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

EBIOS

COMPENDIO

Versión del 4 de febrero de 2004

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

¿Por qué EBIOS tiene tanto éxito?

Un método de referencia en materia de análisis de los riesgos SSI

El procedimiento metodológico propuesto por EBIOS aporta **una visión global y coherente** de la seguridad de los sistemas de información (SSI). Este método, exhaustivo, permite determinar objetivos y requerimientos de seguridad adaptados, proponiendo un vocabulario y conceptos en común. Toma en cuenta todas las entidades técnicas (software, hardware, redes) y no técnicas (organización, aspectos humanos, seguridad física). Permite implicar a todos los actores del SI en la problemática de la seguridad y, por otra parte, propone un procedimiento dinámico que favorece las interacciones entre las distintas profesiones y funciones de la organización, estudiando todo el ciclo de vida del sistema (diseño, realización, puesta en servicio, mantenimiento…).

Promovido por la DCSSI y **reconocido por las instituciones públicas francesas, EBIOS es también una referencia dentro el sector privado y en otros países.** En ese contexto, nuevas perspectivas se abren para EBIOS por el hecho de converger hacia normas internacionales y por haber sido traducido al inglés. En el año 2002, comparaciones realizadas a nivel internacional ubicaron a EBIOS dentro de los tres mejores métodos de análisis de SSI.

Numerosos organismos del sector público y privado utilizan este método **para solicitar o para realizar ellos mismos análisis de los riesgos SSI**: las instituciones públicas (utilizándolo en forma sistemática algunas veces; incitada, otras), el Centro Nacional de Estudios Espaciales (CNES), la Comisaría de Energía Atómica (CEA), la Caja Nacional del Seguro de Enfermedad (CNAM), la Agrupación de Tarjetas Bancarias "CB", ALCATEL CIT, agencias sanitarias, los Aeropuertos de París (ADP), el Consejo de la Unión Europea…

Por otra parte, **varias empresas consultoras han adoptado el procedimiento EBIOS** para cumplir con su rol de asistencia al diseño de proyectos.

Recordemos, por último, que cuando, un sistema procesa datos clasificados de defensa, un ministerio o un industrial deben redactar una FEROS. EBIOS es la herramienta ideal para realizar este trabajo, ya que sus resultados se integran directamente en una FEROS.

Un procedimiento simple y resultados adaptados

EBIOS es un método **fácil de entender y de aplicar**. Efectivamente, su filosofía general es simple e intuitiva, y su desarrollo, natural. Consiste en formalizar las necesidades de seguridad y las amenazas, y en determinar los riesgos que afectan al organismo.

Cada uno puede apropiarse del método y adaptar su enfoque según el tema estudiado. EBIOS ha sido aplicado tanto en sistemas simples (servidor web) como en sistemas complejos (sistema de gestión de concursos y de personal, que supone diversas interconexiones), en sistemas por diseñar como en sistemas existentes, o incluso tanto en sistemas de información completos como en subsistemas.

Una sola y misma herramienta permite realizar distintos procedimientos de seguridad vinculados con la gestión de los riesgos SSI. Efectivamente, EBIOS contribuye a la elaboración

de un plan general de SSI, sirve para diseñar las primeras etapas de una política SSI y de un esquema orientativo SSI, contribuye a la redacción de un perfil de protección (PP), y puede utilizarse para redactar una FEROS o cualquier otro pliego de condiciones SSI.

EBIOS contribuye a la elaboración de las tareas que debe realizar el diseñador de proyecto. Permite determinar el perímetro del estudio manteniendo una visión global del sistema estudiado en su contexto, expresar necesidades (vinculadas con los bienes que deben protegerse), identificar amenazas y definir un plan de proyectos y responsabilidades.

El método EBIOS es una herramienta de elección y de evaluación utilizada por el director de proyecto para cumplir con los objetivos planteados en el diseño del proyecto, para responder a las cuestiones referidas a la factibilidad, a los costos y plazos propuestos, y para elegir soluciones.

Es también una herramienta de medición del impacto y de negociación entre el diseñador del proyecto y la dirección (del proyecto, del organismo…) que ofrece a ésta la posibilidad de controlar la adecuación de los SI y de centralizar los estudios y la SSI.

Su **compatibilidad con otras herramientas metodológicas SSI** permite mantener una coherencia perfecta en el proceso de gestión de los riesgos SSI. Por ejemplo, pueden utilizarse la ISO/IEC 15408 y la ISO/IEC 17799 para determinar los objetivos y los requerimientos de seguridad.

Un software de asistencia bajo licencia libre

El software es gratuito y puede obtenerse simplemente solicitándolo a la DCSSI (conseil.dcssi@sgdn.pm.gouv.fr). De fácil uso, este software **facilita, en forma significativa, la realización de los análisis de riesgos**, ofreciendo la posibilidad de elaborar distintos documentos de síntesis (conjunto de datos, FEROS, síntesis de FEROS, PP, recopilación de elementos estratégicos, política de seguridad…). Permite además reutilizar bases de conocimientos y estudios. Se entrega con su código fuente y documentación de diseño, y puede ser mejorado por todos los usuarios. El software está editado bajo licencia libre, diseñado en UML y realizado en Java y XML.

Gran demanda de formación

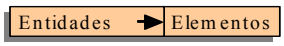
La formación en EBIOS facilita la comprensión del método y de su aplicación. Estos cursos permiten a los asistentes conocer las buenas prácticas para la implementación de este método y dialogar con otros usuarios del mismo. Se ofrece una formación de dos días en el CFSSI (http://www.ssi.gouv.fr/formation/index.html). La Oficina de Consultoría de la DCSSI (conseil.dcssi@sgdn.pm.gouv.fr) queda a disposición de los asistentes a la formación para garantizar un seguimiento del proyecto de análisis de riesgos. La formación está ilustrada con un estudio de caso que materializa el procedimiento y brinda ejemplos a los cuales es posible referirse durante las primeras utilizaciones del método.
Por otra parte, también se ha implementado una sesión para formadores en el método EBIOS con el fin de crear reemplazantes dentro de las mismas instituciones del Estado.

La creación del club EBIOS

En el año 2003, la DCSI creó el club EBIOS con el fin de compartir experiencias y de mejorar el método y sus herramientas.

Dicho club permite reunir regularmente a una comunidad de usuarios preocupados por contribuir al desarrollo del método y por disponer de las últimas informaciones sobre este tema.

Los principios del método EBIOS



El estudio del contexto

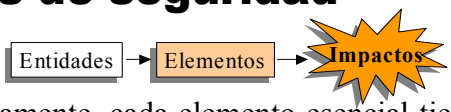
Un sistema de información se basa en **elementos esenciales**, funciones y datos, que constituyen el valor agregado del sistema de información para el organismo.

> *Por ejemplo, para el lanzamiento de un cohete, un sistema de control de trayectoria se basa en diversos datos, tales como parámetros o resultados de cálculos, y en distintas funciones que permiten realizar dichos cálculos.*

Los elementos esenciales están vinculados con un conjunto de **entidades** de distintos tipos: hardware, software, redes, organizaciones, personal y establecimientos.

> *Tomemos el ejemplo de un parámetro de cálculo de trayectoria para el lanzamiento de un cohete. Este parámetro de cálculo está relacionado con los ordenadores de control, el software de procesamiento, los operadores, el cohete, las reglamentaciones del área…*

La expresión de las necesidades de seguridad

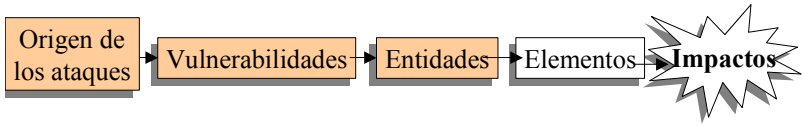


Para que la actividad profesional se desarrolle correctamente, cada elemento esencial tiene una **necesidad de seguridad**.

> Esta necesidad se expresa según distintos **criterios de seguridad** tales como la disponibilidad, la integridad y la confidencialidad. El organismo se vería afectado si no se respetara dicha necesidad. Dicho **impacto** puede adoptar distintas formas: pérdidas financieras, daño al buen funcionamiento de las actividades, daño a la imagen de marca, daño a la seguridad del personal, contaminación…
>
> *Retomemos el ejemplo de un parámetro de cálculo de trayectoria para el lanzamiento de un cohete. Se trata de una información que debería tener una gran necesidad de disponibilidad y de integridad para evitar el daño a la seguridad del personal.*

El estudio de las amenazas

Por otra parte, por su entorno natural, su cultura, su imagen, su área de actividad, cada organismo está expuesto a diversos **elementos peligrosos.**



> Un elemento peligroso puede caracterizarse según su **tipo** (natural, humano o ambiental) y su **causa** (accidental o deliberada).

Cada elemento peligroso puede emplear diversos **métodos de ataque** que es conveniente identificar.

Un método de ataque puede caracterizarse según los criterios de seguridad (disponibilidad, integridad, confidencialidad…) a los cuales puede afectar y según los elementos peligrosos que podrían utilizarlo.

Sigamos con nuestro ejemplo. Un organismo que lanza cohetes debe tener en cuenta una gran cantidad de métodos de ataque y de elementos peligrosos:

- *los accidentes físicos (Ej.: un incendio),*
- *los hechos naturales (Ej.: un fenómeno sísmico),*
- *las pérdidas de servicios esenciales (Ej.: fallo de servicio eléctrico),*
- *el compromiso de las informaciones (Ej.: alteración de programas),*
- *los fallos técnicos (Ej.: mal funcionamiento del hardware),*
- *las agresiones físicas (Ej.: sabotaje),*
- *los errores (Ej.: error de interpretación)...*

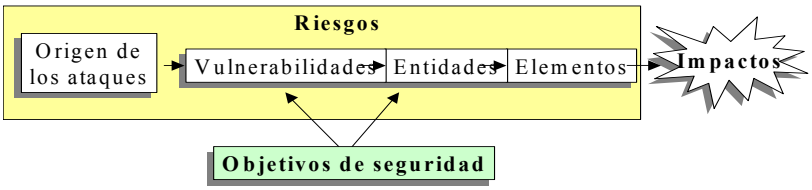
Según cada método de ataque, cada entidad posee **vulnerabilidades** que podrán ser utilizadas por los elementos peligrosos.

De este modo, se podrán identificar varias vulnerabilidades vinculadas con las entidades del organismo que lanza cohetes:

- *la posibilidad de existencia de funciones encubiertas introducidas durante la fase de diseño o de desarrollo (software),*
- *la utilización de hardware no evaluado (hardware),*
- *la posibilidad de crear o de modificar comandos de sistemas (redes),*
- *la posibilidad, que brinda la red, de actuar sobre el software de los recursos del sistema (redes),*
- *la facilidad para penetrar en el establecimiento mediante accesos indirectos (locales),*
- *el incumplimiento de las consignas por parte de algunos operadores (personal),*
- *la falta de medidas de seguridad en las fases de diseño, puesta en servicio y gestión (organización)...*

La expresión de los objetivos de seguridad

Sólo queda determinar cómo pueden afectar los elementos peligrosos y sus métodos de ataque a los elementos esenciales: se trata del **riesgo**.



El riesgo representa un posible siniestro. Consiste en la posibilidad de que un elemento peligroso afecte a los elementos esenciales aprovechando las vulnerabilidades de entidades en las cuales se basan dichos elementos esenciales y utilizando un método de ataque particular.

En nuestro ejemplo, un riesgo consiste en comprometer información sensible mediante la alteración del software gracias a la posibilidad de crear o modificar comandos del sistema vinculados con la red, lo que podría afectar a la seguridad del personal y la imagen de marca.

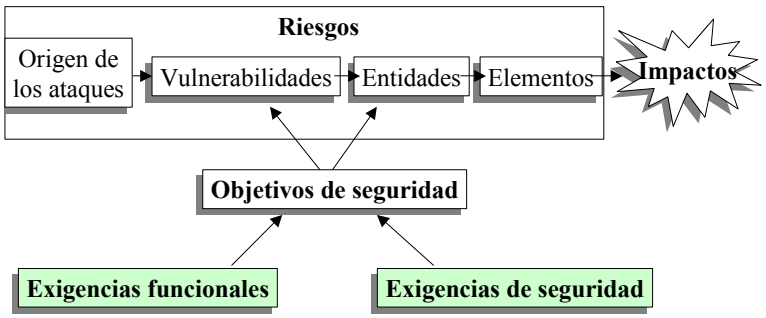
Los **objetivos de seguridad** consisten principalmente en cubrir las vulnerabilidades de las entidades que conforman el conjunto de riesgos aceptados.

Efectivamente, es inútil proteger lo que no está expuesto. También podemos señalar que cuanto más importante sea el riesgo potencial, más importante será el nivel de los objetivos de seguridad. De este modo, dichos objetivos constituirán un pliego de condiciones perfectamente adaptado.

Para el organismo que lanza cohetes, uno de los objetivos de seguridad es brindar seguridad para la creación y la modificación de comandos de sistemas vinculados con la red.

La determinación de los requerimientos de seguridad

El equipo encargado de la aplicación del procedimiento debe especificar luego, en forma precisa, las funcionalidades esperadas en materia de seguridad. Con dichos **requerimientos funcionales,** debe demostrar la perfecta cobertura de los objetivos de seguridad.



En nuestro ejemplo, una de los requerimientos funcionales que cubren la seguridad en la creación y modificación de los comandos del sistema vinculados con la red es la siguiente: durante el funcionamiento normal, el sistema debe ejecutar en forma periódica una serie de autotests para comprobar su correcto funcionamiento.

El equipo encargado debe especificar los **requerimientos de seguridad** que permiten obtener el nivel de confianza necesario para, luego, demostrarlo.

Uno de los requerimientos de seguridad es el siguiente: el desarrollador debe efectuar un análisis de la resistencia de las funciones de seguridad del sistema según el nivel de resistencia requerido.

En resumen

EBIOS formaliza un procedimiento de apreciación y de tratamiento de los riesgos en el área de la seguridad de los sistemas de información.

Su enfoque simple y modular le permite adaptarse a todos los contextos y a distintas acciones de seguridad. Además, EBIOS resulta ser una excelente herramienta de negociación, de arbitraje y de concienciación.

La convergencia hacia las normas internacionales, el software libre, la formación y el club de usuarios hacen de EBIOS un método rico y que los expertos mantienen en el más alto nivel dentro del área de la seguridad de los sistemas de información.

Para mayor información:

- el sitio web de la DCSSI http://www.ssi.gouv.fr
- la dirección electrónica EBIOS ebios.dcssi@sgdn.pm.gouv.fr
- la dirección electrónica de la Oficina de Consultoría conseil.dcssi@sgdn.pm.gouv.fr