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®

SECCIÓN 1
INTRODUCCIÓN

Versión 2 – 5 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

Este documento ha sido realizado por la oficina de consultoría de la DCSSI
(SGDN / DCSSI / SDO / OCS)
en colaboración con el Club EBIOS

Rogamos nos haga llegar sus comentarios y sugerencias a la siguiente dirección:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
FRANCE

ebios.dcssi@sgdn.pm.gouv.fr

Histórico de las modificaciones

Versión	Motivo de la modificación	Situación
02/1997 (1.1)	Publicación de la guía para la expresión de las necesidades e identificación de los objetivos de seguridad (EBIOS).	Validado
23/01/2004	Revisión general: - Explicaciones y armonización con las normas internacionales de seguridad y gestión de los riesgos. - Identificación del referencial reglamentario respecto al conjunto de limitaciones que deben tenerse en cuenta. - Integración de los conceptos de hipótesis y normas de seguridad (ISO/IEC 15408) - Transferencia de la selección de elementos fundamentales al estudio del sistema correspondiente. - Perfeccionamiento de la elaboración de la escala de necesidades: los valores que representan los límites aceptables para el organismo con relación a impactos personalizados. - Integración de la determinación de las necesidades por elemento en la siguiente actividad. - Integración de la determinación del modo de explotación en las hipótesis. - Adaptación de los conceptos a la ISO/IEC 15408: se estudia el origen de las amenazas, es decir, los métodos de ataque y elementos peligrosos, así como sus características, que pueden incluir un tipo (natural, humano, ambiental), una causa (accidental, deliberada, afinando en exposición, recursos disponibles, pericia, motivación), un potencial de ataque. - Identificación de los métodos de ataque no considerados. - Formalización de las amenazas, según la orientación de la ISO/IEC 15408 (elemento peligroso, ataque y bien en forma de entidades), antes de la confrontación con las necesidades de seguridad. - Modificación de la confrontación de las amenazas con las necesidades, que permite identificar los riesgos. - Identificación de los riesgos no considerados. - Integración de la determinación de los objetivos de seguridad mínimos en las actividades de formalización de los objetivos de seguridad, y determinación de los requerimientos funcionales. - Modificación de la determinación de los objetivos de seguridad, que toma en cuenta las hipótesis, las normas de la política de seguridad, las limitaciones, el referencial reglamentario y los riesgos. - Incorporación de la determinación de los niveles de seguridad, que permite determinar el nivel de los objetivos de seguridad (especialmente en función de los potenciales de ataque) y elegir un nivel de aseguramiento. - Incorporación de la determinación de los requerimientos de seguridad funcionales, que permite determinar los requerimientos funcionales que cubren los objetivos de seguridad y presentar esta cobertura. - Incorporación de la identificación de los requerimientos de seguridad del aseguramiento, que permiten determinar los eventuales requerimientos de aseguramiento. Mejoras formales, ajustes y correcciones menores (gramática, ortografía, redacción, presentaciones, coherencia...)	Validado por el Club EBIOS
05/02/2004	Publicación de la versión 2 de la guía EBIOS	Validado

Índice

Prefacio

La búsqueda permanente de una mayor eficiencia en el cumplimiento de su misión ha llevado a los diferentes departamentos de Estado a implementar medios de telecomunicación, informática y ofimática. El recurso generalizado a estas tecnologías hace que estos organismos se vuelvan dependientes de sus sistemas de información y, por tanto, vulnerables a las múltiples amenazas que pesan sobre ellos. Esta situación contribuye notablemente a aumentar los riesgos resultantes del procesamiento, almacenamiento y transferencia de datos, dentro de cualquier organismo.

Las nuevas directrices de la Organización de Cooperación y Desarrollo Económicos [OCDE] son recomendadas a nivel internacional. Tienen por objetivo fundamental el de promover una "cultura de la seguridad" como medio de protección de los sistemas y redes de información. Esto significa que es necesario prestar mucha atención a la seguridad y adoptar nuevos criterios y actitudes durante el desarrollo y utilización de los sistemas de información y las redes. Estas directrices se presentan como nueve principios complementarios que deben ser considerados como un todo.

En el ámbito de la sociedad de la información, el plan de acción [eEuropa 2005] tiene el objetivo de desarrollar los servicios públicos en línea y los accesos a Internet de alta velocidad. Esto se traduce especialmente en servicios públicos en línea modernos ("e-government", "e-learning", "e-health"), un ambiente dinámico para los negocios electrónicos ("e-business"), una infraestructura de información segura, la disponibilidad masiva de un acceso de banda ancha a precios competitivos, la evaluación comparativa ("benchmarking") y la difusión de buenas prácticas.

El gobierno francés ha dado sus primeros pasos en el campo de la administración electrónica. Se trata de poner las tecnologías de la información al servicio de la modernización de los servicios públicos, mejorar la eficacia de la actuación de las instituciones del Estado como comunidades locales y la calidad de las relaciones entre éstas y sus usuarios. Esta desmaterialización "de los servicios públicos" no puede realizarse sin prestar un mínimo de atención a la seguridad. La finalidad de la DCSSI de la SGDN es contribuir a la definición interministerial y a la difusión de la política gubernamental en materia de seguridad de los sistemas de información.

La actuación del Estado podría ser cuestionada por los riesgos surgidos del uso de los sistemas de información. Por esta razón, la protección de la información y la seguridad de los sistemas de información es una obligación nacional capital.

En lo que respecta a los sistemas que procesan información clasificada de defensa, la [IGI 1300] prevé especialmente que los sistemas de información deben "protegerse conforme a una política de seguridad definida en función del nivel de protección requerido, en particular del nivel de clasificación de la información procesada y en base a un análisis de los riesgos".

Este documento forma parte de una serie de guías metodológicas publicadas por la DCSSI. Estas guías están destinadas a contribuir a la mejora de la protección de los sistemas de información de los organismos públicos o privados. Pueden obtenerse solicitándolas a la DCSSI.

Estas guías se basan en documentos que ya han sido largamente discutidos por el gobierno, así como en la experiencia y el *know-how* de numerosos industriales. Los autores consideran que los conceptos e ideas expuestos en dichos documentos y métodos han sido cuidadosamente evaluados y que la estructura elegida optimiza su coherencia, su comprensión y su facilidad de uso.

Nota: Las referencias [entre corchetes] se presentan en la bibliografía, al final del documento. Se adjunta también un glosario de los términos y acrónimos utilizados.

1 Introducción

1.1 El procedimiento de seguridad

1.1.1 La seguridad de los sistemas de información

La seguridad de los sistemas de información (SSI) se refiere en primer lugar y esencialmente a la información y a los "tratamientos" que se le aplican. Las necesidades, requerimientos y objetivos técnicos u organizacionales derivan naturalmente de ella. Se deben tomar en cuenta tres criterios fundamentales: la confidencialidad, la integridad y la disponibilidad, tanto de los datos como de los sistemas y de los entornos en los cuales estos se encuentran. Podemos, en ciertos casos, preocuparnos por las necesidades de no repudio, autorización y autenticación gracias a medios de auditoría que habrá que definir claramente.
La SSI está directamente vinculada con la apreciación y el tratamiento de los riesgos. Estos riesgos se califican como operativos porque afectan directamente a las actividades de las instituciones y empresas. Efectivamente, el organismo que utiliza soportes de las tecnologías de la información y la comunicación (TIC), especialmente Internet, para realizar sus actividades y transacciones comerciales, está directamente involucrado en la SSI.

1.1.2 Los objetos y ámbitos de la seguridad

Dado que la SSI toma en cuenta la información, el tratamiento, el sistema y su entorno, serán objeto del procedimiento de seguridad:

- los datos,
- los procesos, funciones o aplicaciones,
- la tecnología (hardware y sistemas operativos),
- el entorno físico (edificios, locales…),
- el componente humano.

Todos estos elementos -entre los cuales algunos, como los procesos y los hombres, son especialmente activos- deben estar claramente definidos. Cada uno de ellos se ve afectado por un ámbito específico de la seguridad, y cada uno interviene en mayor o menor medida en cada ámbito.
Una política de seguridad que no tomara en cuenta todos estos elementos y ámbitos sería inestable e incompleta. Produciría una solución peligrosa basada en un falso sentimiento de seguridad más dañino aún que no hacer nada.

1.1.3 Los procedimientos normalizados

Desde hace unos diez años, se han realizado numerosos esfuerzos para fijar normas, o al menos directivas generales, para la gestión de la seguridad de las tecnologías de la información. Dichos trabajos se han traducido en normas nacionales e internacionales (tales como las normas [ISO 13335], [ISO 17799]…). Aunque estas normas estén en evolución y aún no totalmente estabilizadas, es posible utilizarlas como una gran fuerte de inspiración.

En Francia es obligatorio redactar una [FEROS] para los sistemas que procesan información clasificada de defensa, lo que también se recomienda para los demás sistemas. Dicha ficha forma parte de la documentación de seguridad que se utiliza para la aprobación de un sistema con miras a su homologación.

Por otra parte, las normas internacionales subordinan la política de seguridad de un sistema de información específico a la política de seguridad global de los sistemas de información, la cual depende a su vez de la seguridad de la información, de la política de tecnologías de la información y de la comunicación, de la política de personal y de la política financiera y presupuestaria. Todo el conjunto solo tiene sentido si las acciones se definen en concordancia con la estrategia y la política general de la empresa u organización.

La elaboración de los Criterios Comunes [ISO 15408], ha permitido que tanto los usuarios como los fabricantes reflexionen sobre la seguridad de los sistemas de información. Los Criterios Comunes permiten evaluar la fiabilidad ofrecida, tanto a nivel de la conformidad de la implementación de las funciones destinadas a la seguridad como desde el punto de vista de su eficacia para contrarrestar las amenazas identificadas. Han sido elaborados conjuntamente con los industriales europeos de la informática, por la DCSSI y los departamentos homólogos alemanes, estadounidenses, británicos, canadienses y holandeses.

Algunas instituciones internacionales impulsan la normalización de los enfoques para la publicación de principios y objetivos precisos. Citemos a la OCDE y sus principios y a la Comisión Europea, que

produce regularmente directivas a las cuales deben conformarse los Estados miembros. El procedimiento de seguridad, por ejemplo, debería intervenir desde el surgimiento de la primera idea para un nuevo sistema de información. De este modo, el diseño de un sistema de información (SI) incorpora los elementos de seguridad necesarios al mismo tiempo que los elementos funcionales y operativos, desde el inicio del estudio del proyecto. Esto asegura la máxima eficacia, costos mínimos y un rendimiento de la inversión muy positivo. Por otra parte, el procedimiento de seguridad debería abarcar la totalidad del SI y su entorno o contexto operativo. Debería estar presente en todos los niveles del organismo y del SI.

1.2 La respuesta de la DCSSI

El método EBIOS ha sido elaborado siguiendo la orientación de estos procedimientos. Se utiliza generalmente a nivel de la fase de elaboración de un esquema director operativo de un sistema de información. Su objetivo principal es permitir que cualquier organismo, incluidas las instituciones estatales, pueda determinar las acciones de seguridad que es conveniente poner en práctica.

Puede ser implementado por el experto en seguridad del organismo y puede aplicarse a todos los niveles de la estructura de un sistema de información existente o futuro (subsistemas, aplicaciones).

En su primera versión, el método EBIOS permitía en particular la redacción de los objetivos de seguridad [FEROS].
En el año 2000, luego de haber considerado la necesaria convergencia hacia la redacción de perfiles de protección y basándose en la versión 2.0 de los Criterios Comunes [ISO 15408], la DCSSI emprendió la adaptación del método EBIOS a dichos criterios.

Los resultados de un estudio EBIOS aportan los datos necesarios para la redacción de un pliego de condiciones de SSI del sistema estudiado (FEROS, perfil de protección u otros) y contribuyen también a la elaboración de una arquitectura funcional segura. Desde el punto de vista de la evaluación de los Criterios Comunes, los resultados del estudio aportan los datos necesarios para determinar las especificaciones del sistema evaluado (contribuyen a elaborar el objetivo de seguridad).

En su esencia y en su filosofía general, el procedimiento EBIOS puede también aplicarse a todos los niveles del SI -desde la política de seguridad del sistema de información (PSSI) global a la aplicación particular- sin cambiar ni su redacción, ni sus técnicas. Podría ser útil realizar únicamente algunas adaptaciones en el vocabulario para adaptar los conceptos del método al contexto particular. Por ejemplo, el término "función" que aparece frecuentemente tanto en el método como en el objeto de estudio, podría traducirse por "oficio, proceso, sistema...".
A fin de facilitar esta adaptación del vocabulario e informar al público sobre la gran variedad de usos del procedimiento y del método EBIOS, se ha desarrollado una serie de guías de "Mejores prácticas".

1.3 Las guías del método

El método EBIOS[1] está formado por cinco secciones complementarias.

- Sección 1 – Introducción
  Esta sección presenta el contexto, el interés y el posicionamiento del procedimiento EBIOS. Contiene también una bibliografía, un glosario y acrónimos.
- Sección 2 – Procedimiento
  Esta sección explica el desarrollo de las actividades del método.
- Sección 3 – Técnicas
  Esta sección propone medios para realizar las actividades del método. Será conveniente adaptar estas técnicas a las necesidades y prácticas del organismo.
- Sección 4 – Herramientas para la apreciación de los riesgos SSI
  Esta sección constituye la primera parte de la base de conocimientos del método EBIOS (tipos de entidades, métodos de ataques, vulnerabilidades).
- Sección 5 – Herramientas para el tratamiento de los riesgos SSI
  Esta sección constituye la segunda parte de la base de conocimientos del método EBIOS (objetivos de seguridad, requerimientos de seguridad, cuadros de determinación de los objetivos y requerimientos de seguridad funcionales).

El presente documento constituye la primera sección del método.

[1] EBIOS es un marca registrada de la Secretaría General de Defensa Nacional de Francia.

2 Presentación del método EBIOS

2.1 ¿Qué es el método EBIOS ?

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) significa "expresión de las necesidades e identificación de los objetivos de seguridad".

No se trata solo de un **método de apreciación de los riesgos de la SSI**, sino también de una verdadera **herramienta de ayuda para el diseño del proyecto** (definición de un perímetro de estudio, expresión de necesidades, responsabilidad de los actores…). Asociada a los Criterios Comunes y a los avances en el campo de la gestión de la seguridad de la información (por ejemplo, la norma [ISO 17799]), EBIOS se transforma también en un **método de tratamiento de los riesgos de SSI**.

EBIOS responde al pedido de una autoridad (jefe de proyecto, diseñador del proyecto, autoridad de homologación del sistema, dirección del organismo…). Permite racionalizar los objetivos y requerimientos de seguridad en función de riesgos identificados y eventualmente seleccionados.

Constituye un apoyo en la percepción del organismo en el plano de la seguridad considerada en su sentido más amplio. Esta visión y este enfoque global del reto de la seguridad permiten, por una parte, tomar en cuenta lo existente en materia de seguridad, y, por otra parte, determinar un referencial coherente en el cual se basarán los desarrollos futuros.

2.2 Antes de realizar un estudio EBIOS

Lo ideal sería que el estudio EBIOS se apoye en diferentes documentos referidos al organismo, a su sistema de información y al sistema que se estudiará:

- el esquema director del organismo,
- la política de seguridad de los sistemas de información (PSSI),
- las especificaciones generales del sistema (existente o futuro).

Sin embargo, podemos comprobar que estos documentos no siempre están formalizados. El trabajo comenzará entonces por la recogida de los elementos que deberían conformar estos documentos estratégicos.

Por otra parte, la precisión del estudio será proporcional al nivel de precisión de las especificaciones generales del sistema. Un sistema del cual se ignora la finalidad no podrá ser objeto de un estudio de seguridad, del mismo modo que no puede tampoco ser objeto de un estudio funcional.

2.3 ¿Cuál es el resultado de EBIOS?

EBIOS sirve para formalizar una idea, a fin de generar el referencial de documentos de seguridad susceptible de ser aprobado por una autoridad.

Este método permite identificar objetivos y requerimientos de seguridad tras una apreciación de los riesgos, contribuyendo por tanto a la realización de:

- un esquema director de SSI;
- una política de seguridad;
- un plan de acción de SSI;
- una ficha de expresión racional de los objetivos de seguridad [FEROS], obligatoria para los sistemas clasificados de defensa [IGI 900], recomendada en todos los otros casos, por ejemplo para información sensible [REC 901];
- especificaciones adaptadas y justificadas para la dirección de proyecto (pliego de condiciones);
- un perfil de protección (PP) o de un objetivo de seguridad (tal como lo define la [ISO 15408])…

Pero EBIOS es mucho más que eso, es también:

- un razonamiento simple, flexible y coherente;
- una herramienta de negociación y mediación en el proceso de SSI;
- un medio para unificar vocabulario, conceptos e interpretación del sistema;
- un enfoque que busca concienciar, responsabilizar e implicar a todos los actores;
- una herramienta compatible con las herramientas SSI existentes ([PSSI], [EOSSI], [MASSIA], [MAQSSIA], [ISO 15408], [ISO 17799]…).

2.4 Lo que no permite el método EBIOS

El estudio EBIOS no es un catálogo de soluciones o normas de seguridad listas para usar. No se trata en ningún caso de una "caja negra" con una entrada y una salida. Siendo así, no permite aportar soluciones inmediatas y genéricas para los retos de seguridad. Si bien se determinarán, efectivamente, las requerimientos de seguridad para especificar medidas de seguridad, su implementación se realizará recién después del estudio.

2.5 Lo que permite el método EBIOS

2.5.1 Colaborar en el diseño del proyecto

El método EBIOS ayuda a la elaboración de las tareas que el diseñador del proyecto debe realizar:

- determinar el objeto de estudio, conservando una visión global del sistema estudiado en su contexto,
- expresar las necesidades (bienes que deben protegerse),
- identificar las amenazas,
- determinar las acciones de seguridad que es conveniente implementar,
- determinar los elementos de especificación que se utilizarán para la redacción de la [FEROS] o del [PP],
- definir un plan de proyecto y las responsabilidades.

2.5.2 Ofrecer a la dirección de proyecto una herramienta de elección y evaluación

El método EBIOS permite a la dirección de proyecto:

- respetar los objetivos expresados por el diseñador del proyecto,
- dar una respuesta sobre la factibilidad, los costos y los plazos propuestos,
- elegir soluciones,
- elaborar objetivos de seguridad.

2.5.3 Ofrecer una herramienta de evaluación del impacto y de negociación entre la entidad contratante y la dirección (del proyecto, del organismo…)

El método EBIOS ayuda a la dirección a:

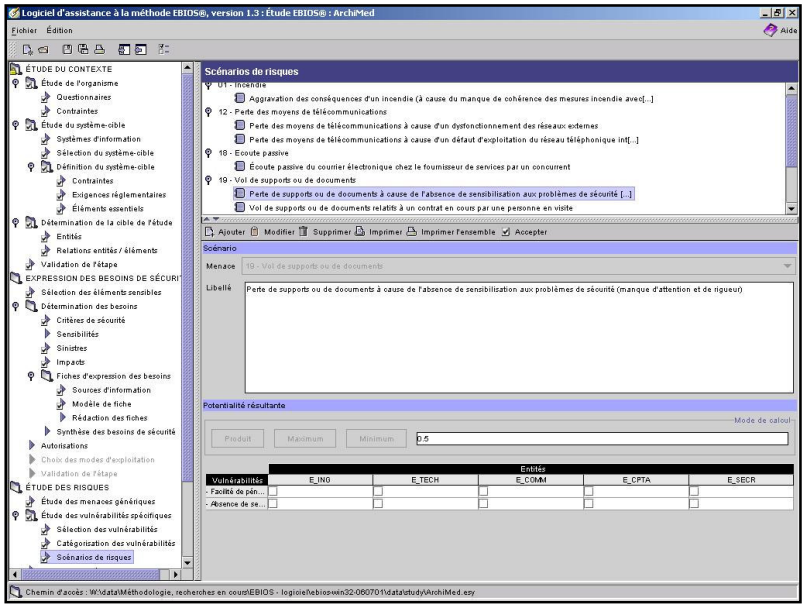
- evaluar el impacto sobre el entorno,
- controlar la adecuación de los SI,
- centralizar los estudios y la SSI,
- tomar decisiones estratégicas en el ámbito de la seguridad y en el ámbito operativo.

3 Las herramientas del método EBIOS

3.1 El software libre

El programa EBIOS facilita mucho la realización de los estudios EBIOS. Permite efectivamente consignar la totalidad de los resultados de un estudio y producir los documentos de síntesis necesarios. Con la mayor facilidad de uso, permite también personalizar sus bases de conocimientos.

Se trata de un software libre, disponible gratuitamente, con sus fuentes, a pedido, enviando sus datos a ebios.dcssi@sgdn.pm.gouv.fr.



Ha sido desarrollado en Java y XML, y la comunidad de usuarios puede introducir mejoras siempre que se comuniquen las mismas a la SGDN.

3.2 Las mejores prácticas

El método EBIOS constituye una verdadera caja de herramientas modular. Efectivamente, el desarrollo de las actividades del método y su precisión pueden variar en función de los objetivos del proyecto. A este respecto, se ha redactado un conjunto de mejores prácticas para explicar cómo utilizar los resultados del método EBIOS en función de la finalidad deseada.

- Elaboración de un esquema director de seguridad de los sistemas de información.
- Elaboración de una política de seguridad de los sistemas de información [PSSI].
- Redacción de una FEROS.
- Redacción de un SSRS (*System-specific Requirement Statement* – OTAN)
- Redacción de un perfil de protección (conforme a la ISO/IEC 15408).
- Redacción de un objetivo de seguridad (conforme a la ISO/IEC 15408).
- Implementación de un marco de gestión de la seguridad de la información.
- Redacción de una política de certificación.
- Estudio de un sistema por diseñar.
- Estudio de un sistema existente...

Estos documentos están disponibles en Internet (http://www.ssi.gouv.fr/).

3.3 La formación

El CFSSI (centro de formación de la DCSSI) organiza cursos de formación en el método EBIOS para el sector público francés.

La DCSSI propone también una formación para formadores a fin de transmitir los conocimientos y evitar eventuales desviaciones en la difusión y el uso de este método..

La información sobre estas formaciones está disponible en Internet en la dirección http://www.ssi.gouv.fr/formation.

3.4 El club EBIOS

El club de los grandes usuarios del método EBIOS fue creado en el año 2003 con el objetivo de reunir a la comunidad de expertos, compartir experiencias y mejorar el método y sus herramientas.

Glosario

La traducción al inglés de los términos del glosario figura entre paréntesis para cada término. El texto en itálica corresponde a los ejemplos. El texto subrayado en las definiciones corresponde a los conceptos definidos en el presente documento.

Aceptación del riesgo
(acceptation du risque, risk acceptance)

Decisión de aceptar un riesgo tratado según los criterios de riesgo.

Amenaza
(menace, threat)

Posible ataque a los bienes por parte de un elemento peligroso.

Ejemplos:

- *Un ex-empleado, que tiene pocos conocimientos técnicos y tiempo pero puede tener una fuerte motivación, altera voluntariamente programas del sistema mediante un virus, aprovechando la facilidad para introducir programas de efectos perniciosos en la red "ofimática del organismo", lo que puede afectar especialmente la función de preparación de presupuestos y la generación de certificados de firmas electrónicas.*
- *Un pirata informático con un buen conocimiento técnico, hardware estándar y pagado para hacerlo, roba archivos confidenciales accediendo remotamente a la red de la empresa.*
- *Un desarrollador, miembro del personal, con un muy buen conocimiento de los códigos fuente pero pocos conocimientos de SSI, modifica por su propia voluntad el código fuente.*
- *Un visitante roba material informático que contiene datos confidenciales.*
- *…*

Análisis del riesgo
(analyse du risque, risk analysis)

Utilización sistemática de datos para la identificación de los orígenes de los ataques y la estimación del riesgo.

Apreciación del riesgo
(appréciation du risque, risk assessment)

Conjunto del proceso de análisis del riesgo y evaluación del riesgo. [ISO Guía 73]

Ataque
(attaque, attack)

Explotación de una o varias vulnerabilidades utilizando un método de ataque con una oportunidad dada.

Ejemplos:

- *gran oportunidad de uso de software falsificado o copiado debido a la ausencia total de concienciación o de información sobre la legislación referida a los derechos de autor;*
- *alteración del software por un virus debido a la facilidad para introducir programas de efectos dañinos en la red ofimática del organismo;*

Bien
(bien, asset)

Cualquier recurso que tenga valor para el organismo y que sea necesario para la realización de sus objetivos. Destacamos especialmente los elementos esenciales y las entidades que es conveniente proteger.

Ejemplos:

- *lista de nombres;*
- *solicitud de certificación;*
- *gestión de la facturación;*
- *algoritmo de cifrado;*
- *microordenador portátil;*
- *Ethernet;*
- *sistema operativo;*

Comunicación referida al riesgo

(communication relative au risque, risk communication)

Acción de intercambiar o compartir datos relacionados con el riesgo, entre el responsable de la toma de decisiones y las otras partes involucradas. [ISO Guía 73]

Confidencialidad
(confidentialité, confidentiality)

Propiedad de los elementos esenciales consistente en ser accesibles sólo para los usuarios autorizados.

Criterio de seguridad
(critère de sécurité, security criteria)

Característica de un elemento esencial que permite apreciar sus diferentes necesidades de seguridad.

Ejemplos:

- *disponibilidad,*
- *integridad,*
- *confidencialidad,*

Criterios de riesgo
(critères de risque, risk criteria)

Términos de referencia que permiten apreciar la importancia de los riesgos.

Disponibilidad
(disponibilité, availability)

Propiedad de los elementos esenciales consistente en ser accesibles por parte de los usuarios autorizados cuando éstos lo requieren.

Elemento esencial
(élément essentiel, essential element)

Información o función que tiene al menos una necesidad de seguridad existente.

Ejemplos:

- *una lista de nombres,*
- *una solicitud de certificación,*
- *gestionar la facturación,*
- *un algoritmo de cifrado,*

Elemento peligroso
(élément menaçant, threat agent)

Acción humana, elemento natural o ambiental que tiene consecuencias potenciales negativas para el sistema. Puede caracterizarse por su tipo (natural, humano o ambiental) y por su causa (accidental o deliberada). Cuando se trata de una causa accidental, puede caracterizarse también en función de la exposición y los recursos disponibles. Cuando se trata de una causa deliberada, puede caracterizarse también en función de la pericia, los recursos disponibles y la motivación.

Ejemplos:

- *ex-empleado que tiene pocas competencias técnicas y tiempo pero puede tener una fuerte motivación;*
- *pirata informático con amplios conocimientos técnicos, bien equipado y con una fuerte motivación vinculada con el dinero que puede ganar;*
- *clima muy lluvioso durante tres meses al año;*
- *virus;*
- *usuarios;*
- *desarrolladores;*

Entidad
(entité, entity)

Se trata de un bien que puede ser del tipo organización, establecimiento, personal, hardware, red, software, sistema.

Ejemplos:

- *empresa de servicios informáticos;*
- *locales del organismo;*
- *administrador del sistema;*
- *microordenador portátil;*
- *Ethernet;*
- *sistema operativo;*
- *portal electrónico;*

Estimación del riesgo
(risk estimation, risk estimation)

Proceso utilizado para atribuir valores a la oportunidad y a las pérdidas que un riesgo puede generar.

Evaluación del riesgo
(évaluation du risque, risk evaluation)

Proceso de comparación del riesgo estimado utilizando determinados criterios de riesgo para establecer la importancia de un riesgo. [ISO Guía 73]

Exposición
(exposition, exposure)

Nivel de exposición natural de un sistema estudiado frente a un elemento peligroso cuya causa es accidental. Este nivel puede caracterizarse por una exposición baja, moderada o intensa.

Ejemplos:

- *exposición baja;*
- *exposición moderada;*
- *exposición intensa.*

Función
(fonction, function)

Tratamiento o conjunto de tratamientos que contribuyen al funcionamiento de la actividad de un organismo, que crea, modifica, destruye o transfiere datos.

Ejemplos:

- *crear planes técnicos;*
- *redactar los presupuestos;*
- *gestionar la facturación;*
- *un algoritmo de cifrado;*
- *generar un certificado;*

Gestión del riesgo
(gestion du risque, risk management)

Actividades coordinadas que buscan dirigir y guiar a un organismo frente a un riesgo. La gestión del riesgo incluye específicamente la apreciación del riesgo, el tratamiento del riesgo, la aceptación del riesgo y la comunicación referida al riesgo. [ISO Guía 73]

Hipótesis
(hypothèse, assumption)

Postulado, planteado sobre el entorno operativo del sistema, que permite aportar las funcionalidades de seguridad esperadas.

Ejemplos:

- *El sistema se instalará en una sala concebida para minimizar las emisiones electromagnéticas.*
- *El administrador se ubicará en una zona de acceso reservado.*
- *Los usuarios no escribirán sus contraseñas.*
- *La red no estará conectada a otra red cuya fiabilidad no haya sido determinada.*
- *Cada uno dentro de la empresa conoce sus responsabilidades en caso de difusión ilícita de información de su área de trabajo o manipulación ilegal de datos personales.*

Identificación de los orígenes de los ataques
(identification des origines des attaques, source identification)

Proceso que permite encontrar, enumerar y caracterizar los orígenes de los ataques (elementos peligrosos y métodos de ataque).

Impacto
(impact, impact)

Consecuencia para el organismo de la materialización de una amenaza.

Ejemplos:

- *pérdida de imagen de marca frente a la clientela;*
- *pérdida financiera del orden del 10% de la facturación;*
- *violación de las leyes y reglamentos que da lugar a acciones judiciales iniciadas al director;*

Información
(information, information)

Dato o elemento de conocimiento susceptible de ser representado bajo una forma adaptada a una comunicación, un registro o un tratamiento. [IGI 900] [REC 901]

Ejemplos:

- *un mensaje;*
- *una lista de nombres;*
- *una solicitud de certificación;*
- *una lista de revocación;*

Integridad
(intégrité, integrity)

Calidad de elementos esenciales exactos y completos.

Medida de seguridad
(mesure de sécurité, security measure)

Medio destinado a mejorar la seguridad, especificado para un requerimiento de seguridad y que es necesario implementar para satisfacerla. Puede tratarse de medidas de previsión o de preparación, de disuasión, protección, detección, aislamiento, de "lucha", de recuperación, restauración, compensación...

Método de ataque
(méthode d'attaque, attack method)

Medio típico (acción o acontecimiento) con el que un elemento peligroso realiza sus ataques.

Ejemplos:

- *robo de soportes informáticos o de documentos;*
- *alteración de programas;*
- *atentado contra la disponibilidad del personal;*
- *escucha pasiva;*
- *inundación;*

Motivación
(motivation, motivation)

Motivo de un elemento peligroso. Puede tener un carácter estratégico, ideológico, terrorista, codicioso, lúdico o vengador y varía según se trate de un acto accidental (curiosidad, aburrimiento…) o deliberado (espionaje, afán de lucro, intención de perjudicar, ideología, juego, fraude, robo, piratería, reto intelectual, venganza, chantaje, extorsión monetaria…).

Ejemplos [Guía 650]:

- *carácter estratégico;*
- *carácter ideológico;*
- *carácter terrorista;*
- *carácter codicioso;*
- *carácter lúdico;*
- *carácter vengativo;*

[…]

- *Cuando se trata de un acto deliberado:*
  - *espionaje,*
  - *afán de lucro,*
  - *intención de perjudicar,*
  - *ideología,*
  - *juego,*
  - *fraude,*
  - *robo,*
  - *piratería,*
  - *reto intelectual,*
  - *venganza,*
  - *chantaje,*
  - *extorsión monetaria,*
  - *…*
- *Cuando se trata de un acto accidental:*
  - *curiosidad,*
  - *aburrimiento,*

Necesidad de seguridad
(besoin de sécurité, sensitivity)

Definición precisa y sin ambigüedad de los niveles correspondientes a los criterios de seguridad (disponibilidad, confidencialidad, integridad...) que es conveniente garantizar para un elemento esencial.

Norma de seguridad
(règle de sécurité, organisational security policy)

Regla, procedimiento, código de conducta o directriz de seguridad que una organización impone para su funcionamiento. [ISO 15408]

Ejemplos:

- *Todos los productos utilizados por el Estado deben conformarse a las normas nacionales en materia de criptología para la generación de contraseñas.*
- *Todos los productos utilizados en el ámbito bancario deben estar certificados al nivel EAL4 sumado el componente ADV_IMP.2.*
- *El control de acceso se realiza mediante una identificación / contraseña.*
- *Cada ingeniero es responsable por el archivo que procesa.*
- *Una alarma anti-intrusión se activa durante las horas de cierre (19 h – 7 h) .*

Objetivo de seguridad
(objectif de sécurité, security objective)

Expresión de la intención de contrarrestar amenazas o riesgos identificados (según el contexto) y/o de satisfacer políticas de seguridad organizacionales e hipótesis. Un objetivo puede centrarse en el sistema evaluado, en su entorno de desarrollo o en su entorno operativo.

Ejemplos:

- *Objetivos "abiertos" (amplio margen de maniobra para cubrir el objetivo de seguridad):*
  - *las configuraciones de las terminales de la red interna deben ser escalables;*
  - *los locales deben estar protegidos contra los rayos;*
- *Objetivos "cerrados" (poco margen de maniobra para cubrir el objetivo de seguridad):*
  - *el sistema debe identificar y autenticar de manera única a los usuarios, y debe hacerlo antes de cualquier interacción entre el sistema y el usuario;*
  - *deben instalarse dos antivirus diferentes y compatibles y deben actualizarse sus bases de datos de virus cada dos semanas;*

Oportunidad
(opportunité, opportunity)

Medición de la posibilidad de aparición de un ataque.

Ejemplos:

- *improbable;*
- *muy probable;*
- *totalmente impracticable;*
- *15 % de posibilidades de que se produzca;*

Pericia
(expertise, expertise)

Nivel esperado de competencia técnica de un elemento peligroso cuya causa es deliberada. Este nivel puede caracterizarse por competencias técnicas escasas, moderadas o elevadas.

Ejemplos [Guía 650]

- *competencias técnicas escasas;*
- *competencias técnicas moderadas;*
- *competencias técnicas elevadas.*

Política de seguridad de los sistemas de información
(politique de sécurité de système d'information, information systems security policy)

Conjunto, formalizado en un documento aplicable, de elementos estratégicos, directivas, procedimientos, códigos de conducta, normas organizacionales y técnicas, que tiene por objetivo la protección del (o de los) sistema(s) de información del organismo. [PSSI]

Principio de seguridad
(principe de sécurité, security principle)

Los principios de seguridad son la expresión de las orientaciones de seguridad necesarias y de las características importantes referentes a la seguridad para la elaboración de una política y, especialmente, de las normas de seguridad que la conforman. [PSSI]

Recursos disponibles
(ressources disponibles, available resources)

Medios con los que se espera cuente el elemento peligroso. El nivel de recursos disponibles constituye su potencial de ataque y puede caracterizarse por recursos escasos, moderados o amplios.

Ejemplos:

- *recursos escasos;*
- *recursos moderados;*
- *recursos amplios.*

Reducción del riesgo
(réduction du risque, risk reduction)

Proceso que busca minimizar las consecuencias negativas y las oportunidades de una amenaza.

Requerimiento de aseguramiento
(exigence d'assurance de sécurité, security assurance requirement)

Especificación de aseguramiento de las funciones de seguridad que deben implementarse para alcanzar uno o varios objetivos de seguridad, centrada generalmente en el entorno de desarrollo del sistema.

Ejemplos:

- *el desarrollador debe aportar especificaciones funcionales;*
- *las especificaciones funcionales deben describir el objetivo y las instrucciones de uso de todas las interfaces externas de las funciones de seguridad, aportando, cuando sea conveniente, los detalles completos sobre todos los efectos, excepciones y mensajes de error;*
- *los elementos de prueba deben justificar que las medidas de seguridad aportan el nivel de protección necesaria para mantener la confidencialidad y la integridad del sistema;*

Requerimiento de seguridad
(exigence de sécurité, security requirement)

Especificación funcional o de aseguramiento referida al sistema de información o al entorno de éste, centrada en los mecanismos de seguridad que deben implementarse y que cubre uno o varios objetivos de seguridad.

Requerimiento funcional de seguridad
(exigence fonctionnelle de sécurité, security functional requirement)

Especificación funcional de las funciones de seguridad que debe implementarse para satisfacer uno o varios objetivos de seguridad, centrada en el sistema estudiado.

Ejemplos:

- *El sistema debe generar las claves criptográficas conforme a un algoritmo de generación de claves criptográficas específico y a los tamaños de claves criptográficas especificados que satisfacen las normas específicas.*
- *El sistema debe detectar de manera no ambigua una intrusión física que pudiera comprometerlo.*

Es necesario instalar un pararrayos en los locales del organismo.

Riesgo
(risque, risk)

Combinación de una amenaza y de las pérdidas que puede generar, es decir: de la oportunidad que tiene un elemento peligroso de aprovechar una o varias vulnerabilidades de una o varias entidades, empleando un método de ataque, y del impacto que tendría para los elementos esenciales y el organismo.

Ejemplos:

- *Un ex-empleado, que tiene pocos conocimientos técnicos y tiempo pero puede tener una fuerte motivación, altera voluntariamente programas del sistema por un virus, aprovechando la facilidad para introducir programas de efectos perniciosos en la red "ofimática del organismo", pudiendo afectar especialmente la disponibilidad y la integridad de la función de preparación de presupuestos y la generación de certificados de firmas electrónicas, lo que podría generar la incapacidad para ofrecer un servicio, la imposibilidad de cumplir obligaciones contractuales y consecuencias graves en términos de imagen de marca.*
- *Un pirata informático con buenos conocimientos técnicos, con hardware estándar y pagado para hacerlo, roba archivos confidenciales accediendo remotamente a la red de la empresa, provocando con ello el fracaso de una transacción con un socio y una pérdida de la imagen de marca.*

Riesgo residual
(risque résiduel, residual risk)

Riesgo que subsiste tras el tratamiento del riesgo. [ISO Guía 73]

Seguridad de los sistemas de información (SSI)
(sécurité des systèmes d'information, information security)

Protección de los sistemas de información, y especialmente de los elementos esenciales, contra cualquier acceso no autorizado, accidental o deliberado, a los criterios de seguridad.

Sistema de información (SI)
(système d'information, information system)

Conjunto de entidades organizado para cumplir funciones de procesamiento de datos.

Toma de riesgos
(prise de risque, risk retention)

Aceptación del costo de la pérdida por un riesgo particular.

Transferencia del riesgo
(transfert du risque, risk transfer)

Acción de compartir con otra parte el costo de la pérdida generada por un riesgo particular.

Ejemplos:

- *suscripción de un seguro;*

Tratamiento del riesgo
(traitement du risque, risk treatment)

Proceso de selección e implementación de medidas tendiente a modificar el riesgo, lo que implica una reducción del riesgo, una transferencia del riesgo o una toma de riesgo.

Usuario
(utilisateur, user)

Persona o cosa que utiliza los servicios de una organización.

Vulnerabilidad
(vulnérabilité, vulnerability)

Característica de una entidad que puede ser una debilidad o un fallo desde el punto de vista de la seguridad de los sistemas de información.

Ejemplos:

- *ausencia de planificación de seguridad en caso de incendios, para una entidad del tipo Organización;*
- *poca concientización respecto de los retos de seguridad, para una entidad del tipo Personal;*
- *facilidad para penetrar en el establecimiento, para una entidad del tipo Establecimiento;*
- *posibilidad de crear o modificar comandos de los sistemas, para una entidad del tipo Red;*

Acrónimos

BCS	Oficina de consultoría en seguridad de los sistemas de información (Bureau Conseil en Sécurité des systèmes d'information)
CC	(*Common Criteria*) – Criterios Comunes, el título utilizado históricamente para la norma en lugar del título oficial de la ISO: "Criterios de evaluación de la seguridad de las tecnologías de la información"
CFSSI	Centro de formación en seguridad de los sistemas de información (Centre de Formation en Sécurité des Systèmes d'Information)
DCSSI	Dirección Central de Seguridad de los Sistemas de Información (Direction Centrale de la Sécurité des Systèmes d'Information)
EBIOS	Expresión de las necesidades e identificación de los objetivos de seguridad (Expression des Besoins et Identification des Objectifs de Sécurité)
FEROS	Ficha de expresión racional de los objetivos de seguridad de los SI (Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI)
PP	(*Protection Profile*) – Perfil de protección
PSSI	Política de seguridad de los sistemas de información (Politique de Sécurité des Systèmes d'Information)
SDO	Subdirección de Operaciones (Sous-Direction des Opérations)
SDSSI	Esquema director de seguridad de los sistemas de información (Schéma Directeur de la Sécurité des Systèmes d'Information)
SGDN	Secretaría General de Defensa Nacional (Secrétariat Général de la Défense Nationale)
SI	Sistema de información
SSI	Seguridad de los sistemas de información
TIC	Tecnologías de la información y la comunicación

Referencias bibliográficas

[eEuropa 2005] *Plan d'action eEurope 2005 : une société de l'information pour tous, COM(2002)263 final* – Commission européenne (2002).
(*Plan de acción eEuropa 2005: una sociedad de información para todos - Comisión Europea*)

[FEROS] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)* – SGDN/SCSSI (1991).
(*Ficha de expresión racional de los objetivos de seguridad de los SI*)

Disponible en el sitio http://www.ssi.gouv.fr

[Guía 650] *La menace et les attaques informatiques* – N°650 / DISSI / SCSSI (1994).
(*La amenaza y los ataques informáticos*)

Disponible en el sitio http://www.ssi.gouv.fr

[IGI 1300] *Instruction générale interministérielle sur la protection du secret de la défense nationale* – N°1300 / SGDN / PSE / SSD (2003).
(*Instrucción general interministerial sobre la protección del secreto de defensa nacional*)

[IGI 900] *La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées* – SGDN y DISSI (1993).
(*La seguridad de los sistemas de información clasificados como de defensa por sí mismos o por los datos que procesan*)

[ISO 13335] *Information technology – Security techniques – Guidelines for the management of IT security (GMITS)* – International Organization for Standardization (ISO) (2001).
(*Tecnología de la información - Técnicas de seguridad - Guía para la gestión de la seguridad de la tecnología de la información - Organización Internacional de Normalización*)

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information - International Organization for Standardization (ISO) - version 2.0 (1998).*
(Los Criterios Comunes para la evaluación de la seguridad de las tecnologías de la información - Organización Internacional de Normalización)

[ISO 17799] *Information technology - Code of practice for information security management - International Organization for Standardization (ISO) (2000).*
(Tecnología de la información - Código de práctica para la gestión de la seguridad de la tecnología de la información - Organización Internacional de Normalización)

[ISO Guía 73] *Gestion du risque - Vocabulaire - Principes directeurs pour l'utilisation dans les normes - International Organization for Standardization (ISO) (2002).*
(Gestión del riesgo - Vocabulario - Principios rectores para la utilización dentro de las normas - Organización Internacional de Normalización)

[MASSIA] *Méthode d'Audit de la Sécurité des Systèmes d'Information de l'Armement - CELAR/CASSI/GESSI - version 1.0 (1994).*
(Método de auditoría de la seguridad de los sistemas de información de armamentos)

[OCDE] *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité - Organisation de coopération et*

de développement économiques (OCDE) (2002).
(Las directrices que rigen la seguridad de los sistemas y redes de información - hacia una cultura de la seguridad - Organización de Cooperación y Desarrollo Económicos)

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information - DCSSI (2004).*
(Guía para la elaboración de una política de seguridad de sistemas de información)

Disponible en el sitio http://www.ssi.gouv.fr

[REC 901] *Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense - SGDN et DISSI (1994).*
(Recomendación para la protección de los sistemas de información que procesan datos sensibles no clasificados de defensa)

TDBSSI *Guide d'élaboration de tableaux de bord de sécurité de système d'information pour les administrations - DCSSI (2004).*
(Guía para la elaboración de esquemas orientativos de seguridad de los sistemas de información para las instituciones públicas)

Disponible en el sitio http://www.ssi.gouv.fr

Formulario de recogida de comentarios

Este formulario puede enviarse a la siguiente dirección:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identificación del aporte
Nombre y organismo (facultativo): .....
Dirección de correo electrónico: .....
Fecha: .....

Observaciones generales sobre este documento
¿El documento responde a sus necesidades? Si □ No □

En caso afirmativo:

¿Piensa que puede mejorarse su contenido? Si □ No □

En caso afirmativo:

¿Qué otros temas hubiera deseado que tratáramos?
.....
.....

¿Qué partes del documento le parecen inútiles o inadecuadas?
.....
.....

¿Piensa que puede mejorarse su formato? Si □ No □

En caso afirmativo:

¿En qué aspecto podríamos mejorarlo?
- legibilidad, comprensión □
- presentación □
- otro □

Indique sus preferencias en cuanto al formato:
.....
.....

En caso negativo:

Indique el aspecto que no le resulta conveniente y defina lo que le hubiera resultado conveniente:
.....
.....

¿Qué otros temas desearía que se trataran?
.....
.....

Observaciones específicas sobre este documento

Puede formular comentarios detallados utilizando el siguiente cuadro.

"N°" indica un número de orden.

El "tipo" está compuesto por dos letras:

La primera letra indica la categoría de la observación:

- O Error de ortografía o de gramática
- E Falta de explicaciones o de aclaración en un punto existente
- I Texto incompleto o faltante
- R Error

La segunda letra indica su carácter:

- m menor
- M Mayor

La "referencia" indica la ubicación precisa en el texto (número de párrafo, línea...).

El "enunciado de la observación" permite formalizar el comentario.

La "solución propuesta" permite presentar la forma de resolver el reto enunciado.

N°	Tipo	Referencia	Enunciado de la observación	Solución propuesta
1				
2				
3				
4				
5				

Gracias por su colaboración