VERSION PRELIMINAR
SUSCEPTIBLE DE CORRECCION
UNA VEZ CONFRONTADO
CON EL EXPEDIENTE ORIGINAL

DIRECCION GENERAL DE PUBLICACIONES

(S-1713/2023)

PROYECTO DE LEY

El Senado y Cámara de Diputados,…

ARTÍCULO 1°. Créase la AGENCIA NACIONAL DE CIBERSEGURIDAD (ANCIBER) como ENTE AUTÓNOMO en el ámbito de la JEFATURA DE GABINETE DE MINISTROS, con autarquía económica financiera, con personería jurídica propia y con capacidad de actuar en el ámbito del derecho público y privado.

ARTÍCULO 2º. Los objetivos de la ANCIBER serán:

a) Diseñar y ejecutar políticas de ciberseguridad, en coordinación con los organismos del Estado Nacional con competencia en la materia.

b) Elaborar y ejecutar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad.

c) Impulsar acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de ciberseguridad, articulando proyectos con las diferentes áreas del Estado Nacional involucradas.

d) Participar en instancias de cooperación internacional en la materia.

e) Proponer proyectos de normas relacionados con la ciberseguridad en la República Argentina.

f) Desarrollar el Programa Nacional de Infraestructuras Críticas de la Información de la Administración Pública Nacional incluyendo la generación de capacidades de detección, defensa, respuesta y recuperación ante incidentes cibernéticos y de seguridad.

g) Impulsar y promover la resiliencia de los sistemas definidos como críticos en el Sector Público Nacional.

h) Desarrollar y ejecutar un plan de capacitación permanente en materia de ciberseguridad en el ámbito de la Administración Pública Nacional, contemplando las buenas prácticas y experiencias internacionales exitosas en la materia.

i) Colaborar, junto a organismos y centros de investigación públicos y privados, en la promoción de planes, programas y proyectos de innovación

DIRECCIÓN GENERAL DE PUBLICACIONES

tecnológica en materia de ciberseguridad, en coordinación con los organismos competentes en la materia.

ARTÍCULO 3°. Funciones. Son tareas de la ANCIBER:

a) Desarrollar la Estrategia Nacional de Ciberseguridad, que incluya capacitación federal, en coordinación con las áreas competentes de la Administración Pública Nacional.

b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.

d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.

e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional.

g) Informar a la población respecto de incidentes cibernéticos y de seguridad según corresponda en la medida que no se contraponga con la seguridad de las redes y sistemas de información.

h) Promover la investigación académica sobre ciberdelito, fomentando la perspectiva de género y federal en el ámbito profesional de especialistas en ciberseguridad, articulando con las instituciones educativas que considere pertinente.

i) Crear y mantener actualizado el registro permanente de infraestructuras críticas nacionales.

j) Crear el registro de equipos de respuesta ante incidentes de seguridad informática.

k) Proteger las Infraestructuras Críticas de la Información del Sector Público Nacional y Organismos Privados, cuya interrupción o destrucción pueden tener una repercusión significativa para la sociedad.

l) Generar iniciativas y capacitaciones orientadas a mejorar los niveles de ciberseguridad de la ciudadanía y la sociedad en general.

DIRECCIÓN GENERAL DE PUBLICACIONES

ARTÍCULO 4°. El gobierno y administración de la ANCIBER estará a cargo de un Directorio integrado por UN (1) Presidente con rango de Secretario y DOS (2) Vocales con rango de Subsecretario, los que durarán CUATRO (4) años en sus funciones pudiendo ser designados nuevamente.

El Directorio formará quórum con DOS (2) de sus miembros. Sus resoluciones se adoptarán por mayoría simple. El Presidente tendrá doble voto en caso de empate. La totalidad de los funcionarios antes mencionados serán designados por el PODER EJECUTIVO NACIONAL.

ARTÍCULO 5°. El Directorio de la ANCIBER tendrá las siguientes funciones y facultades:

a) Dictar el reglamento interno del cuerpo.

b) Promover las relaciones institucionales de la Agencia y, en su caso, suscribir convenios con organizaciones públicas o privadas, nacionales o extranjeras, para el logro de sus objetivos en coordinación con los organismos con competencia en la materia.

c) Dictar las normas reglamentarias necesarias para el funcionamiento de la Agencia.

d) Proveer la información pertinente para la confección del presupuesto anual de la Agencia.

e) Elevar el anteproyecto de presupuesto del organismo.

f) Administrar los recursos provenientes del presupuesto nacional y los bienes del organismo.

g) Aceptar herencias, legados y donaciones, subvenciones que le asignen organismos públicos o privados, nacionales o extranjeros.

h) Implementar el Plan Estratégico definido por el Comité Asesor.

i) Requerir a los distintos organismos de la Administración Pública Nacional, la información necesaria a fin de fortalecer el accionar de la Agencia.

j) Remitir a las Comisiones correspondientes del Congreso los informes correspondientes de acuerdo a la presente ley.

DIRECCIÓN GENERAL DE PUBLICACIONES

ARTÍCULO 6°. COMITÉ ASESOR. El Comité asesor de la ANCIBER estará integrada por:

a) Dos (2) representantes de la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la JEFATURA DE GABINETE DE MINISTROS;

b) Dos (2) representantes del MINISTERIO DE DEFENSA;

c) Dos (2) representantes del MINISTERIO DE SEGURIDAD;

d) Dos (2) representantes del MINISTERIO DE RELACIONES EXTERIORES Y CULTO y;

e) Dos (2) representantes del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS,

f) Un (1) representante del MINISTERIO CIENCIA, TECNOLOGÍA E INNOVACIÓN,

g) Un (1) representante del Sistema Universitario Nacional,

El Presidente de la ANCIBER actuará como Director Ejecutivo del Comité Asesor. En tal carácter, deberá proponer el reglamento interno de funcionamiento del mismo.

ARTÍCULO 7º. El COMITÉ ASESOR deberá presentar el Plan Estratégico Nacional de Ciberseguridad a los fines de su implementación.

El COMITÉ ASESOR se reunirá periódicamente para merituar el impacto del Plan e introducir las enmiendas y adecuaciones que fueren menester.

Artículo 8°. La ANCIBER será asistida en sus funciones por un CONSEJO CONSULTIVO conformado por expertos nacionales y/o internacionales de reconocida especialización en la materia, a los fines de formular recomendaciones para el mejor cumplimiento de los objetivos de la ANCIBER.

ARTÍCULO 9º. Los procesos de conservación, transmisión, consulta, divulgación y tratamiento de información realizados en el marco de la presente ley deben llevarse a cabo siguiendo las normas nacionales sobre Protección de Datos y estándares internacionales de acuerdo a lo definido por el Comité Asesor.

ARTÍCULO 10º. Las dependencias de la Administración Pública Nacional y sus organismos descentralizados tendrán la obligación de reportar a la ANCIBER respecto de aquellos incidentes que tengan o puedan tener

DIRECCIÓN GENERAL DE PUBLICACIONES

efectos adversos reales en la seguridad de las redes y sistemas de información.

ARTÍCULO 11º. La relación del personal se encuadrará en el marco de la Ley de Contrato de Trabajo Nº 20.744 (t.o. 1976) y sus modificatorios.

ARTÍCULO 12º. Las Comisiones de Seguridad Interior y Narcotráfico y de Seguridad de las Cámaras de Senadores y Diputados serán competentes para intervenir en el seguimiento de la Agencia creada en el artículo 1° de la presente. A tal fin, tendrán las siguientes funciones:

a) Recibir el 31 de marzo de cada año el plan de acciones previstas al 31 de marzo del año siguiente;

b) Recibir informes semestrales, el 31 de mayo y el 30 de noviembre de cada año, acerca de la marcha y la implementación de las partidas presupuestarias establecidas en el Presupuesto Nacional en el marco de la presente ley;

c) Requerir al Directorio de la ANCIBER los informes necesarios sobre el cumplimiento de la presente ley;

d) Formular las observaciones y sugerencias que se estime pertinente remitir al Directorio de la ANCIBER.

ARTÍCULO 13º. Los recursos operativos de la ANCIBER serán los siguientes:

a) Las partidas presupuestarias asignadas por la Ley de Presupuesto o leyes especiales;

b) Los fondos provenientes de los servicios prestados a terceros;

c) Las donaciones, aportes no reembolsables y legados que reciba;

d) Los intereses y beneficios resultantes de la gestión de sus propios fondos y/o activos;

e) Todo otro ingreso no previsto en los incisos anteriores, provenientes de la gestión del Organismo.

ARTÍCULO 14°. Deróganse todas las disposiciones del decreto N° 480/19 y sus modificatorios, y toda norma que se oponga a la presente.

DIRECCIÓN GENERAL DE PUBLICACIONES

ARTÍCULO 15°. Reglamentación. El Poder Ejecutivo, dentro de los noventa (90) días de la promulgación de la presente ley, dictará la reglamentación necesaria.

ARTÍCULO 16°. Comuníquese al Poder Ejecutivo.

Matías D. Rodríguez

FUNDAMENTOS

Señora Presidente:

El objetivo de esta iniciativa es la creación de una Agencia Nacional de Ciberseguridad (ANCIBER) como ente autónomo en la órbita de la Jefatura de Gabinete de Ministros, para elaborar y ejecutar políticas de ciberseguridad por sí mismo o en coordinación con otros organismos nacionales a fin de fortalecer la ciberseguridad en Argentina.

La ciberseguridad es el conjunto de medidas, herramientas y técnicas que se utilizan para proteger los sistemas informáticos y redes de posibles amenazas, tales como el robo, la alteración o la destrucción de datos, y la interrupción de servicios críticos. Esto incluye la protección de la información y los recursos de las organizaciones, así como la privacidad y la seguridad de los usuarios. Abarca múltiples áreas de seguridad, de la información, de las aplicaciones y de los sistemas y dispositivos remotos.

El uso permanente y cotidiano de dispositivos electrónicos con conectividad a internet por parte de diversas organizaciones, tales como Estados, empresas y/o personas trae aparejado un aumento en los riesgos asociados con el ciberdelito, que pueden poner en peligro la privacidad, la intimidad y la seguridad de los datos personales, financieros y comerciales. Todas estas amenazas a la seguridad de los sistemas informáticos, ya sean públicos o privados, son un problema de origen global ya que la virtualidad no cuenta con fronteras, de modo que es de gran relevancia el establecimiento de lazos de cooperación internacional para la elaboración de una respuesta a las mismas.

Realizar una adecuada protección en materia de ciberseguridad es una tarea compleja pero sumamente necesaria dado el incremento de las amenazas y ataques informáticos, así como el impacto que los mismos pueden ocasionar en las infraestructuras críticas de un país y su población.

En línea con la creciente preocupación por estos temas, la Unión Internacional de Telecomunicaciones (UIT) lanzó una iniciativa denominada Agenda sobre Ciberseguridad Global, con el objeto de desarrollar un marco de trabajo para la cooperación internacional que

DIRECCIÓN GENERAL DE PUBLICACIONES

busca aumentar la confianza y seguridad en la sociedad de la información. Esta agenda se basa en cinco pilares estratégicos o áreas de trabajo: medidas legales, medidas técnicas y de procedimiento, estructuras institucionales, creación de capacidades y cooperación internacional.

En respuesta a esta creciente amenaza, muchos países han adoptado estrategias conjuntas y han formulado leyes y convenciones para combatir el ciberdelito. Por ejemplo, en la Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos (OEA), los Estados Miembros adoptaron la Estrategia Interamericana Integral de Seguridad Cibernética.

Una de las convenciones más importantes en este sentido es el Convenio sobre Ciberdelincuencia del Consejo de Europa, también conocido como la Convención de Budapest sobre delitos informáticos. Esta convención, adoptada en 2001 por el Consejo de Europa, establece medidas para prevenir y sancionar los delitos informáticos y para mejorar la cooperación internacional en este ámbito.

Este convenio tiene por objeto la prevención de los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando su detección.

Establece un marco legal para la cooperación internacional en la investigación y el enjuiciamiento de delitos informáticos, como el acceso ilegal a sistemas informáticos, la interceptación ilegal de datos, el fraude informático y la pornografía infantil en línea. Además, el Convenio también establece medidas para proteger los derechos humanos en el contexto de la lucha contra el ciberdelito, incluyendo la protección de la privacidad y la libertad de expresión en línea.

En Argentina se sancionó en 2017 la ley N° 27.411 a través de la cual se aprueba la adhesión al Convenio sobre ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest en noviembre de 2001 con algunas reservas.

En el mismo sentido, en febrero de 2023, se firmó la adhesión al Segundo Protocolo Adicional de este convenio. Este instrumento establece una política penal común entre los países firmantes; brinda herramientas de mejora para la cooperación internacional; facilita la provisión de pruebas electrónicas; y promueve la cooperación directa con proveedores de servicios y registros de internet.

DIRECCIÓN GENERAL DE PUBLICACIONES

Asimismo, establece medios eficaces para obtener información sobre los abonados y datos de tráfico y proporciona herramientas de cooperación inmediata ante casos de emergencia y de investigaciones conjuntas. En definitiva, se agilizan los procesos de requerimientos de forma más directa y ágil, ayudando a reducir el tiempo de las investigaciones de los delitos mediados por las tecnologías de información y comunicación (TIC´s).

En nuestro país, existen diferentes iniciativas en materia de fortalecer las capacidades en ciberseguridad. El Decreto N° 577/17 creó el Comité de Ciberseguridad integrado actualmente por representantes de diversos Ministerios, con el objetivo de elaborar una Estrategia Nacional de Ciberseguridad. Este comité ha conformado grupos de trabajo enfocados en “Estrategia Nacional de Ciberseguridad”, “Infraestructuras Críticas de Información”, “Concientización y educación” y “CERT/CSIRT”.

Según la Resolución de Jefatura de Gabinete de Ministros 1523/2019, se define a las Infraestructuras Críticas como 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.

Por su parte, las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

En cuanto al CERT, se trata de un Equipo de Respuesta ante Emergencias Informáticas nacional, que coordina la gestión de incidentes de seguridad informática, a fin de dar prevención y protección a las entidades del Sector Público Nacional. Asimismo, asesora técnicamente ante incidentes de seguridad, confecciona diversas publicaciones para la prevención de incidentes, el intercambio de buenas prácticas y recomendaciones, entre otras funciones.

Asimismo, en el ámbito de la Unidad de Gabinete de Asesores del Ministerio de Seguridad se creó el “PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACIÓN DEL CIBERCRIMEN (ForCIC)” con el objetivo de coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales y en técnicas de investigación en materia de ciberdelitos y delitos con presencia de la tecnología y/o utilización de tecnologías.

Resulta de suma importancia que nuestro país, avance en una estrategia nacional de ciberseguridad. La creación de la Agencia Nacional de

DIRECCIÓN GENERAL DE PUBLICACIONES

Ciberseguridad (ANCIBER) busca jerarquizar las políticas de ciberseguridad, en coordinación con los organismos del Estado Nacional con competencia en la materia.

Entre sus objetivos, se encuentran la elaboración y ejecución de planes, programas y proyectos con perspectiva federal en materia de ciberseguridad. Participará, asimismo, en instancias de cooperación internacional en la materia, y propondrá con criterio estratégico proyectos de normas relacionados con la ciberseguridad en la República Argentina.

Los objetivos de la Agencia incluyen diseñar y ejecutar políticas de ciberseguridad en coordinación con los organismos del Estado Nacional, elaborar planes y programas federales en materia de ciberseguridad, impulsar acciones para implementar una Estrategia Nacional de Ciberseguridad, participar en instancias de cooperación internacional, proponer proyectos de normas relacionados con la ciberseguridad en Argentina, desarrollar el Programa Nacional de Infraestructuras Críticas de la Información, promover la resiliencia de los sistemas críticos del Sector Público Nacional, capacitar permanentemente en materia de ciberseguridad en la Administración Pública Nacional, y colaborar con organismos y centros de investigación públicos y privados en la promoción de proyectos innovadores en ciberseguridad.

Dentro de las funciones de la Agencia se incluyen desarrollar una Estrategia Nacional de Ciberseguridad, elaborar un plan de acción para su implementación y convocar a otros organismos para participar en la implementación. Asimismo, debe impulsar el dictado de un marco normativo en materia de ciberseguridad, fijar lineamientos y criterios para la protección de infraestructuras críticas nacionales, informar a la población sobre incidentes cibernéticos y promover la investigación académica en ciberdelito.

Deberá, en el mismo sentido, mantener registros permanentes de infraestructuras críticas nacionales y equipos de respuesta ante incidentes de seguridad informática, proteger las infraestructuras críticas del Sector Público Nacional y generar iniciativas y capacitaciones para mejorar los niveles de ciberseguridad de la sociedad.

El análisis de las vulnerabilidades de software en la Administración Pública Nacional, así como la identificación de Infraestructuras Críticas de Información, mejorarán las capacidades de detección, defensa, respuesta y recuperación ante incidentes cibernéticos y de seguridad informática.

Las Comisiones de Seguridad Interior y Narcotráfico y de Seguridad de las Cámaras de Senadores y Diputados deberán recibir el plan de acciones anual, informes semestrales sobre el presupuesto y requerir informes al

DIRECCIÓN GENERAL DE TAQUÍGRAFOS

Directorio de la ANCIBER, además de poder hacer observaciones y sugerencias.

El desarrollo, difusión y uso masivo de las nuevas Tecnologías de la Información y Comunicación (TIC´s) han generado un cambio de paradigma en la sociedad. En la actualidad, el nivel de conectividad se relaciona de manera directa en el desarrollo económico, la gestión de la administración pública y todo el espectro de relaciones sociales en un país.

En el mismo sentido la implementación de las TIC´s ha permitido crear nuevos servicios, relacionados con todos los ámbitos (educativos, financieros, relacionados a la salud, entre tantos otros). No obstante, estos avances tecnológicos no se encuentran excluidos de un conjunto de riesgos y amenazas que traen aparejadas complejidades muy variadas.

Frente a las distintas modalidades que genera el cibercrimen, los Estados deben actuar garantizando la seguridad en redes, sistemas de información, así como en las infraestructuras para mantener la integridad de los sistemas y recursos utilizados en la red.

En la última década los ataques cibernéticos han aumentado considerablemente. Tanto las personas como las instituciones y los sistemas están expuestas en forma creciente a distintas modalidades de ciberdelito. Resulta primordial que las políticas públicas y los marcos legales se discutan para ajustarse a esta creciente amenaza.

Por lo desarrollado, resulta necesaria la creación de la Agencia, que actuará, en coordinación con las áreas competentes en la materia, como impulsora de los procesos necesarios a nivel nacional y como nexo entre los distintos sectores gubernamentales. De esta manera, se busca aumentar la protección de la información sensible que la ciudadanía deposita en la Administración Pública Nacional y las infraestructuras críticas para su normal funcionamiento.

Por todo lo expuesto, solicito a mis pares que acompañen el presente proyecto de ley.

Matías D. Rodríguez

DIRECCIÓN GENERAL DE PUBLICACIONES