



JEFATURA DE GABINETE DE MINISTROS SECRETARÍA DE GABINETE SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD

Disposición 5/2015

Bs. As., 10/11/2015

VISTO el Expediente N° CUDAP: EXP-JGM: 0053637/2015 del Registro de la JEFATURA DE GABINETE DE MINISTROS, el Decreto N° 1067 de fecha 10 de junio de 2015 y la Resolución de la JEFATURA DE GABINETE DE MINISTROS N° 580 de fecha 28 de julio de 2011, y

CONSIDERANDO:

Que por la Resolución de la JEFATURA DE GABINETE DE MINISTROS N° 580 de fecha 28 de julio de 2011 se creó en el ámbito de esta jurisdicción el “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD” el que fue transferido a la órbita de la DIRECCIÓN NACIONAL DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS.

Que los equipos de respuestas a emergencias informáticas son los encargados de proteger las infraestructuras de información sobre las cuales el Sector Público Nacional y el sector privado proveen sus servicios esenciales a los ciudadanos.

Que resulta por tanto pertinente y relevante reconocer a los actores fundamentales, sus competencias, ámbitos de aplicaciones, finalidad, marco legal, políticas de confidencialidad y detalles técnicos de intercambio de información con el fin de establecer políticas conjuntas para el intercambio de información en casos de incidentes.

Que con la finalidad de coordinar las acciones del equipo de respuesta a emergencias informáticas como asimismo actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa, estándares y buenas prácticas, deviene necesario la creación del “REGISTRO DE EQUIPOS DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA” en el ámbito de la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS.

Que, atento lo manifestado precedentemente, las empresas del sector privado que así lo requieran podrán incorporarse al mencionado registro.



Que ha tomado la intervención de su competencia la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA Y EVALUACIÓN PRESUPUESTARIA de la JEFATURA DE GABINETE DE MINISTROS.

Que la presente medida se dicta en virtud de las facultades conferidas por los artículos 6° del Decreto N° 1067 de fecha 10 de junio de 2015 y 4° de la Resolución de la JEFATURA DE GABINETE DE MINISTROS N° 580/11.

Por ello,

EL SUBSECRETARIO
DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS
DE INFORMACIÓN Y CIBERSEGURIDAD
DISPONE:

ARTÍCULO 1° — Créase en la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS el “REGISTRO DE EQUIPOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA”.

ARTICULO 2° — El “REGISTRO DE EQUIPOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA” será administrado por la DIRECCIÓN NACIONAL DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS.

ARTÍCULO 3° — Apruébanse los requisitos de inscripción al “REGISTRO DE EQUIPOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA” que, como Anexo, forma parte integrante de la presente.

ARTÍCULO 4° — Invítase a las provincias, municipios y a la CIUDAD AUTÓNOMA DE BUENOS AIRES a adherirse a la presente disposición.

ARTÍCULO 5° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — EMILIANO OGANDO, Subsecretario de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

ANEXO
REQUISITOS DE INSCRIPCIÓN EN EL REGISTRO DE EQUIPOS DE RESPUESTAS ANTE INCIDENTES INFORMÁTICOS

a) En caso de tratarse de un organismo del SECTOR PÚBLICO NACIONAL se deberá presentar:

- Norma de creación.
- Designación del responsable del área.

b) En caso de tratarse de una empresa del sector privado se deberá presentar:

- Estatuto societario, en copia certificada.



- Actas de designación del responsable en copia certificada.
- c) Los organismos del SECTOR PÚBLICO NACIONAL y las empresas del sector privado que así lo requieran, deberán presentar la siguiente “Carta de Constitución”, basada en la “Solicitud de Comentario” (RFC en inglés) N° 2350, del cual surge la descripción del Equipo de Respuestas a Incidentes de Seguridad Informática (CSIRT). Las Solicitudes de comentarios (RFC en inglés) son una serie de publicaciones del Grupo de Trabajo de Ingeniería de Internet (IETF en inglés) y la Sociedad de Internet (Internet Society en inglés), siendo ambos los principales organismos internacionales de desarrollo técnico y estándares de configuración para Internet.

1. Información del documento

Este documento contiene la descripción del equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) basada en el RFC N° 2350, en el cual se encuentra información sobre nuestro equipo de trabajo, canales de comunicación, misión y responsabilidades.

1.1. Fecha y versión del presente documento

El presente documento fue elaborado el (día) del (mes) del (año). La versión del presente documento es:
Versión (número)

1.2. Lugar de publicación del documento

Este documento y las posibles actualizaciones serán publicadas en el sitio web del CSIRT en la dirección <http://> (sitio web)

1.3 Autenticación digital del documento

La versión digital de este documento se encuentra firmada con firma digital acorde a Ley N° 25.506 y sus modificatorios.

2. Información de contacto

2.1. Nombre del equipo

Nombre: (ejemplo CSIRT del organismo)

Nombre corto: (ejemplo CSIRT-org)

2.2. Locación

Dirección:

Ciudad:

Código postal:

País: Argentina

(Nota: el CSIRT debe estar radicado, conformado y operativo en territorio nacional argentino.)

2.3. Zona horaria

Zona horaria: GMT-3

2.4. Teléfono de contacto

+54-(código de área y número de teléfono)

2.5 Número de fax

+54-(código de área y número de teléfono)

2.6 Correo electrónico

Todos los incidentes deben ser reportados a: (mail de reportes)

2.7 Llaves públicas e información de encriptación

Las llaves públicas de las firmas y/o encriptación con que firma el CSIRT es/son las/s siguiente/s:

ID:

FINGERPRINT:

2.10 Información adicional

2.11 Punto de contacto

El método de contacto preferido es

El mismo es atendido de (día de la semana) a (día de la semana) en la franja horaria (horas en formato





de VEINTICUATRO (24) horas

3. Constitución

3.1 Misión

El (nombre corto del CSIRT) tiene por misión (detallar el objeto de la creación del (CSIRT)).

3.2 Circunscripción

El (nombre corto del CSIRT) tiene por circunscripción (detallar el ámbito en el que se desempeña y detallar. Ejemplo: sector bancario/financiero, sector provincial).

3.3 Patrocinio y/o Afiliación

El (nombre corto del CSIRT) posee el patrocinio de (detallar).

Asimismo se informa que nos encontramos participando de las siguientes organizaciones:

(Nombre corto) - (nombre largo)

(Ejemplo: FIRST - Fórum of Incident Response and Security Teams)

3.4 Autoridad

El establecimiento del (nombre corto del CSIRT) es bajo el mandato de (detallar organismo, organización, empresa, universidad, u otro).

4. Políticas

4.1 Tipos de incidentes y nivel de soporte

(Detallar el tipo de incidentes que atiende y que nivel de soporte o asistencia brinda a cada uno de ellos.)

4.2 Cooperación, interacción y divulgación de información

(Detallar marco de cooperación, interacción y políticas de seguridad de la información del CSIRT.)

5. Servicios

(Detallar los tipos de servicio que ofrece. Ejemplo: alertas, análisis de malware, forenses, otros.)

6. Formulario de notificación de incidentes

(Detallar donde se publica el formulario de notificación de incidentes.)

7. Aviso legal

(Detallar si poseen otros avisos legales. Detallar si el servicio que ofrecen es arancelado o gratuito.)

Toda la documentación e información requerida en el presente Anexo, deberá ser remitida en soporte papel a la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD en el ámbito de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS.

e. 17/11/2015 N° 167907/15 v. 17/11/2015

Fecha de publicación: 17/11/2015

