JEFATURA DE GABINETE DE MINISTROS
DIRECCIÓN NACIONAL DE CIBERSEGURIDAD

Disposición 1/2021

DI-2021-1-APN-DNCIB#JGM

Ciudad de Buenos Aires, 19/02/2021

VISTO el Expediente EX-2021-00473060- APN-SIP#JGM, el Decreto N° 260 de fecha 12 de marzo de 2020, la Decisión Administrativa N° 1865 de fecha 14 de octubre de 2020, la Resolución de la JEFATURA DE GABINETE DE MINISTROS N° 580 de fecha 28 de julio de 2011, la Resolución de la ex SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN N° 1523 de fecha 12 de septiembre de 2019, la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2 de fecha 8 de agosto de 2013, y

CONSIDERANDO:

Que mediante la Resolución de la JEFATURA DE GABINETE DE MINISTROS N° 580 de fecha 28 de julio de 2011, se creó el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” (ICIC) en el ámbito de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN, con el objetivo de elaborar un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.

Que la mencionada medida, estableció, de igual manera, que la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION tendría entre otras, la atribución de dictar las normas que resulten necesarias para la implementación del Programa creado.

Que, dentro de ese marco normativo, mediante la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2 de fecha 8 de agosto de 2013, se crearon, en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, y bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, entre otros, los Grupos de Trabajo: ICIC-GAP (Grupo de Acción Preventiva), ICIC-GICI (Grupo de Infraestructuras Críticas de Información) e ICIC-INTERNET SANO, los cuales se encuentran actualmente inactivos.

Que, asimismo, la Disposición ya citada creó, también, el grupo de trabajo “ICIC - CERT” (Computer Emergency Response Team) en el marco del referido Programa y también bajo la órbita de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN.

Que, desde la creación del mencionado Grupo de Trabajo, han surgido en nuestro país otros equipos especializados de similar naturaleza, que atienden la gestión de incidentes de

seguridad de distintos sectores y organizaciones, y cuyo accionar es necesario articular a nivel nacional.

Que mediante Decisión Administrativa N° 1865 de fecha 14 de octubre de 2020 se aprobó la estructura organizativa de primer y segundo nivel operativo de la JEFATURA DE GABINETE DE MINISTROS creándose, entre otras, la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD en el ámbito de la SECRETARÍA DE INNOVACIÓN PÚBLICA dependiente la JEFATURA DE GABINETE DE MINISTROS, estableciendo como responsabilidad primaria la de "Entender en los aspectos relativos a la ciberseguridad y la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional".

Que, la citada medida, determinó, asimismo, entre las acciones de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD las de "Diseñar políticas de ciberseguridad, en coordinación con los organismos del ESTADO NACIONAL con competencia en la materia, elaborar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, en el ámbito de competencia de la Secretaría, participar en las acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de Ciberseguridad, articulando proyectos con las diferentes áreas del ESTADO NACIONAL involucradas, asistir a la Secretaría en su participación ante el Comité de Ciberseguridad creado por Decreto N° 577/17 y sus modificatorios, y colaborar en la ejecución de las decisiones que se adopten, proponer proyectos de normas relacionados con la ciberseguridad en la REPÚBLICA ARGENTINA, en coordinación con las áreas con competencia en la materia" y "entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL)".

Que, de la normativa antes citada, surge que tanto la actividad del Programa de Infraestructuras Críticas de Información como de los diferentes grupos de trabajo creados por la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2/2013, se encuentran actualmente bajo la órbita de competencia de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD.

Que, por la Resolución N° 1523 de la ex SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de fecha 12 de septiembre de 2019 se aprueba la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

Que, la Resolución citada en el Considerando anterior 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.

Que, de igual modo, la mencionada Resolución determina como Infraestructuras Críticas de Información a aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

Que durante el transcurso de vigencia de la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2/2013, se ha producido un incremento exponencial en

el uso de las Tecnologías de la Información y las Comunicaciones, por parte de las personas humanas y jurídicas, tanto públicas como privadas.

Que, particularmente en el curso del presente año, la ampliación de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, mediante el dictado por el Decreto N° 260 de fecha 12 de marzo de 2020 y sus complementarias, a raíz de la pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19, ha obligado a una más intensa utilización de las plataformas tecnológicas, especialmente en el ámbito de las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios, al punto que se han tornado indispensables para el desenvolvimiento de toda su actividad, tanto en lo que se refiere a la gestión interna como a los servicios que prestan a la sociedad.

Que esta notable expansión en el uso de las herramientas digitales, tanto en el campo del trabajo, como en las actividades económica y educativa, entre otros aspectos de la vida social ha producido también un aumento considerable de los riesgos y amenazas a la seguridad de la información, particularmente, en aquellos sistemas informáticos mediante los cuales son brindados por el Sector Público Nacional de manera eficiente y constante los servicios esenciales a la sociedad.

Que, la celeridad del cambio tecnológico antes referenciado, así como la complejidad creciente de los sistemas informáticos, obliga a mantener actualizados los medios para su protección a fin de la efectiva gestión de los incidentes de seguridad y de la prestación de la asistencia necesaria, en aquellas situaciones que afecten a las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a)del artículo 8° de la Ley Nº 24.156 y sus modificatorios, en especial en aquellos vinculados a las Infraestructuras Críticas de Información.

Que, todo ello hace indispensable la derogación de la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2/2013 puesto que la misma ha perdido virtualidad.

Que, en el ámbito internacional, el Informe UNGGE 2015 aprobado por Resolución AG 70/237 de las Naciones Unidas, ha recomendado a los países miembros: “Establecer a nivel nacional un equipo de respuesta ante emergencias informáticas o u equipo de respuesta a incidentes de seguridad informática”.

Que, consecuentemente, de todo lo expuesto surge que resulta necesaria la creación de un CENTRO NACIONAL DE RESPUESTA A INCIDENTES INFORMATICOS, como punto de referencia nacional confiable, especializado y de consulta para la respuesta a incidentes de seguridad informática que puedan afectar a los sistemas informáticos de las entidades y jurisdicciones antes citadas y que tenga por objetivo coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que las afecten y, en particular, a las Infraestructuras Críticas de Información, declaradas como tales.

Que ha tomado la intervención de su competencia la DIRECCIÓN DE ASUNTOS LEGALES DE INNOVACIÓN PÚBLICA de la SECRETARIA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que la presente medida se dicta en virtud de las facultades conferidas por el artículo 4° inciso a) de la Resolución de la Jefatura de Gabinete de Ministros Nº 580/2011 y la Decisión Administrativa N° 1865/2020.

Por ello,

El DIRECTOR NACIONAL DE CIBERSEGURIDAD

DISPONE:

ARTICULO 1°.- Crease en el ámbito de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD el CENTRO NACIONAL DE RESPUESTA A INCIDENTES INFORMÁTICOS (CERT.ar.), con el objetivo de coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales.

ARTICULO 2°.- El CERT.ar, tendrá las siguientes funciones específicas:

a) Administrar y gestionar toda la información sobre reportes de incidentes de seguridad en las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios.

b) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten las entidades y jurisdicciones enumeradas en el artículo 1° de la presente medida.

c) Coordinar las acciones a seguir, ante incidentes de seguridad, con otros Programas y equipos de respuesta a incidentes de la REPÚBLICA ARGENTINA.

d) Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática que puedan afectar activos de información críticos del país.

e) Interactuar y cooperar con equipos de similar naturaleza de otros países.

f) Llevar un registro de estadísticas y establecer métricas a nivel nacional.

g) Coordinar la gestión de incidentes de seguridad informáticos que afecten recursos críticos a nivel nacional

h) Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de seguridad informática.

i) Cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes de seguridad informática.

ARTICULO 3°.- Deróguese la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 2 del 8 de agosto de 2013.

ARTICULO 4°.- La presente medida entrará en vigencia a partir del día siguiente a su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

ARTICULO 5°.- Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese.

Gustavo Raúl Sain

e. 22/02/2021 N° 8965/21 v. 22/02/2021

Fecha de publicación 22/02/2021