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 2
PROCEDIMIENTO

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 de 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 esenciales al Estudio del sistema evaluado. - 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 funcionamiento en las hipótesis. - Adaptación de los conceptos a la ISO/IEC 15408: se estudia el origen de las amenazas, es decir, los métodos de ataque y elementos peligrosos, así como sus características, que pueden incluir un tipo (natural, humano, ambiental), una causa (accidental, deliberada, afinando: en exposición, recursos disponibles, pericia, motivación), un potencial de ataque. - Identificación de los métodos de ataque no considerados. - Formalización de las amenazas, según la orientación de la ISO/IEC 15408 (elemento peligroso, ataque y bien, en forma de entidades), antes de la confrontación con las necesidades de seguridad. - Modificación de la confrontación de las amenazas con las necesidades, que permite identificar los riesgos. - Identificación de los riesgos no considerados. - Integración de la determinación de los objetivos de seguridad mínimos en las actividades de formalización de los objetivos de seguridad, y determinación de los requerimientos funcionales. - Modificación de la determinación de los objetivos de seguridad, que toma en cuenta las hipótesis, las normas de la política de seguridad, las 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 determinación de los requerimientos de seguridad de 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

Índice de ilustraciones

Introducción

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

- Sección 1 – Introducción
  Esta sección presenta el contexto, el interés y la disposición del procedimiento EBIOS. También contiene una bibliografía, un glosario y presenta 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 segunda sección del método. Presenta el procedimiento metodológico en forma de fichas descriptivas.

Cada etapa es objeto de una descripción, de un esquema que la sitúa en el procedimiento EBIOS completo y de un cuadro sinóptico que describe las actividades de dicha etapa.

Cada actividad se describe según el siguiente formalismo.

DESCRIPCIÓN
Resumen del procedimiento metodológico y esquema que permite situar la actividad en el seno de la etapa.

PREVIAS
Previamente a la actividad se deben realizar otras actividades.

DATOS DE ENTRADA
Datos necesarios para la puesta en marcha de la actividad.

ACCIONES
Acciones que se deben realizar con el fin de llevar a cabo la actividad.

DATOS DE SALIDA
Datos producidos por las acciones de la actividad.

CONSEJOS PRÁCTICOS
Comentarios y consejos necesarios para la puesta en marcha de la actividad.

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

Presentación del procedimiento

El método formaliza un procedimiento de apreciación y de tratamiento de los riesgos en el ámbito de la seguridad de los sistemas de información.

Se aplica a los sistemas que se van a diseñar y a los sistemas existentes, en el perímetro general del sistema de información o en un perímetro particular de éste.

Se divide en cinco etapas representadas en la siguiente ilustración:

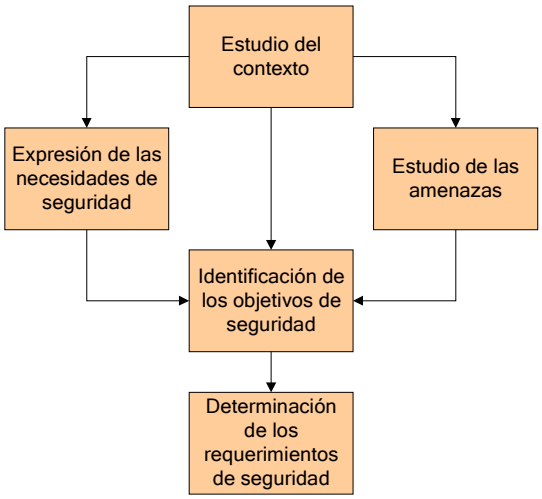
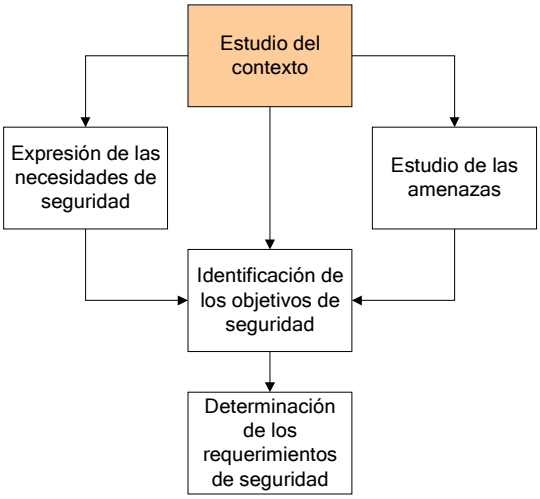


Figura 1 – Procedimiento EBIOS general

- Al terminar la primera etapa, se conoce perfectamente el entorno, el objetivo y el funcionamiento del sistema estudiado, se identifican los elementos esenciales y las entidades en las cuales se basan.
- La segunda etapa contribuye a la apreciación de los riesgos (estimación de los riesgos y definición de los criterios de riesgos). Permite formalizar los impactos y evaluar las necesidades de seguridad de los elementos esenciales en términos de disponibilidad, de integridad, de confidencialidad…
- La tercera etapa se inscribe también en el marco de la apreciación de los riesgos (análisis de los riesgos). Consiste en enumerar y en describir las amenazas que recaen sobre el sistema. Para esto se estudian los métodos de ataque y los elementos peligrosos susceptibles de utilizarlos, las vulnerabilidades aprovechables de las entidades y sus posibilidades.
- La cuarta etapa contribuye a la evaluación y al tratamiento de los riesgos. Permite formalizar los riesgos reales que recaen sobre el sistema confrontando las amenazas (hechos negativos) con las necesidades de seguridad (consecuencias). Están cubiertos por objetivos de seguridad, en coherencia con las hipótesis, las normas de seguridad, las referencias reglamentarias, el modo de funcionamiento y las restricciones identificadas que constituyen el pliego de condiciones de seguridad.
- La quinta y última etapa se inscribe en el marco del tratamiento de los riesgos. Explica cómo determinar los requerimientos funcionales que permiten realizar los objetivos de seguridad y los requerimientos de aseguramiento que permiten aumentar la confianza sobre su realización.

Etapa 1 – Estudio del contexto

Esta etapa fundamental tiene por objeto identificar globalmente el sistema evaluado y situarlo en su entorno para determinar con precisión el objeto del estudio de seguridad.



Permite especialmente especificar para el sistema los retos, el contexto de utilización, las misiones o servicios que debe prestar y los medios utilizados para esto. También permite reunir todos los datos necesarias para la planificación del estudio.

Al terminar esta etapa, se delimita claramente el campo de investigación del estudio, se enumeran las hipótesis, las obligaciones y las restricciones y se conocen los temas que se van a tratar.

La etapa se divide en tres actividades:

- Estudio del organismo
- Estudio del sistema evaluado
- Determinación del objeto del estudio de seguridad

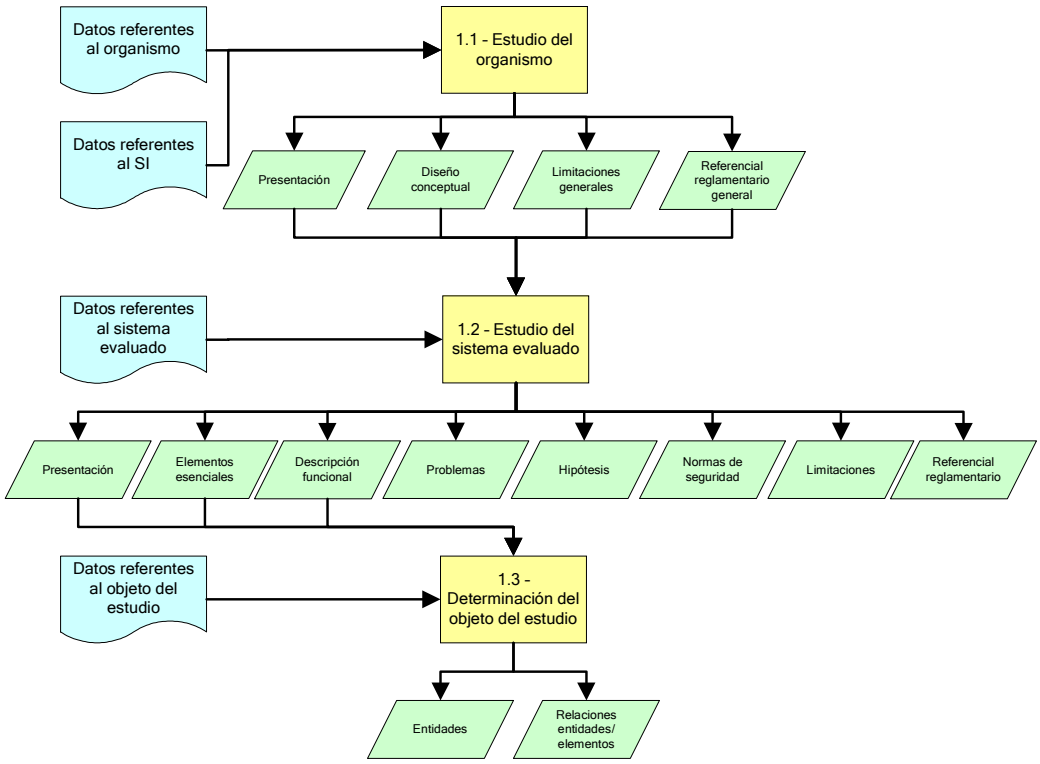
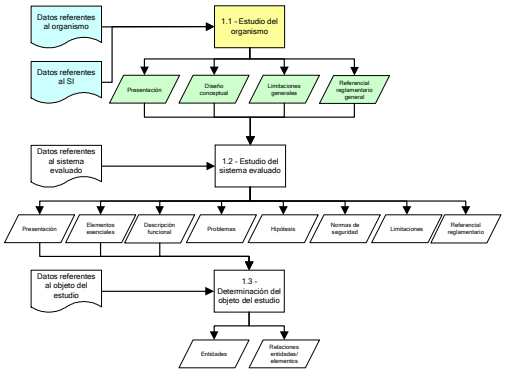


Figura 2 – Cuadro sinóptico detallado del estudio del contexto

Actividad 1.1 – Estudio del organismo



DESCRIPCIÓN

Esta actividad consiste en definir el marco del estudio. Se deben reunir datos generales sobre el organismo concerniente para el proyecto de seguridad con el fin de apreciar mejor su naturaleza; su organización y las restricciones que recaen sobre éste. También es necesario obtener una visión general del sistema de información del organismo. Dichos elementos permitirán para este organismo, precisar en las siguientes actividades los retos del sistema evaluado y monitorear la coherencia de los objetivos y de los requerimientos de seguridad con sus misiones.

PREVIAS

Sin objeto

DATOS DE ENTRADA

- Datos referentes al organismo y a su sistema de información (documentos estratégicos, documentos referentes a las misiones, las atribuciones y la organización, documentos referentes al sistema de información, síntesis de entrevistas con los responsables del organismo).

ACCIONES

- Presentar el organismo.
- Enumerar las restricciones que recaen sobre el organismo.
- Enumerar las referencias reglamentarias que se aplican al organismo.
- Hacer una descripción funcional del SI general.

DATOS DE SALIDA

- Presentación del organismo.
- Lista de las restricciones que recaen sobre el organismo.
- Lista de las referencias reglamentarias generales que se aplican al organismo.
- Diseño conceptual del sistema de información.

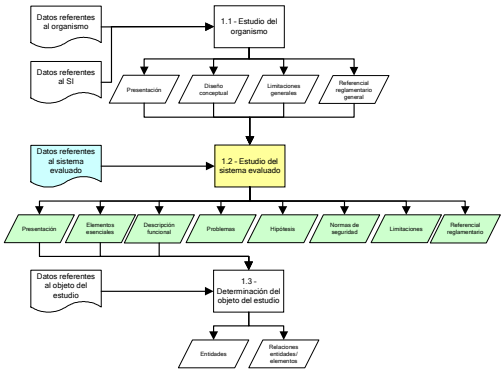
CONSEJOS PRÁCTICOS

- Esta primera actividad es fundamental para la continuación del estudio, ya que permite comprender mejor el contexto del estudio.
- Se debe constituir un grupo de trabajo (o comité de conducción), se deben identificar las personas que se van a encontrar y se deben planificar entrevistas.
- Una primera entrevista debe permitir verificar la naturaleza del reto inicialmente planteado y si éste le corresponde al equipo constituido. En dicha entrevista se debe poder obtener el máximo de información.
- Será conveniente juzgar la posibilidad de abordar tal o cual tema propuesto, en función de la extensión del proyecto, de los primeros elementos recogidos antes de la entrevista, de las responsabilidades del interlocutor…
- El estudio del organismo debe incluir la parte de toma de decisiones de éste al más alto nivel jerárquico.
- Los datos se obtienen de los responsables operativos involucrados en el estudio.
- Los cuestionarios permiten preparar las entrevistas que guiarán a las personas interrogadas con el fin de formalizar las respuestas.

Actividad 1.2 – Estudio del sistema evaluado

DESCRIPCIÓN

Esta actividad tiene por objeto precisar el contexto de utilización del sistema que se va a diseñar o que ya existe. Para esto es necesario precisar el subconjunto del sistema de información del organismo que constituye el sistema evaluado del estudio y sus retos. Se describe entonces el sistema evaluado y se enumeran las hipótesis, las normas de seguridad y sus restricciones.



PREVIAS

- Actividad 1.1.

DATOS DE ENTRADA

- Datos referentes al sistema evaluado.
- Presentación del organismo.
- Lista de las restricciones generales que recaen sobre el organismo.
- Lista de las referencias reglamentarias generales que se aplican al organismo.
- Diseño conceptual del sistema de información.

ACCIONES

- Presentar el sistema evaluado.
- Enumerar los retos.
- Enumerar los elementos esenciales.
- Hacer una descripción funcional del sistema evaluado.
- Enumerar las hipótesis.
- Enumerar las normas de seguridad.
- Enumerar las restricciones que recaen sobre el sistema evaluado.
- Enumerar las referencias reglamentarias específicas al sistema evaluado.

DATOS DE SALIDA

- Presentación del sistema evaluado.
- Lista de los elementos esenciales.
- Descripción funcional del sistema evaluado.
- Lista de los retos del sistema evaluado.
- Lista de las hipótesis.
- Lista de las normas de seguridad.
- Lista de los retos específicos del sistema evaluado.
- Lista de las referencias reglamentarias específicas al sistema evaluado.

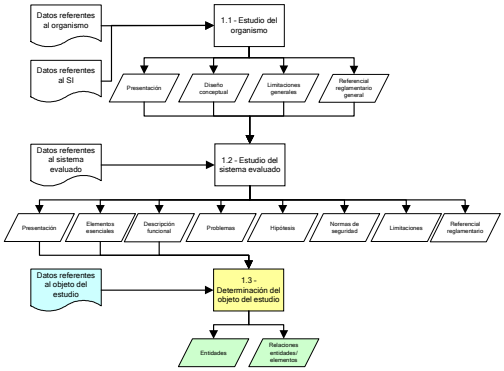
CONSEJOS PRÁCTICOS

- La cantidad y la granularidad de los elementos esenciales dependerán de la finalidad del estudio y de la naturaleza del sistema evaluado. En efecto, el estudio de un sistema de información global que pretenda obtener una visión general de los riesgos no requerirá el mismo nivel de detalle que el estudio de un sistema concreto que deba ser homologado formalmente.
- La ausencia de especificaciones del sistema puede detener la continuación del estudio de seguridad. Efectivamente, es poco útil brindar seguridad a un sistema que no se conoce bien. Por el contrario, puede ser interesante realizar un estudio rápido, general, que luego deberá ajustarse a medida que se enriquezcan las especificaciones.
- La división en subsistemas podrá considerarse cuando se trate de sistemas complejos. En ese caso, convendrá realizar varios estudios en paralelo.

Actividad 1.3 - Determinación del objeto del estudio de seguridad

DESCRIPCIÓN

Esta actividad tiene por objeto la determinación precisa de las entidades en las cuales se apoyan los elementos esenciales del sistema evaluado (funciones y datos). La actividad consiste en enumerar y describir las diferentes entidades ya sean de tipo hardware, software, red, personal, sitio u organización. Se trata también de catalogar los elementos esenciales que se apoyan en cada una de estas entidades.



PREVIAS

- Actividad 1.2.

DATOS DE ENTRADA

- Datos referentes al objeto del estudio de seguridad.
- Presentación del sistema evaluado.
- Lista de los elementos esenciales.
- Descripción funcional del sistema evaluado.

ACCIONES

- Enumerar y describir las entidades del sistema.
- Relacionar los elementos esenciales y las entidades.

DATOS DE SALIDA

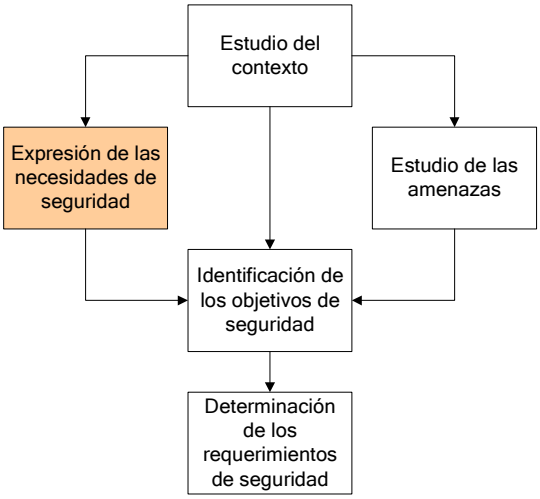
- Lista de las entidades.
- Cuadros entidades/elementos.

CONSEJOS PRÁCTICOS

- Se aconseja utilizar los tipos y subtipos de entidades que se describen en la guía “Herramientas para la apreciación de los riesgos SSI” para enumerar y describir las entidades del sistema.
- Es importante no olvidarse de identificar una entidad de tipo organización (al igual que una entidad de tipo sitio) en caso de que el sistema evaluado se base únicamente en la organización (un solo sitio). En efecto, a menudo para muchos sistemas evaluados, algunas entidades son únicas pero igualmente es necesario enumerarlas ya que poseen vulnerabilidades que habrá que tomar en cuenta en la continuación del estudio. Generalmente encontramos al menos una entidad de cada tipo.
- Es posible incorporar a la descripción funcional las entidades en las cuales se basa el sistema evaluado superponiéndolas a los esquemas. Esto permite visualizar mejor y comprender el sistema.

Etapa 2 – Expresión de las necesidades de seguridad

Esta etapa contribuye a la estimación de los riesgos y a la definición de los criterios de riesgos. Permite a los usuarios del sistema expresar sus necesidades en materia de seguridad para las funciones y datos que éstos manipulen.



La expresión de las necesidades de seguridad resulta de los requerimientos operativos del sistema, independientemente de cualquier solución técnica.

Se basa en la elaboración y utilización de una escala de necesidades y en la identificación de los impactos inaceptables para el organismo.

La expresión de las necesidades permite definir también el modo de explotación del sistema, es decir, la manera general de administrar los usuarios del sistema.

La etapa se divide en dos actividades:

- Realización de las fichas de necesidades.
- Síntesis de las necesidades de seguridad.

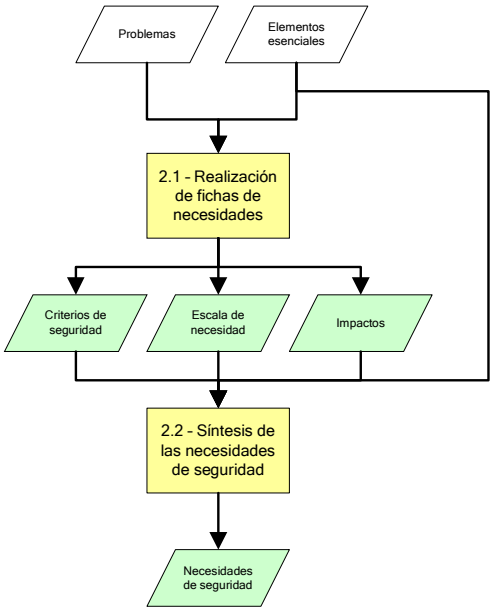
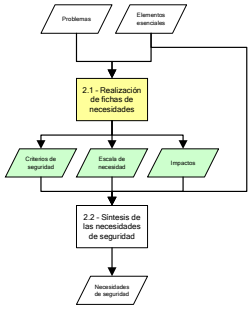


Figura 3 – Cuadro sinóptico de la expresión de las necesidades de seguridad

Actividad 2.1 – Realización de las fichas de necesidades



DESCRIPCIÓN

Esta actividad tiene como finalidad crear los cuadros necesarios para la expresión de las necesidades de seguridad por parte de los usuarios. Dichos cuadros permitirán expresar las necesidades de seguridad de los elementos que manipulan habitualmente los usuarios en el marco de su actividad, en forma objetiva y coherente. Se trata de una actividad que contribuye a la estimación de los riesgos y a la definición de los criterios de riesgos en el proceso de gestión de riesgos.

PREVIAS

- Actividad 1.2.

DATOS DE ENTRADA

- Lista de los retos del sistema evaluado.
- Lista de los elementos esenciales.

ACCIONES

- Elegir los criterios de seguridad que se van a tomar en cuenta.
- Determinar la escala de necesidades.
- Determinar los impactos pertinentes.

DATOS DE SALIDA

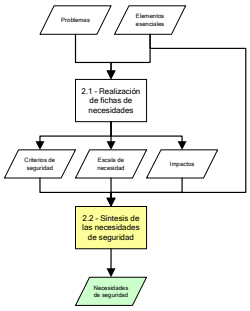
- Lista de los criterios de seguridad.
- Escala de necesidades.
- Lista de impactos.

CONSEJOS PRÁCTICOS

- La escala de necesidades es uno de los instrumentos de discusión más importante del estudio. Debe ser determinada por el grupo de trabajo y servirá no sólo a las discusiones sobre el tema de las necesidades de seguridad sino también a las discusiones referentes a los objetivos de seguridad.
- La escala de necesidades debe ser objetiva y coherente. Ésta incluirá ponderaciones y valores de referencia y se basará en la lista de criterios de seguridad que se van a considerar y en una lista de impactos con ejemplos representativos.
- Para los impactos, una representación bajo la forma de un árbol de causas permitirá presentar mejor la idea al grupo de trabajo.
- Con el fin de determinar sus necesidades de seguridad, se realizará una ficha para cada elemento esencial y por persona interrogada. La creación de una ficha por función o subfunción se justifica en la medida que las necesidades de seguridad de una función no se deducen directamente de los datos que ésta procesa. Ejemplos:
  - Una función puede ser confidencial, no por el hecho de que manipule datos confidenciales sino únicamente por la naturaleza del proceso que realiza.
  - El acceso a un servicio puede no requerir una fuerte disponibilidad; por el contrario, el funcionamiento de éste puede requerir la disponibilidad máxima de los datos que utiliza.

Actividad 2.2 – Síntesis de las necesidades de seguridad

DESCRIPCIÓN



Esta actividad tiene como finalidad asignar a los elementos esenciales sus necesidades de seguridad que resultan de la síntesis de los valores que se atribuyen a los usuarios. Al terminar esta actividad será posible disponer de una visión objetiva y coherente de las necesidades de seguridad del sistema evaluado. Se trata de una actividad que contribuye a la evaluación de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividad 2.1.

DATOS DE ENTRADA

- Lista de los elementos esenciales.
- Lista de criterios de seguridad.
- Escala de necesidades.
- Lista de impactos.

ACCIONES

- Atribuir una necesidad de seguridad por criterio de seguridad (disponibilidad, integridad, confidencialidad…) a cada elemento esencial.

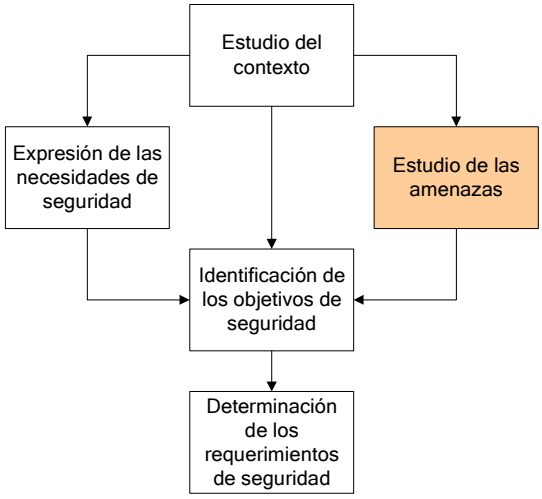
DATOS DE SALIDA

- Ficha de síntesis de las necesidades de seguridad.

CONSEJOS PRÁCTICOS

- La atribución de necesidades de seguridad a los elementos esenciales representa el límite aceptable para el organismo.
- La estimación de las necesidades de seguridad representa la visión del sistema que puede tener un usuario, es importante que éste justifique los valores extremos de su punto de vista para efectuar luego una síntesis coherente a nivel del organismo.
- En la medida de lo posible, todas las necesidades de seguridad deben estar justificadas.
- Los usuarios considerados para la apreciación de las necesidades de seguridad deben ser representativos respecto de la utilización del sistema. Por lo tanto, deben expresarse en elementos que utilicen habitualmente.
- Es posible incorporar a la descripción funcional las necesidades de seguridad de cada uno de los elementos esenciales superponiéndolas a los esquemas. Esto permite comprender mejor las eventuales dependencias entre los valores de las necesidades de seguridad. En efecto, a veces las necesidades de seguridad de las funciones y de los datos están vinculadas, así como las funciones entre sí y los datos entre sí. Pueden propagarse desde el momento en que los elementos estén vinculados.

Etapa 3 – Estudio de las amenazas



Esta etapa contribuye a la apreciación de los riesgos. Tiene como objetivo la determinación de las amenazas que recaen sobre el sistema.

Dichas amenazas están formalizadas identificando sus componentes: los métodos de ataque a los cuales se expone el organismo, los elementos peligrosos que pueden utilizarlos, las vulnerabilidades aprovechables de las entidades del sistema y su nivel.

Las amenazas identificadas a través de esta etapa son específicas del sistema. Su caracterización es independiente de las necesidades de seguridad, de los datos procesados y de las funciones que soporta el sistema.

El estudio de las amenazas abarca tres actividades:

- Estudio de los orígenes de las amenazas.
- Estudio de las vulnerabilidades.
- Formalización de las amenazas.

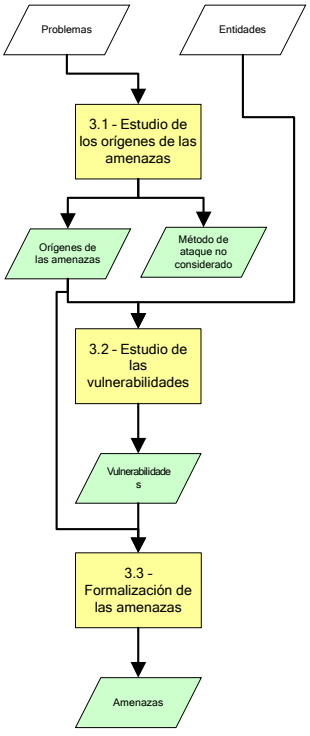
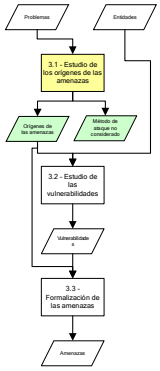


Figura 4 – Cuadro sinóptico detallado del estudio de las amenazas

Actividad 3.1 – Estudio de los orígenes de las amenazas

DESCRIPCIÓN



Esta actividad tiene como finalidad seleccionar los métodos de ataque que son pertinentes para el sistema evaluado. Cada uno de estos métodos de ataque está caracterizado por los criterios de seguridad que puede afectar (disponibilidad, integridad, confidencialidad…). Está asociado a elementos peligrosos. Dichos elementos peligrosos pueden caracterizarse por su tipo (natural, humano o ambiental) y por sus posibles causas (accidental o deliberada). Esta caracterización puede ser sintetizada bajo la forma de un potencial ataque. Si los métodos de ataque constituyen riesgos reales para el sistema evaluado, el nivel de medidas de seguridad deberá ser coherente con dicho ataque potencial. Esta actividad corresponde a la identificación de los orígenes en el proceso de gestión de los riesgos.

PREVIAS

- Actividad 1.2.

DATOS DE ENTRADA

- Lista de los retos del sistema evaluado.

ACCIONES

- Enumerar los métodos de ataque pertinentes.
- Caracterizar los métodos de ataque por los criterios de seguridad que pueden afectar.
- Caracterizar, para cada método de ataque considerado, los elementos peligrosos vinculados por su tipo (natural, humano o ambiental) y su causa (accidental o deliberada).
- Incorporar un valor representativo del potencial de ataque del elemento peligroso.
- Identificar los métodos de ataque no considerados justificándolo.

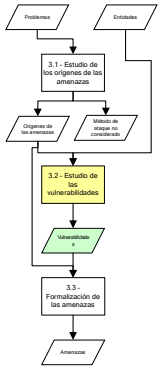
DATOS DE SALIDA

- Lista de los orígenes de las amenazas (métodos de ataque y elementos peligrosos).
- Lista de métodos de ataque no considerados y justificaciones.

CONSEJOS PRÁCTICOS

- Se aconseja utilizar los métodos de ataque y los elementos peligrosos genéricos que se describen en la guía “Herramientas para la apreciación de los riesgos SSI” para enumerar y caracterizar los métodos de ataque pertinentes y los elementos peligrosos.
- Los métodos de ataque son identificados por un experto en seguridad ante el responsable del sistema involucrado o ante las misiones consideradas.
- Las justificaciones que permiten seleccionarlas o rechazarlas deben estar claramente expresadas.
- La caracterización de los elementos peligrosos debería expresarse también como un valor representativo del potencial de ataque, lo que va a facilitar la determinación de la resistencia de los mecanismos para los objetivos y requerimientos de seguridad.

Actividad 3.2 – Estudio de las vulnerabilidades



DESCRIPCIÓN

Esta actividad tiene por objeto la determinación de las vulnerabilidades específicas del sistema evaluado y eventualmente la caracterización de éstas en términos de nivel. Estas vulnerabilidades intrínsecas al sistema evaluado provienen de las características de las entidades que lo componen. Dichas vulnerabilidades son utilizadas para afectar la seguridad del sistema, por lo tanto, los objetivos de seguridad consistirán esencialmente en disminuirlas. Esta actividad contribuye a la estimación de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividades 1.3 y 3.1.

DATOS DE ENTRADA

- Lista de las entidades.
- Lista de los orígenes de las amenazas (métodos de ataque y elementos peligrosos).

ACCIONES

- Identificar las vulnerabilidades de las entidades según los métodos de ataque.
- Estimar eventualmente el nivel de las vulnerabilidades.

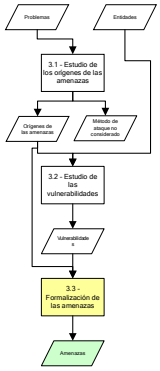
DATOS DE SALIDA

- Lista de las vulnerabilidades consideradas y de su nivel.

CONSEJOS PRÁCTICOS

- Se aconseja utilizar las vulnerabilidades genéricas que se describen en la guía “Herramientas para la apreciación de los riesgos SSI” para identificar las vulnerabilidades de las entidades según los métodos de ataque.
- El estudio de las vulnerabilidades se efectúa con los mismos responsables que actúan en el estudio de los orígenes de las amenazas.
- Es necesario observar que si por el hecho de su carácter genérico, la lista de los métodos de ataque propuesta puede pretender la exhaustividad, la de las vulnerabilidades es variable por naturaleza y debe ser personalizada.

Actividad 3.3 – Formalización de las amenazas



DESCRIPCIÓN

Esta actividad tiene como finalidad determinar las amenazas que puedan afectar al sistema evaluado. Resultan de la asociación de los métodos de ataque (utilizados por elementos peligrosos identificados) con las vulnerabilidades consideradas (que se basan en entidades identificadas). Al terminar esta actividad será posible disponer de una visión objetiva y exhaustiva de las amenazas reales que pesan sobre el sistema evaluado. Esta actividad contribuye a la estimación de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividades 3.1 y 3.2.

DATOS DE ENTRADA

- Lista de los orígenes de las amenazas (métodos de ataque y elementos peligrosos).
- Lista de las vulnerabilidades consideradas y de su nivel.

ACCIONES

- Formular explícitamente las amenazas.
- Jerarquizar eventualmente las amenazas según su posibilidad.

DATOS DE SALIDA

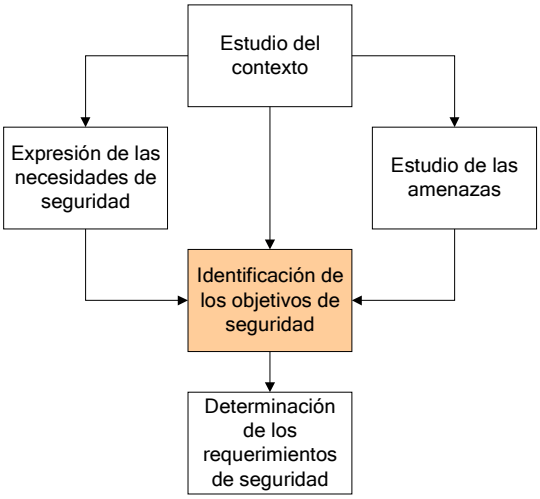
- Lista de las amenazas consideradas.

CONSEJOS PRÁCTICOS

- La formalización de las amenazas debe ser lo más precisa posible y debe permitir identificar el método de ataque, el elemento peligroso, la o las vulnerabilidades aprovechadas así como las entidades concernientes.
- Las amenazas pueden caracterizarse según su posibilidad. Esta se determina según el nivel de las vulnerabilidades aprovechadas por los elementos peligrosos.

Etapa 4 – Identificación de los objetivos de seguridad

Esta etapa tiene como objetivo evaluar y tratar los riesgos que recaen sobre el sistema.



La confrontación de las amenazas con las necesidades de seguridad permite identificar los riesgos que van a ser cubiertos mediante los objetivos de seguridad. Dichos objetivos constituyen el pliego de condiciones de seguridad del sistema evaluado y de su entorno. Estos deben ser coherentes con el conjunto de las hipótesis, de las restricciones, de las referencias reglamentarias y con las normas de seguridad identificadas durante el estudio.

Durante esta etapa, se debe determinar también el nivel de los objetivos de seguridad y el nivel de aseguramiento.

La etapa abarca tres actividades:

- Confrontación de las amenazas con las necesidades.
- Formalización de los objetivos de seguridad.
- Determinación de los niveles de seguridad.

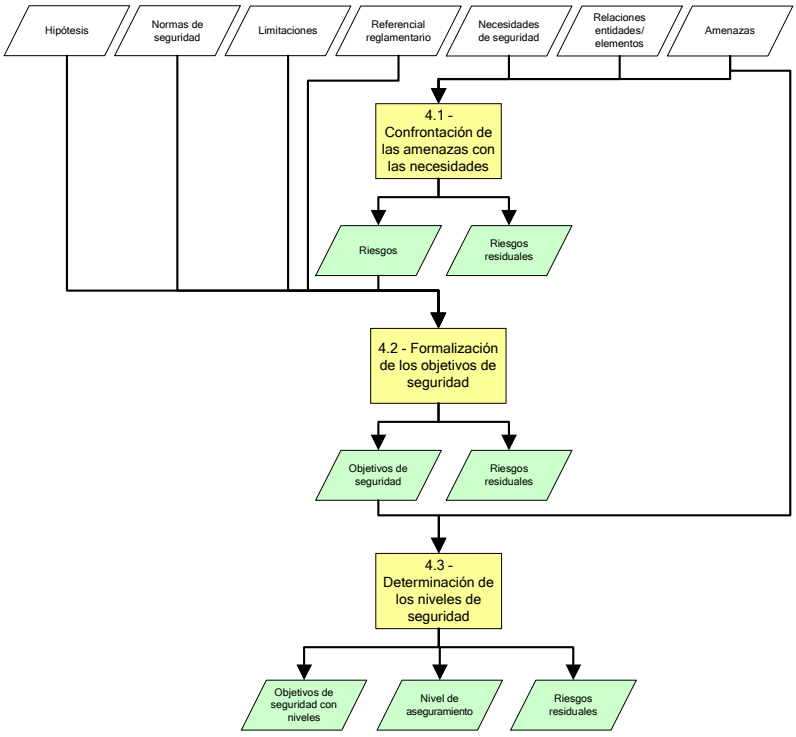
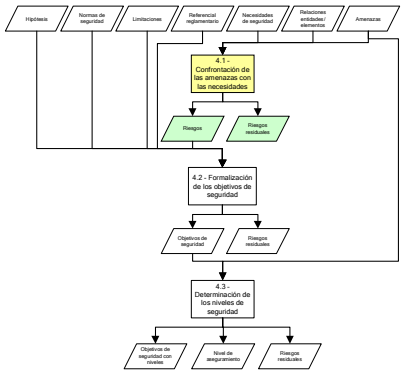


Figura 5 – Cuadro sinóptico detallado de la identificación de los objetivos de seguridad

Actividad 4.1 – Confrontación de las amenazas con las necesidades



DESCRIPCIÓN

Esta actividad tiene como finalidad determinar los riesgos reales que recaen sobre el sistema evaluado. La confrontación de las amenazas con las necesidades de seguridad permite seleccionar y jerarquizar los riesgos que son verdaderamente susceptibles de dañar los elementos esenciales. El conjunto de dichos riesgos deberá ser evaluado, la mayoría de ellos deben ser cubiertos por objetivos de seguridad. Esta actividad contribuye a la evaluación de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividades 1.3, 2.2 y 3.3.

DATOS DE ENTRADA

- Cuadros entidades/elementos.
- Ficha de síntesis de las necesidades de seguridad.
- Lista de las amenazas consideradas.

ACCIONES

- Determinar los riesgos confrontando amenazas y necesidades de seguridad.
- Formular explícitamente los riesgos.
- Jerarquizar los riesgos según el impacto sobre los elementos esenciales y la posibilidad de las amenazas.
- Identificar los riesgos no considerados (riesgos residuales) justificadamente.

DATOS DE SALIDA

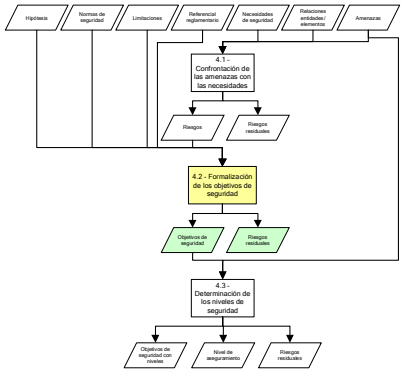
- Lista jerarquizada de los riesgos.
- Lista de los riesgos residuales (fallos de cobertura de los riesgos) y justificaciones.

CONSEJOS PRÁCTICOS

- Cuanto más precisa es la formulación de un riesgo, más fácil será para el lector comprender el riesgo y para las personas que realizan el estudio, identificar los objetivos de seguridad precisos y concretos. En efecto, el riesgo tiene un carácter específico al sistema evaluado. De este modo, lo que abarca un riesgo es el elemento peligroso, las vulnerabilidades aprovechadas, las entidades sobre las cuales se basan, los elementos esenciales que pueden verse afectados y las consecuencias posibles en términos de necesidades de seguridad y de impactos.
- Son los usuarios y los responsables del sistema quienes deben jerarquizar los riesgos y no las personas que realizan el estudio. Sin embargo será posible facilitar esta tarea con ayuda del estudio. Por ejemplo, los valores máximos de las necesidades de seguridad que pueden ser afectadas por los riesgos y la posibilidad de las amenazas permiten juzgar la importancia de los riesgos.
- La clasificación de los riesgos permite la determinación de las prioridades en la elección y la puesta en marcha de contra-medidas.

Actividad 4.2 – Formalización de los objetivos de seguridad

DESCRIPCIÓN



Esta actividad tiene por objeto determinar los objetivos de seguridad que permiten cubrir los riesgos, conforme a la determinación de los niveles de seguridad. La exhaustividad de la cobertura del conjunto de los riesgos por parte de los objetivos de seguridad deberá ser demostrada tomando en cuenta las hipótesis, las normas de seguridad y las restricciones. Esta actividad contribuye al tratamiento de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividades 1.1, 1.2, 2,4 y 4.1.

DATOS DE ENTRADA

- Lista de las hipótesis.
- Lista de las normas de seguridad.
- Lista de las restricciones.
- Lista de las referencias reglamentarias.
- Elección del modo de explotación de seguridad.
- Lista jerarquizada de los riesgos.

ACCIONES

- Enumerar los objetivos de seguridad.
- Justificar la exhaustividad de la cobertura, verificando la compatibilidad con las restricciones que recaen sobre el organismo y el sistema evaluado:
  - riesgos,
  - hipótesis (y los retos),
  - normas de seguridad (y las referencias reglamentarias).
- Clasificar eventualmente los objetivos de seguridad en dos categorías:
  - objetivos de seguridad referentes al sistema evaluado,
  - objetivos de seguridad referentes al entorno del sistema evaluado.
- Identificar los riesgos no considerados (riesgos residuales) justificadamente.

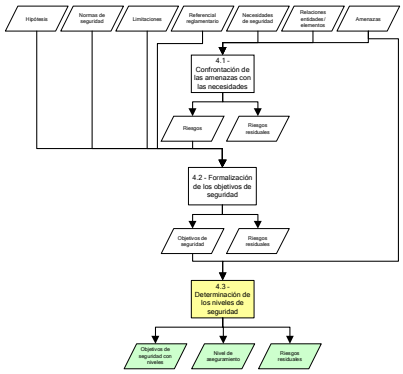
DATOS DE SALIDA

- Lista de los objetivos de seguridad.
- Lista de los riesgos residuales (falta de cobertura mediante los objetivos de seguridad) y justificación.

CONSEJOS PRÁCTICOS

- 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 SSI” para enumerar los objetivos de seguridad que cubren las vulnerabilidades.
- Los objetivos de seguridad podrán constituir un pliego de condiciones de seguridad abierto en términos de soluciones de seguridad que permitan cubrir los riesgos.

Actividad 4.3 – Determinación de los niveles de seguridad



DESCRIPCIÓN

Esta actividad tiene por objeto determinar el nivel de resistencia adecuado para los objetivos de seguridad. También permite elegir el nivel de los requerimientos de seguridad de aseguramiento. Esta actividad contribuye al tratamiento de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividades 3.3 y 4.2.

DATOS DE ENTRADA

- Lista de los objetivos de seguridad.
- Lista de las amenazas consideradas.

ACCIONES

- Para cada objetivo de seguridad determinar el nivel de resistencia adecuado.
- Elegir el nivel de los requerimientos de aseguramiento.

DATOS DE SALIDA

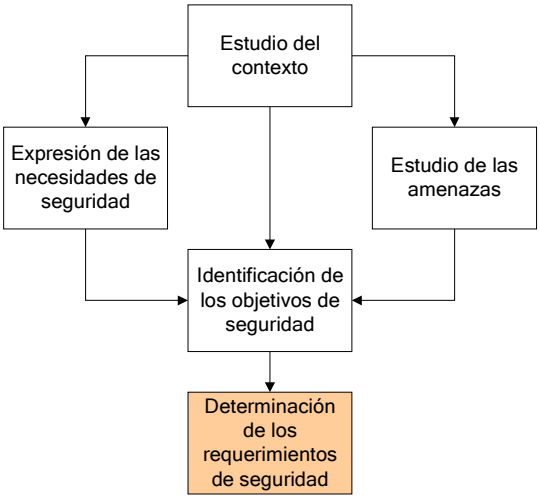
- Lista de los objetivos de seguridad con el nivel de resistencia.
- Lista de los riesgos residuales (fallo de cobertura del nivel de resistencia mediante los objetivos de seguridad) y justificaciones.
- Elección del nivel de los requerimientos de aseguramiento.

CONSEJOS PRÁCTICOS

- El potencial de ataque de los elementos peligrosos permite determinar el nivel de resistencia adecuado de los objetivos de seguridad. Este nivel depende de varios factores entre los cuales están el potencial de ataque, las restricciones, las necesidades de seguridad y la posibilidad de la amenaza.

Etapa 5 – Determinación de los requerimientos de seguridad

La finalidad de esta etapa es determinar cómo realizar los objetivos de seguridad, es decir cómo tratar los riesgos que actúan sobre el sistema.



Para esto se determinan:

- Los requerimientos de seguridad funcionales describen el comportamiento de seguridad esperado y están destinados a satisfacer los objetivos de seguridad tales como fueron formulados en la etapa anterior.
- Los requerimientos de seguridad de aseguramiento que constituyen la base de la confianza en el hecho que el producto o el sistema satisfaga sus objetivos de seguridad.

Dichos requerimientos se establecen, particularmente, a partir de componentes funcionales y de aseguramiento propuestos por la [ISO 15408] (Criterios Comunes).

La cobertura de los objetivos de seguridad por parte de los requerimientos funcionales y de aseguramiento debe justificarse bajo la forma de argumentación, indicando la necesidad y la suficiencia de estas últimos.

Esta etapa abarca dos actividades principales:

- Determinación de los requerimientos de seguridad funcionales.
- Determinación de los requerimientos de seguridad de aseguramiento.

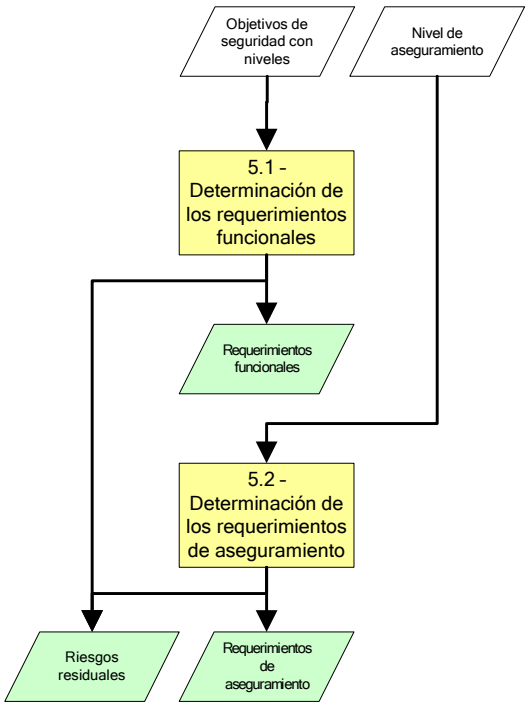
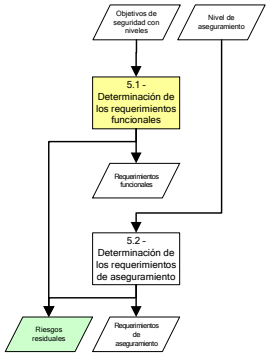


Figura 6 – Cuadro sinóptico detallado de la determinación de los requerimientos de seguridad

Actividad 5.1 – Determinación de los requerimientos de seguridad funcionales



DESCRIPCIÓN

Esta actividad tiene por objeto determinar los requerimientos de seguridad funcionales que permiten cubrir los objetivos de seguridad identificados para el sistema evaluado. Permite decidir la manera en que se deberá tratar cada riesgo identificado. Los riesgos podrán ser rechazados, optimizados, transferidos o asumidos y el riesgo residual deberá ser claramente identificado y aceptado. Esta actividad contribuye al tratamiento de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividad 4.3.

DATOS DE ENTRADA

- Lista de los objetivos de seguridad con el nivel de resistencia.

ACCIONES

- Enumerar los requerimientos de seguridad funcionales.
- Justificar la exhaustividad de la cobertura de los objetivos de seguridad.
- Identificar los eventuales fallos de cobertura (riesgos residuales) con justificaciones.
- Clasificar los requerimientos de seguridad funcionales en dos categorías:
  - requerimientos de seguridad funcionales que traten sobre el sistema evaluado.
  - requerimientos de seguridad funcionales que traten sobre el entorno del sistema evaluado.
- Justificar eventualmente la cobertura de la dependencia de los requerimientos de seguridad funcionales.

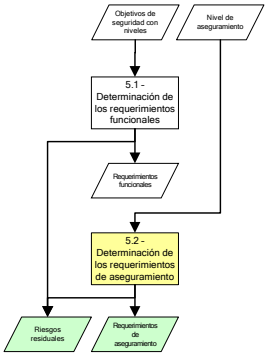
DATOS DE SALIDA

- Lista de los requerimientos de seguridad funcionales justificados.
- Lista de riesgos residuales (fallo de cobertura mediante los requerimientos de seguridad funcionales) y justificaciones.

CONSEJOS PRÁCTICOS

- 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 SSI” para enumerar los requerimientos de seguridad funcionales destinados a satisfacer los objetivos de seguridad que cubren las vulnerabilidades.
- Los requerimientos de seguridad funcionales pueden ser seleccionados entre los componentes funcionales de la base de conocimientos o redactados completamente. Cada uno de los objetivos de seguridad deberá estar cubierto por al menos un requerimiento de seguridad y la cobertura completa debe ser debidamente justificada. Los requerimientos son luego ajustados, en la medida de lo posible, y las dependencias entre componentes deben ser estudiadas y justificadas.
- Según el nivel de peritaje en el sistema, los componentes pueden ser dejados sin ajustar precisando sin embargo que éstos serán ajustados por la dirección en el marco de su respuesta.

Actividad 5.2 – Determinación de los requerimientos de seguridad de aseguramiento



DESCRIPCIÓN

Esta actividad tiene como finalidad la expresión completa de los requerimientos de seguridad de aseguramiento del objeto del estudio de seguridad. Éstos son seleccionados según el nivel de aseguramiento elegido durante la determinación de los niveles de seguridad. Constituyen la base de la confianza en el hecho que un sistema evaluado satisface sus objetivos de seguridad. Esta actividad contribuye al tratamiento de los riesgos en el proceso de gestión de los riesgos.

PREVIAS

- Actividad 4.3.

DATOS DE ENTRADA

- Elección del nivel de los requerimientos de aseguramiento.

ACCIONES

- Enumerar los requerimientos de seguridad de aseguramiento.
- Clasificar eventualmente los requerimientos de seguridad de aseguramiento en dos categorías:
  - requerimientos de seguridad de aseguramiento que traten sobre el sistema evaluado.
  - requerimientos de seguridad de aseguramiento que traten sobre el entorno del sistema evaluado.
- Justificar eventualmente la cobertura de la dependencia de los requerimientos de seguridad de aseguramiento.

DATOS DE SALIDA

- Lista de los requerimientos de seguridad de aseguramiento justificados.
- Lista de riesgos residuales (fallo de cobertura mediante los requerimientos de seguridad de aseguramiento) y justificaciones.

CONSEJOS PRÁCTICOS

- Los requerimientos de seguridad de aseguramiento pueden seleccionarse entre los componentes funcionales de la base de conocimientos o redactarse completamente.

Anexo – Datos producidos

- Presentación del organismo.
- Lista de las restricciones generales que recaen sobre el organismo.
- Lista de las referencias reglamentarias generales que se aplican al organismo.
- Diseño conceptual del sistema de información.
- Presentación del sistema evaluado.
- Lista de los elementos esenciales.
- Descripción funcional del sistema evaluado.
- Lista de los retos del sistema evaluado.
- Lista de las hipótesis.
- Lista de las normas de seguridad.
- Lista de las restricciones específicas del sistema evaluado.
- Lista de las referencias reglamentarias específicas al sistema evaluado.
- Lista de las entidades.
- Cuadros entidades/elementos.
- Lista de criterios de seguridad.
- Escala de necesidades.
- Lista de impactos.
- Ficha de síntesis de las necesidades de seguridad.
- Elección del modo de explotación de seguridad.
- Lista de los orígenes de las amenazas (métodos de ataque y elementos peligrosos).
- Lista de métodos de ataque no considerados y justificaciones.
- Lista de las vulnerabilidades consideradas y de su nivel.
- Lista de las amenazas consideradas.
- Lista jerarquizada de los riesgos.
- Lista de los riesgos residuales (fallo de cobertura de los riesgos) y justificaciones.
- Lista de los objetivos de seguridad.
- Lista de riesgos residuales (fallo de cobertura mediante los objetivos de seguridad) y justificaciones.
- Lista de los objetivos de seguridad con el nivel de resistencia.
- Lista de los riesgos residuales (fallo de cobertura del nivel de resistencia mediante los objetivos de seguridad) y justificaciones.
- Elección del nivel de los requerimientos de aseguramiento.
- Lista de los requerimientos de seguridad funcionales justificados.
- Lista de los riesgos residuales (fallo de cobertura mediante los requerimientos de seguridad funcionales) y justificaciones.
- Lista de los requerimientos de seguridad de aseguramiento justificados.
- Lista de los riesgos residuales (falta de cobertura mediante los requerimientos de seguridad de aseguramiento) y justificaciones.

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