Estrategia de Ciberseguridad 2021-2024 de la Provincia de Buenos Aires

Sandra D'Agostino, Alejandro Steinmetz y Damián Kruse

Sandra D'Agostino, Subsecretaria de Gobierno Digital, Ministerio de Jefatura de Gabinete de Ministros, Provincia de Buenos Aires, Argentina.
Alejandro, Steinmetz, Director Provincial de Sistemas de Información y Tecnologías, Subsecretaría de Gobierno Digital, Ministerio de Jefatura de Gabinete de Ministros, Provincia de Buenos Aires, Argentina.
Damián Kruse, Director de Seguridad Informática, Dirección Provincial de Sistemas de Información y Tecnologías.

{sandra.dagostino, alejandro.steinmetz, damian.kruse}@gba.gob.ar

Resumen. La revolución que ha vivido en los últimos años el denominado ciberespacio no solo trajo avances a la humanidad, sino que también está causando un aumento en las ciberamenazas. La confidencialidad, la integridad, la disponibilidad y la privacidad de la información se ven amenazadas por la rápida evolución de los ciberdelitos y el cibercrimen. El Estado Provincial no están exento de todos estos riesgos, sus infraestructuras tecnológicas críticas y los activos de información pueden verse seriamente comprometidos por un ciberataque. Por todo ello, la ciberseguridad se ha transformado en una necesidad para la gestión confiable de los activos de información, así como para asegurar los servicios digitales que el Estado Provincial brinda a toda la ciudadanía. Para dar respuesta a esa problemática se diseñó el Plan Estratégico de Ciberseguridad que tienen como objetivo fundamental implementar acciones de diversa índole: jurídica, formativa, cultural y metodológica, a fin de coordinar un conjunto de políticas de gestión que permitan un buen gobierno de seguridad de la información, para proteger los activos de información de la Provincia y sus infraestructuras críticas, así como para asegurar los servicios digitales que brinda el Estado a la ciudadanía.

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 propuesta.

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, requiere 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 ciudadanos. 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 Plan Integral de Ciberseguridad

Mediante el Decreto 8/21[1] se establece el Plan Integral de Ciberseguridad, el cual busca definir una taxonomía común y los mecanismos para:

- Describir la situación actual de ciberseguridad.

- Describir los objetivos estratégicos en materia de ciberseguridad.

- Establecer e implementar controles de ciberseguridad alineados a los objetivos de este Plan.

- Identificar y priorizar oportunidades de mejora mediante un proceso continuo y repetible.

- Monitorear el estado hacia la meta.

- Comunicar acerca de los riesgos de ciberseguridad a las partes involucradas.

Gobernanza y Gestión de Riesgos

Se define como Gobernanza al "…arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía…" [2].
Gobernanza de la seguridad de la información es la forma mediante la cual quienes gobiernan la organización proveen la dirección general y el control de actividades que afectan la seguridad de la información de la organización [3]. Proporciona dirección estratégica, garantiza que se alcancen los objetivos, maneja riesgos y usa responsabilidad de recursos de la organización, y supervisa el éxito o fracaso del programa de seguridad de la organización [4]. Es un subconjunto de la gobernanza institucional.
Un Plan de estas características debe tener un enfoque orientado a garantizar razonablemente el funcionamiento institucional desde la gestión de los riesgos, administrando adecuadamente los recursos del Estado Provincial.
Dentro de una organización hay distintas áreas de gobernanza que deben trabajar en forma integrada. Los objetivos de la gobernanza de la seguridad de la información no pueden definirse sin tener en cuenta los objetivos de las otras gobernanzas.
La gestión de riesgos de seguridad de la información es el proceso continuo de identificación, evaluación y tratamiento al riesgo. Las organizaciones deben conocer la probabilidad de que ocurra un evento y los posibles impactos resultantes. En base a ello, se puede determinar el nivel aceptable de riesgo de acuerdo a sus objetivos, su tolerancia y priorizar las actividades de ciberseguridad.
La gestión de riesgos de seguridad de la información involucra la identificación de los activos de información, determinar su valor y su criticidad, y proponer medidas de protección que sean justificables económicamente.

2 Objetivos y Aportes

- Promover acciones que garanticen la confidencialidad, integridad, disponibilidad y privacidad de los activos de información.

- Mejorar y generar nuevas instancias de comunicación, coordinación y cooperación entre los organismos que integran la administración pública provincial, asociaciones civiles sin fines de lucro, municipios y demás entidades tanto provinciales, nacionales e internacionales, con el propósito de fortalecer la confianza y unificar acciones frente a los riesgos del ciberespacio.

- Desarrollar procesos de análisis y de gestión que permitan identificar las vulnerabilidades, amenazas y riesgos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la preven-

ción y la recuperación ante incidentes cibernéticos.

- Identificar y priorizar las inversiones y recursos en materia de ciberseguridad, con el objetivo de disponer de un proceso efectivo, eficiente y armónico que permita identificar, proteger, detectar, responder y recuperar ante incidentes cibernéticos.

- Promover soluciones de ciberseguridad que permitan maximizar la robustez, resiliencia y continuidad de las operaciones frente a incidentes cibernéticos.

- Generar acciones de cultura y compromiso con la ciberseguridad potenciando capacidades humanas y tecnológicas.

2.1 Estructura

Con el objetivo de garantizar la gobernanza del plan se definió la siguiente estructura en tres niveles: Estratégico, Táctico y Operativo.

Plano Estratégico: Unidad Estratégica

Plano Táctico: Consejo Consultivo

Plano Operativo: Grupo de Trabajo de Ciberseguridad

Comités de Ciberseguridad

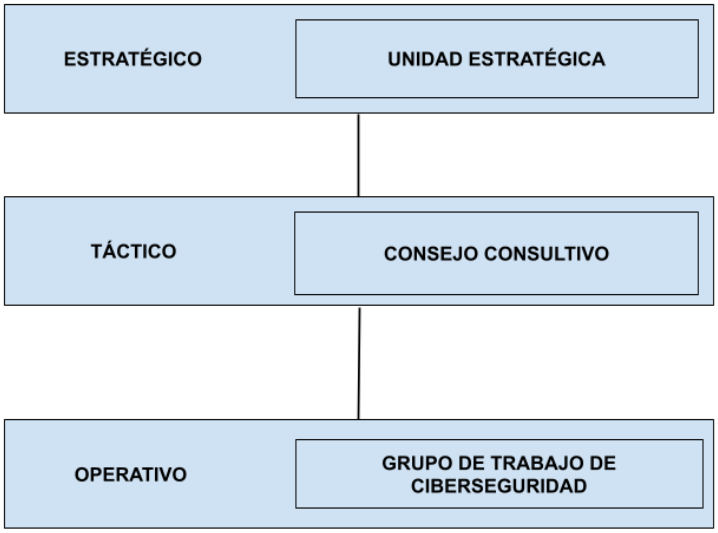

Fig.1: Estructura organizativa

La Unidad Estratégica tiene como objetivo principal el aprobar la estrategia en materia de ciberseguridad, definir los lineamientos de la gestión de riesgos y evaluar los reportes acerca de la efectividad y operación del Plan en el marco de las prioridades del Gobierno.

El Consejo Consultivo tiene como propósito proponer las mejoras del Plan Integral de Ciberseguridad, participar en todo lo concerniente a la mejor gestión de la Ciberseguridad en los temas específicos que les sean requeridos y colaborar en el fortalecimiento de las relaciones institucionales.

El Grupo de Trabajo en el plano Operativo tiene como objetivo principal el implementar las iniciativas aprobadas e informar su estado de avance.

Los Comités de Ciberseguridad de cada Organismo velan por que se trasladen los lineamientos y acciones definidas por la Unidad Estratégica, el Consejo Consultivo y el Grupo de Trabajo de Ciberseguridad.

3 Propósitos y principios

En el marco de la aprobación del Plan Integral de Ciberseguridad, se desarrolla la presente estrategia, la cual define los lineamientos de la provincia de Buenos Aires en la materia con relación al período 2021-2024, cuyo objetivo radica en contar con nive-

les adecuados de protección basados en la confidencialidad, la integridad, la 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.

4 Principios rectores

La estrategia provincial de ciberseguridad se sustenta e inspira en los siguientes principios rectores:

- **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.

- **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 cada amenaza y posibilitará el empleo de los recursos disponibles de forma más rápida y eficiente.

- **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.

- **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 recur-

sos disponibles, lo cual obliga a orientar las acciones hacia la optimización y la eficiencia.

5 Objetivos estratégicos

Para implementar este plan se plantean cinco objetivos estratégicos junto con los resultados esperados correspondientes a cada uno.

5.1. Establecer reglamentación complementaria en la materia

Es necesaria 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.

Resultados Estratégicos

- Establecer la definición de las infraestructuras críticas.
- Generar regulación complementaria al Decreto Nº 8/2021 e impulsar su difusión y aplicación, así como verificar el cumplimiento del marco normativo de ciberseguridad y regulación complementaria.
- 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.
- Normalizar y promover la generación de lineamientos de ciberseguridad en los productos y servicios de las TICs, facilitando el acceso a los mismos.

5.2 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 debe 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.

Resultados Estratégicos

- 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.

- Impulsar el desarrollo de métricas de ciberseguridad que permita determinar los niveles actuales y su evolución.

- 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.

- 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.

5.3. 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.

Asimismo, 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.

Resultados Estratégicos

- Ampliar y fortalecer las capacidades de prevención, identificación, detección, protección, respuesta, recuperación y resiliencia a los ciberataques e implementar mecanismos estandarizados de gestión.

- 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.

- Responder de manera conjunta y ágil a una cibercrisis o ciberataque que afecte a la seguridad provincial.

- Fortalecer las capacidades y habilidades en técnicas defensivas frente a ciberataques complejos en tiempo real; en la adquisición de experiencias; en la evaluación; en el testeo de nuevas tecnologías; en la coordinación y cooperación entre diferentes organismos y sectores, por ejemplo, fuerzas de seguridad, de protección de infraes-

tructuras críticas, sector financiero, sector de salud, sector de educación entre otros, y a la identificación de talento.

- 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).

5.4. 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, los/as trabajadores/as deben 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 los/as ciudadanos/as y a todas las organizaciones.

Resultados Estratégicos

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

- Identificar las necesidades de capacidades profesionales en materia de ciberseguridad, fomentando la colaboración con las instituciones educativas, impulsando la capacitación continua y la formación de profesionales en la materia.

- Identificar, proponer y fomentar proyectos de ciberseguridad, con especial atención en el campo de la investigación y desarrollo.

- 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.

- 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.

5.5. Impulsar acciones coordinadas contra el ciberdelitos y el cibercrimen

Los ciberdelitos afectan a los/as ciudadanos/as, las entidades e infraestructuras tecnológicas, los sistemas de información y las comunicaciones, conforme lo dispuesto en el Código Penal Argentino, legislación complementaria y concordante. La delimitación territorial y legal del origen del potencial delito es difícil de alcanzar sin la co-

laboración 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.

Resultados Estratégicos

- 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.

- Colaborar con la definición de los protocolos adecuados para la denuncia, los lineamientos y prioridades estratégicas en la prevención de los ciberdelitos y cibercrimen.

- Contribuir el desarrollo de programas sensibilización, concientización, capacitación y formación para la prevención de ciberdelitos y cibercrimen.

- Fomentar el intercambio de información, experiencia y conocimientos, con las áreas de competencia.

- 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.

6. Comparación regional

- Según los datos otorgados por el ultimo reporte de OEA (Organización de Estados Americanos) en materia de madurez en ciberseguridad[5,6], comparando los periodos 2016 - 2020, cabe destacar que, en el 2016 cuatro de cada cinco paises carecían de estrategias de ciberseguridad, mientras que a principios de 2020, un total de 12 paises habían aprobado estrategias nacionales de ciberseguridad, entre los que se pueden destacar, Colombia, Paraguay, Chile, Mexico, Argentina y Brasil. Se puede concluir además en que, si bien han mejorado las capacidades de ciberseguridad en la región desde el año 2016, el nivel de madurez promedio de la región, todavía se encuentra entre 1 y 2 (de acuerdo con el CMM[7], donde 1 significa etapa Inicial y 5 significa Dinámica). Es de destacar también que todas las dimensiones en el anterior informe, entre las cuales se incluye Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad) presentan niveles similares de madurez en ciberseguridad, lo que permite concluir que los paises de la región están abordando la ciberseguridad desde una perspectiva integral. Uruguay fue el país calificado con la madurez más alta de la región, en cuatro de las cinco dimensiones, entre las que se

pueden destacar con la madurez mas alta la organización y coordinación en respuesta a incidentes, la mentalidad gubernamental en materia de ciberseguridad y la confianza del usuario en los servicios del gobierno electrónico.

7. Conclusiones

El plan integral de ciberseguridad y la estrategia 2021-2024 sientan un precedente en la Provincia de Buenos Aires en materia de definición y planificación de la Ciberseguridad, estableciendo una visión estratégica acorde a los tiempos y necesidades de la Provincia.

La generación de capacidades en materia de ciberseguridad es fundamental en los ambitos de Gobierno, y resulta imprescindible fortalecer los marcos y procesos de gestión existentes mediante la definición de normativa y estrategia en la materia.

Referencias

1. Decreto 8/2021: https://normas.gba.gob.ar/ar-b/decreto/2021/8/225112
2. Real Academia Española y Asociación de Academias de la Lengua Española
3. ISO/IEC 27014, Recomendación ITU-T X.1054
4. IT Governance Institute. “Information Security Governance: Guidance for Boards of Directors and Executive Management” 2a edición, IT Governance Institute, 2006. ISACA edición, IT Governance Institute, 2006.
5. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
6. https://observatoriociberseguridad.org/
7. https://es.wikipedia.org/wiki/Capability_Maturity_Model

Referencias Bibliograficas

- “Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local” - Eduardo Alfredo Leiva
- “Ciberseguridad un nuevo desafío para la comunidad internacional” - Agnese Carlini