JEFATURA DE GABINETE DE MINISTROS

SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA

SUBSECRETARIA DE TECNOLOGIAS DE GESTION

OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION

Disposición Nº 2/2013

Bs. As., 8/8/2013

VISTO el Expediente CUDAP: EXP-JGM: 0021755/2012 del Registro de la Jefatura de Gabinete de Ministros, la Resolución JGM Nº 580 del 28 de julio de 2011, y

CONSIDERANDO:

Que mediante la Resolución JGM Nº 580/11 se crea en el ámbito de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION DE INFORMACION dependiente de la SUBSECRETARIA DE TECNOLOGIAS DE GESTION de la ex SECRETARIA DE GABINETE, actual SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, el “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”.

Que el artículo 2° de la citada norma establece que el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” tiene como objetivo la elaboración de 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 8° 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 el 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 por el artículo 3° de la Resolución JGM Nº 580/11 antes mencionada se establecen los objetivos que llevará adelante el PROGRAMA NACIONAL.

Que el artículo 4° de la Resolución JGM Nº 580/11 antes citada, establece que el citado PROGRAMA NACIONAL estará a cargo de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.

Que asimismo, el inciso a) del citado artículo indica que la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION deberá dictar las normas que resulten necesarias para la implementación del “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”.

Que el Comité Interamericano contra el terrorismo (CICTE) perteneciente a la Organización de los Estados Americanos (OEA), del cual nuestro país forma parte, ha suscripto el día 7 de Marzo del año 2012 la Declaración “Fortalecimiento de la Seguridad Cibernética en las Américas” mediante la cual reconoce la necesidad de hallar formas efectivas de prevenir, impedir y atenuar las consecuencias de posibles amenazas a la infraestructura crítica y de estar preparados para responder a tales amenazas, así como de garantizar la seguridad de las instalaciones y de quienes las ocupan como asimismo la necesidad de alentar a los Estados Miembros a estrechar vínculos con el sector privado y la sociedad civil, cuando corresponda, en sus respectivos países, para desarrollar programas de fomento de la capacidad preventiva y de protección contra las amenazas a la infraestructura crítica.

Que resulta vital ampliar la protección de las infraestructuras críticas de información, como eje de una política de Estado en su interacción con el ciudadano el cual garantice servicios con el objetivo de hacerlos sustentables y eficientes, generando planes de acción responsable, en constante actualización y de manera mancomunada entre los diferentes sectores involucrados.

Que consecuentemente, se torna imprescindible a fin de impulsar una implementación coordinada de los distintos objetivos planteados por el “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”, establecer grupos de trabajo con objetivos y tareas definidas bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION con el fin de desarrollar y formular proyectos y propuestas que promuevan, a través de la aplicación de las TIC, la protección de infraestructuras críticas de información y ciberseguridad, la reducción de las desigualdades sociales y regionales, la protección del ciudadano y que mejoren la calidad de vida de las personas, así como otras herramientas, normas y medios necesarios para el logro de estos objetivos.

Que ha tomado la intervención de su competencia la DIRECCION GENERAL DE ASUNTOS JURIDICOS de la SUBSECRETARIA DE COORDINACION ADMINISTRATIVA de la SECRETARIA DE GABINETE y COORDINACION ADMINISTRATIVA 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 JGM Nº 580/11.

Por ello,

EL DIRECTOR NACIONAL DE LA OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION

DISPONE:

ARTICULO 1° — Créase el grupo de trabajo “ICIC - CERT” (Computer Emergency Response Team) 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.

ARTICULO 2° — El grupo de trabajo “ICIC - CERT” tendrá a su cargo los siguientes objetivos:

a) Administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encausar sus posibles soluciones de forma organizada y unificada.

b) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos del Sector Público Nacional que hubieren adherido.

c) Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos.

d) Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.

e) Promover la coordinación entre las unidades de administración de redes informáticas del Sector Público Nacional, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.

f) Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.

g) Interactuar con equipos de similar naturaleza.

ARTICULO 3° — Créase el grupo de trabajo “ICIC - GAP” (Grupo de Acción Preventiva) en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.

ARTICULO 4° — El grupo de trabajo “ICIC - GAP” tendrá a su cargo los siguientes objetivos:

a) Investigar nuevas tecnologías y herramientas en materia de seguridad informática.

b) Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional.

c) Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información.

d) Monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad.

e) Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.

f) Interactuar con equipos de similar naturaleza.

ARTICULO 5° — Créase el grupo de trabajo “ICIC - GICI” (Grupo de Infraestructuras Críticas de Información) en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.

ARTICULO 6° — El grupo de trabajo “ICIC - GICI” tendrá a su cargo los siguientes objetivos:

a) Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Público Nacional.

b) Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas.

c) Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

d) Alertar a los organismos que se adhieran al presente Programa sobre casos de detección de intentos de vulneración de infraestructuras críticas, sean éstos reales o no.

e) Coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de las infraestructuras críticas del Sector Público Nacional.

f) Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.

g) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.

h) Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.

i) Interactuar con equipos de similar naturaleza.

ARTICULO 7° — Créase el grupo de trabajo “ICIC - INTERNET SANO” en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, bajo la órbita de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.

ARTICULO 8° — El grupo de trabajo “ICIC - INTERNET SANO” tendrá a su cargo el siguiente objetivo:

a) Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica.

b) Interactuar con equipos de similar naturaleza.

ARTICULO 9° — El resguardo de la integridad de la información que brindarán al “ICIC” las entidades y jurisdicciones definidas en el artículo 8° de la Ley Nº 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado será responsabilidad de estos últimos siendo ellos los encargados de generarla y/o administrarla. La investigación del origen de los incidentes de seguridad o ataques y de quiénes son sus responsables corresponde a las autoridades de cada organismo que haya sufrido el mismo.

ARTICULO 10. — La reparación de las consecuencias de incidentes que afecten recursos específicos de las entidades y jurisdicciones definidas en el artículo 8° de la Ley Nº 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado, será responsabilidad del organismo objeto del incidente.

ARTICULO 11. — El “ICIC” mantendrá la confidencialidad sobre la identidad de la organización afectada por los incidentes reportados.

ARTICULO 12. — Los objetivos de los cuatro (4) Grupos de Trabajo antes mencionados, sólo serán llevados adelante por personal dependiente de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.

ARTICULO 13. — La presente Disposición entrará en vigencia a partir del día siguiente al de su publicación en el Boletín Oficial, y se publicará en el sitio web de la JEFATURA DE GABINETE DE MINISTROS (www.jefatura.gob.ar).

ARTICULO 14. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — PEDRO JANICES, Director Nacional, Oficina Nacional de Tecnologías de Información.

e. 03/09/2013 Nº 67872/13 v. 03/09/2013