CÁMARA DE DIPUTADOS
DE LA PROVINCIA DE SANTA FE

CÁMARA DE DIPUTADOS
MESA DE MOVIMIENTO
Recibido 16:22 Hs.
Exp. Nº 48533 C.D.

LA LEGISLATURA DE LA PROVINCIA DE SANTA FE

SANCIONA CON FUERZA DE

LEY:

ARTÍCULO 1 - Objeto. La presente ley establece las bases jurídicas, orgánicas y funcionales del Sistema Provincial de Ciberprotección y cuyo fin es conservar y fortalecer la Seguridad y Protección de los datos y la seguridad cibernética en las operaciones digitales de los ciudadanos, empresas e instituciones frente a incidentes de seguridad, incidentes de defensa, eventos, amenazas, riesgos y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.

ARTÍCULO 2 - Orden Público. Las disposiciones pertinentes de la presente ley son de orden público y de aplicación en todo el territorio de la Provincia de Santa Fe.

ARTÍCULO 3 - Definiciones. Para aplicar, concordar, relacionar e interpretar la presente Ley se consideran las siguientes definiciones:

a) Activo de información: cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

b) Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada.

c) Análisis de riesgos: proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo. Permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

d) Ciberataque: acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

e) Ciberespacio: ambiente complejo, que resulta de la interacción de personas, software y servicios en internet, por medio de dispositivos y redes conectadas.

f) Ciberseguridad: preservación de la disponibilidad, integridad y confidencialidad de la información en el ciberespacio.

g) Disponibilidad: capacidad de un servicio, un sistema o una información de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

h)Evento o suceso de seguridad de la información: ocurrencia o cambio detectado en el estado de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, un fallo de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

i) Incidente: ocurrencia que real o potencialmente resulte en una consecuencia adversa o amenaza para un sistema de información, o la información que el sistema procesa, almacena o transmite y que puede requerir una acción de respuesta para mitigar las consecuencias.

j) Incidente de defensa: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información e infraestructura tecnológica de las Fuerzas Armadas Argentinas, menoscabe o impida el cumplimiento de sus misiones y funciones conforme la legislación vigente.

k) Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u organismo.

i) Infraestructuras críticas: son aquellas que resultan indispensables 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.

m) Infraestructura tecnológica: conjunto de dispositivos de hardware, software y comunicaciones, utilizados por las organizaciónes para el cumplimiento de sus funciones, incluyendo el ámbito físico donde se encuentran ubicados.

n) Riesgo: potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/ o daño a los activos. Por lo general, se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

o) Seguridad Provincial: es la acción del Estado dirigida a proteger la paz, el orden, estabilidad, los principios, valores y derechos constitucionales, su acervo, recursos, orden público, bienestar y forma de vida de su pueblo.

p) Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

ARTÍCULO 4 - Finalidades. Conforme el objeto general, la presente ley tiene por finalidad:

1. Procurar la disponibilidad y uso seguro del ciberespacio.
2. Ampliar las capacidades de anticipación, prevención, respuesta y mitigación frente a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.
3. Velar por el cumplimiento de las mandas específicas de la Estrategia de Seguridad en la Provincia de Santa Fe y las particulares de la Estrategia Provincial de Ciberseguridad y la colaboración con el estado nacional en la Ciberdefensa.
4. Promover el cumplimiento de los fines establecidos en los artículos 14, 19, 20, 23, 29, 30, 35 y concordantes del Convenio sobre Cibercriminalidad o Convenio de Budapest, conforme la Ley Nacional 27.411.

ARTÍCULO 5 - Consejo Provincial de Ciberprotección. Dependencia funcional. El Consejo Provincial de Ciberprotección, así como el Centro Provincial de Ciberprotección, estarán bajo la dirección, competencia y aplicación del Ministerio de Gobierno Justicia y derechos Humanos de la Provincia de Santa Fe, absorbiendo y concentrando todo elemento o función que en materia de ciberseguridad que operen en otros ministerios, áreas o entes del Estado Provincial.

ARTÍCULO 6 - El Consejo Provincial de Ciberprotección será conducido por un Director General propuesto por el Gobernador de la Provincia de Santa Fe, tres Directores Adjuntos a propuestas del Ministerio de Gobierno Justicia y Derechos Humanos, el Ministerio de Seguridad y el Ministerio Coordinador de la Provincia respectivamente. El resto de su integración será plural debiendo estar representados al menos un representante del Ministerio Publico de la Acusación, un Representante del Poder Judicial de la Provincia y un representante de cada una de las Cámaras Legislativas.

ARTÍCULO 7 - Comité Provincial de Expertos. El Consejo Provincial de Ciberprotección contará, como órgano consultor, con un Comité Provincial de Expertos integrado por un titular y un suplente, por cada region de la provincia de Santa Fe. El Comité será presidido por el Director General del Consejo Provincial de Ciberprotección, quien lo convocará periódicamente y coordinará la producción de sus informes y recomendaciones.

ARTÍCULO 8 - Misiones y funciones del Consejo Provincial de Ciberprotección.

1. Diseñar las políticas, planes y acciones necesarias para prevenir ciberataques y restablecer, resguardar, fortalecer y consolidar un entorno digital seguro.
2. Realizar análisis de riesgos y fortalecer la ciberseguridad de la Provincia.

3. Diseñar y supervisar políticas de innovación, formación, especialización, difusión, prevención, forenses, de investigación, de compatibilidad, asistencia y cooperación nacional e internacional en la materia y sus afines.
4. Definir técnicamente una escala de riesgo que permita caracterizar a las infraestructuras críticas en todos los niveles sean éstas públicas, privas o mixtas.
5. Elaborar y actualizar el inventario de infraestructuras críticas de acuerdo con el grado de riesgo de las mismas. La elaboración se hará con la información suministrada por los entes territoriales, los Ministerios y entidades que tengan a su cargo dichas estructuras, y de las organizaciones privadas que sean incluidas.
6. Preservar debidamente la información y datos sensibles o aquella que pueda afectar la seguridad en la Provincia.
7. Interactuar con el sector privado, fijar controles, homologaciones, y solicitar medidas, planes, estándares y compromisos para mantener un entorno digital seguro, prevenir y responder a incidentes, incidentes de seguridad, eventos, amenazas y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.
8. Poner en funcionamiento el Centro Provincial de Ciberprotección, coordinar, supervisar y controlar el cumplimiento de sus misiones y funciones, así como garantizar su modernización, actualización y fortalecimiento continuo.
9. Conformar una Comisión Edilicia, que será la encargada de identificar la locación segura, de dirigir, coordinar y controlar la construcción y posterior actualización y fortalecimiento del Centro de Ciberprotección. Esta comisión contemplará las construcciones, equipamientos y necesidades propias y separadas a la seguridad, trabajará y exigirá los máximos criterios de seguridad y confidencialidad.
10. Receptar, considerar y supervisar el cumplimiento de las directivas y recomendaciones emergentes de la Estrategia de Seguridad Provincial.
11. Diseñar las estrategias de acción y asesorar en la implementación de medidas preventivas y operativas.

12. Generar planes, protocolos, normas, interacciones y cooperaciones para cumplir con sus fines y competencias.
13. Recibir las recomendaciones e informes del Comité Provincial de Expertos y desarrollar todas las políticas de interacción necesarias a sus fines.
14. Desarrollar un sistema de gestión de seguridad de la información de la Administración Pública Provincial.
15. Instrumentar mecanismos de capacitación y especialización de los operadores del Sistema de Ciberprotección, así como promover las actividades de investigación y desarrollo.
16. Se priorizarán los principios de eficacia y concentración y todas las instrumentaciones que correspondan, se cursarán por ante en Centro Provincial de Ciberprotección o los efectores que este anexe o coopere.

ARTÍCULO 9 - Centro Provincial de Ciberprotección. El Centro Provincial de Ciberprotección contará con un Director en Jefe, un Director Adjunto y una Mesa Operativa. Los roles, sus alcances, misiones y funciones serán dados por un reglamento interno confeccionado por el Director General, con el asesoramiento de la mesa operativa. Asimismo para operar contará con técnicos, administrativos y personal propio.

ARTÍCULO 10 - Misiones y funciones del Centro Provincial de Ciberprotección. Serán sus principales objetivos:
a) Aplicar las políticas, recomendaciones, directrices o encomiendas emergentes de la Estrategia de Seguridad, o la especial de Ciberseguridad.
b) Aplicar las políticas, planes y acciones emergentes del Consejo Provincial de Ciberprotección.
c) Centralizar, coordinar, optimizar, ejecutar los procesos, medidas e intervenciones preventivas, anticipatorias, reactivas y de mitigación frente a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas y ataques en el ciberespacio, que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.

d) Realizar todas las interacciones, cooperaciones y procesos de homogeneización necesarios al cumplimiento de sus fines.

e) Aplicar el sistema de gestión de seguridad de la información de la administración pública Provincial.

f) Podrá solicitar y contará con el acceso, disponibilidad y apoyo inmediato de todas las agencias, elementos y áreas del Estado para el cumplimiento de sus fines.

g) Deberá disponer lo necesario para el trabajo articulado y presente, con el Fiscal de Estado de la Provincia, Ministerio Público de la Acusación y el Poder Judicial Federal y Ordinario.

h) Cuando se trate de incidencias a la Seguridad de la Administración Provincial, el Gobernador será informado y ordenará el curso de acción correspondiente.

i) Instrumentar un mando de situación, gerenciamiento de eventos y emergencias.

j) Instrumentar un laboratorio de innovación, desarrollo y evaluación forense.

k) Anualmente elevará al Consejo Provincial de Ciberprotección un presupuesto de funcionamiento y fortalecimiento para que sea considerado al momento del diseño del Presupuesto General de la Provincia.

l) Ejecutar las mejores prácticas de transparencia y rendición de cuentas. Se preservará debidamente la información y datos sensibles.

ARTÍCULO 11 - Interagencialidad. Se invitará al Fiscal General de la Provincia a tener un ámbito integrado dentro del Centro de Provincial de Ciberprotección, para que sus efectores especializados puedan ejecutar la política de persecución penal y el ejercicio eficaz de la acción penal pública con inmediatez y oportunidad. La vía reglamentaria determinará lo necesario al funcionamiento coordinado. También se contará con un ámbito reservado como despacho de la Justicia Federal y Provincial competente, cuando se trate de incidencias de seguridad que requieran de su intervención in situ.

ARTÍCULO 12 - Los fondos y recursos para la construcción y ulterior funcionamiento de los órganos y estructuras creados por la presente se imputarán al presupuesto general de gastos y recursos de la provincia. El Poder Ejecutivo deberá afectar los recursos materiales y humanos en cantidad y calificación necesarias para el cumplimiento de la presente ley. A tal efecto en el primer presupuesto que remita a la legislatura, luego de promulgada la presente, deberá incluir los cargos y los recursos materiales necesarios para su implementación.

ARTÍCULO 13 - Autorizar al Poder Ejecutivo para reglamentar la presente y otorgar los actos administrativos necesarios para su implementación. El régimen de remuneración de los empleados de los órganos creados por la presente regirá por el Estatuto General del Personal de la Administración Publica Ley N.º 8525- Decreto 2695/83 y sus modificatorias. Se tales efectos se los encuadrara dentro del agrupamiento perteneciente a los agentes pertenecientes al S.I.P. aplicándose su régimen y remuneraciones.

ARTÍCULO 14 - El régimen de remuneración de los empleados de los órganos creados por la presente regirá por el Estatuto General del Personal de la Administración Publica Ley N.º 8525- Decreto 2695/83 y sus modificatorias. Se tales efectos se los encuadrara dentro del agrupamiento perteneciente a los agentes pertenecientes al S.I.P. aplicándose su régimen y remuneraciones

ARTÍCULO 15 - Créase en el ámbito de la Legislatura de la Provincia se crea la Comisión Bicameral Provincial de Fiscalización y Seguimiento del Centro Provincial de Ciberprotección, la que tendrá como finalidad fiscalizar que su funcionamiento se ajuste estrictamente a las normas constitucionales, legales y reglamentarias vigentes, verificando la observancia y respeto de las garantías individuales consagradas en la Constitución Nacional y Provincial La Comisión Bicameral tendrá amplias facultades para controlar e investigar de oficio. A su requerimiento, el

Centro Provincial de Ciberprotección, deberá suministrar la información o documentación que la Comisión solicite.

ARTÍCULO 16 - Comuníquese al Poder Ejecutivo.

DIPUTADO PROVINCIAL
OSCAR ARIEL MARTÍNEZ

FUNDAMENTOS

Señor presidente:

Como punto de partida ha de notarse que el presente se trata de un cuerpo normativo para el aseguramiento y protección frente incidentes que operan y transitan en el "ciberespacio". Este nuevo dominio es un ámbito virtual e intangible, pero generador de peligros y afectaciones absolutamente reales y por ende, un problema público que necesita ser legislado.

El término "ciberespacio" fue acuñado por el famoso novelista de ciencia ficción William Gibson en 1981, con lo cual queda claro que ninguna interpretación teleológica de las posteriores leyes 23.554 (Defensa Nacional) y 24.049 (Seguridad Interior), puede remontarnos o aplicar a esas virtualidades.

La modernidad ha puesto en una encrucijada al plexo reglamentario (Decretos, 727/06, 1691/06, 1714/09) y las doctrinas de respaldo.

En primer lugar, el ciberespacio ponía en "jaque" la separación orgánica y funcional entre la defensa y la seguridad interior. En segundo lugar, la decisión sobre cómo se resolvía esa separación frente a la problemática que el ciberespacio representaba para la seguridad.

Tanto la Ley de Defensa Nacional 23554, como la Ley de Seguridad Interior 24.059, obedecieron a un contexto histórico nacional e internacional determinado. Ambos cuerpos legales, que han permitido transitar años de la vida nacional, hoy han quedado atrasados a los nuevos fenómenos a regular, anticipar y prevenir.

En relación al quinto dominio, la doctrina especializada ha dicho: "El espacio cibernético, junto con los tradicionales ambientes terrestre, marítimo, aéreo y espacial es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. Esto puede demostrarse si se observa a las instituciones universales y regionales de seguridad como la ONU, la OEA, la NATO y la OSCE que han incorporado en sus estructuras a organismos competentes

sobre el tema, así como diversos países que han incluido la problemática del espacio cibernético a sus agendas de estrategia de seguridad ya que los incidentes y los ataques cibernéticos se han convertido en una fuente de amenazas en el mundo globalizado, debido a su capacidad de acceso a sistemas de información.

En consecuencia es necesario flexibilizar los esquemas rígidos y compartimentados, buscando miradas multidimensionales en ámbitos donde la complementariedad se transforme en valor agregado, dinamismo y fortaleza.

También el desarrollo de nuestra seguridad se lentificaría por desinversión y falta de hipótesis de asistencia y colaboración en situaciones que demandan de su presencia y auxilio profesional.

En algunos momentos puntuales de nuestra historia reciente, el salto colaborativo pudo expresarse en los hechos. Prueba de ello es la fundamentación del Decreto 1091/11, que da lugar al operativo llamado "Escudo Norte", donde para luchar contra la narcocriminalidad y el contrabando en nuestras fronteras establecen un operativo específico.

Nuevas amenazas y riesgos vuelven permeables y obsoletas nuestras respuestas individuales. Hay campos, como el quinto dominio, necesariamente mixtos e incluso superpuestos, que requieren de la utilización de los recursos tanto de la seguridad como de la defensa e incluso de otras áreas del Estado en forma integrada.

A la indefinición por falta de previsión del legislador original ha de sumarse la súper población de efectores, la concurrencia de competencias y un desorden organizativo que en lugar de minimizar vulnerabilidades las acrecienta.

En cuanto a mandas relativas a la tipificación legal, a los institutos procesales y la cooperación internacional, la República Argentina por Ley N° 27.411, adhirió al Convenio sobre Ciberdelito del Consejo de Europa, adoptado en la Ciudad de Budapest, República de Hungría, el 23 de noviembre de 2001.

Este ingreso a las protecciones y cooperaciones internacionales además es dinámico, pues de la norma madre se desprenden los protocolos que nuestro país también afirma y consolida.

En esta materia nuestro derecho interno está en constante progreso, abarcando entre otras: la Ley 26.388 (Ley de delito informático); 25.326 (Ley de protección de datos personales); 25.506 (Ley de firma digital); 26.904 (Ley de Grooming); los Decretos reglamentarios 1558/2001, 2628/2002 (dictados por el Poder Ejecutivo Nacional); los Decretos 577/2017, 480/2019 (de creación del Comité de Ciberseguridad, dictados por el Poder Ejecutivo Nacional); las Decisiones Administrativas 641/2021, 6/2021 (de la Jefatura de Gabinete de Ministros); las Disposiciones 6/2021, 1/2021, 3/2013 (de la Administración Pública Nacional) y las Resoluciones 580/2011, 1523/2019, 829/2019 y 141/2019 (de la Jefatura de Gabinete de Ministros), con más sus antecedentes.

Que la voluntad emergente de estas normas, de los órganos por ellas instrumentados, así como de la modernización de la ley penal, refiere el interés nacional permanente en mantener un "entorno digital seguro".

La velocidad, la mutación y el camuflaje son características esenciales de los ciberataques, es por ello que los Estados están cambiando sus marcos legales y estrategias de acción.

Nuevos dominios como el ciberespacio no sólo son puertas de acceso directas y poco detectables al menoscabo de los bienes jurídicos sujetos de protección, sino a la propia integridad, estabilidad y permanencia de los Estados, la paz y el bienestar de sus pueblos.

El Presidente del Gobierno de España Mariano Rajoy Brey, en su mensaje de presentación de la Estrategia de Seguridad Nacional de 2013, ya advertía: "A los riesgos y amenazas tradicionales se suman, en efecto, otros nuevos de naturaleza generalmente transnacional, que se interconectan y potencian su peligrosidad, a la vez que aparecen nuevos espacios abiertos que facilitan su expansión e impacto. El ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil

control, y en consonancia, la ciberseguridad es uno de los principales ámbitos de actuación de esta Estrategia".

"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".

Es importante recordar también que el desarrollo del marco normativo, al fortalecimiento de capacidades de prevención, detección y respuesta, a la protección y recuperación de los sistemas de información del sector público y a la cooperación con el sector privado es objetivo de esta norma. Cada una de estas previsiones y fines se reflejan en el articulado del presente proyecto de ley.

En la faz criminal, el ciberdelito es una variedad ilícita que se monta en la innovación y por lo tanto hay que construir, no sólo nuevas definiciones y tipicidades que recepten sus prácticas, sino la herramienta material donde las capacidades humanas de nuestros expertos puedan desarrollar todo su potencial preventivo, forense y auxiliar.

Las estrategias de Ciberseguridad son herramientas esenciales al Estado moderno, como compendio totalizador de riesgos y amenazas posibles al Estado, a los Derechos y el progreso de su gente.

Una estrategia de Seguridad Nacional puede ser un libro arrumbado en un cajón, un documento que sólo pueden entender unos pocos, o una herramienta útil a la "defensa común y el bienestar general".

Si tuviese que emplear un sólo término para expresar lo que significa para el Estado contar con una Estrategia de Seguridad Nacional y su entorno instrumental, sin dudas la definiría como un ACTIVO.

En base a las realidades antes descriptas, que ya no tocan nuestra puerta, sino que nos dañan en el interior de la casa, es necesario desarrollar un efector potente, especialmente diseñado a sus fines y que nos proteja en forma organizada, correctamente financiada y sostenida como política consensuada del Estado.

Por lo antes dicho, solicito a nuestros pares que nos acompañen con su voto.