PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

MEJORES PRÁCTICAS PARA LA GESTIÓN DE LOS RIESGOS DE SSI

Explotación de los resultados del método EBIOS®
en el marco de un procedimiento BS 7799

Versión del 21 de marzo de 2003

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP – Tel. 01 71 75 84 15 - Fax 01 71 75 84 00

¿Qué es el BS 7799?

El *British Standard* 7799 (BS 7799) está formado por dos guías: la ISO/IEC 17799:2000 y la BS 7799-2:2002.
La ISO/IEC 17799:2000 es un catálogo que agrupa 36 objetivos de control, divididos en 127 medidas de control, y referidos a 10 ámbitos de aplicación (política de seguridad, seguridad del personal, control de accesos, etc.). Los objetivos de control presentan una meta que hay que alcanzar y lo que es necesario hacer para lograrlo. Luego se dividen en medidas de control que explican con mayor o menor grado de detalle los puntos que deben implementarse para poner en práctica dichas medidas.
El BS 7799-2:2002 presenta un sistema de gestión de la seguridad de la información (*Information Security Management System - ISMS*) en cuatro etapas sucesivas (planificar, implementar, verificar, mejorar), asemejándose a las normas de calidad ISO 9001 e ISO 14001. La etapa de planificación propone la utilización de la ISO/IEC 17799:2000.

¿Cuáles son las ventajas del método EBIOS en el marco de un procedimiento BS 7799?

La realización previa de un estudio EBIOS ofrece varias ventajas:

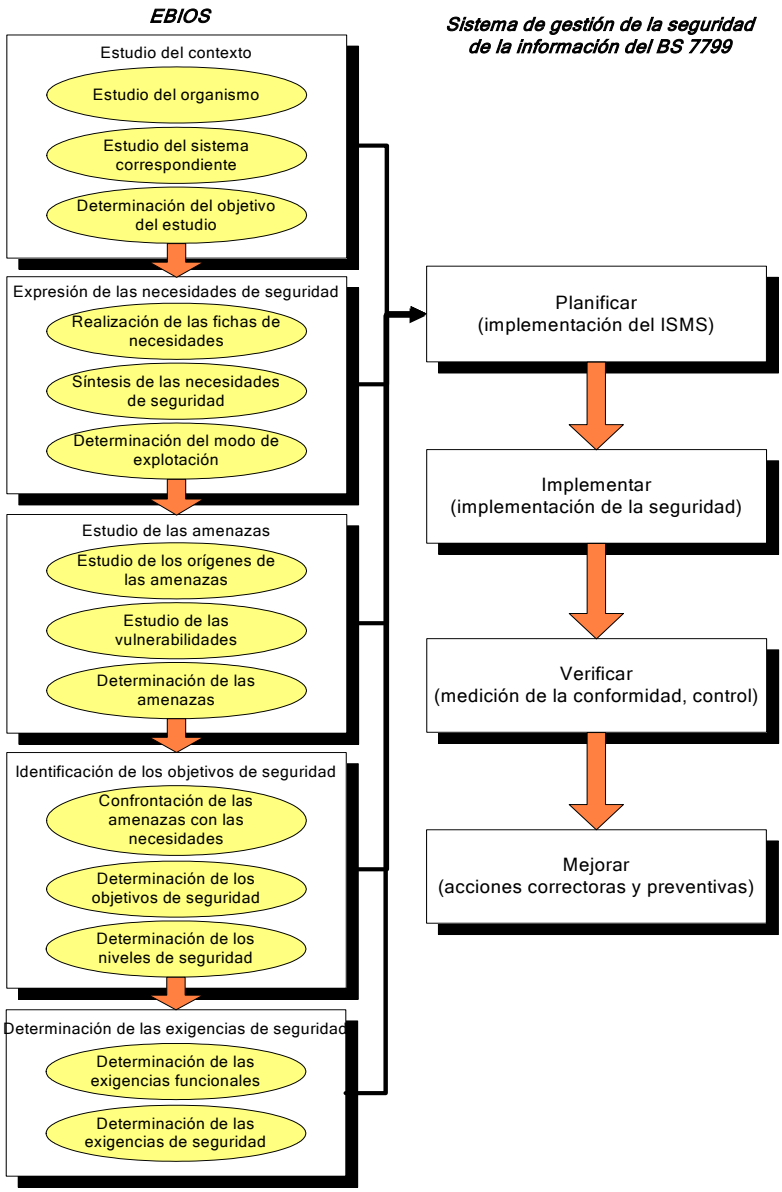
- La justificación de la elección de los objetivos y las medidas de control del catálogo en función de las necesidades reales del organismo.
- El respeto del marco del procedimiento propuesto en el BS 7799, que preconiza una apreciación de los riesgos previa a la elección de los objetivos y medidas de control.
- El suministro de resultados reutilizables (contexto, necesidades de seguridad, amenazas, riesgos, objetivos de seguridad, exigencias de seguridad) con miras a iteraciones posteriores del sistema de gestión de seguridad de la información.

¿Cómo implementar un procedimiento BS 7799 utilizando EBIOS?

Una solución eficaz para implementar un procedimiento BS 7799 consiste en:

- Definir el ámbito de aplicación del sistema de gestión de la seguridad de la información (formalizar el perímetro).
- Elaborar una política de seguridad.
- Realizar un estudio EBIOS global a fin de efectuar el análisis, la evaluación y el tratamiento de los riesgos, seleccionando los objetivos y medidas de control que permitan cubrir los riesgos que deben minimizarse.
- Elaborar una declaración de aplicabilidad.
- Realizar el seguimiento del proceso con otras herramientas.

Para ello pueden utilizarse los siguientes datos:



(Para mayor información, escribir a: ebios.dcssi@sgdn.pm.gouv.fr)