1. Información del Documento

1.1. Fecha de la última actualización

Viernes 18 de diciembre febrero de 2020

1.2. Listas de Distribución

csirt@secureit.es

1.3. Ubicación del Documento

https://www.secureit.es/csirt/RFC2350.pdf

1.4. Autenticación del Documento

Este documento ha sido firmado digitalmente por Secure and IT Proyectos, S.L.

2. Información de Contacto

2.1. Nombre del Equipo

SECURE&IT SOC-CSIRT

2.2. Dirección

Secure and IT Proyectos, S.L.

C/Perú, 8, Edificio A, bajo 3º

28290 Las Rozas

Madrid

2.3. Zona Horaria

CET / CEST

2.4. Número de Teléfono

+34 900 670 038

2.5. Número de Fax

+34 918 050 578

2.6. Otras Comunicaciones

+34 911 196 995

Dirección de Correo Electrónico csirt@secureit.es

2.7. Claves Públicas y cifrado de información

Los correos de contacto y claves PGP asociadas se encuentran publicadas en https://www.secureit.es/csirt/

2.8. Miembros del Equipo

- Francisco Valencia Arribas
- Luis Carlos Garcia
- Andrei Badea
- Edorta Echave García
- Javier Martí Sanz
- Jose María García Benítez
- Natalia Patiño
- Miembros del equipo de Sistemas de Secure&IT
- Miembros del equipo de Soporte 24x7 de Secure&IT

2.9. Más Información

La información general sobre los servicios proporcionados por Secure&IT y sobre la compañía se encuentra publicada en el portal web:

https//www.secureit.es

2.10. Horario de Atención

El equipo de respuesta a incidentes está disponible en los siguientes horarios:

- Consultas sobre servicios: horario de oficina (8.00h-18.00h)
- Incidentes catalogados con peligrosidad baja o media: horario de oficina (8.00h18.00h)
- Incidentes catalogados con peligrosidad alta, muy alta o crítica: 24x7x365.

2.11. Puntos de contacto para la comunidad

El método preferido para la comunicación con el CERT de Secure&IT es el correo electrónico.

Por favor, escríbanos a la cuenta csirt@secureit.es. Esto creará un caso en nuestro sistema de tickets y será tratado por nuestro personal.

3. Constitución

3.1. Misión

La misión fundamental de **Secure&IT** es ayudar a las empresas a disminuir los riesgos a que se exponen a causa de la gestión de su información.

Secure&IT ofrece un servicio integral en dimensiones como auditoría en seguridad global, servicios de hacking ético, consultoría, formación, asesoría, y adecuación en Derecho de las TIC y adecuación a procesos y Gobierno IT.

Ofrecemos servicios de seguridad de gestión, administración y alerta temprana de eventos de seguridad que facilitan el control total del estado de seguridad y salud de los activos de información para infraestructuras críticas, instituciones educativas, organismos públicos y entidades privadas.

Todo ello, con el fin último de conseguir la compleja tarea de gestionar la seguridad de las organizaciones, mediante la implementación conjunta de medidas preventivas, de vigilancia y de respuesta rápida ante incidentes de seguridad.

3.2. Comunidad a la que brinda servicios

Secure&IT empresa española dedicada a las Tecnologías de la Información y Comunicaciones que ayuda a sus clientes en cuatro áreas:

- Auditoría, Consultoría, Formación, Adecuación a Procesos y Gobierno IT.
- Auditoría, Asesoría, Adecuación en Derecho de las TIC
- Telecomunicaciones, Sistemas de Información y Seguridad Lógica
- Gestión 24x7x365 de Sistemas IT, Telecomunicaciones y Seguridad.

Secure&IT presta, en sus cuatro líneas de negocio, sus servicios de formación, auditoría, consultoría, ejecución de proyectos, soporte y mantenimiento a grandes, medianas y pequeñas organizaciones, privadas o públicas.

3.3. Patrocinio y/o Afiliación

El CERT/CSIRT/SOC de **Secure&IT** es el equipo de respuesta ante incidentes de seguridad de la compañía Secure and IT Proyectos, S.L.

En la actualidad se encuentra en proceso para ingresar en FIRST, Foro de Respuesta a Incidentes y Equipos de Seguridad de la Información (Forum of Incident Response and Security Teams) el principal foro mundial de Ciberseguridad.

El ingreso en FIRST permitirá al SOC de **Secure&IT** compartir con las principales organizaciones de todo el mundo, objetivos, ideas e información sobre ataques, vulnerabilidades de seguridad y la utilización de soluciones para afrontar y mitigar las amenazas del ciberespacio.

3.4. Autoridad

SECURE&IT SOC-CSIRT colabora, a estos efectos, con CCN-CERT, CERT Gubernamental Nacional e INCIBE

4. Políticas

4.1. Tipo de Incidentes y nivel de soporte

El equipo de **SECURE&IT SOC-CSIRT** evaluará los incidentes que les sean reportados y desplegará, progresivamente, sus servicios dependiendo de la peligrosidad del incidente.

El nivel de apoyo que brinde **SECURE&IT SOC-CSIRT** y el tiempo de respuesta del mismo, dependerá de la gravedad del incidente reportado, la carga de trabajo del equipo y la integridad de la información disponible. La gravedad de los mismos se determinará haciendo uso de criterios establecidos por el CCN-CERT:

- Tipo de amenaza (código dañino, intrusiones, fraude, etc.)
- Origen de la amenaza: interna o externa.
- La categoría de seguridad de los sistemas afectados.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.
- El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
- Los requerimientos legales y regulatorios.

La respuesta se realizará en base al uso de una metodología contrastada para la gestión de incidentes.

SECURE&IT ofrece consejos de seguridad a sus clientes, con el fin de reducir las vulnerabilidades técnicas y las provenientes de las amenazas internas de las organizaciones. De manera periódica a través de su boletín o puntual cuando se recibe alguna alerta notificada por entidades gubernamentales, como el CCN-CERT o INCIBE.

4.2. Cooperación, Interacción y divulgación de la Información

La información manejada por **SECURE&IT SOC-CSIRT** es tratada con absoluta confidencialidad acorde a las políticas y procedimientos para la Gestión de Incidentes establecidos para el **SECURE&IT SOC-CSIRT** mediante los pertinentes acuerdos de cooperación establecidos previamente con otros equipos CSIRTs.

4.3. Comunicación y Autenticación

Los medios disponibles para la comunicación con **SECURE&IT SOC-CSIRT** son:

- Correo electrónico cifrado con las claves públicas dedicadas para ello y publicadas en el portal web: https://www.secureit.es/csirt/

5. Servicios

El servicio fundamental de **SECURE&IT SOC-CSIRT** es que, en caso de que se materialice algún ataque, la respuesta sea inmediata, las consecuencias puedan ser mitigadas y el impacto para la organización sea mínimo. El equipo de expertos que ponemos a disposición de la entidad afectada, asesora a la compañía con el objetivo de recuperar la normalidad en las operaciones o conseguir que se prevengan nuevos incidentes en el futuro. La evolución de las amenazas, así como la aparición de normativa dirigida a proteger la información, han hecho que los equipos de respuesta ante incidentes sean de vital importancia para las compañías.

5.1. Prevención

Desde **SECURE&IT SOC-CSIRT** se promueven iniciativas de divulgación de información con el objetivo de concienciar y prevenir incidentes de seguridad, entre las que destacan:

- Elaboración de políticas de seguridad.
- Formación y concienciación en materia de ciberseguridad, derecho tecnológico y estándares relacionados con la gestión de la información.
- Alertas y avisos a su comunidad sobre nuevas amenazas y vulnerabilidades, recopiladas de fuentes reconocidas.
- Confección de procedimientos y buenas prácticas.
- Organización y participación en jornadas y eventos de ciberseguridad.

5.2 Respuesta a Incidentes

La respuesta ante incidentes es una tarea compleja para las organizaciones, ya que es necesario disponer de recursos capaces de atender y ofrecer soluciones a los eventos que puedan ocurrir.

5.2.1 Clasificación del incidente

- Investigación en profundidad del incidente acaecido.
- Determinación de la extensión del incidente.

5.2.2 Coordinación del incidente

- Categorización del incidente
- Determinación de la causa inicial del incidente (vulnerabilidad explotada)
- Coordinación con otras organizaciones involucradas en el incidente
- Informar, si procede, a otros equipos CSIRT.

5.2.3 Resolución del incidente

- Resolución y erradicación del incidente, en base a la metodología implementada por el equipo.

5.3 Análisis forense y de malware

Secure&IT dispone de equipamiento y personal especializado para realizar el análisis forense de equipos implicados en incidentes

6. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

Buzón de correo específico: csirt@secureit.es

Teléfonos proporcionados en la información de contacto.

7. Exclusión de responsabilidad

El Equipo CSIRT de **Secure&IT** no se responsabiliza del mal uso que pueda darse de la información aquí contenida.