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

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECCIÓN 3
TÉCNICAS

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
(ver formulario de recogida de comentarios que se encuentra al final del compendio):

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

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 restricciones 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, , 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 restricciones, 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

Introducción

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 conforma la tercera sección del método. Detalla las actividades del método y propone soluciones para llevaras a la práctica.

Las técnicas presentadas en esta sección son sólo propuestas. Cada uno tendrá que elegir las más adecuadas a su contexto, es decir, a la cultura y a las costumbres de su organismo, así como a las herramientas de su preferencia. Podrán realizarse, por lo tanto, ajustes menores.

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

Etapa 1 – Estudio del contexto

Actividad 1.1 – Estudio del organismo

Presentar al organismo

La presentación del organismo permite recordar los elementos característicos que definen la identidad de un organismo. Se trata de la vocación, el oficio, las misiones, los valores propios y los ejes estratégicos de este organismo. Debe identificarse de este modo a quienes contribuyen a su elaboración (Ej.: subcontratación).

Lo difícil de esta actividad reside en la comprensión de la verdadera organización del organismo. La estructura real permite comprender el rol y la importancia atribuida a cada división en el alcance de los objetivos del organismo.
Por ejemplo, el hecho de que el responsable de la seguridad dependa de la Dirección General y no de la Dirección de Informática puede mostrarnos el compromiso asumido por la dirección respecto de la seguridad de los sistemas de información.

La vocación principal (lo que el organismo quiere hacer)

La vocación principal de un organismo puede definirse como lo que constituye su razón de ser (su ámbito de actividad, su segmento de mercado…). La vocación puede ser, por ejemplo, de servicio público o de industria.

El oficio (lo que el organismo sabe hacer)

El oficio del organismo, caracterizado por el conjunto de técnicas o *know-how* de los empleados, permite el cumplimiento de las misiones. Es característico del ámbito de actividad del organismo y define a menudo su cultura.

Las misiones (lo que el organismo debe hacer)

La vocación se realiza mediante el cumplimiento de las misiones. Hay que especificar los servicios prestados y/o los productos fabricados, indicando quiénes son sus destinatarios finales.

Los valores propios (lo que el organismo hace bien)

Se trata de los grandes principios o de una ética bien definida que están vinculados con la manera de ejercer un oficio. Esto puede involucrar al personal, las relaciones con los participantes externos (clientela...), la calidad de los productos entregados o de las prestaciones de servicios.
Un organismo puede, por ejemplo, tener vocación de servicio público, tener como oficio el transporte y cumplir misiones de transporte escolar. Sus valores podrían ser la puntualidad del servicio y la seguridad durante su ejecución.

Estructura del organismo

La estructura del organismo puede ser de diferentes tipos:
- Estructura divisional: cada división constituida está subordinada a la autoridad de un director de división responsable de las decisiones estratégicas, administrativas y operativas para su unidad.
- Estructura funcional: la autoridad funcional se ejerce sobre los procedimientos, la naturaleza del trabajo y a veces sobre las decisiones o la planificación (Ej.: la producción, la informática, los recursos humanos, el marketing...).

Observaciones:
- Una división dentro de un organismo de estructura divisional puede organizarse en estructura funcional y viceversa.
- Diremos que un organismo tiene una estructura matricial si toda la organización está basada en los dos tipos de estructura.

- Cualquiera sea la estructura del organismo, podemos distinguir los siguientes niveles:
  - el nivel de la toma de decisiones (definición de las orientaciones estratégicas);
  - el nivel de la conducción (coordinación y gestión);
  - el nivel operativo (producción y actividades auxiliares).

Organigrama

Consiste en obtener, utilizando un esquema, la representación de la estructura del organismo. Esta representación debe identificar los vínculos de subordinación y de delegación de autoridad, pero también debe tener en cuenta las otras relaciones de dependencia. Efectivamente, existen relaciones que, aún sin ser portadoras de ninguna autoridad formal, permiten la circulación de la información.
Por ejemplo, el interlocutor informático que es un usuario que depende del jefe de su departamento, puede también recibir recomendaciones de la Dirección de Informática.

Los ejes estratégicos (lo que el organismo quiere hacer mejor)

Se trata de formalizar las directrices del organismo que determinan su evolución a fin de comprender mejor los retos vinculados con la misma, así como las grandes evoluciones previstas.

Enumerar las restricciones que afectan al organismo

Se trata de tener en cuenta la totalidad de las restricciones que afectan al organismo y que podrían determinar ciertas orientaciones en materia de seguridad. Dichas restricciones pueden ser de origen interno, en cuyo caso el organismo podrá eventualmente manejarlas, o externo al organismo, y, por tanto, en general, inevitables. Las restricciones de recursos (presupuesto, personal) y de urgencia son las más importantes.

El organismo se fija objetivos por alcanzar (relativos al oficio, a su comportamiento...) que comprometerán su futuro a mayor o menor plazo. Define así en qué quiere transformarse, y los medios que le convendrá implementar. Para precisar estos grandes ejes, el organismo tiene en cuenta la evolución de las técnicas y del *know-how*, de los deseos expresados por los usuarios, los clientes... Esta finalidad puede expresarse en forma de políticas de funcionamiento o de desarrollo. Se trata por ejemplo de la reducción de los costos de funcionamiento, de la mejora de la calidad de servicio…

Estas políticas tienen probablemente un aspecto dedicado al sistema de información (SI), que debe, en lo que le compete, contribuir a la aplicación de dichas políticas. En consecuencia, la consideración de las características vinculadas con la identidad o la misión y la estrategia del organismo es fundamental para el análisis del reto porque el perjuicio ocasionado a un elemento del SI (en términos de seguridad) podría generar un cuestionamiento de estos objetivos estratégicos. Además, es fundamental que las propuestas de medidas de seguridad guarden coherencia respecto de las normas, costumbres y medios vigentes en el organismo.

Los siguientes párrafos presentan una lista no exhaustiva de los tipos de restricciones.

Las restricciones de orden político

Éstas pueden involucrar a las instituciones del Estado, los establecimientos públicos o, por lo general, a todo organismo que deba aplicar las decisiones gubernamentales. En líneas generales, se trata de decisiones de orientación estratégica u operativa, que emanan de una Dirección o de un órgano responsable de la toma de decisiones y que deben ser aplicadas.
El principio de desmaterialización de las facturas o documentos administrativos, por ejemplo, genera problemas de seguridad.

Las restricciones de orden estratégico

Algunas restricciones pueden resultar de evoluciones previstas o posibles de las estructuras u orientaciones del organismo. Éstas se expresan en los esquemas directores estratégicos u operativos de la organización.
Por ejemplo, las instancias de cooperación internacional sobre la puesta en común de informaciones sensibles pueden requerir acuerdos a nivel de intercambios seguros.

Las restricciones territoriales

La estructura y/o la vocación del organismo puede generar restricciones particulares tales como la dispersión de los establecimientos por todo el territorio nacional o en el extranjero.
Por ejemplo, las agencias de correos, las embajadas, los bancos, las diferentes filiales de un gran grupo industrial...

Las restricciones coyunturales

El funcionamiento del organismo puede verse profundamente modificado por situaciones particulares tales como huelgas, crisis nacionales o internacionales.
La continuidad de ciertos servicios, por ejemplo, debe poder garantizarse incluso durante una crisis grave.

Las restricciones estructurales

La estructura del organismo puede generar, debido a su naturaleza (divisional, funcional u otra), una política de seguridad que le es propia y una organización de la seguridad adaptada a estas estructuras.
Por ejemplo, una estructura internacional debe poder conciliar los requerimientos de seguridad propios de cada país.

Las restricciones funcionales

Se trata de las restricciones que derivan directamente de las misiones generales o específicas del organismo.
Por ejemplo, un organismo puede tener una misión de guardia que requerirá la máxima disponibilidad de sus medios.

Las restricciones referidas al personal

Las restricciones referidas al personal son de naturaleza muy variada y están relacionadas con las siguientes características: nivel de responsabilidad, contratación, cualificación, formación, concienciación respecto de la seguridad, motivación, disponibilidad…
Por ejemplo, puede ser necesario que la totalidad del personal de un organismo de defensa esté habilitado para niveles de confidencialidad superiores.

Las restricciones de orden temporal

Éstas pueden resultar de la reorganización de los departamentos o de la implementación de nuevas políticas nacionales o internacionales que imponen plazos de vencimiento fijo.
Por ejemplo, la creación de una Dirección de Seguridad.

Las restricciones referidas a los métodos

Teniendo en cuenta el *know-how* interno del organismo, resultará imprescindible la adopción de ciertos métodos (a nivel de la planificación del proyecto, de las especificaciones, del desarrollo...).
La restricción puede ser, por ejemplo, tener que combinar la política en materia de seguridad con las acciones referidas a la calidad, vigentes en el organismo.

Las restricciones de orden cultural

En ciertos organismos los hábitos de trabajo o el oficio principal dan nacimiento a una "cultura" propia de este organismo, que puede llegar a ser incompatible con las medidas de seguridad. Esta cultura constituye el marco de referencia general de las personas del organismo y puede involucrar numerosos parámetros tales como el carácter, la educación, la instrucción, la experiencia profesional o extraprofesional, las opiniones, la filosofía, las creencias, los sentimientos, la situación social …

Las restricciones de orden presupuestario

Las medidas de seguridad recomendadas tienen un costo que puede, en algunos casos, ser muy importante. Si bien las inversiones en materia de seguridad no pueden basarse en criterios de rentabilidad, generalmente se exige a los departamentos financieros de la organización que presenten una justificación económica.
Por ejemplo, en el sector privado y para algunos organismos públicos, el coste total de las medidas de seguridad no debe sobrepasar las consecuencias de los riesgos previstos. La dirección debe, por lo tanto, apreciar y tomar riesgos calculados si quiere evitar un coste prohibitivo para la seguridad.

Enumerar las referencias reglamentarias aplicables al organismo

El respeto de las leyes, normas o reglamentos puede modificar el entorno, los hábitos de trabajo, el cumplimiento de las misiones, o influir en la organización interna.
Por ejemplo, el funcionamiento de las instituciones del Estado está regido por códigos específicos (código aduanero, código para contratos públicos...).

En consecuencia, es conveniente identificar las referencias reglamentarias aplicables al organismo, ya sea que se trate de leyes, decretos, códigos específicos de la rama de actividad del organismo o de reglamentos internos o externos. Esto afecta tanto a los contratos como a los convenios y, en líneas generales, a las obligaciones de carácter jurídico.

Realizar una descripción funcional del SI global

Se trata de identificar los ámbitos funcionales que contribuyen al alcance de los objetivos estratégicos y sus interacciones. En este nivel intentamos representar las interacciones existentes y/o futuras de los ámbitos funcionales con el ámbito al cual el sistema evaluado pertenece.
Este procedimiento implica la redacción previa clara y funcional de la necesidad.
Dado que esta actividad tiene por objetivo formalizar el diseño conceptual del SI, a fin de que se pueda luego delimitar y caracterizar el sistema evaluado, es a veces posible obtener los estudios que han permitido establecer el SI (modelos de diseño de comunicación y procesos según [MERISE] por ejemplo).

Una subdivisión en ámbitos funcionales permite tener un panorama general de conjunto sobre el funcionamiento del SI y sus eventuales relaciones con actores externos. Esta división permitirá situar mejor al sistema evaluado en el SI y comprender mejor los retos con él vinculados.

Por lo general, cualquier sistema de información puede dividirse en:
- funciones operativas o de apoyo operativo;
- funciones auxiliares;
- funciones de control y seguimiento de las actividades.

Las funciones operativas dependen de las misiones del organismo.
Las funciones auxiliares dependen de la gestión de los medios necesarios para la realización de las funciones operativas.
En cuanto a las funciones de control y seguimiento de las actividades, éstas le competen a la gestión.

La evolución de una función del tipo operativo puede tener incidencias fuertes sobre otras funciones; por el contrario, la modificación de una función auxiliar o de control no tiene generalmente impacto directo sobre las funciones operativas.

Actividad 1.2 – Estudio del sistema evaluado

El sistema de información (SI) contribuye, en parte, a la realización de los objetivos estratégicos del organismo. Es necesaria una comprensión suficientemente clara del SI y de su funcionamiento para extraer todos los elementos útiles para la elaboración de las necesidades de seguridad del sistema evaluado. Para ello es conveniente reubicar al sistema evaluado en el SI del organismo.

Presentar el sistema evaluado

El sistema evaluado debe ser descrito de manera sintética, identificando claramente su perímetro, sus relaciones con los otros ámbitos o actores externos y sus finalidades dentro del sistema de información global.

Enumerar los retos

A esta altura de la reflexión, se supone que los objetivos estratégicos ya se conocen (cf. esquema director informático, estudio de posibilidades...), que las necesidades funcionales han sido identificadas y definidas, que las restricciones del sistema evaluado a nivel de la información y a nivel organizacional han sido catalogadas. Resulta entonces conveniente analizar los retos y el contexto en el cual se sitúa el sistema evaluado.

Este análisis permite identificar el peso estratégico del sistema evaluado para el organismo y evaluar el nivel de importancia de las funciones en el sistema evaluado. Consiste en identificar el impacto de la realización o utilización del sistema, las expectativas de los usuarios o de sus superiores, el aporte esperado... Los retos pueden ser, por ejemplo, de orden técnico, financiero o político.

Enumerar los elementos esenciales

Para describir con mayor precisión el sistema evaluado, la siguiente operación consiste en identificar sus elementos esenciales. Un grupo de trabajo heterogéneo y representativo del SI (responsables, especialistas en informática y usuarios) realiza esta selección.
Los elementos esenciales son generalmente las funciones e informaciones centrales de la actividad del sistema evaluado. También es posible considerar otros elementos esenciales tales como los procesos del organismo. Este segundo enfoque será más adecuado para la elaboración de una política de seguridad de los sistemas de información, de un esquema director de seguridad de los sistemas de información o de un plan de contingencia. Los elementos esenciales constituyen el patrimonio de información o los "bienes inmateriales" que se desea proteger. Dependiendo de la finalidad que persigan, ciertos estudios no merecerán un análisis exhaustivo de la totalidad de los elementos que conforman el sistema evaluado. En este contexto, el alcance del estudio podrá limitarse a los elementos vitales del sistema evaluado.
La selección de los elementos esenciales se realiza conjuntamente con un responsable usuario del sistema (existente o futuro). Dicho usuario indica, en un primer análisis, aquellos elementos que presentan un carácter sensible. Los elementos esenciales son generalmente funciones o informaciones cuya falta de cumplimiento en términos de disponibilidad, integridad, confidencialidad, incluso de otros criterios de seguridad, pondría en tela de juicio la responsabilidad del propietario o del depositario, o causaría un perjuicio a éstos o a terceros.

Las funciones (o subfunciones) esenciales son principalmente:

- las funciones cuya pérdida o deterioro haría imposible el cumplimiento de la misión del sistema;
- las funciones que implican procesos secretos o procesos tecnológicos de alto nivel;
- funciones cuya alteración puede afectar considerablemente el cumplimiento de la misión del sistema.

El carácter sensible de los datos que hay que seleccionar puede provenir de los siguientes casos:

- datos afectados por el secreto de defensa definidos en la [IGI 900] y cuyo nivel de requerimientos de seguridad no es negociable;
- datos sensibles no clasificados de defensa tal como han sido definidos en la [Rec 901] y cuyo nivel de requerimientos es negociable en función de las consideraciones del entorno propias del organismo.

Por lo general, los datos esenciales abarcan principalmente:

- la información clasificada, afectada o no por el secreto de defensa;
- la información vital para el ejercicio de la misión o del oficio del organismo;
- la información personal, especialmente los datos personales en el sentido que les da la ley francesa "Informática y libertades";
- la información estratégica necesaria para el logro de los objetivos correspondientes a las orientaciones estratégicas;
- los datos costosos, cuya recogida, almacenamiento, procesamiento o transmisión requiere una gran inversión de tiempo y/o un elevado costo de adquisición.

Las funciones y datos que no hayan sido seleccionados al finalizar esta actividad, no presentarán en la continuación del estudio ninguna necesidad de seguridad. Esto significa que si se vieran eventualmente comprometidos, esto no afectaría el buen desarrollo de la misión que cumple el sistema.
Sin embargo, a menudo estas funciones y datos heredarán las medidas adoptadas para proteger las funciones y datos seleccionados.

Las fichas de expresión de las necesidades de seguridad van a permitir a los usuarios expresar su opinión sobre cuán delicadas son las funciones y los datos esenciales.

Realizar una descripción funcional del sistema global

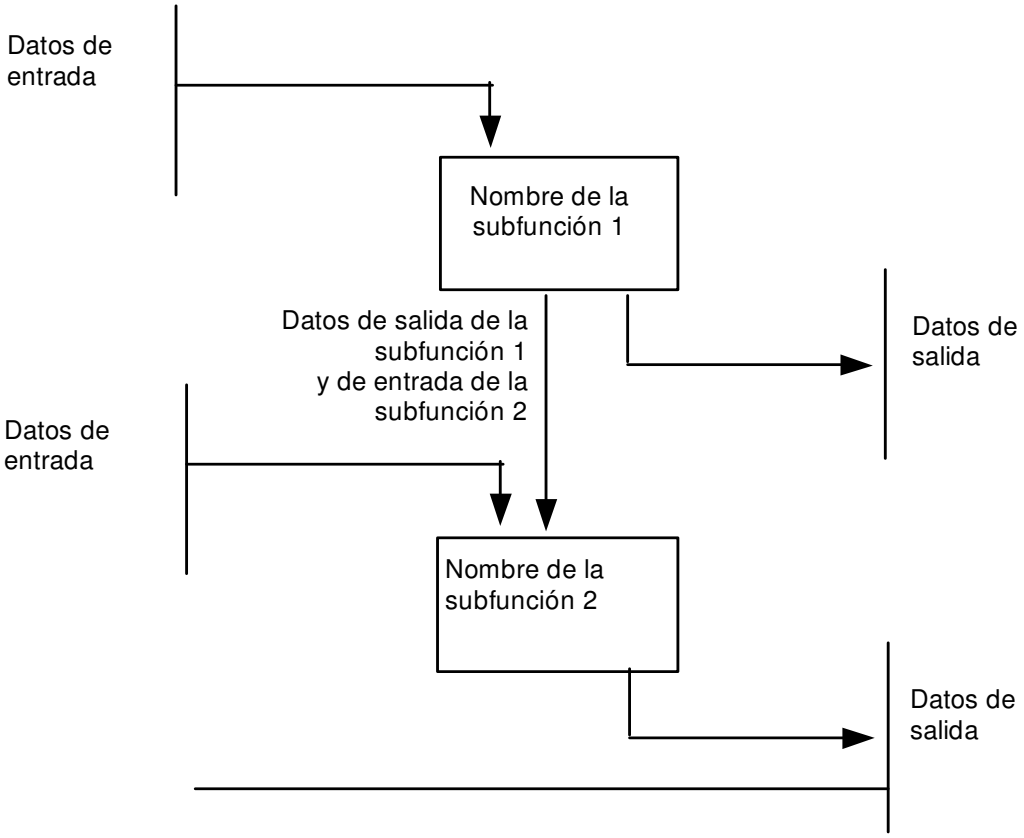
A este nivel, las finalidades del sistema evaluado han sido claramente expresadas y se ha determinado su lugar respecto de lo existente; resulta entonces conveniente especificar para cada función esencial identificada:

- los datos de entrada y de salida (resultados esperados);
- los procesamientos que deben efectuarse (indicando también las interfaces que permiten al sistema evaluado intercambiar información con los otros SI).

Podrá descomponerse una función en subfunciones, dado que la subfunción es un conjunto coherente de procesos (agregado de tareas elementales) y datos.

Para un sistema por diseñar, se utiliza, para realizar la modelización del sistema proyectado, el método general de diseño elegido (Ejemplos: MERISE, SADT, UML…).

Para un sistema existente o en caso de falta de modelización durante su diseño, se propone utilizar la siguiente representación: Las funciones se representan mediante un diagrama, según un enfoque descendente, ilustrando la relación entre las subfunciones y los datos de entrada y de salida de las funciones (ver el ejemplo en la siguiente página).



Ejemplo : Representación de una función de gestión de recursos humanos

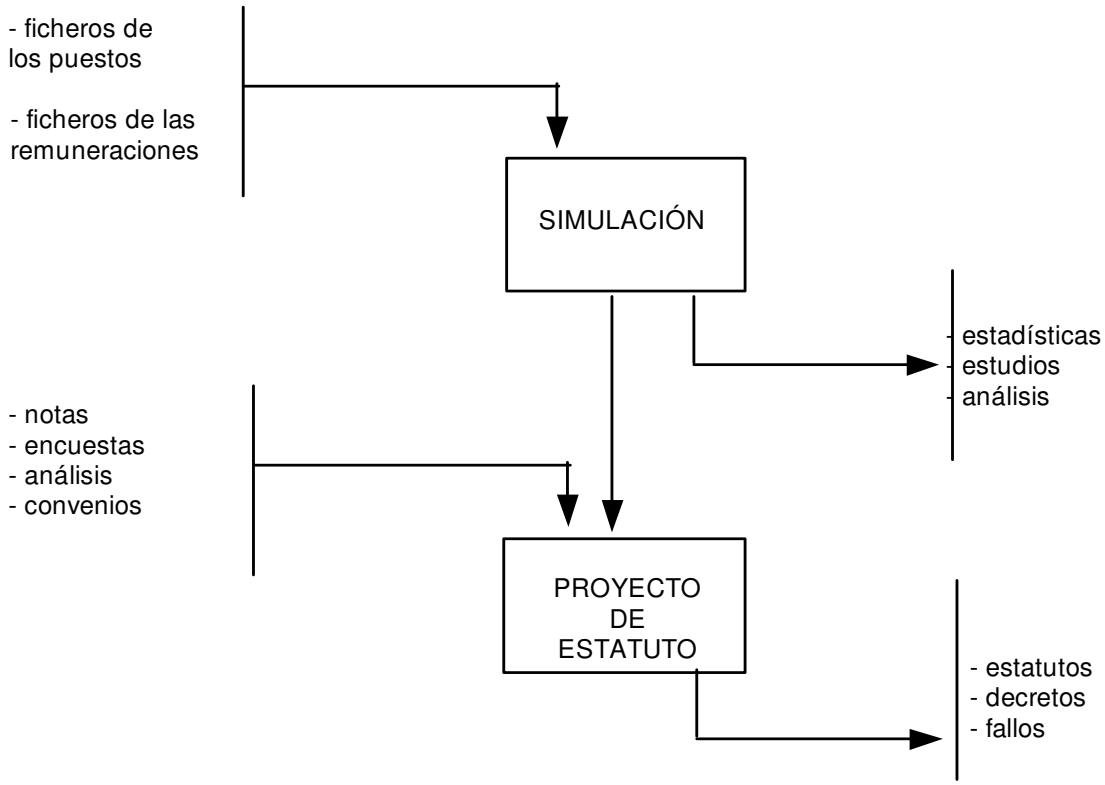


Figura 1 – Representación de las funciones e informaciones

Subdivisión del sistema en subsistemas

Para facilitar la continuación del estudio puede considerarse la subdivisión del sistema en subsistemas .

El objetivo principal de la descomposición en subsistemas es simplificar la aplicación del método EBIOS. Así, el responsable del estudio puede decidir descomponer el sistema en varios subsistemas. Determinará de este modo si trabajará con varios sistemas evaluados, más simples de estudiar por separado, o bien con un solo sistema evaluado, en el cual se centrará específicamente el estudio.

La descomposición en subsistemas queda a criterio del responsable del estudio. El estudio de varios subsistemas es generalmente más simple que el estudio global de un sistema de formas múltiples, pero la cantidad de subsistemas debe ser escasa (menos de cinco) porque cada uno será objeto de un estudio por separado.

La descomposición en subsistemas facilita:
- la selección de ejes de trabajo: puede permitir identificar subsistemas para los cuales un estudio es inútil o menos prioritario;
- la organización del estudio: el estudio de un subsistema puede confiarse a un equipo pequeño.

No existe un método propiamente dicho que permita descomponer un sistema en subsistemas, sino más bien un conjunto de criterios que hay que analizar. Los principales criterios de descomposición aplicables son los siguientes:

- Criterio Nº 1: Considerando la arquitectura material
  Establecer tantos subsistemas cómo máquinas (o conjuntos de máquinas) autónomas haya. Si, en general, las diferentes máquinas están vinculadas unas a otras, la descomposición depende del nivel de interoperabilidad de las diferentes partes (máquinas o conjuntos de máquinas) del sistema.
  Ejemplo: nivel creciente de interoperabilidad
  - Máquinas físicamente separadas. Transferencia de datos por bandas magnéticas o disquetes.
  - Máquinas comunicadas por un vínculo dedicado a la transferencia de ficheros.
  - Conjunto de máquinas autónomas que colaboran entre sí utilizando una red local.
  - Conjunto de máquinas comunicadas por una red local, provistas del mismo sistema operativo y administradas de manera centralizada.

- Criterio Nº 2: Descomposición por funciones o datos esenciales
  Puede ser posible descomponer un mismo subsistema físico considerando las funciones realizadas por tal o cual máquina o parte del sistema o en función de la manera en que es procesada la información más sensible.

- Criterio Nº 3: Autonomía de responsabilidad
  Un conjunto de entidades que forman un todo desde el punto de vista de la responsabilidad de implementación (conjunto de usuarios o implementación técnica), podrá ser considerado como un subsistema que hay que estudiar por separado. Podrá tratarse de una parte del sistema que se encuentra bajo la responsabilidad de un departamento debidamente identificado en un organigrama del organismo. Este criterio puede aplicarse también cuando hay varias documentaciones separadas.

- Criterio Nº 4: Instalación en diferentes subzonas
  Si los componentes (hardware, soportes, personal) se encuentran en diferentes subzonas (edificios, subzonas reservadas, subsuelos...), cada subzona es susceptible de conformar un subsistema (siempre que el nivel de interoperabilidad con el exterior sea suficientemente bajo).

- Criterio Nº 5: Aislamiento de "subsistemas comunes"
  Una vez aplicados los cuatro primeros criterios, podemos llegar a observar que ciertos conjuntos de entidades o componentes se encuentran en la intersección de varios subsistemas (servidores comunes, redes comunes, personal o subzonas

comunes, por ejemplo), siendo susceptibles de formar subsistemas que será posible estudiar por separado. Los resultados de estos estudios serán luego tenidos en cuenta dentro de los subsistemas que los engloban. Se trata de alguna manera de una división del trabajo.

Enumerar las hipótesis

Consiste en formalizar las hipótesis referidas al sistema evaluado. La mayoría de las veces las hipótesis son impuestas por el organismo responsable del estudio, por razones de política interna o externa al organismo, financieras o temporales.
Las hipótesis pueden también constituir un riesgo aceptado a priori en un entorno dado.
En el caso de la redacción de un perfil de protección o de un objetivo de seguridad -que deben demostrar la perfecta y total cobertura de las amenazas mediante los objetivos de seguridad- puede tratarse de vulnerabilidades que no pueden ser cubiertas por un objetivo de seguridad en las etapas siguientes. En este mismo caso, puede tratarse de la aceptación formalizada de restricciones identificadas, mientras que las otras serán sólo ayudas para la comprensión del contexto.

Se propone adoptar la siguiente nomenclatura para las hipótesis: H.xx (siendo H hipótesis y xx el nombre de la hipótesis).

<u>El caso particular de la elección del modo de explotación de seguridad</u>

La determinación del modo de explotación de seguridad del sistema consiste en indicar cómo el sistema permite a los usuarios de diferentes categorías procesar, transmitir o conservar datos en mayor o menor medida sensibles. Permite tomar conciencia de los retos de la seguridad general porque el modo de explotación de seguridad define el contexto de gestión de la información de un sistema de información.

En líneas generales, el modo de explotación de seguridad del sistema pertenece a una de las siguientes categorías:

- Categoría 1: Modo de explotación exclusivo
  - Todas las personas que tienen acceso al sistema están habilitadas para el más alto nivel de clasificación y tienen una necesidad de conocerlo idéntica (o equivalente) para todas las informaciones procesadas, almacenadas o transmitidas por el sistema.
- Categoría 2: Modo de explotación dominante
  - Todas las personas que tienen acceso al sistema están habilitadas para el más alto nivel de clasificación, pero no todas tienen una necesidad de conocerlo idéntica (o equivalente) para todas las informaciones procesadas, almacenadas o transmitidas por el sistema.
- Categoría 3: Modo de explotación multinivel
  - Las personas que tienen acceso al sistema no están todas habilitadas para el más alto nivel de clasificación y no tienen todas una necesidad de conocerlo idéntica (o equivalente) para todas las informaciones procesadas, almacenadas o transmitidas por el sistema.

Para seleccionar el modo de explotación de seguridad del sistema, es importante saber si existe o debe existir:

- una clasificación jerárquica de los datos (Ej.: confidencial, secreto…) y/o por sector (médico, empresa, nuclear…),
- categorías de usuarios,
- una noción de la necesidad de conocerlo, modificarlo o disponer de él…

La elección del modo de explotación de la seguridad puede reconsiderarse teniendo en cuenta los riesgos identificados en el transcurso de las etapas siguientes. Sin embargo, es importante plantearse este aspecto lo antes posible porque su implementación tiene importantes consecuencias en el diseño del SI y de la SSI.

Enumerar las normas de seguridad

La seguridad de los sistemas de información puede haber sido objeto de un referencial de estudios y documentos; aunque un análisis detallado no sea útil en esta etapa, pueden buscarse algunos datos: prioridades, resultados, normas...
El objetivo es identificar las principales instrucciones y medidas de seguridad, formalizadas o no. La recogida de esta información podrá realizarse a partir de los siguientes documentos:

- política de seguridad del sistema de información;
- planes de contingencia para las aplicaciones;
- instrucciones de seguridad de los desarrollos;
- resultados de auditorías de seguridad;
- proyectos de seguridad...

Se propone adoptar la siguiente nomenclatura para las normas de seguridad: P.xx (siendo P política y xx el nombre de la norma de seguridad).

Enumerar las restricciones que afectan al sistema evaluado

La identificación de las restricciones permite identificar aquellas que tienen un impacto sobre el sistema evaluado y determinar aquellas sobre las cuales es, no obstante, posible actuar. Completan y corrigen las restricciones del organismo precedentemente determinadas. Los siguientes párrafos presentan una lista no exhaustiva de los tipos de restricciones que pueden preverse.

Restricciones de anterioridad

No se pueden desarrollar simultáneamente todos los proyectos de aplicaciones. Algunos dependen de realizaciones previas. Un sistema puede ser objeto de una descomposición en subsistemas; un sistema no está forzosamente condicionado por la totalidad de los subsistemas (por extensión a las funciones de un sistema) de otro sistema.

Restricciones técnicas

En general las restricciones técnicas, de orden físico, pueden provenir del hardware y el software instalados, de los locales o establecimientos que albergan al SI:

- los ficheros (requerimientos en materia de organización, de gestión de soportes, de gestión de las normas de acceso…);
- la arquitectura general (requerimientos de materia en topología, ya sea centralizada, repartida, distribuida, o de tipo cliente-servidor, de arquitectura física…);
- las aplicaciones (requerimientos en materia de diseño de programas específicos, de estándares del mercado…);
- los paquetes (requerimientos de estándares, de nivel de evaluación, calidad, conformidad con las normas, seguridad…);
- el hardware (requerimientos de estándares, de nivel de evaluación, calidad, conformidad con las normas…);
- las redes de comunicación (requerimientos en materia de cobertura, de estándares, de capacidad, de fiabilidad…);
- las infraestructuras de los inmuebles (requerimientos en materia de ingeniería civil, construcción de edificios, altas potencias, bajas potencias…).

Restricciones financieras

La implementación de medidas de seguridad se ve limitada a menudo por el presupuesto que el organismo puede acordarle; sin embargo, la restricción financiera debe considerarse en último lugar (pudiendo negociarse la parte del presupuesto asignada a la seguridad en función del estudio de seguridad).

Restricciones del entorno

Las restricciones del entorno provienen del entorno geográfico o económico en el cual está instalado el SI: país, clima, riesgos naturales, situación geográfica, coyuntura económica…

Restricciones temporales

El tiempo necesario para la implementación de las medidas de seguridad debe vincularse con la escalabilidad del SI; efectivamente, si el tiempo de implementación es muy largo, la respuesta de seguridad podría no relacionarse ya con los riesgos, que habrán evolucionado. El tiempo es determinante en la elección de las soluciones y prioridades.

Restricciones referidas a los métodos

Teniendo en cuenta el *know-how* y los hábitos del organismo, resultará imprescindible la adopción de ciertos métodos (a nivel de la planificación del proyecto, de las especificaciones y del desarrollo...).
Sobre la base de los elementos identificados, se deducirán y catalogarán un conjunto de hipótesis organizacionales.

Restricciones organizacionales

Algunas claves para la reflexión:

- la utilización (requerimientos en materia de plazos, provisión de resultados, de servicios, requerimientos de control, de seguimiento, de planes de emergencia, funcionamiento en modo funcionalidad reducida...);
- el mantenimiento (requerimientos de acciones de diagnóstico de incidentes, de prevención, de corrección rápida...);
- la gestión de los recursos humanos (requerimientos en materia de formación del personal operativo y de los usuarios, de cualificación para ocupar puestos tales como el de administrador de sistema o administrador de base de datos...);
- la gestión administrativa (requerimientos en materia de responsabilidades de los actores…);
- la gestión de los desarrollos (requerimientos en materia de herramientas de desarrollo, entorno de software, planes de gastos, organización que hay que implementar…);
- la gestión de las relaciones externas (requerimientos en materia de organización de relaciones con terceros, en materia de contratos…).

Enumerar las referencias reglamentarias específicas del sistema evaluado

El respeto de las leyes, normas o reglamentos puede limitar la elección de soluciones materiales o de procedimientos y modificar el entorno o los hábitos de trabajo.

Resulta por tanto conveniente identificar la totalidad de las referencias reglamentarias aplicables al sistema evaluado.

Actividad 1.3 – Determinación del objetivo del estudio de seguridad

Enumerar y describir las entidades del sistema

El sistema evaluado está conformado por un conjunto de entidades técnicas y no técnicas que es conveniente identificar y describir. Estas entidades tienen vulnerabilidades que algunos métodos de ataque podrán aprovechar, atentando así contra los elementos esenciales, inmateriales, del sistema evaluado (funciones y datos). Será pues necesario proteger a esas entidades. Las mismas pueden ser de diferentes tipos.

En los siguientes párrafos presentamos los tipos de entidades (se aconseja utilizar los tipos y subtipos de entidades de la guía "Herramientas para la apreciación de los riesgos de SSI" para enumerar y describir las entidades del sistema).

El hardware

El tipo "hardware" está conformado por el conjunto de elementos físicos de un sistema informático, pudiendo tratarse de soportes informáticos de procesamiento de datos activos o pasivos.

El software

El tipo "software" está conformado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesamientos de la información.

Las redes

El tipo "redes" está conformado por el conjunto de dispositivos de telecomunicación que permite la interconexión de varios ordenadores o componentes de un sistema de información físicamente alejados.

El personal

El tipo "personal" está conformado por el conjunto de grupos de individuos vinculados con el sistema de información.

Los establecimientos

El tipo "establecimiento" está conformado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.

Las organizaciones

El tipo "organización" describe el marco organizacional, constituido por el conjunto de estructuras de personal afectadas a una tarea y de procedimientos que regulan estas estructuras.

Los sistemas (opcional)

El tipo "sistema" está conformado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos. Este tipo es útil en caso de un análisis macroscópico.

A fin de aportar una mejor comprensión de este tipo de entidad, tomemos como ejemplo la conexión en red de terminales móviles que permiten la consulta de bases de datos de vehículos en el marco de operaciones de control.

Tipos de hardware:

- *terminal móvil en un vehículo terrestre, de tipo microordenador portátil compatible con ordenador, que utiliza una minibase de datos;*
- *sistema de servidor central con terminales de comunicaciones de arquitectura modular, que utiliza una base de datos nacional.*

Tipos de software:

- *sistema operativo del servidor central: grandes capacidades de procesamiento transaccional;*
- *sistema de gestión de base de datos relacional que funciona en modo cooperativo de dos niveles, instalada en el servidor nacional.*

Tipos de redes:

- *red nacional de conmutación de paquetes X25 (restricción existente);*
- *red de radio de cobertura nacional entre terminales móviles y la red nacional X25.*

Tipos de personal:

- *personal de desarrollo y mantenimiento de las aplicaciones: personal interno y asistencia externa;*
- *personal operativo del centro informático habilitado y especialistas que trabajan en la plataforma técnica;*
- *usuarios de las terminales móviles: personal habilitado.*

Tipos de establecimientos:

- *centro de informática protegido por cerco y sistema de videovigilancia en zona geográfica no clasificada como lugar de riesgos importantes;*
- *vehículos ligeros repartidos en todo el territorio nacional.*

Tipos de organizaciones:

- *desarrollo y mantenimiento explotado por la administración;*
- *procedimientos de actualización de las bases locales y central realizados por brigadas especializadas en puestos fijos conectados directamente con la red nacional.*

Los tipos de entidades pueden descomponerse en subtipos de entidades cuya descripción será más precisa.

Cruzar los elementos esenciales y las entidades

Esta tarea permite identificar:

- los vínculos entre las funciones esenciales y las entidades que contribuyen a la realización de estas función para el sistema evaluado,
- los vínculos entre los datos esenciales y las entidades que participan en el procesamiento de esta información para el sistema evaluado.

Estos vínculos serán utilizados en la confrontación de las amenazas con las necesidades. Se representan mediante una matriz en la cual figuran los elementos esenciales y las entidades seleccionadas. El vínculo elemento esencial/entidad se representa en el cuadro mediante una o varias cruces en la intersección del elemento esencial y de las entidades involucradas con este elemento esencial.

Ejemplo de matriz de elementos esenciales/entidades:

Entidades / ***Elementos esenciales***	***HARDWARE***				***SOFTWARE***				***REDES***				***PERSONAL***					***ESTA-BLECIM.***			***ORGAN.***		
	H1	***H2***	***H3***	***H4***	***S1***	***S2***	***S3***	***S4***	***R1***	***R2***	***R3***	***R4***	***P1***	***P2***	***P3***	***P4***	***P5***	***E1***	***E2***	***E4***	***O1***	***O2***	***O3***
Función 1	+					+	+	+					+	+	+	+			+			+	+
…	+					+	+	+					+	+	+	+	+	+	+		+		+
Función N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Dato 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
…	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
…	+					+	+	+					+	+	+	+			+	+	+	+	+
Dato N	+					+	+	+					+	+	+	+	+	+	+	+			+

Etapa 2 – Expresión de las necesidades de seguridad

Actividad 2.1 – Realización de las fichas de necesidades

Elegir los criterios de seguridad que hay que tener en cuenta

Las necesidades de seguridad vinculadas con las funciones e informaciones se expresan según criterios de seguridad[2]. Hay tres criterios de seguridad ineludibles:

- Disponibilidad (D): cualidad de los elementos esenciales de ser accesibles por parte de los usuarios autorizados cuando éstos lo requieren.
  - Para una función: garantía de continuidad de los servicios de procesamiento de información; ausencia de problemas vinculados con los tiempos de respuesta en el sentido amplio del término.
  - Para una información: garantía de disponibilidad prevista para el acceso a los datos (plazos y horarios). No hay pérdida total de la información. Mientras exista una versión archivada de la información, se considera que la información está disponible. Para estudiar la disponibilidad de una información, se supone la existencia de una versión archivada y se evalúa la disponibilidad que corresponde a la función de archivado de dicha información.
- Integridad (I): cualidad de exactitud y exhaustividad de los elementos esenciales.
  - Para una función: aseguramiento de conformidad del algoritmo o de la implementación de los procesamientos automatizados o no respecto de las especificaciones; ausencia de resultados incorrectos o incompletos de la función.
  - Para un dato: garantía de exactitud y exhaustividad de los datos frente a errores de manipulación o usos no autorizados; no alteración de la información.
- Confidencialidad (C): cualidad de los elementos esenciales de ser accesibles sólo para los usuarios autorizados.
  - Para una función: protección de los algoritmos que describen las reglas de gestión y los resultados cuya divulgación a un tercero no autorizado sería perjudicial; ausencia de divulgación de un proceso o mecanismo de carácter confidencial.
  - Para un dato: protección de los datos cuyo acceso o uso por parte de terceros no autorizados sería perjudicial; ausencia de divulgación de datos de carácter confidencial.

Las necesidades pueden expresarse también en términos de prueba (imputabilidad), control (auditabilidad), anonimato o cualquier otro criterio de seguridad cuya violación en una función o dato podría poner en peligro los objetivos del sistema.

- Prueba, control: garantía de no poder refutar la emisión o recepción de una información, con posibilidad de poder auditar los resultados obtenidos (ejemplo: un giro de fondos y la verificación del libro contable a partir de los datos de entrada).
- Anonimato: disposición por la cual cualquier persona que cree una información (un voto por ejemplo) y/o efectúe una acción (una llamada telefónico por ejemplo) procesada informáticamente, no puede ser identificada.
- Fiabilidad: cualidad de coherencia entre un comportamiento esperado y un resultado.
- …

Determinar la escala de necesidades

Deberán expresarse las necesidades de seguridad para cada criterio de seguridad seleccionado. Es necesario elaborar una graduación de las necesidades de seguridad en forma de niveles de necesidades. Para ello debe redactarse una definición para cada nivel de necesidades de cada criterio de seguridad.
La escala presenta generalmente niveles que van de 0 (ningún perjuicio) a 4 (perjuicio muy importante). Sin embargo, es posible pensar en definir una escala que abarque una cantidad de niveles diferente.
Es preferible que la cantidad de niveles sea la misma para cada criterio de seguridad.

[2] Parcialmente, según el libro blanco sobre la seguridad de los sistemas de información en los establecimientos de crédito.

Dentro de lo posible, los valores de referencia deben ser explícitos y abarcar un conjunto de valores limitados.

Este trabajo se realiza generalmente en un cuadro de doble entrada, con los criterios de seguridad en columnas y los niveles en filas, debiendo indicarse las definiciones en cada intersección.

El siguiente cuadro presenta un ejemplo de escala para los criterios de seguridad disponibilidad, integridad y confidencialidad, y una escala de 5 niveles.

Necesidades de seguridad	***Disponibilidad***	***Integridad***	***Confidencialidad***
0	*Ninguna necesidad de disponibilidad*	*Ninguna necesidad de integridad*	*Público*
1	*A largo plazo (especificar)*	*[valor no utilizado]*	*Restringido*
2	*A mediano plazo (especificar)*	*Necesidad moderada de integridad*	*Confidencial (asociados)*
3	*A corto plazo (especificar)*	*[valor no utilizado]*	*Confidencial (interno)*
4	*A muy corto plazo (especificar)*	*Perfectamente integrado*	*Secreto*

Esta escala debe adaptarse al contexto del estudio con la participación de las personas que van a determinar las necesidades De este modo, cada valor tendrá un significado real para estas personas y los valores serán coherentes.

Determinar los impactos pertinentes

Las consecuencias de la realización de un siniestro pueden apreciarse según diferentes puntos de vista. El responsable usuario debe identificar los impactos significativos para el organismo. Éstos permitirán considerar diferentes ámbitos que pueden verse afectados y aportar elementos para la justificación de las necesidades de seguridad.

Estos impactos pueden seleccionarse entre los propuestos aquí abajo, aunque la lista no es exhaustiva y puede ser necesario adaptarla al contexto estudiado:

- Interrupción de servicio:
  - incapacidad para ofrecer el servicio.
- Pérdida de imagen de marca:
  - pérdida de credibilidad interna de la informática,
  - pérdida de notoriedad.
- Alteración del funcionamiento interno:
  - inconveniente para el organismo en sí mismo,
  - costos internos adicionales.
- Alteración del funcionamiento para terceros:
  - inconveniente para terceros con los cuales el organismo se relaciona,
  - perjuicios varios.
- Violación de leyes, reglamentos:
  - imposibilidad de cumplir con las obligaciones legales.
- Violación del contrato:
  - imposibilidad de cumplir con las obligaciones contractuales.
- Atentado contra la disponibilidad del personal, de los usuarios:
  - peligro para el personal y/o los usuarios del organismo.
- Atentado contra la vida privada de los usuarios.
- Pérdidas financieras.
- Gastos financieros de respaldo y actualización:
  - en personal,
  - en hardware,
  - en estudios, pericias.
- Pérdida de bienes, fondos, valores.
- Perdida de clientes, pérdida de proveedores.
- Acciones legales y multas.
- Pérdida de una ventaja competitiva.
- Pérdida de ventaja tecnológica, técnica.

- Pérdida de eficacia, de confianza.
- Pérdida de reputación técnica.
- Debilitamiento de la capacidad de negociación.
- Crisis social (huelgas).
- Crisis gubernamental.
- Remoción del personal.
- Daños materiales.
- ...

Estos impactos se han propuesto a modo indicativo, el grupo de trabajo debe proponer los más significativos para el organismo y adaptarlos específicamente al organismo. Los resultados de las actividades precedentes, especialmente aquellos vinculados con el estudio del organismo, con los retos y el contexto del sistema podrán utilizarse para la selección de estos impactos. Elegiremos, como impactos significativos, el cuestionamiento de las misiones, del oficio o de los valores del organismo. A fin de objetivar los impactos, es conveniente ofrecer ejemplos explícitos de cada uno de ellos en términos de consecuencias previsibles.

Una vez que se han determinado los criterios de seguridad y los impactos, es posible realizar las fichas de expresión de las necesidades de seguridad para cada elemento esencial.

Ficha de expresión de las necesidades de seguridad:

Nombre del elemento esencial	***Impacto 1***	***…***	***Impacto N***	***Necesidades de seguridad***	***Comentarios***
Criterio de seguridad 1	*N11*	*…*	*N1n*	*f(N11…N1n)*	
…	*…*	*…*	*…*	*…*	
Criterio de seguridad N	*Nn1*	*…*	*Nnn*	*f(Nn1…Nnn)*	

La síntesis de la necesidad de seguridad para cada elemento esencial y cada criterio de seguridad (columna "Necesidades de seguridad") se determinará en función del conjunto de valores expresados según los impactos.

Estas fichas pueden ampliarse con los siniestros para cada criterio de seguridad, a fin de facilitar la expresión de las necesidades de seguridad considerando diferentes puntos de vista.

Algunos ejemplos de siniestros vinculados con los principales criterios de seguridad (la situación y el contexto deberían llevarnos a enumerar siniestros específicos para cada criterio seleccionado):

- Para la disponibilidad:
  - degradación del rendimiento,
  - interrupción de corta duración,
  - interrupción de larga duración,
  - inaccesibilidad,
  - pérdida total (destrucción).
- Para la integridad:
  - modificación accidental,
  - modificación deliberada,
  - resultados incorrectos,
  - resultados incompletos.
- Para la confidencialidad:
  - divulgación interna,
  - divulgación externa.

Ficha de expresión de las necesidades de seguridad ampliada:

Nombre del elemento sensible	***Siniestros***	***Impacto 1***	***…***	***Impacto N***	***Necesidades de seguridad***	***Comentarios***
Criterio de seguridad 1	*Siniestro 1*	*N111*	*…*	*N11n*	*f(N111…N1nn)*	
Criterio de seguridad 1	*…*	*…*	*…*	*…*		
Criterio de seguridad 1	*Siniestro N*	*N1n1*	*…*	*N1nn*		
…	*…*	*…*	*…*	*…*	*…*	
Criterio de seguridad N	*Siniestro 1*	*Nn11*	*…*	*Nn1n*	*f(Nn11…Nnnn)*	
Criterio de seguridad N	*…*	*...*	*…*	*...*		
Criterio de seguridad N	*Siniestro N*	*Nnn1*	*…*	*Nnnn*		

En este caso, la síntesis de la necesidad de seguridad para cada elemento esencial y cada criterio de seguridad (columna "Necesidades de seguridad") se determinará en función del conjunto de valores expresados según los impactos.

Actividad 2.2 – Síntesis de las necesidades de seguridad

Asignar una necesidad de seguridad por criterio de seguridad para cada elemento esencial

Para llevar a cabo su estudio, debe conformarse un grupo de trabajo heterogéneo y representativo del SI (responsables, especialistas en informática y usuarios). Este grupo podrá discutir las necesidades de seguridad expresadas y sus justificaciones.

Recogida de las necesidades de seguridad

La recogida de las necesidades de seguridad se realiza por medio de fichas de expresión de las necesidades de seguridad y de la escala de necesidades entregadas a los usuarios involucrados. Los valores informados reflejan el punto de vista de los usuarios frente a sus necesidades de seguridad. Este punto de vista podrá justificarse mediante un comentario (especialmente para valores extremos). Debe realizarse una síntesis a nivel de la ficha a fin de obtener un vector de necesidades de seguridad para cada elemento esencial.

Los mismos usuarios deberán realizar esta evaluación expresando los valores aceptables, dado que superarlos sería inaceptable. Asignarán una nota a cada intersección fila-columna de las fichas de expresión de las necesidades a fin de obtener un vector disponibilidad – integridad – confidencialidad... Sin embargo, los usuarios del sistema no son forzosamente expertos en seguridad de los SI, ni concientes de la SSI. El grupo de trabajo o las personas que realizarán las entrevistas a los usuarios jugará por lo tanto un papel importante, garantizando la buena comprensión de la escala de necesidades y la homogeneidad de los resultados obtenidos.

Las necesidades de seguridad son independientes de los riesgos corridos y de los medios de seguridad implementados. Representan por lo tanto un valor intrínseco del carácter sensible de la información, de las funciones o subfunciones. Por ejemplo, en el ámbito de la defensa, asignar un valor de confidencialidad a los documentos consiste en clasificarlos (secreto de defensa, confidencial de defensa...).

Si un elemento esencial tiene necesidades que varían con el tiempo, es conveniente estudiar por separado sus diferentes estados, como si se tratara de otros tantos elementos esenciales.

Es recomendable completar la totalidad de las fichas de expresión de las necesidades de seguridad si se quieren obtener riesgos cuya redacción sea precisa en cuanto a sus impactos.

Síntesis de las necesidades de seguridad

El grupo de trabajo completa los resultados obtenidos conjuntamente con los usuarios en la ficha de síntesis de las necesidades de seguridad y determina el valor considerado como síntesis. Luego se valida esta síntesis, armonizando los diferentes puntos de vista. El validador debe tener una visión global de los elementos esenciales (por ejemplo, podría ser el responsable usuario, o de manera más general, el propietario de los elementos esenciales). Puede lograrse un consenso mediante la expresión de los argumentos de cada uno y posterior arbitraje. En última instancia, se puede considerar que la síntesis de la necesidad de seguridad, según los criterios de seguridad de un elemento esencial, es el máximo de los valores asignados por los usuarios en cada una de las fichas.

En caso de observarse divergencias demasiado importantes, podría ser necesario solicitar a los usuarios que reconsideren sus valores o que los expliciten aún más. La síntesis debe, en todos los casos, justificarse respecto de los elementos importantes del organismo identificado durante el estudio del contexto.

Ejemplo de ficha de síntesis de las necesidades de seguridad:

Lista de elementos esenciales	***Síntesis de las necesidades de seguridad***		
	Confidencialidad	***Integridad***	***Disponibilidad***
Función 1	*0*	*3*	*3*
Función 2	*1*	*3*	*2*
…	*…*	*…*	*…*
Función N	*0*	*4*	*2*
Dato 1	*2*	*1*	*1*
…	*…*	*…*	*…*
Dato N	*4*	*3*	*0*

Etapa 3 – Estudio del contexto

Actividad 3 – Estudio de los origines de las amenazas

Enumerar los métodos de ataque pertinentes

La selección de los métodos de ataque consiste en seleccionar, basándose en la lista de métodos de ataques y elementos peligrosos genéricos propuesta en la guía "Herramientas para la apreciación de los riesgos de SSI", aquellas que se consideran pertinentes en función del contexto, de las misiones y de las entidades que conforman el sistema evaluado. Se realiza con el grupo de trabajo a partir de una lista de métodos de ataque vinculados con ciertos temas. Estos temas son:

- siniestros físicos,
- hechos naturales,
- pérdida de servicios esenciales,
- alteraciones debidas a las ondas radioeléctricas,
- datos comprometidos,
- fallos técnicos,
- actos ilícitos,
- funciones comprometidas.

Esta clasificación permite seleccionar más fácilmente los métodos de ataque involucrados. Algunos temas (siniestros físicos, hechos naturales, pérdida de servicios esenciales) podrían desestimarse, siempre que se justifique. Por ejemplo, puede ser que estudios anteriores ya hayan tratado ese tema.

Un método de ataque debe seleccionarse si su cumplimiento es realista y si puede suponerse que tendrá un impacto.

Se recomienda justificar la no selección de un método de ataque o de un tema, a fin de conservar un registro de las elecciones efectuadas. Para que la trazabilidad de las elecciones efectuadas sea lo más clara posible, es posible transformar todos los métodos de ataque no seleccionados en hipótesis (teniendo en cuenta que varios métodos de ataques no seleccionados pueden reagruparse en una sola hipótesis).

Los métodos de ataque propuestos en las bases de conocimientos son denominados genéricos, porque definen una categoría en la cual pueden entrar métodos de ataque descritos en un nivel de granularidad mucho más preciso. Por lo tanto, la lista propuesta puede pretender ser exhaustiva por cuanto siempre es posible hacer entrar un método de ataque determinado en una categoría propuesta. Sin embargo, esta lista puede adaptarse al contexto del organismo y al contexto de utilización del sistema evaluado.

También pueden seleccionarse métodos de ataque a partir de estudios de seguridad efectuados en los sistemas vecinos o surgidos de documentos de alcance general (política de seguridad, guía de seguridad).

Caracterizar a los métodos de ataque mediante los criterios de seguridad a los que pueden afectar

Cada método de ataque puede afectar al menos a un criterio de seguridad (disponibilidad, integridad, confidencialidad...).
Es conveniente, por lo tanto, caracterizar a todos los métodos de ataque seleccionados mediante los criterios de seguridad a los que pueden afectar. Esta caracterización consiste en determinar los impactos directos sobre los criterios de seguridad, y no todas las posibilidades generadas.
Ejemplo: El incendio afecta en primer lugar al criterio de disponibilidad, aunque puede, por consecuencia, afectar también a la integridad y a la confidencialidad. Caracterizaremos pues generalmente al incendio como un atentado a la disponibilidad.
La caracterización de cada método de ataque mediante los criterios de seguridad (idénticos a los que han permitido expresar las necesidades de seguridad) permitirá, en una etapa posterior, confrontar fácilmente las necesidades de seguridad con las amenazas a fin de determinar los riesgos reales.

Caracterizar a los elementos peligrosos vinculados por su tipo y causas

Los métodos de ataque son utilizados por elementos peligrosos que es conveniente caracterizar para cada método de ataque. Deben describirse:

- El tipo de elemento peligroso (natural, humano o ambiental, es decir, externo al sistema evaluado).
- Las causas (accidentales o deliberadas) de cada elemento peligroso. Puede afinarse esta clasificación indicando la exposición y los recursos disponibles cuando se trata de una causa accidental e indicando la pericia, los recursos disponibles y la motivación cuando se trata de una causa deliberada.

Se aconseja utilizar la parte referida a los métodos de ataque y elementos peligrosos genéricos de la guía "Herramientas para la apreciación de los riesgos de SSI", para caracterizar a los elementos peligrosos.

También puede aplicarse la tipología de amenazas propuesta en la [IGI 900] y la [Rec 901]. Puede especificarse por lo tanto su origen lúdico, codicioso, estratégico o terrorista.

Añadir un valor que represente el potencial de ataque del elemento peligroso

La caracterización de los elementos peligrosos puede sintetizarse mediante un único valor para cada método de ataque seleccionado. Se trata de un potencial de ataque, generalmente igual a uno de los siguientes valores:

- 1 (accidental y aleatorio),
- 2 (posibilidades o recursos limitados),
- 3 (gran nivel de pericia, posibilidad y recursos).

Este potencial de ataque permitirá determinar un nivel de resistencia adecuado para los objetivos de seguridad.

El siguiente cuadro presenta un ejemplo de selección y caracterización de métodos de ataque::

		Elementos peligrosos						***Criterios de seguridad afectados***		
		Tipo			***Causa***		***Potencial de ataque***			
	Métodos de ataque	***Natural***	***Humano***	***Ambiental***	***Accidental***	***Deliberado***		***Disponibilidad***	***Integridad***	***Confidencialidad***
1	*Incendio*	*+*	*+*	*+*	*+*	*+*	*2*	*+*	*+*	
13	*Pérdida de los medios de telecomunicaciones*			*+*	*+*	*+*	*1*	*+*		
19	*Escucha pasiva*		*+*	*+*		*+*	*2*			*+*
20	*Robo de soportes informáticos o de documentos*			*+*		*+*	*2*			*+*
21	*Robo de hardware*			*+*		*+*	*1*	*+*		*+*
23	*Divulgación*		*+*	*+*	*+*	*+*	*1*			*+*
26	*Alteración de programas*			*+*		*+*	*1*	*+*	*+*	*+*
42	*Atentado contra la disponibilidad del personal*	*+*	*+*	*+*	*+*	*+*	*1*	*+*		

Identificar los métodos de ataque no considerados justificándolo

Es conveniente justificar debidamente la desestimación de cualquier método de ataque. Aunque se considere que es improbable, que no tendrá consecuencias, que será tratado aparte o voluntariamente dejado de lado, es importante explicar por qué no se lo ha seleccionado, ya que no será analizado en el resto del estudio aunque pueda ser una fuente de riesgos para el organismo.

Actividad 3.2 – Estudio de las vulnerabilidades

Identificar las vulnerabilidades de las entidades según los métodos de ataque

Es conveniente determinar, para cada método de ataque seleccionado, las vulnerabilidades del sistema estudiado que permiten su materialización (se aconseja utilizar las vulnerabilidades genéricas de la guía "Herramientas para la apreciación de los riesgos de SSI" para identificar las vulnerabilidades según los tipos y subtipos de entidades y los métodos de ataque).

Una vulnerabilidad es una característica del sistema que un elemento peligroso podría utilizar y que permitiría pues la materialización de un método de ataque. Esta característica, atribuida a las entidades del sistema, puede constituir una debilidad o un fallo de seguridad.
Ejemplos:

- *para una entidad del tipo hardware, la capacidad de emitir ondas radioeléctricas o el atractivo del hardware (ordenador portátil) constituye una característica;*
- *para una entidad del tipo establecimiento, la facilidad para ingresar en él constituye también una característica.*

Estas características se transforman en vulnerabilidades si los métodos de ataque pueden aprovecharlas:

- *la utilización de ordenadores portátiles es una vulnerabilidad frente al método de ataque robo de hardware;*
- *la capacidad de emitir ondas radioeléctricas es una vulnerabilidad frente al método de ataque intercepción mediante señales parásitas que comprometen la seguridad del sistema.*

Un método de ataque puede aprovechar varias vulnerabilidades para actuar.
Ejemplo: El método de ataque alteración de programas puede concretarse si:

- *es fácil ingresar al establecimiento (vulnerabilidad del tipo de entidades establecimiento);*
- *el hardware permite la instalación de elementos adicionales (vulnerabilidad de los tipos de entidades hardware y software);*
- *no hay plan de control del hardware (entidad del tipo organización).*

En las bases de conocimientos se ofrece una lista de vulnerabilidades genéricas vinculadas con cada método de ataque y cada subtipo de entidades. La selección se realiza a partir de esta lista pero puede basarse en elementos propios del sistema. Es importante destacar que la lista propuesta es una base para la reflexión que puede personalizarse y que deberá adaptarse al contexto estudiado. Esta lista está, por naturaleza, en continua evolución.

Estimar eventualmente el nivel de las vulnerabilidades

Las vulnerabilidades pueden caracterizarse por su nivel, que representa la posibilidad de actuar de los métodos de ataque que las aprovechan.

Este nivel se aprecia en función de varios criterios:

- del contexto propio del sistema;
- de estado de la tecnología en el campo considerado.

En muchos casos no existen datos estadísticos que permitan elaborar normas de comportamiento del sistema de información. Sólo los riesgos naturales y tecnológicos disponen de cifras que hacen posible una evaluación utilizando técnicas cuantitativas, pero hay que señalar que estos análisis son subjetivos por naturaleza.

Estimar el nivel de las vulnerabilidades tiene por objetivo conservar sólo las vulnerabilidades pertinentes y jerarquizarlas. Podemos contentarnos con seleccionarlas, pero la estimación de este valor permite lograr una mayor precisión.

Para ello es posible utilizar la siguiente escala:

0	*Totalmente improbable o impracticable.*
1	*Poco probable o que requiere medios muy importantes y/o conocimientos muy avanzados en el campo considerado.*
2	*Medianamente probable o que requiere cierto nivel de pericia y/o hardware específico.*
3	*Muy probable o realizable con medios estándar y/o con conocimientos básicos.*
4	*Cierto o realizable por cualquiera.*

En caso de métodos de ataque naturales o humanos, la estimación del nivel de las vulnerabilidades se basa en su factibilidad efectiva observada. En caso de delito informático, la estimación del nivel de las vulnerabilidades se basa más bien en la factibilidad en términos de medios, competencias y conocimientos necesarios.

Se obtiene la lista de la vulnerabilidades estimadas vinculadas con los métodos de ataque seleccionados por tipos o subtipos de entidades.

El siguiente cuadro propone un ejemplo del resultado.

Métodos de ataque		*Vulnerabilidades*	*Hardware y software*	*Redes internas*	*Redes externas*	*Establecimientos*	*Personal*	*Organización*
1	*Incendio*	*Falta de coherencia entre la medidas en caso de incendio y el sistema informático*				*2*		
		Ausencia de instrucciones (alerta, prevención, formación...)						*2*
		Falta de organización de seguridad en caso de incendio						*3*
13	*Pérdida de los medios de telecomunicaciones*	*Fallos en la utilización de la red telefónica interna*				*1*		
		Mal funcionamiento de las redes externas (RTPC)			*1*			
		Mal funcionamiento de las redes externas (servicios de redes)			*1*			
…	…	…	…	…	…	…	…	…

Actividad 3.3 – Formalización de las amenazas

Formular explícitamente las amenazas

La redacción de las amenazas puede ser más o menos detallada. Se trata ante todo de expresar de manera explícita una situación de ataque, pudiendo el nivel de detalle variar en función de la finalidad del estudio .

En el mejor de los casos, la redacción de la amenaza abarca:
- el elemento peligroso con sus características, especialmente su potencial de ataque;
- el método de ataque que utiliza el elemento peligroso y los criterios de seguridad afectados;
- las vulnerabilidades aprovechadas, indicando su nivel;
- las entidades que presentan dichas vulnerabilidades.

Las amenazas pueden caracterizarse por un valor de posibilidad determinado en función del nivel de las vulnerabilidades aprovechadas.
Aunque la valoración de la posibilidad pueda ser subjetiva, su interés reside en el hecho de que sean relativas unas respecto de las otras.
Si una amenaza implica el aprovechamiento de una sola vulnerabilidad, la posibilidad de la amenaza es igual al nivel de la vulnerabilidad.
Si una amenaza implica el aprovechamiento de varias vulnerabilidades, es conveniente determinar la posibilidad de la amenaza según los respectivos niveles de las vulnerabilidades:
- generalmente reconsiderando la posibilidad de la amenaza,
- ya sea seleccionando el nivel más bajo de vulnerabilidades en caso de que la amenaza sólo actúe aprovechando la totalidad de las vulnerabilidades,
- ya sea seleccionando el nivel más alto de vulnerabilidades en caso de que la amenaza pueda actuar aprovechando sólo una de las vulnerabilidades.

Ejemplo:

Amenazas		*Método de ataque*	*Potencial de ataque*	*D*	*I*	*C*	*Posibilidad*
M.INCENDIE	*Agravamiento de las consecuencias de un incendio a causa de la falta de coherencia de las medidas en caso de incendio con el sistema informático (lugar de la oficina de estudios), de la ausencia de instrucciones o de organización de seguridad en caso de incendio (organización de la oficina de estudios).*	*1*	*2*	*+*			*2*
M.TELECOM	*Pérdida de los medios de telecomunicaciones a causa de un mal funcionamiento de las redes externas (Internet)*	*12*	*1*	*+*			*1*
M.VOL-DOC	*Robo de soportes informáticos o de documentos perpetrado por una persona de visita o por personal de limpieza debido a la facilidad para ingresar en los locales en horario laboral (lugar de la oficina de estudios).*	*19*	*2*			*+*	*3*
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Jerarquizar eventualmente las amenazas según su posibilidad

La lista de amenazas resultante puede ordenarse por orden decreciente de posibilidad de las amenazas. Esta lista es una herramienta de comunicación a la que es conveniente prestar mucha atención. Permite, efectivamente, expresar lo más explícitamente posible aquello a lo que el organismo está expuesto. Las amenazas cuya posibilidad es importante deberían por lo tanto aparecer en primer lugar en la lista a fin de concienciar eficazmente a los actores.

Etapa 4 – Identificación de los objetivos de seguridad

Actividad 4.1 – Confrontación de las amenazas con las necesidades

Determinar los riesgos confrontando las amenazas con las necesidades de seguridad

La determinación de los riesgos a los cuales está confrontado el organismo consiste en identificar la manera en que los elementos esenciales pueden verse afectados por las amenazas, es decir, en determinar cómo aquello a que el organismo valora puede verse afectado por aquello a lo que está expuesto.

Esta asociación se realiza confrontando las amenazas con las necesidades. Por un lado, las amenazas de seguridad de los elementos esenciales se han expresado en función de diferentes criterios de seguridad (disponibilidad, integridad, confidencialidad...). Por otro lado, las amenazas han sido caracterizadas usando los criterios de seguridad que pueden afectarlas (en función de la caracterización de los métodos de ataque y en función de los mismos criterios de seguridad). Es posible por lo tanto confrontar cada elemento esencial con cada amenaza en función de los criterios de seguridad, a fin de determinar las posibles consecuencias de la concretización de las amenazas.

Para cada elemento esencial se realiza un cuadro que enumere los métodos de ataque. Los métodos de ataque seleccionados en esta fase del estudio no son únicamente aquellos susceptibles de aprovechar vulnerabilidades del elemento esencial (se realiza esta verificación utilizando los cuadros de las relaciones entidades/elementos efectuados durante el estudio del contexto). Se informarán entonces las necesidades de seguridad del elemento esencial estudiado y los criterios de seguridad que pueden verse afectados por cada método de ataque seleccionado.

Las fichas pueden realizarse por método de ataque o detalladas por amenaza, pero los datos útiles son los criterios de seguridad afectados por los métodos de ataque. Éstos se informan por lo tanto para cada amenaza correspondiente. Es posible hacer constar las amenazas en lugar de los métodos de ataque, pero lo que se confronta son los perjuicios de los métodos de ataque con las necesidades; por esta razón, generalmente se divide esta operación en función de los métodos de ataque.

Se aplican entonces las siguientes reglas para cada criterio de seguridad:

- Si un criterio de seguridad no puede verse afectado, entonces las necesidades de seguridad involucradas son nulas.
- Si un criterio de seguridad puede verse afectado, entonces las necesidades de seguridad involucradas son iguales a las necesidades de seguridad del elemento considerado.

Ejemplo:

I. VISU. ***(Visualización)***		*Necesidades de seguridad:*			*D* *2*	*I* *2*	*C* *0*
Métodos de ataque		*Perjuicio*			***Necesidades de seguridad involucradas***		
		D	*I*	*C*	***D***	***I***	***C***
1	*Incendio*	*+*	*+*		*2*	*2*	
13	*Pérdida de los medios de telecomunicaciones*	*+*			*2*		
19	*Escucha pasiva*			*+*			
20	*Robo de soportes informáticos o de documentos*			*+*			
21	*Robo de hardware*	*+*		*+*	*2*		
23	*Divulgación externa*			*+*			
26	*Alteración de programas*	*+*	*+*	*+*	*2*	*2*	
42	*Atentado contra la disponibilidad del personal*	*+*			*2*		
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Los valores resultantes representan el riesgo para el organismo, dado que conforman el valor de la necesidad

Buscamos en realidad determinar los riesgos de perjudicar a las necesidades de seguridad de los elementos esenciales. Si una amenaza se concretiza, puede efectivamente ser susceptible de perjudicar a estas necesidades y a los impactos importantes identificados y utilizados para establecerlas.

La totalidad de los cuadros puede entonces sintetizarse a fin de obtener un panorama global de los riesgos. Esta síntesis puede realizarse utilizando métodos de ataque o amenazas. Mediante esta síntesis, la reflexión se centra en el impacto real de las amenazas sobre los elementos esenciales, y, por lo tanto, sobre el organismo

Ejemplo de síntesis de los riesgos en función de los métodos de ataque:

Síntesis de los riesgos				*Elemento 1*			…			*Elemento N*		
				D	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
				3	*2*	*0*	…	…	…	*0*	*1*	*0*
				Necesidades de seguridad involucradas								
Métodos de ataque	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
Escucha pasiva			*X*	*0*	*0*	*0*	…	…	…	*0*	*0*	*0*
Robo de hardware	*X*		*X*	*3*	*0*	*0*	…	…	…	*0*	*0*	*0*
…	…	…	…	…	…	…	…	…	…	…	…	…

Es posible determinar los valores máximos de las necesidades de seguridad involucradas por amenaza o método de ataque. Esto constituirá un elemento de jerarquización de los riesgos.

Formular explícitamente los riesgos

Utilizando el cuadro de síntesis de los riesgos, la redacción de la amenazas y eventualmente la escala de necesidades, es conveniente redactar la descripción de los riesgos lo más explícitamente posible. La precisión de la redacción depende de la granularidad deseada.

En el mejor de los casos, la redacción de un riesgo abarca:

- el elemento peligroso con sus características, especialmente su potencial de ataque;
- el método de ataque empleado por el elemento peligroso;
- las vulnerabilidades aprovechadas;
- las entidades que presentan estas vulnerabilidades;
- la posibilidad de la amenaza;
- las principales necesidades de seguridad involucradas;
- los impactos sobre el organismo (según la escala de necesidades).

Ejemplo:

Riesgos		*necesidades de seguridad*	*Posibilidad de la amenaza*	*Potencial de ataque*
R.PIEGEAGE	*Un intruso altera el software mediante la modificación de los comandos del sistema, la instalación de programas piratas, la alteración de una aplicación (hardware, software e Internet) o una acción sobre los programas de los recursos del sistema (Internet), atentando contra la confidencialidad de los datos sensibles (presupuestos, carpeta de litigios…) y contra la integridad de los elementos esenciales (cálculos de estructuras, presupuestos, planos técnicos, especificaciones técnicas, carpeta de litigios…)*	*4*	*3*	*1*
R.VOL-VISITEUR	*Dada la facilidad para ingresar en los locales (lugar de la oficina de estudios), una persona que está de visita o personal de limpieza roba hardware reconocido como particularmente atractivo (valor en el mercado, tecnología de la mayor parte del hardware, software y elementos de red) atentando así contra la disponibilidad de varios elementos esenciales y contra la confidencialidad de la información sensible (presupuestos, carpeta de litigios…)*	*2*	*1*	*1*
…	…	…	…	…

Jerarquizar los riesgos según su impacto sobre los elementos esenciales y la posibilidad de las amenazas

La lista de riesgos resultante puede ordenarse por orden decreciente de valores máximos de las necesidades de seguridad involucradas y por orden decreciente de posibilidad de las amenazas involucradas. Esta lista es una herramienta de comunicación a la que es conveniente prestar mucha atención. Permite, efectivamente, expresar lo más explícitamente posible los riesgos reales a los que el organismo está expuesto. Los riesgos que pueden afectar a las necesidades de seguridad más importantes y para los cuales la posibilidad de las amenazas es importante deberían por lo tanto aparecer en primer lugar en la lista a fin de concienciar eficazmente a los actores. Esto permitirá priorizar su tratamiento.

Otra forma de jerarquizar los riesgos obteniendo al mismo tiempo la adhesión de los participantes es pedirles que jerarquicen ellos mismos los riesgos. Efectivamente, son ellos quienes tomarán la decisión de considerar o no cada riesgo y de tratarlo. Es importante pues que se involucren en esta fase del estudio.

También es posible proponer una jerarquización de los riesgos según el primer método y revisarla utilizando el segundo método.

Identificar los riesgos no considerados justificándolo

El grupo de trabajo puede sugerir desestimar los riesgos que sólo afectan a pocas necesidades de seguridad y para los cuales la posibilidad de las amenazas es escasa. Es conveniente entonces identificar esos riesgos y justificar debidamente su desestimación porque constituyen riesgos residuales para el organismo.

Actividad 4.2 – Formalización de los objetivos de seguridad

Enumerar los objetivos de seguridad

Los objetivos de seguridad deben cubrir la totalidad de los riesgos que se ha decidido cubrir, teniendo en cuenta al mismo tiempo las hipótesis, las normas de seguridad y los diferentes elementos del contexto (especialmente las restricciones y los retos). Deben ser coherentes con el objetivo operativo o el objetivo "producto" declarado del sistema evaluado y con todo el conocimiento sobre su entorno físico.

Los objetivos de seguridad consisten generalmente en la expresión de la voluntad de cubrir los riesgos por parte del diseñador del proyecto, sin especificar las soluciones para lograrlo.
Conformarán así un pliego de condiciones completo, abierto (sin presuponer qué soluciones deben adoptarse) y perfectamente adaptado a los retos del organismo.

Los componentes del riesgo que los objetivos de seguridad pueden tratar son los siguientes:

- El origen de las amenazas (elementos peligrosos y métodos de ataque).
- Las vulnerabilidades aprovechadas (es posible utilizar los objetivos de seguridad genéricos y el cuadro de determinación de los objetivos y requerimientos de seguridad de la guía "Herramientas para el tratamiento de los riesgos de SSI" para identificar los objetivos de seguridad que cubren las vulnerabilidades).
- Las consecuencias (elementos esenciales afectados y impactos sobre el organismo).

Se propone adoptar la siguiente nomenclatura para los objetivos de seguridad: O.xx (siendo O objetivo técnico y xx el nombre del objetivo de seguridad).

Ejemplos:

O.INC-ORIGINE	*Deben tomarse medidas para evitar que se inicie un incendio.*
O.INC-CSQ	*Deben tomarse medidas para reducir las consecuencias de un incendio sobre los elementos esenciales y en términos de pérdidas financieras.*
O.INC-COHERENCE	*El lugar de la oficina de estudios debe disponer de medidas contra incendios coherentes con el sistema informático.*
O.INC-ORGA	*La organización de la oficina de estudios debe disponer de instrucciones y de una organización de seguridad en caso de incendio.*
O.TELECOM-ORIGINE	*Deben tomarse medidas para evitar el mal funcionamiento de las redes externas.*
O.TELECOM-CSQ	*Deben tomarse medidas para reducir las consecuencias del mal funcionamiento de las redes externas sobre los elementos esenciales y en términos de alteración del funcionamiento interno.*
O.TELECOM	*El mal funcionamiento de las redes externas no deben entorpecer el uso de Internet por parte de los usuarios de la oficina de estudios.*

Justificar la exhaustividad de la cobertura

Los objetivos de seguridad determinados anteriormente tienen por finalidad contrarrestar o minimizar los riesgos a los que está expuesto el sistema evaluado y tomar en cuenta las hipótesis y normas de seguridad.
Las personas que hacen el estudio tendrán ahora que garantizar que dichos objetivos son necesarios y suficientes para cubrir la totalidad de los riesgos, hipótesis y normas de seguridad identificados.

Una primera justificación consiste en demostrar que los objetivos de seguridad:

- cubren suficientemente todos los riegos,
- respetan las normas de seguridad (y las referencias reglamentarias),
- son pertinentes respecto de las hipótesis (y los retos del sistema evaluado).

Es conveniente verificar la compatibilidad de cada objetivo de seguridad con las restricciones que pesan sobre el organismo y sobre el sistema evaluado.

La cobertura puede sintetizarse mediante un valor utilizando la siguiente escala:

0	Ninguna cobertura
1	Cobertura parcial
2	Cobertura completa

Ejemplo:

Riesgos	*Objetivos de seguridad*	*Justificación de la cobertura*	*Cobertura*	*Potencial de ataque*
R.PIEGEAGE	*O.SYS-COMMANDES* *O.SYS-ACTIONS*	*Los dos objetivos de seguridad cubren la totalidad de las vulnerabilidades aprovechadas en el riesgo:* *- posibilidad de modificar los comandos de los sistemas vía Internet,* *- posibilidad de instalar programas piratas vía Internet,* *- posibilidad de modificar una aplicación vía Internet,* *- posibilidad de actuar sobre los programas de los recursos del sistema vía Internet.*	*2*	*1*
R.VOL-VISITEUR	*O.LOCAUX* *O.VOL-PROTECTION* *O.PRISE-EN-CHARGE* *O.AUTH-DOC*	*Los dos primeros objetivos de seguridad cubren las vulnerabilidades aprovechadas en el riesgo:* *- Facilidad para ingresar en la oficina de estudios.* *- Hardware reconocido como particularmente atractivo (valor en el mercado y valor tecnológico).* *El tercer objetivo de seguridad mejora la reducción del riesgo responsabilizando a los usuarios.* *El último objetivo de seguridad ofrece una garantía de autenticación del redactor de los documentos*	*2*	*1*
…	…	…	…	…

Una segunda justificación consiste en demostrar que cada objetivo de seguridad responde al menos a un riego, una norma de seguridad (o una referencia reglamentaria) o una hipótesis (o un reto del sistema evaluado o del modo de explotación de seguridad).

Ejemplo:

Objetivos de seguridad	*R.PIEGEAGE*	*R.VOL-VISITEUR*	*R.VOL-RIGUEUR*	*R.VOL-UTIL*	*R.VIRUS-VERIF*	*R.INCENDIE*	*R.VIRUS-MAIL*	*R.PABX*	*R.TELECOM*	*R.MALADIE*	*R.VOL-DOC*	*R.ECOUTE*	*R.PERTE-DOC*	*R.DIVULGATION*
O.INC-COHERENCE						+								
O.INC-ORGA						+								
O.TELECOM									+					
O.ECOUTE												+		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Clasificar eventualmente los objetivos de seguridad en dos categorías

La determinación de los objetivos de seguridad tiene por objeto considerar todas las preocupaciones referidas a la seguridad y declarar los aspectos de seguridad que son:

- tomados en cuenta directamente por el sistema evaluado (son objetivos de seguridad que se centran en el sistema evaluado), o bien
- tomados en cuenta por el entorno (son objetivos de seguridad que se centran en el entorno del sistema evaluado),

Se basa en un análisis de los impactos provocados sobre el desarrollo (credibilidad técnica, temporal...), la política de seguridad (conformidad con los elementos de la política general), los factores económicos (costes generados por la integración de medidas técnicas u organizacionales) y las decisiones de aceptar los riesgos (riesgos para los cuales la posibilidad de las amenazas es despreciable o incluso riesgos para los cuales pueden tomarse medidas externas, como la suscripción de pólizas de seguro).

Identificar los fallos de coberturas justificándolo

El grupo de trabajo puede decidir no cubrir perfectamente los riesgos, normas de seguridad o hipótesis mediante los objetivos de seguridad. Es conveniente entonces indicarlo claramente y justificar debidamente esta falta de exhaustividad porque esto genera riesgos residuales para el organismo.

Ejemplos:

- *Un empleado divulga datos a la competencia en el marco de una operación de contratación, debido a la facilidad para intercambiar informaciones mediante hardware, software y redes de la oficina de estudios, y atenta así contra la confidencialidad de la información sensible (presupuestos, carpeta de litigios…).*
- *Un empleado divulga datos a la competencia en el marco de una operación de contratación, debido a la falta de procedimientos de control de uso de las herramientas de comunicación, y atenta así contra la confidencialidad de la información sensible (presupuestos, carpeta de litigios…).*

Actividad 4.3 – Determinación de los niveles de seguridad

Determinar el nivel de resistencia adecuado para cada objetivo de seguridad

El nivel de resistencia[3] esperado de las medidas de seguridad destinadas a alcanzar los objetivos de seguridad está determinado principalmente en función del potencial de ataque de los elementos peligrosos que dan origen a los riesgos que pesan sobre el organismo. Efectivamente, el nivel de protección adecuado depende del nivel del atacante.

No obstante, depende también de otros factores tales como las necesidades de seguridad de los elementos esenciales que pueden verse afectados, la posibilidad de las amenazas, el contexto general…

Consideramos tres niveles de resistencia, que expresan los esfuerzos mínimos que se consideran necesarios para generar un fallo en el comportamiento de seguridad esperado por ataque directo de los mecanismos de seguridad subyacentes:

1 – Nivel elemental	Un nivel de resistencia tal que el análisis muestra que la función involucrada ofrece una protección adecuada frente a una violación fortuita de la seguridad del sistema por parte de atacantes que poseen escaso potencial de ataque.
2 – Nivel moderado	Un nivel de resistencia tal que el análisis muestra que la función involucrada ofrece una protección adecuada frente a una violación fácil de poner en práctica o una violación intencional de la seguridad del sistema por parte de atacantes que poseen un potencial de ataque moderado.
3 – Nivel alto	Un nivel de resistencia tal que el análisis muestra que la función involucrada ofrece una protección adecuada frente a una violación deliberadamente planificada u organizada de la seguridad del sistema por parte de atacantes que poseen un alto potencial de ataque.

En lo que respecta a los objetivos de seguridad que cubren los riesgos, el nivel requerido depende del potencial de ataque. Si un objetivo de seguridad cubre varios riesgos cuyos potenciales de ataque difieren, se selecciona el nivel más elevado. Es necesario ajustar este valor tomando en cuenta las necesidades de seguridad de los elementos esenciales que pueden verse afectados, la posibilidad de las amenazas, el contexto general…
En lo que respecta a los objetivos de seguridad que cubren las normas de seguridad (o las referencias reglamentarias), su nivel lo elige el organismo en función de la importancia que le otorga a éstas y de los esfuerzos que planea realizar para hacerlas respetar.

El nivel de resistencia de cada objetivo de seguridad debe justificarse.

Elegir el nivel de los requerimientos de aseguramiento

Existen siete niveles de aseguramiento[4] predeterminados (denominados EAL – *Evaluation Assurance Level:* Evaluación del nivel de aseguramiento):

EAL 1	Probado funcionalmente
EAL 2	Probado estructuralmente

[3] Niveles surgidos de la definición de los niveles de resistencia de las funciones de la ISO/IEC 15408.
[4] El nivel de garantía de seguramiento representa un paquete de elementos de aseguramiento extraídos de la Parte 3 de la ISO/IEC 15408 que representa un nivel de la escala de aseguramiento predefinida.

EAL 3	Probado y verificado metódicamente
EAL 4	Diseñado, probado y controlado metódicamente
EAL 5	Diseñado utilizando métodos semiformales y probado
EAL 6	Diseñado controlado utilizando métodos semiformales y probado
EAL 7	Diseñado controlado utilizando métodos formales y probado

Estos niveles están conformados por diferentes componentes de rigor creciente que permiten evaluar la seguridad implementada.

El nivel de aseguramiento EAL representa el nivel de confianza que podemos atribuirle a la puesta en práctica de los objetivos de seguridad. El nivel de aseguramiento se centra más precisamente en la implementación de los requerimientos funcionales de seguridad, que conforman una descripción más detallada de los objetivos de seguridad. Cuando más elevado sea, mayores garantías de dichos requerimientos tendrá el organismo. Pero es importante considerar el costo de la implementación de los requerimientos de aseguramiento, así como la factibilidad para el organismo o sus proveedores.

No existe método simple para determinar el nivel de aseguramiento, que sigue siendo más bien una elección financiera o de marketing.

El nivel de aseguramiento EAL elegido puede eventualmente aumentarse mediante otros componentes de aseguramiento.

No es necesario basarse en un EAL. El organismo también puede definir sus propios requerimientos de aseguramiento seleccionando requerimientos entre los componentes existentes o incluso definiendo otros nuevos.

Los requerimientos de seguridad de aseguramiento abarcan generalmente a la vez requerimientos por la presencia de comportamientos deseados y por la ausencia de comportamientos no deseados. Normalmente es posible demostrar, mediante el uso o el ensayo, que un comportamiento deseado se encuentra efectivamente presente.
Por el contrario, no siempre es posible efectuar una demostración concluyente de la ausencia de un comportamiento no deseado. Por esta razón, los ensayos y el análisis del diseño y de la implementación contribuyen de manera significativa a la reducción del riesgo de que un comportamiento de ese tipo se encuentre presente. Los elementos de la argumentación deben por tanto apuntalar la información de que un comportamiento no deseado de ese tipo se encuentra ausente.

Etapa 5 – Determinación de los requerimientos de seguridad

Actividad 5.1 – Determinación de los requerimientos de seguridad funcionales

Enumerar los requerimientos de seguridad funcionales

Los requerimientos de seguridad funcionales representan los medios para alcanzar los objetivos de seguridad y de tratar por lo tanto los riesgos vinculados de SSI. Deben ser determinados por el director del proyecto o conjuntamente con él (es posible utilizar los requerimientos de seguridad funcionales genéricos y el cuadro de determinación de los objetivos y requerimientos de seguridad de la guía "Herramientas para el tratamiento de los riesgos de SSI" para identificar los requerimientos de seguridad funcionales que cubren las vulnerabilidades identificadas).

Para reducir los riesgos de SSI, el siguiente cuadro presenta, a modo indicativo, los principales tipos de medidas de seguridad especificadas para los requerimientos de seguridad funcionales en función de los componentes de los riesgos:

	Componentes principales del riesgo		
Principales tipos de medidas	Vulnerabilidades	Origen de las amenazas (métodos de ataque y elementos peligrosos)	Consecuencias (elementos esenciales y impactos)
Previsión y preparación	X	X	X
Disuasión		X	
Protección	X		
Detección	X	X	
Aislamiento		X	X
"Lucha"	X		X
Recuperación			X
Restauración			X
Compensación			X

Este cuadro constituye una ayuda para la determinación de los requerimientos de seguridad funcionales. Efectivamente, permite recordar los diferentes tipos de medidas posibles.

Los requerimientos funcionales de seguridad contribuyen al tratamiento de los riesgos de SSI, que puede consistir no sólo en reducirlos, sino también en rechazarlos, transferirlos o asumirlos.
El rechazo de un riesgo se representará mediante requerimientos funcionales de seguridad que se centran en una modificación estructural de la situación del sistema evaluado de modo tal que no se encuentre más expuesto al riesgo.
La transferencia de un riesgo se representará mediante requerimientos funcionales de seguridad específicos tales como el recurso a contratos de seguro o de subcontratación.
La toma de riesgo se representará mediante la ausencia de requerimiento funcional de seguridad o la satisfacción incompleta de los objetivos de seguridad. Se identificarán entonces riesgos residuales.

Los requerimientos funcionales se imponen a las funciones del sistema evaluado que soportan especialmente la seguridad de las tecnologías de la información y que determinan el comportamiento deseado en términos de seguridad, así como al entorno del sistema evaluado.
Estos requerimientos funcionales pueden extraerse de la ISO/IEC 15408 (Criterios Comunes) o crearse completamente. Se recomienda especialmente crear completamente un requerimiento funcional sólo si se demuestra que trata un aspecto funcional no existente entre los componentes de la ISO/IEC 15408.
La lista de los requerimientos de seguridad funcionales surgidos de los Criterios Comunes se compone de clases, familias y componentes funcionales. Pueden existir relaciones de dependencia entre los componentes. Estas relaciones de dependencia aparecen cuando un componente no es autosuficiente y depende de la presencia de otro componente. Pueden existir relaciones de

dependencia entre los componentes funcionales y entre los componentes funcionales y los componentes de aseguramiento. Según el nivel de conocimiento del sistema y el nivel de pericia de los actores del grupo de trabajo, los componentes pueden no especificarse, aclarando sin embargo que serán detallados por el director de proyecto.

La ISO/IEC 1540 deja la posibilidad de recurrir a requerimientos funcionales no contenidos en la lista provista, para representar la totalidad de los requerimientos de seguridad de las tecnologías de la información. Las siguientes normas deben aplicarse a la incorporación de estos requerimientos funcionales extendidos:

- Todos los requerimientos de seguridad funcionales deben formularse refiriéndose a componentes de requerimientos funcionales. En caso de que ningún componente de requerimientos se aplique fácilmente al todo o a parte de los requerimientos de seguridad, el grupo de trabajo puede formular estos requerimientos de manera explícita sin referirse a la ISO/IEC 15408.
- Cualquier requerimiento funcional extendido debe expresarse claramente y sin ambigüedad para que la evaluación sea factible. Se deben utilizar como modelos el nivel de detalle y el modo de expresión de los componentes funcionales existentes en la ISO/IEC 15408.
- Los resultados de evaluación obtenidos utilizando los requerimientos funcionales extendidos deben mencionarlo mediante un aviso.
- La incorporación de requerimientos funcionales extendido debe realizarse conforme a las clases APE o ASE de la parte 3 de la ISO/IEC 15408, cuando sea conveniente.

En el mejor de los casos, la redacción de un requerimiento de seguridad funcional debe ser:

- S – específica (un actor, un ámbito a la vez),
- M – medible (definición del medio de control),
- A – alcanzable (eventualmente en varias etapas, indicando los recursos necesarios),
- R – realista (en función de los actores, de sus capacidades),
- T – vinculada con el tiempo (hay una fecha tope, un plazo, un período definido).

La determinación de los requerimientos de seguridad funcionales requiere tomar en cuenta todos los elementos del contexto, especialmente las restricciones presupuestarias y técnicas.

Ejemplos:

EF.INC-DETECT	*Los locales de la oficina de arquitectura deben estar equipados con un sistema de detección de incendios provisto de un informe de alarma a un supervisor que podría ser tercerizado. Estas medidas deben ser estudiadas e implementadas por expertos en ese campo. Deben ser probadas al menos una vez por año.*
EF.FOURN-ACCES	*La oficina de estudios debe estar suscrita al menos a dos proveedores de acceso a Internet distintos.*
EF.MAINTENANCE	*Un contrato de mantenimiento debe garantizar la disponibilidad de los medios de comunicación internos y externos en un plazo conforme a los requerimientos del oficio de la oficina de estudios (12 horas de falta de disponibilidad).*
EF.CHIFFREMENT	*Los intercambios de mensajes de correo electrónico deben estar protegidos en cuanto a su confidencialidad por algún sistema de encriptación disponible comercialmente. Las herramientas que utilizan claves de cifrado deben contar con una política de gestión de dichas claves.*
EF.LOCAUX	*Las personas que no pertenecen a la oficina de estudios no deben ingresar a la parte "profesional" de dicha oficina sin estar acompañados.* *El personal de mantenimiento, limpieza o cualquier otra persona no perteneciente a la oficina de estudios no debe ingresar en los locales en ausencia de los miembros de la oficina de estudios.* *Los locales deben estar protegidos mediante cerraduras de seguridad cuyas llaves sólo deberán estar en poder del Director y su adjunto.*
…	*…*

Justificar la exhaustividad de la cobertura de los objetivos de seguridad

Deberá realizarse una matriz de cobertura a fin de asegurar que todos los objetivos de seguridad centrados en el sistema evaluado o en su entorno están cubiertos por al menos un requerimiento de seguridad funcional. Del mismo modo, cada requerimiento de seguridad funcional debe cubrir como mínimo uno de dichos objetivos de seguridad.

La argumentación referida a los requerimientos de seguridad debe demostrar que la totalidad de los requerimientos de seguridad alcanza para cumplir los objetivos de seguridad y que están vinculados con estos últimos. Debe poder demostrarse que:

- la combinación de los componentes individuales de requerimientos funcionales satisface los objetivos de seguridad declarados;
- la totalidad de los requerimientos de seguridad constituye un todo con coherencia interna y cuyos elementos se apoyan mutuamente;
- el nivel de resistencia de las funciones elegido, al igual que cualquier resistencia de función explícita anunciada, es coherente con los objetivos de seguridad.

Así, una primera justificación consiste en demostrar la cobertura de los objetivos de seguridad.

La cobertura puede sintetizarse mediante un valor según la siguiente escala:

0	Ninguna cobertura
1	Cobertura parcial
2	Cobertura completa

Ejemplo:

Objetivos de seguridad	*Niveles de resistencia*	*Requerimientos de seguridad funcionales*	*Justificación de la cobertura*	*Cobertura*
O.INC-COHERENCE	*2*	*EF.INC-LUTTE*	*La coherencia de las medidas de seguridad contra incendios con el sistema informático está completamente tomada en cuenta por el requerimiento de seguridad referido a la lucha contra incendios.*	*2*
O.PABX	*1*	*EF.MAINTENANCE EF.REPRISE*	***La molestia ocasionada por un fallo operativo de la red telefónica interna (centralita averiada en el establecimiento de la oficina de estudios) se reduce gracias a estos requerimientos de seguridad, pero el siniestro puede ocurrir.***	***1***
O.TELECOM	*1*	*EF.FOURN-ACCES EF.MISES-A-JOUR EF.REPRISE*	*El mal funcionamiento de las redes externas se previene gracias al primer requerimiento de seguridad. Los dos siguientes permiten disminuir la falta de disponibilidad.*	*2*
O.ECOUTE	*2*	*EF.CHIFFREMENT*	*La encriptación satisface el objetivo de protección en términos de confidencialidad. La redacción de una política de gestión de las claves permite alcanzar el nivel de resistencia requerido.*	*2*
…	*…*	*…*	*…*	*…*

Una segunda justificación consiste en demostrar que cada requerimiento de seguridad funcional cubre al menos un objetivo de seguridad.

Ejemplo:

Requerimiento de seguridad	*O.INC-COHERENCE*	*O.INC-ORGA*	*O.PABX*	*O.TELECOM*	*O.ECOUTE*	*O.LOCAUX*	*O.PERS-SENSIB*	*O.VOL-PROTECTION*	*O.PRISE-EN-CHARGE*	*O.MANIPULATION*	*O.ORGA-SENSIB*	*O.MALICIEUX*	*O.SUPP-CONTRÔLE*	*O.SYS-COMMANDES*	*O.SYS-ACTIONS*	*O.MALADIE*	*O.PSSI*	*O.REGLEMENT*	*O.AUTH-DOC*
EF.INC-DETECT		+																	
EF.INC-LUTTE	+	+																	
EF.INC-CONSIGNES		+																	
EF.INC-ORGA		+																	
EF.MAINTENANCE			+																
EF.FOURN-ACCES				+															
EF.CHIFFREMENT					+														
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Identificar los eventuales fallos de cobertura justificándolo

Es necesario lograr un consenso sobre los medios que permitirán cumplir los objetivos de seguridad. Este consenso sólo puede obtenerse comparando los riesgos corridos con el costo de las medidas de seguridad correspondiente a los requerimientos de seguridad funcionales previstos.
Es razonable considerar en primer lugar los riesgos más importantes y los más probables, ya que el hecho de tratarlos puede desembocar ocasionalmente en el tratamiento de riesgos menos importantes.

El grupo de trabajo puede decidir no cubrir perfectamente los objetivos de seguridad mediante los requerimientos de seguridad. Es conveniente entonces indicarlo claramente y justificar debidamente esta falta de exhaustividad porque esto genera riesgos residuales para el organismo.

Ejemplos:

- *Pérdida de los medios de telecomunicaciones a causa de un fallo operativo de la red telefónica interna (centralita averiada en el establecimiento de la oficina de estudios). Un plan de recuperación y una garantía de mantenimiento dentro de las 12 horas reducen la falta de disponibilidad de estos medios.*
- *Un miembro del personal se deja manipular, aún cuando haya sido concienciado, y divulga datos a la competencia en el marco de una operación de contratación, atentando así contra la confidencialidad de informaciones sensibles (presupuestos, carpeta de litigios…).*
- *Un intruso altera el software mediante una acción sobre los programas de los recursos del sistema vía Internet, a pesar de los derechos restringidos en las máquinas conectadas, el uso de firewalls y la actualización regular de los programas. Esto puede atentar contra la confidencialidad de los datos sensibles (presupuestos, carpeta de litigios…) y contra la integridad de los elementos esenciales (cálculos de estructuras, presupuestos, planos técnicos, especificaciones técnicas, carpeta de litigios…)*

Clasificar los requerimientos de seguridad funcionales en dos categorías

Los requerimientos de seguridad resultan de la especificación detallada de los objetivos de seguridad en un conjunto:

- de requerimientos de seguridad para el sistema evaluado,
- de requerimientos de seguridad para el entorno.

Si se satisfacen, garantizarán que el objetivo del estudio de seguridad puede satisfacer estos objetivos de seguridad.

Justificar eventualmente la cobertura de las dependencias de los requerimientos de seguridad funcionales

Deben satisfacerse todas las dependencias entre los requerimientos de seguridad. Existen, efectivamente, requerimientos de seguridad que implican, por razones de coherencia, la existencia de otros requerimientos de seguridad. Las dependencias pueden satisfacerse incluyendo el componente funcional involucrado en los requerimientos funcionales de seguridad del sistema evaluado o como requerimiento de su entorno.
La falta de satisfacción de una dependencia debe justificarse rigurosamente.

Actividad 5.2 – Determinación de los requerimientos de seguridad de aseguramiento

Enumerar los requerimientos de seguridad de aseguramiento

Los requerimientos de seguridad de aseguramiento de la ISO/IEC 15408 se imponen a las acciones del desarrollador, a los elementos de prueba de productos y a las acciones del evaluador (ejemplo: restricciones sobre el rigor del proceso de desarrollo y requerimientos para encontrar y analizar el impacto de las vulnerabilidades de seguridad potenciales).

El aseguramiento de que los objetivos de seguridad se alcanzan gracias a las funciones de seguridad seleccionadas proviene de los dos factores siguientes:

- la confianza en la conformidad de la implementación de las funciones de seguridad, es decir, la estimación de que han sido correctamente implementadas;
- la confianza en la eficacia de las funciones de seguridad, es decir, la estimación de que satisfacen efectivamente los objetivos de seguridad expresados.

Los requerimientos de seguridad de aseguramiento pueden reformularse según la finalidad del estudio a fin de hacer su descripción más accesible para los actores involucrados en el estudio.

Ejemplo de una descripción en blanco:

ACM_CAP.1 *Números de la versión*

Objetivos:

Se exige una referencia única para garantizar que no haya ambigüedad en el ejemplar de la TOE evaluado. La identificación de la TOE por su referencia garantiza que los usuarios de la TOE sean capaces de saber qué ejemplar de la TOE utilizan.

Dependencias:

Ninguna dependencia.

Tareas del desarrollador:

ACM_CAP.1.1D El desarrollador debe aportar una referencia para la TOE.

Contenido y presentación de los elementos de prueba:

ACM_CAP.1.1C La referencia de la TOE debe ser única para cada versión de la TOE.

ACM_CAP.1.2C La TOE debe estar identificada por su referencia.

Tareas del evaluador:

ACM_CAP.1.1E El evaluador debe confirmar que las informaciones provistas satisfacen todos los requerimientos referidos al contenido y a la presentación de los elementos de prueba.

Ejemplo de la descripción reformulada:

EA.NUM-VERSION *La oficina de estudios debe disponer de una referencia única (o equivalente, número de versión por ejemplo) de cada versión de las*

entidades del sistema evaluado. Esta referencia las identifica.

Clasificar eventualmente los requerimientos de seguridad de aseguramiento en dos categorías

Los requerimientos de seguridad de aseguramiento pueden pertenecer a una de las siguientes categorías:

- requerimientos de seguridad de aseguramiento centrados en el sistema evaluado,
- requerimientos de seguridad de aseguramiento centrados en el entorno del sistema evaluado.

Justificar eventualmente la cobertura de las dependencias de los requerimientos de aseguramiento

Los requerimientos de seguridad de aseguramiento pueden depender de otros requerimientos que es conveniente tomar en cuanta para que todo el conjunto sea coherente.
Debe demostrarse que la cobertura es completa.
La falta de satisfacción de una dependencia debe justificarse rigurosamente.

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