ANEXO I

PLAN INTEGRAL DE CIBERSEGURIDAD

I. Glosario

Activo de Información: todo aquello que genere, procese, almacene y transmita información, que tenga valor para una organización, y por lo tanto deba protegerse, incluido, pero no limitado a: hardware, software, información almacenada en cualquier tipo de medio, personas, reputación e imagen, entre otros.

Ciberamenazas: causa potencial de un incidente, que puede afectar a la Ciberseguridad.

Ciberdelincuencia: cualquier tipo de actividad en la que se utilice el ciberespacio y cuya consecuencia final recaiga en un hecho considerado como ilícito.

Ciberdelitos: conductas ilegales realizadas en el ciberespacio a través de dispositivos electrónicos y redes informáticasc, omo medio o fin.

Ciberespacio: un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes interdependientes, que incluye Internet, redes de telecomunicaciones y sistemas de información.

Ciberincidente: evento cibernético que pone en peligro la Ciberseguridad de un sistema de información o la información que el sistema procesa, almacena o transmite; o infringe las políticas de seguridad, los procedimientos de la misma o las políticas de uso aceptable, sea o no producto de una actividad maliciosa.

Ciberresiliencia: capacidad de una organización de continuar llevando a cabo su misión

anticipando y adaptándose a ciberamenazas y otros cambios relevantes en el entorno, y resistiendo, conteniendo y recuperándose rápidamente de ciberincidentes.

Ciberseguridad: es un conjunto de herramientas, políticas, directrices, enfoque de gestión de riesgos, procesos, acciones, formaciones, prácticas idóneas, aseguramiento y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de información.

Evento cibernético: ocurrencia observable en un sistema de información.

Infraestructura Crítica: aquella que resulta indispensable 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.

Sistema de información: conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

TIC: tecnologías de información y comunicación.

II. Introducción.

Es indiscutible que Internet ha evolucionado desde un lugar de intercambio de información a un espacio de comunicación e interacción para la economía, el trabajo, la cultura, la educación y el entretenimiento, tanto en el ámbito público como en el privado. Con el afán de hacer accesibles y asequibles los beneficios derivados del uso de Internet y de las tecnologías de la Información y las comunicaciones (TIC), a menudo no se tienen en cuenta los riesgos del ciberespacio.

El uso de las TIC trae consigo desafíos permanentes, no solo en lo que se refiere a sus cambios tecnológicos, sino también respecto del aumento del riesgo de delitos informáticos.

La confidencialidad, la integridad, la disponibilidad y la privacidad de la información se ven amenazadas por la rápida evolución de las ciberamenazas: el fraude electrónico, el robo y la destrucción de la información y la interrupción de los servicios, entre otros. La Ciberseguridad es una necesidad para la gestión confiable de los activos de información.

La revolución que ha vivido el denominado ciberespacio no solo ha traído consigo avances a la humanidad, sino que también está causando un aumento en las ciberamenazas. A ello se suma el peligro al que están expuestas las infraestructuras tecnológicas y activos de información de un Estado, el cual puede verse seriamente colapsado por un ciberataque. Por ello es que la Ciberseguridad ha dejado de ser un tema circunscrito al ámbito técnico, pasando a ser parte de la Política Pública.

Los gobiernos han definido políticas e han implementado estrategias para el acceso digital a los recursos del Estado por parte de otros organismos públicos, privados, funcionarios y ciudadanía en general. Se debe destacar también que las políticas anteriormente mencionadas deben ser objeto de evaluación y actualización constantes, a fin de garantizar un ciberespacio libre, abierto, seguro y resiliente.

En este escenario, resulta imprescindible contar con políticas de gestión y controles para la minimización de riesgos de seguridad de la información, que se enfoquen especialmente en la protección de los activos de información, considerando la seguridad desde el diseño, con reglas especiales para la adquisición y operación de soluciones tecnológicas.

Las características de los delitos informáticos, tales como el costo reducido de los ataques y su facilidad de ejecución, pueden causar graves dificultades en la seguridad de la información de la Administración Pública y los ciudadanos.

El avance de la tecnología debe estar soportado por un plan de Ciberseguridad, a los efectos de generar las capacidades y habilidades necesarias, buscando garantizar una buena gestión en la materia.

Una estrategia de Ciberseguridad es una expresión de la visión, los objetivos de alto nivel, los principios y las prioridades que orientan a abordar la Ciberseguridad de forma global, en todo el ecosistema digital. Es por eso que el Estado debe establecer una estrategia de Ciberseguridad en conjunto con la sociedad, de forma multidisciplinaria y multisectorial.

Su finalidad es brindar un contexto seguro para el aprovechamiento por parte de las organizaciones públicas y privadas, desarrollando acciones de identificación, protección, detección, respuesta y recuperación frente a las ciberamenazas.

El Estado debe implementar un conjunto de políticas de seguridad de la información, las cuales son declaraciones de alto nivel donde se plasman la intención, las expectativas y la dirección de un buen Gobierno de Seguridad de la Información. Estas políticas definen las pautas de gerenciamiento de la seguridad de la información, de acuerdo con los requisitos de la administración pública, normativos y legales.

Proteger los activos provinciales de la información es proteger los datos personales de la ciudadanía, resguardar apropiadamente la documentación generada, transmitida y almacenada por la Provincia, garantizando razonablemente la confidencialidad, integridad, disponibilidad y privacidad de la información.

Hay datos relacionados con el Estado cuya naturaleza determinan su característica estratégica para el desarrollo económico y productivo. Pero aquellos relacionados con infraestructuras críticas (IC) merecen un tratamiento adecuado: su administración inadecuada no solo pone en peligro a la industria sino también a toda actividad de la ciudadanía, tal como el sistema de salud, el educativo, la provisión de agua, de electricidad, de gas, transporte, seguridad, TIC, financiero, administración pública y servicios imprescindibles de consumo, entre otros.

Establecer este Plan define una taxonomía común y los mecanismos para:

1. Describir la situación actual de Ciberseguridad.
2. Describir los objetivos estratégicos en materia de Ciberseguridad.
3. Establecer e implementar controles de Ciberseguridad alineados a los

objetivos de este Plan.

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

5. Monitorear el estado hacia la meta.

6. Comunicar acerca de los riesgos de Ciberseguridad a las partes involucradas.

III. 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…".

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. 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. Es un subconjunto de la gobernanza institucional.

Un Plan de estas características debe enfocarse 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 del 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.

IV. Objetivos

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

2.- 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.

3.- 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 prevención y la recuperación ante incidentes cibernéticos.

4.- 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.

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

6.- Generar acciones de cultura y compromiso con la Ciberseguridad, potenciando capacidades humanas y tecnológicas.

V. Ámbito de Aplicación

El ámbito de aplicación del presente Plan comprende a todas las reparticiones del Gobierno de la Provincia de Buenos Aires, incluyendo a sus entes centralizados, descentralizados y autárquicos, como asimismo a las sociedades y empresas del Estado Provincial con participación estatal mayoritaria

VI. Alcance:

Los dominios sobre los que tiene alcance el plan son:

1.- Cultura, concientización, capacitación y formación

La necesidad de educar y concientizar en la materia lleva al reforzamiento de este pilar estratégico, cuyos objetivos son el desarrollo de una cultura de Ciberseguridad, el desarrollo de procesos de sensibilización e información a los ciudadanos y la formación de recursos humanos en materia de Ciberseguridad.

Para que la implementación del “Plan Integral de Ciberseguridad” sea sostenible a largo plazo es de gran importancia que se sensibilice y capacite a los ciudadanos sobre la importancia del uso seguro y responsable de las TIC. Por medio de la concientización ciudadana, se puede afectar positivamente el comportamiento, desarrollando una comprensión amplia sobre la ciberseguridad en toda la sociedad. El cambio se logra a través de la incorporación progresiva de buenas prácticas de Ciberseguridad, hasta que la misma se vuelva un hábito diario de los individuos, de las empresas y del gobierno.

Se deben promover campañas de sensibilización pública que aumenten el conocimiento sobre buenas prácticas de ciberseguridad y comportamiento seguro en el ciberespacio. Además, es importante elaborar proyectos de sensibilización enfocados en grupos específicos, a fin de que los mensajes sean más efectivos.

La falta de profesionales capacitados en Ciberseguridad es una preocupación a nivel mundial. Es un perfil que requiere de una capacitación constante y experiencia en el campo, es por ello que se debe garantizar la disponibilidad de personal entrenado en Ciberseguridad, en todos los sectores, Organismos y Áreas de Gobierno y en particular en aquellos especializados en el tratamiento y gestión de incidentes cibernéticos.

2.- Definición, identificación y protección de los activos de información

Todos los activos de información tienen que identificarse claramente y ser localizables. Debe definirse quién tiene su propiedad. Se debe identificar, documentar e implementar reglas para su uso aceptable y un adecuado nivel de protección.

Estos activos tienen que clasificarse en función a su valor, requerimientos legales, sensibilidad y criticidad para la organización. Además, se deben determinar las medidas de protección adecuadas.

3.- Capacidad de prevención, detección y respuesta ante incidentes

La Provincia debe contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes cibernéticos, bajo la óptica de gestión de riesgos.

Para el logro de lo planteado se debe cumplir con:

Diseñar e implementar medidas técnicas tendientes a prevenir, gestionar y superar los riesgos cuando estos se detectan, a fin de proteger los activos de información.

Implementar mecanismos estandarizados de reporte, gestión y recuperación de incidentes cibernéticos.

Fortalecer al Equipo de Respuesta frente a Incidencias de Seguridad Informática de la Provincia de Buenos Aires, identificado institucionalmente por las siglas CSIRT-PBA como repositorio de toda la información sobre ciberincidentes, herramientas, técnicas de protección y defensa, estándares y buenas prácticas

Fomentar la creación de equipos de respuesta a incidentes cibernéticos en los organismos dependientes del Gobierno de la Provincia de Buenos Aires, haciéndose extensivo a Organismos del Poder Ejecutivo y entes autárquicos, y a los Municipios y Organismos de otros poderes que deseen sumarse en cooperación con el CSIRT-PBA.

Mejorar las capacidades operativas y herramientas de los equipos de respuesta a incidentes, incorporando capacidades de detección, herramientas y procesos de intercambio de información, inteligencia de amenazas, entre otras.

4.- Definición, detección y protección de Infraestructuras Críticas

En el contexto de las Infraestructuras Críticas se hace necesario analizar, definir, implementar y revisar las cinco funciones continuas y concurrentes: identificación, protección, detección, respuesta y recuperación.

Se debe determinar qué se considera crítico y qué variables intervienen para determinar el impacto. Es una tarea inicial que requiere una identificación previa de los activos de información.

5.- Investigación de ciberdelitos y cibercrimen

El desarrollo de las TIC y el avance en su uso por parte de toda la sociedad han tenido un reflejo en la delincuencia y criminalidad, aprovechando estas últimas las tecnologías, ya sea como objeto y/o medio para cometer delitos tradicionales. Estos cambios en la delincuencia han convertido a la ciberdelincuencia en un reto significativo y merecedor de una respuesta adecuada por parte del Estado.

Por lo dicho anteriormente resulta fundamental destacar la necesidad de la definición y difusión de protocolos y cooperación con los organismos especialistas en la materia en los casos de detección de un posible ciberdelito.

6.- Establecimiento de alianzas de cooperación y colaboración

Se deberá potenciar la relación con otras organizaciones relacionadas con la Ciberseguridad, ya sean las mismas municipales, provinciales, nacionales, regionales o internacionales, a los efectos de generar los mecanismos de intercambio de información, experiencias y aquellas medidas de construcción de confianza que fomenten la cooperación y asistencia mutua en materia de Ciberseguridad.

7.- Cumplimiento de requerimientos externos e internos

Se debe fomentar la generación de un conjunto de normas y políticas de Ciberseguridad para entidades provinciales y operadores de infraestructuras esenciales. Dichas políticas deberán abarcar los requisitos de gobernanza, operacionales y técnicos, definirán las funciones y responsabilidades de las partes interesadas y establecerán mecanismos específicos a los efectos de promover la confianza y la seguridad en el ciberespacio.

Estas políticas deberán tener lineamientos relacionados con la Ciberseguridad en las etapas

de adquisición o desarrollo de software, definir programas de intercambio de información, coordinar la divulgación de vulnerabilidades, especificar criterios de seguridad, exigir la respuesta y notificación de incidentes de Ciberseguridad.

G O B I E R N O DE LA P R O V I N C I A DE B U E N O S A I R E S
2020 - Año del Bicentenario de la Provincia de Buenos Aires

Hoja Adicional de Firmas
Anexo

Número: IF-2020-30166421-GDEBA-DPAJSGG

LA PLATA, BUENOS AIRES
Lunes 28 de Diciembre de 2020

Referencia: Anexo I

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

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: 2020.12.28 18:15:20 -03'00'

Daniel Herrera
Director Provincial
Dirección Provincial de Asuntos Jurídicos
Secretaría General de Gobierno

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: 2020.12.28 18:15:20 -03'00'