado de su operación y desarrollo. Además, el escenario actual y futuro está marcado por la necesidad de obtener el máximo rendimiento de los recursos disponibles, lo cual obliga a orientar las acciones hacia la optimización y la eficiencia.

4. OBJETIVOS ESTRATÉGICOS

1. Establecer reglamentación complementaria en la materia

Es necesario la generación de regulación específica y complementaria al Decreto Nº 8/2021 en materia de ciberseguridad para la protección de los activos de información, basado en estándares internacionales y prácticas profesionales recomendadas.

Se debe impulsar un marco de trabajo sobre ciberseguridad que, desde un punto de vista neutral en cuanto a la tecnología, promueva e incentive la adopción de prácticas de ciberseguridad, aumente el volumen y la calidad de la información existente sobre ciberamenazas, e incorpore privacidad y protección de los datos personales en todas las iniciativas orientadas a asegurar las infraestructuras críticas.

1. **Líneas de Acción**

a. Establecer la definición de las infraestructuras críticas.
b. Generar regulación complementaria al Decreto Nº 8/2021 e impulsar la difusión, aplicación y verificación del cumplimiento del marco normativo de ciberseguridad y regulación complementaria.
c. Impulsar la generación de un marco de trabajo sobre ciberseguridad para todas las áreas de la Administración pública provincial y todas aquellas externas que quieran adherirse.
d. Normalizar y promover la generación de lineamientos de ciberseguridad en los productos y servicios de las TICs, facilitando el acceso a los mismos.

2. **Garantizar la identificación y niveles razonables de protección de los activos de información del sector público provincial, de los servicios esenciales y de las infraestructuras críticas.**

Es necesario asegurar la identificación, clasificación y establecer los niveles razonables de protección para los activos de información del sector público, los servicios esenciales, la cadena de suministro y de las infraestructuras críticas.

Para ello, se deben implementar medidas de seguridad enfocadas a mejorar las capacidades de prevención, identificación, protección, detección, repuesta y recuperación ante un potencial incidente cibernético, desarrollando nuevas soluciones y reforzando el trabajo coordinado.

1. **Líneas de Acción**

a. Identificar y clasificar las infraestructuras estratégicas, esenciales o críticas y de soporte de la Provincia de Buenos Aires, estableciendo los criterios necesarios que determinen el grado de criticidad de cada una de ellas incluyendo aquellos servicios que las soportan.
b. Impulsar el desarrollo de métricas de ciberseguridad que permita determinar los niveles actuales y su evolución.
c. Promover la detección activa de vulnerabilidades, la comprensión de su impacto y la aplicación de manera efectiva y eficiente de los controles que las mitiguen.
d. Establecer procesos relacionados con la gestión de continuidad del negocio para la protección de los activos de información del sector público, los servicios esenciales, la cadena de suministro y de las infraestructuras críticas.

3. **Generar capacidad de detección temprana, prevención de ciberamenazas y respuesta para limitar el impacto de posibles ciberincidentes.**

Se debe contar con capacidades adecuadas de detección temprana y prevención de ciberamenazas. De igual manera se debe disponer de una infraestructura robusta y resiliente, bajo la óptica de la gestión de riesgos.

Se debe prevenir, desalentar, disuadir y responder eficazmente a los incidentes cibernéticos y, en particular, aquellos que dañen las infraestructuras críticas, cadenas de suministro, instituciones y procesos democráticos.

1. **Líneas de Acción**

a. Ampliar y fortalecer las capacidades de prevención, identificación, detección, protección, respuesta, recuperación y resiliencia a los ciberataques e implementar mecanismos estandarizados de gestión. que incluya la investigación forense digital.
b. Asegurar la coordinación técnica y operacional de ciberseguridad entre los organismos, el intercambio de información sobre incidentes cibernéticos e indicadores de compromiso en el sector público provincial, privado, la sociedad civil, el mundo académico y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.
c. Responder de manera conjunta y ágil a una cibercrisis o ciberataque que afecte a la seguridad provincial.
d. Fortalecer las capacidades en técnicas defensivas frente a ciberataques complejos en tiempo real; a la adquisición de experiencias; a la evaluación; al testeo de nuevas tecnologías; a la coordinación y cooperación entre diferentes organismos y sectores, por ejemplo, fuerzas de seguridad, de protección de infraestructuras críticas, sector financiero, sector de salud, sector de educación entre otros, y ala identificación de talento
e. Intensificar la coordinación y cooperación, crear capacidades de ciberseguridad, fortaleciendo y ampliando las asociaciones e intercambios con diversos tipos de organizaciones de la sociedad civil, el mundo académico y el sector privado (municipales, provinciales, nacionales, internacionales).

4. **Generar la cultura en materia de ciberseguridad, su concientización, capacitación y formación.**

Para hacer frente a la complejidad de las actividades relacionadas con la ciberseguridad y a la rápida evolución tecnológica asociada con ella, el personal debe recibir concientización, capacitación, y una formación especializada de calidad y permanente en ciberseguridad tanto desde el punto de vista técnico, de gestión y jurídico.

Se debe promover un alto nivel de sensibilización sobre los riesgos relacionados con la ciberseguridad, dirigidas a la ciudadanía y a todas las organizaciones.

1. **Líneas de Acción**

a. Establecer un Programa de sensibilización, concientización, capacitación y formación continua en ciberseguridad a nivel técnico, de gestión y jurídico.

b. Identificar las necesidades de capacidades profesionales en materia de ciberseguridad, fomentando la colaboración con las instituciones educativas y de formación específica, impulsando la capacitación continua y la formación de profesionales en la materia.
c. Identificar, proponer y fomentar proyectos de ciberseguridad, con especial atención en el campo de la investigación y desarrollo.
d. Incrementar las campañas de sensibilización y concientización de ciberseguridad a todos los niveles, de manera coordinada entre las distintas entidades gubernamentales, evitando la duplicación de esfuerzos y garantizando la efectividad del proceso.
e. Promover eventos y talleres de ciberseguridad en primer lugar dirigidos a la administración Pública Provincial para luego poder avanzar con el resto de la sociedad civil y asegurar la participación en los foros y eventos especializados en la materia.

5. **Mejorar las capacidades para la detección, prevención y respuesta de ciberdelitos y cibercrimen**

Los ciberdelitos afectan a la ciudadanía las entidades e infraestructuras tecnológicas, los sistemas de información y las comunicaciones, conforme lo dispuesto con Código Penal Argentino, legislación complementaria y concordante. La delimitación territorial y legal del origen del potencial delito es difícil de alcanzar sin la colaboración de todas las partes interesadas. Para ello, es necesario establecer acuerdos y alcanzar un consenso lo más extenso posible.

Ninguna organización es autosuficiente para prevenir y perseguir la totalidad de los ciberdelitos que la afectan, es por eso que la cooperación en materia de ciberseguridad es vital. Resulta necesario la definición y difusión de protocolos, y los mecanismos de cooperación con los organismos especialistas en la materia.

1. **Líneas de Acción**

a. Establecer acuerdos de cooperación, intercambio de experiencias e información relacionada con la ciberseguridad y la lucha contra la ciberdelincuencia con entes idóneos en la materia.
b. Colaborar con la definición de los protocolos adecuados para la denuncia, los lineamientos y prioridades estratégicas en la prevención de los ciberdelitos y cibercrimen.
c. Contribuir al desarrollo de programas de sensibilización, concientización, capacitación y formación para la prevención de ciberdelitos y cibercrimen.
d. Fomentar el intercambio de información, experiencia y conocimientos, con las áreas de competencia.
e. Implementar canales institucionales para la radicación de las denuncias que se estimen pertinentes en aquellos casos que se considere que la acción de las amenazas persistentes pueda llegar a configurar una acción delictiva pasible de ser perseguida judicialmente.

Digitally signed by D'AGOSTINO Sandra Noemi
Date: 2021.08.30 15:56:46 ART
Location: Provincia de Buenos Aires

Sandra Noemi Dagostino
Subsecretaria
Subsecretaría de Gobierno Digital
Ministerio de Jefatura de Gabinete de Ministros

Digitally signed by GDE BUENOS AIRES
DN: cn=GDE BUENOS AIRES, c=AR, o=MINISTERIO DE JEFATURA DE GABINETE DE MINISTROS BS AS, ou=SUBSECRETARIA DE GOBIERNO DIGITAL, serialNumber=CUIT 30715471511
Date: 2021.08.30 15:56:48 -03'00'