PROCEDIMIENTO DE REPORTE Y DIFUSIÓN DE VULNERABILIDADES

A partir de este procedimiento, se publican y difunden los resultados a fin de informar a la población potencialmente vulnerable, dándoles a su vez recomendaciones para su protección o mitigación del riesgo. Dicho procedimiento consiste en:

1. Intentar identificar al responsable o fabricante del software.

2. Notificar el problema al responsable, informándole la intención de ayudar a su resolución y aclarándole que se publicará y difundirá el problema y su potencial solución para protección de los usuarios.

3. Acordar y coordinar con el responsable o fabricante la forma y tiempo necesario para la resolución del problema.

4. Resuelto el problema de seguridad o cumplido el plazo acordado con el fabricante para tal fin, publicar un reporte técnico (boletín de seguridad o “security advisory”) que incluirá:

. Descripción general (no técnica) del problema, alcance e impacto.

. Detalles técnicos necesarios para identificarlo o reproducirlo.

. Recomendación sobre cómo solucionarlo o mitigar sus efectos.

. Descripción detallada de las comunicaciones entre el descubridor, el reportador (en este caso el Programa STIC de la Fundación Sadosky) y el responsable o fabricante.

Dado que el objetivo que se persigue es el de informar y ayudar a los usuarios vulnerables y si bien el escenario ideal es la solución del problema por parte del fabricante, se decidirá la publicación de la información de manera unilateral tanto en los casos detallados a continuación como en casos no contemplados pero que se ajusten a los criterios ya mencionados:

1- Cuando no se haya podido identificar al fabricante o responsable del software con problemas.

2- Cuando no se haya podido identificar al contacto del fabricante o responsable adecuado para reportarle problemas de seguridad o al encargado de la resolución.

3- Cuando se determine que el fabricante o responsable no tiene intención o capacidad para resolver el problema.

4- Cuando la información sobre el problema se hiciera pública por algún tercero.

5- Cuando se descubra que el problema ya está siendo explotado para cometer ilícitos.