1. Información del Documento

1.1 Listas de Distribución
Información reservada.

1.2 Fecha de la última actualización
Versión 1.0 03/09/2015

1.3 Ubicación del Documento
La versión actual del documento está disponible en el sitio web de http://www.icic.gob.ar

1.4 Autenticación del Documento
El presente documento ha sido firmado con la llave PGP del ICIC-CERT

2. Información de Contacto

2.1 Nombre del Equipo
CERT de Infraestructuras Críticas de Información y Ciberseguridad de la REPUBLICA ARGENTINA
Nombre corto: “ICIC – CERT”.

2.2 Dirección
Avda. Roque Sáenz Peña 511 Piso 5– CABA – CP 1035 – ARGENTINA

2.3 Zona horaria
UTC-GMT-3

2.4 Número de teléfono
+54-11 5985-8654/5

2.5 Número de Fax
No disponible

2.6 Otras comunicaciones
No disponible

2.7 Dirección de Correo Electrónico
cert@icic.gob.ar

2.8 Llaves Públicas y encriptación de información
PGP es usado para el intercambio entre ICIC CERT para reportes de incidentes, alertas, etc.

ID
0x0977 2CB1
Fingerprint es: 556F FB47 176B A40A B91C 03C3 FD72 8FEF 0977 2CB1

2.9 Miembros del equipo

Sr. Darío Hidalgo
Sr. Enrique Beláustegui
Sr. Arturo Busleiman
Sra. Claudia Lacanna
Sr. Marcelo Soto
Sra. Magdalena Marcenaro

2.10 Más información

Información general acerca del ICIC CERT, recomendaciones de seguridad y más puede encontrarla en http://www.icic.gob.ar

2.11 Horario de Atención

De 08:00 a 18:00 hs.

2.12 Puntos de contacto para clientes

Para reporte de incidentes, puede utilizar medios como correo electrónico o teléfono para comunicarse con el equipo ICIC CERT.

3. Constitución

3.1 Misión

La misión del ICIC CERT bajo el marco normativo de la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS DE INFORMACIÓN Y CIBERSEGURIDAD de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS es la de proteger los activos críticos de información de la Nación Argentina de los posibles ataques que pudiera ser objetivo, las acciones que desempeña son de prevención, detección, respuesta y recupero.

Entre sus acciones específicas podemos señalar:

•Entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes.
•Administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional y encausar sus posibles soluciones de forma organizada y unificada.
•Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos

•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.
•Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.
•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.
•Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.
• Interactuar con equipos de similar naturaleza.

3.2 Comunidad a la que se brinda Servicios

Infraestructuras estratégicas y críticas de las entidades y jurisdicciones del SECTOR PUBLICO NACIONAL, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran.

3.3 Patrocinio/Afiliación

JEFATURA DE GABINETE DE MINISTROS – PRESIDENCIA DE LA NACIÓN.

3.4 Autoridad

JEFATURA DE GABINETE DE MINISTROS asumiendo la coordinación de las actividades para la definición de las estrategias, normas, procedimientos y la reglamentación necesaria.

4. Políticas

4.1 Tipo de Incidentes y nivel de soporte

El Equipo ICIC CERT desplegará progresivamente sus servicios, a partir de avisos, alertas y Coordinación de Respuesta de Incidentes.

4.2 Cooperación, Interacción y divulgación de la Información

La información será manejada con absoluta confidencialidad de acuerdo a las políticas y procedimientos para la Gestión de Incidentes establecidos para el ICIC CERT y de los acuerdos de cooperación establecidos previamente con otros equipos CSIRTs.
Las comunicaciones se establecen con CSIRTs nacionales y CERTs internacionales a través de otorgamiento de tickets que son asignados con un número único para realizar seguimiento.
Asimismo ICIC CERT se comunica con las Fuerzas de Ley y con el MINISTERIO PÚBLICO FISCAL a través de su punto de contacto de cibercrimen.

.

4.3 Comunicación y Autenticación

Las llaves públicas se encuentran publicadas en el servidor pgp.mit.edu

5. Servicios

5.1 avisos

Este servicio tiene como objetivo proporcionar la información (por ejemplo, en el panorama de amenazas, vulnerabilidades publicadas, nuevas herramientas de ataque o artefactos, las medidas de seguridad / protección, etc.) necesarios para proteger los sistemas y redes.

5.2 Alertas y advertencias

Este servicio tiene como objetivo difundir información sobre los ciberataques o interrupciones, las vulnerabilidades de seguridad, alertas de intrusión, virus informáticos, y proporcionar recomendaciones a abordar el problema de los miembros a los cuales brinda servicios.

5.3 Coordinación de Respuesta de Incidentes

Este servicio tiene como objetivo la coordinación de la respuesta a los incidentes de seguridad de la información en las instituciones y órganos de la República Argentina, en cooperación con los propietarios y proveedores de partes afectadas, CSIRTS, operadores de telecomunicaciones, ISPs y otras entidades públicas y privadas (policía, investigadores, tribunales) según corresponda.

6. Formas de notificación de incidentes

Para realizar el reporte de incidentes debe utilizar la dirección de correo electrónico cert@icic.gob.ar o llamar al teléfono: +54-11 5985-8654/5.

7. Disclaimer

El Equipo ICIC CERT Argentina no se responsabiliza por el mal uso que se dé a la información aquí contenida