ICIC

Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad

REPORTE DE INCIDENTE INFORMÁTICO

Toda denuncia relacionada con algún tipo de incidente informático sobre equipos y/ó servicios deberá realizarse mediante el envío de un mail dirigido a cert@icic.gob.ar.

El citado mail deberá ser originado desde una cuenta del tipo gubernamental en caso de tratarse de dominios/servicios del sector público (.gov.ar, .gob.ar, .mil.ar y .edu.ar); desde una cuenta del tipo institucional en caso de tratarse de asociaciones y empresas del sector privado (.com.ar, .org.ar) y desde una cuenta personal en caso de tratarse de ciudadanos.

Se deja en claro que los datos solicitados en el citado mail son importantes para evaluar los posibles riesgos asociados y conocer un poco más la operatoria del incidente.
De no contar con alguno de ellos ó no conocer la forma de obtenerlos, por favor indicarlo claramente.

Datos solicitados:

1.- Asunto: deberá indicar: "INCIDENTE" + el tipo del mismo + el dominio afectado"

- ejemplo: "INCIDENTE DEFACEMENT www.organismo.gob.ar"
- ejemplo: "INCIDENTE PHISHING www.empresa.com.ar"
- ejemplo: "INCIDENTE PHISHING nombre@empresa.com"

En el cuerpo del mensaje deberá detallar lo siguiente:

2.- Información de contacto del denunciante

- Nombres y Apellido completos:
- E–mail (oficial / institucional / particular según el caso)
- Teléfono y horarios de contacto (oficial / institucional / particular según el caso):
- Teléfono celular y horarios de contacto (oficial / institucional / particular según el caso):

3.- Equipos y/ó servicios afectados por el incidente denunciado
(Si son varios equipos deberá realizarse un detalle por cada equipo involucrado en el incidente).
(Si desconoce los datos, por favor indique "DESCONOCIDO")

- Nombre:
- IP pública:
- IP privada:
- Time zone:
- Sistema Operativo:
- Servidor Web:
- Aplicaciones:

4.- Equipos atacantes

(Si son varios equipos deberá realizarse un detalle por cada equipo involucrado en el incidente)
(Si desconoce los datos, por favor indique "DESCONOCIDO")

- Nombre:
- IP publica:
- IP privada:
- ¿Ha contactado al administrador?

5.- Descripción del incidente

- Realice una descripción de lo sucedido de forma detallada y descriptiva, incluyendo fecha y hora del incidente según los registros con los que se cuenta.
- Recuerde que cuantos más datos se posean, más efectivo será el estudio del incidente.

6.- Muestras

- Es recomendable adjuntar captura de pantallas, logs, emails y cualquier otro dato que crea conveniente.

Para enviar información sensible, se recomienda utilizar un mecanismo de claves asimétricas, que pueden ser PGP o Certificados X.509.

En caso de enviar información sensible, la llave pública del CERT es la siguiente:

```
Key-ID: 3BEF44D2

Fingerprint: 31AF BCAD 003C 7824 E135  4F2D 7983 7715 3BEF 44D2
```