Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Utilización del método EBIOS®
para redactar un objetivo de seguridad de producto

Versión del 10 de noviembre de 2004

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

¿Qué es un objetivo de seguridad de producto?

Un objetivo de seguridad (ST – *Security Target*), tal como lo define la norma ISO 15408 – criterios comunes para la evaluación de la seguridad de las tecnologías de la información–, es "un conjunto de requerimientos de seguridad y de especificaciones que deben utilizarse como base para la evaluación de un TOE identificado" (el TOE – *Target Of Evaluation* es el objetivo de evaluación, es decir el producto estudiado).

Se trata de un documento cuyo contenido se encuentra normalizado, que puede servir como pliego de condiciones que define en forma más detallada el contenido de un perfil de protección (PP) y que también puede ser evaluado. Este ST propone especialmente una definición detallada justificada de los requerimientos de seguridad formalizados en el PP. Permite al usuario del TOE darse cuenta de la adecuación del TOE a sus necesidades.

Fuera del contexto de la evaluación técnica (evaluación de producto certificada por la DCSSI), es posible redactar pliegos de condiciones de SSI en forma de PP, fundamentalmente con el fin de utilizar un esquema de trabajo y una terminología reconocidos.

¿Cuáles son las ventajas del método EBIOS para la redacción de un ST de producto?

Un ST de producto debe estar perfectamente completo y debe ser coherente. Su redacción requiere, por lo tanto, un riguroso trabajo, pero la norma no propone ningún método para realizarlo. EBIOS permite contar con todos los elementos necesarios para la redacción de un ST, garantizando, al mismo tiempo, su coherencia. Ofrece además varias ventajas:

- la pertinencia de los objetivos de seguridad que cubren amenazas, hipótesis, normas de política de seguridad y requerimientos de seguridad,
- la justificación de los objetivos y de los requerimientos mediante la apreciación de los riesgos SSI,
- la exhaustividad del estudio gracias a su procedimiento estructurado,
- la implicación de las partes involucradas (dirección, diseñador del proyecto, director de proyecto, usuarios…).

¿Cómo redactar un ST de producto utilizando EBIOS?

Una solución eficaz para redactar un ST consiste en:

- realizar un estudio EBIOS (en un perímetro que será el del ST) detallando los requerimientos de seguridad,
- redactar un PP y hacerlo validar sobre la base del estudio realizado,
- extraer los datos necesarios del estudio (una gran parte del mismo),
- redactar la introducción (identificación del ST y perspectiva de conjunto),
- reorganizar los objetivos de seguridad (que deberán ser clasificados según su alcance),
- reorganizar los requerimientos de seguridad (que deberán ser clasificados según su alcance),
- redactar los avisos de conformidad con el PP.

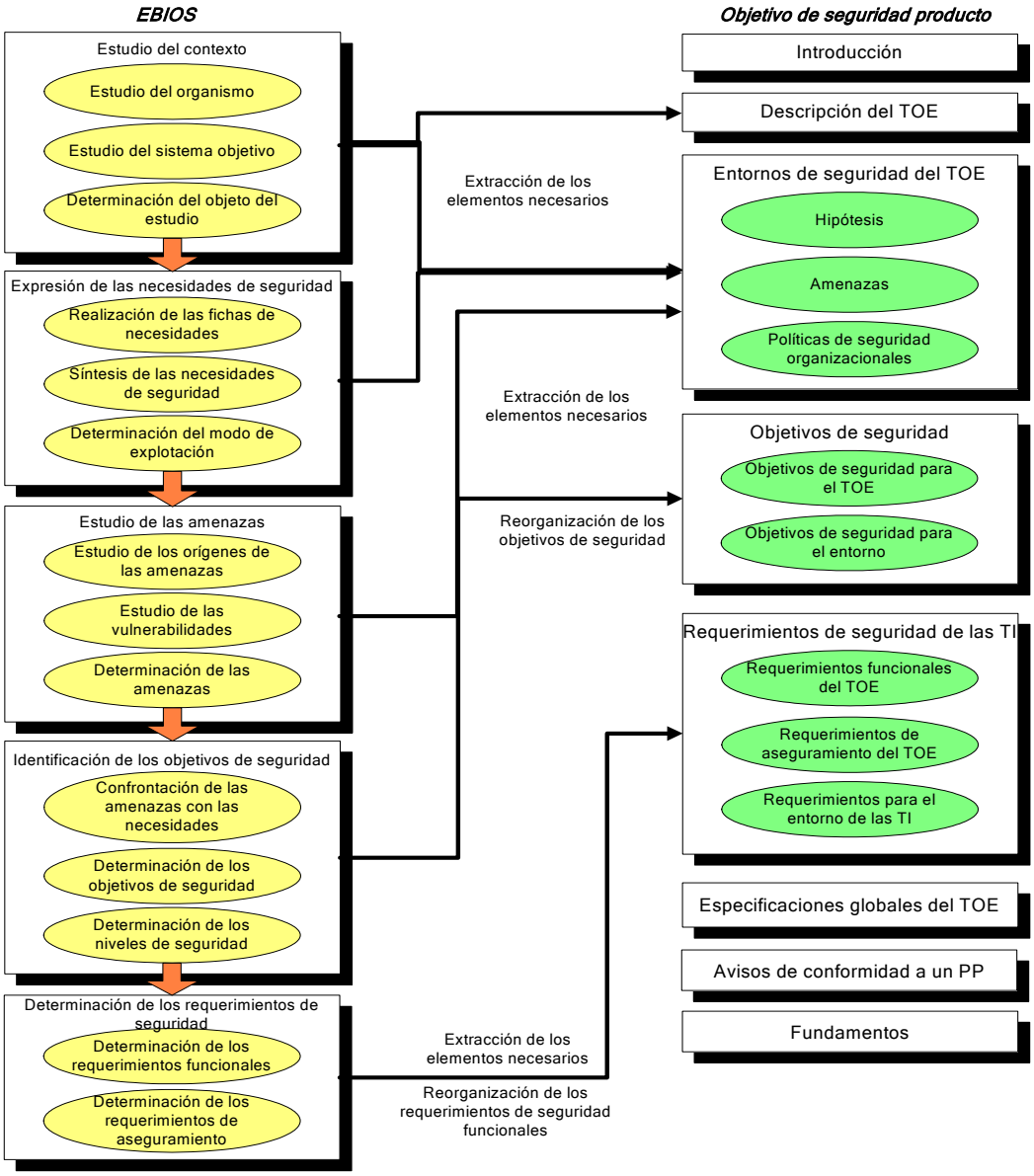
Para lograrlo, las actividades del método EBIOS se utilizan del siguiente modo:

Actividades EBIOS	**Implementación con el fin de redactar un ST de producto**
ETAPA 1 Estudio del contexto	En resumen: el estudio del contexto está centrado únicamente en los datos necesarios para la redacción de un objetivo de seguridad.
1.1 – Estudio del organismo	Puede resultar útil describir los organismos o tipos de organismos en los cuales el producto de seguridad debe ser utilizado a fin de definir las hipótesis de entorno. Sin embargo, generalmente no se utiliza esta actividad.
1.2 – Estudio del sistema evaluado	Se pone énfasis en la recogida de los elementos necesarios para la redacción de un ST: - presentación del TOE y descripción funcional, - lista de los elementos esenciales, - lista de las hipótesis, - lista de las normas de seguridad. Los demás elementos de esta actividad sólo deberían ser estudiados si sirven para ampliar la lista anterior.
1.3 – Determinación del objetivo del estudio de seguridad	Esta actividad debe ser detallada y completa, aunque generalmente sólo nos interesamos en las entidades técnicas de tipo software, hardware y redes.
ETAPA 2 Expresión de las necesidades de seguridad	En resumen: las necesidades de seguridad están determinadas según una escala de necesidades simple.
2.1 – Elaboración de fichas de necesidades	Los criterios de seguridad, la escala de necesidades y los impactos seleccionados deben ser simples. Por ejemplo, pueden definirse: - los tres criterios de seguridad habituales (disponibilidad, integridad y confidencialidad), - eventualmente uno o dos impactos (esencialmente vinculados con la pérdida de fiabilidad de los mecanismos),una escala binaria.
2.2 – Síntesis de las necesidades de seguridad	La síntesis de las necesidades de seguridad puede realizarse directamente, sin pasar por las fichas de necesidades de seguridad unitarias.

Actividades EBIOS	Implementación con el fin de redactar un ST de producto
ETAPA 3 Estudio de las amenazas	En resumen: el estudio de las amenazas es detallado.
3.1 – Estudio de los orígenes de las amenazas	Esta actividad debe ser detallada y completa. La caracterización de los métodos de ataque y de los elementos peligrosos debe ser particularmente clara y precisa. Se debe indicar, explicitar y justificar el potencial de ataque de cada elemento peligroso. Se debe elaborar una lista de los métodos de ataque no considerados, incluyendo las justificaciones correspondientes.
3.2 – Estudio de las vulnerabilidades	Las vulnerabilidades pueden provenir de las bases de conocimientos del método EBIOS, pero se utilizan generalmente otros referenciales, más técnicos y detallados. La determinación de los niveles de vulnerabilidad sirve únicamente para jerarquizar las amenazas en las etapas subsiguientes del estudio.
3.3 – Formalización de las amenazas	Esta actividad debe ser clara (con fines comunicativos) y precisa. Es preferible formular amenazas unitarias, homogéneas, específicas (una vulnerabilidad por amenaza) y conformes a los perfiles de protección y ST existentes.
ETAPA 4 Identificación de los objetivos de seguridad	En resumen: los riesgos explicitan las consecuencias de las amenazas, los riesgos residuales deben "desaparecer" en favor de modificaciones del contexto.
4.1 – Confrontación de las amenazas con las necesidades	Los riesgos deben ser identificados y formulados, de manera uniforme, sobre la base de la redacción de las amenazas. Estos riesgos podrán incorporarse al ST en lugar de las amenazas (menos precisas en lo que respecta a las consecuencias).
4.2 - Formalización de los objetivos de seguridad	La redacción de los objetivos de seguridad debe ser clara, precisa y uniforme, para poder justificar dichos objetivos mediante su contenido. Los objetivos de seguridad deben clasificarse en dos categorías: - los objetivos centrados en el TOE, - los objetivos centrados en el entorno del TOE. Los eventuales riesgos residuales identificados deben ser objeto de una modificación del contexto (esencialmente en la actividad 1.2), de tal modo que no existan ya riesgos residuales en este nivel del estudio. La demostración de la cobertura de los elementos del estudio mediante los objetivos de seguridad debe ser detallada.
4.3 – Determinación de los niveles de seguridad	Los niveles de seguridad deben ser explícitos y deben estar debidamente justificados.

Actividades EBIOS	Implementación con el fin de redactar un ST de producto
ETAPA 5 Determinación de los requerimientos de seguridad	
5.1 – Determinación de los requerimientos de seguridad funcionales	Los requerimientos de seguridad funcionales deberían surgir de la ISO 15408 o crearse según las recomendaciones que figuran en dicha norma y adecuarse para que las especificaciones sean directamente aplicables. Los eventuales riesgos residuales identificados deben ser objeto de una modificación del contexto (esencialmente en la actividad 1.2), de tal modo que ya no exista ningún riesgo residual en este nivel del estudio. Los requerimientos de seguridad deben clasificarse en dos categorías: - los requerimientos centrados en el TOE, - eventualmente, los requerimientos centrados en el entorno del TOE. La demostración de la cobertura de los elementos del estudio mediante los objetivos de seguridad funcionales debe ser detallada.
5.2 – Determinación de los requerimientos de seguridad de aseguramiento	Los requerimientos de seguridad de aseguramiento deberían surgir de la ISO 15408 o crearse según las recomendaciones que figuran en dicha norma. Los fundamentos de los requerimientos de seguridad de aseguramiento deben ser detallados.

En resumen, los datos que pueden utilizarse son los siguientes:



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