MAGERIT – versión 3.0
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Libro II - Catálogo de Elementos

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS
DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
Libro II - Catálogo de Elementos

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Índice

1. Introducción

El objetivo de este catálogo de elementos que aparecen en un proyecto de análisis y gestión de riesgos es doble:

1. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Persiguiendo estos objetivos, y sabiendo que la tecnología cambia rápidamente, las secciones que siguen describen un catálogo[1] que marca unas pautas en cuanto a

Tipos de activos, sabiendo que aparecerán nuevos tipos de activos continuamente.

Dimensiones de valoración, sabiendo que en casos específicos pueden aparecer dimensiones específicas; pero en la certidumbre de estar recogido lo esencial.

Criterios de valoración, sabiendo que hay un fuerte componente de estimación por los expertos; pero marcando una primera pauta de homogeneidad. El ánimo es relativizar el valor de los diferentes activos en sus diferentes dimensiones de valoración, de forma que no sólo se propone una escala dentro de una dimensión, sino que también se propone cómo se relacionan las diferentes dimensiones entre sí.

Amenazas, sabiendo que no todas las amenazas son significativas sobre todos los sistemas; pero con una razonable esperanza de que este catálogo crezca lentamente.

Salvaguardas, sabiendo que es un terreno extremadamente complejo por su riqueza de tecnologías, productos y combinaciones ingeniosas de elementos básicos. Las salvaguardas se tratan con un enfoque de “identificación de necesidades” por parte de los responsables de los sistemas de información, mientras que se tratan con un enfoque de “controles de eficacia y eficiencia” por los auditores de sistemas. Se ha intentado un lenguaje intermedio que satisfaga a ambos colectivos.

Cada sección incluye una notación XML que se empleará para publicar los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas informáticas.

1 Este catálogo deberá adaptarse a la evolución de los sistemas de información. Es por ello que para cada categoría de elementos se define una notación XML que permitirá publicar ágilmente actualizaciones de este catálogo.

2. Tipos de activos

La tipificación de los activos es tanto un información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

La siguiente tabla no puede ser exhaustiva, ni tan siquiera válida para siempre.

La relación que sigue clasifica los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe. Nótese que las pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos.

2.1. Activos esenciales

En un sistema de información hay 2 cosas esenciales:

- la **información** que se maneja y
- los **servicios** que prestan.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos:

[essential] Activos esenciales

```
[info] información
    [adm] datos de interés para la administración pública
    [vr] datos vitales (registros de la organización) (1)

    [per] datos de carácter personal (2)
        [A] nivel alto
        [M] nivel medio
        [B] nivel bajo

    [classified] datos clasificados (3)
        [C] nivel confidencial
        [R] difusión limitada
        [UC] sin clasificar
        [pub] de carácter público

[service] servicio
```

(1) Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar aquellos que son imprescindibles para que la Organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas, aquellos sustancian la naturaleza legal o los derechos financieros de la Organización o sus usuarios.

(2) Dícese de cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

(3) Dícese de aquellos sometidos a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante. La tipificación de qué datos deben ser clasificados y cuales son las normas para su tratamiento, vienen determinadas por regulaciones sectoriales, por acuerdos entre organizaciones o por normativa interna.

2.1.1. Datos de carácter personal

Existen leyes relativas a los datos de carácter personal que, en función de su naturaleza y las circunstancias, establecen una serie de obligaciones a los sistemas de información que los tratan. En el caso de la legislación española, se ajusta a los dispuesto en

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. número 298, de 14/12/1999)
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (BOE número 17 de 19/1/2008)

El reglamento establece medidas específicas de nivel básico, medio y alto.

2.2. Arquitectura del sistema

Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.

[arch] Arquitectura del sistema
[sap] punto de [acceso al] servicio (1) [ip] punto de interconexión (2) [ext] proporcionado por terceros (3)
(1) Establece una frontera entre la prestación de un servicio (proveedor) y el usuario (consumidor). Los requisitos de seguridad del usuario se convierten en obligaciones del prestatario, mientras que los incidentes de seguridad en el proveedor repercuten en el usuario. (2) Establece una frontera inter-pares: cuando dos sistemas se interconectan para intercambiar información. (3) Establece una frontera inferior, cuando para la prestación de nuestros servicios recurrimos a un tercero.

2.3. [D] Datos / Información

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

[D] Datos / Información
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [int] datos de gestión interna [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2)

[D] Datos / Información
[source] código fuente [exe] código ejecutable [test] datos de prueba
(1) Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información. (2) Los registros de actividad sustancian los requisitos de trazabilidad.

2.4. [K] Claves criptográficas

Las criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

[keys] Claves criptográficas
[info] protección de la información [encrypt] claves de cifra [shared_secret] secreto compartido (clave simétrica) (1) [public_encryption] clave pública de cifra (2) [public_decryption] clave privada de descifrado (2) [sign] claves de firma [shared_secret] secreto compartido (clave simétrica) [public_signature] clave privada de firma (2) [public_verification] clave pública de verificación de firma (2) [com] protección de las comunicaciones [channel] claves de cifrado del canal [authentication] claves de autenticación [verification] claves de verificación de autenticación [disk] cifrado de soportes de información [encrypt] claves de cifra [x509] certificados de clave pública
(1) Por ejemplo, DES, 3-DES, AES, etc. (2) Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc.

2.5. [S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

[S] Servicios
[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización)

[S] Servicios
[www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio (1) [idm] gestión de identidades (2) [ipm] gestión de privilegios [pki] PKI - infraestructura de clave pública (3)

(1) Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado.

(2) Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización.

(3) Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.

2.6. [SW] Software - Aplicaciones informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

[SW] Aplicaciones (software)

[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf)
  [browser] navegador web
  [www] servidor de presentación
  [app] servidor de aplicaciones
  [email_client] cliente de correo electrónico
  [email_server] servidor de correo electrónico
  [file] servidor de ficheros
  [dbms] sistema de gestión de bases de datos
  [tm] monitor transaccional
  [office] ofimática
  [av] anti virus
  [os] sistema operativo
  [hypervisor] gestor de máquinas virtuales
  [ts] servidor de terminales
  [backup] sistema de backup

2.7. [HW] Equipamiento informático (hardware)

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos,

soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[HW] Equipos informáticos (hardware)

[host] grandes equipos (1)
[mid] equipos medios (2)
[pc] informática personal (3)
[mobile] informática móvil (4)
[pda] agendas electrónicas
[vhost] equipo virtual
[backup] equipamiento de respaldo (5)
[peripheral] periféricos
  [print] medios de impresión (6)
  [scan] escáneres
  [crypto] dispositivos criptográficos
[bp] dispositivo de frontera (7)
[network] soporte de la red (8)
  [modem] módems
  [hub] concentradores
  [switch] conmutadores
  [router] encaminadores
  [bridge] pasarelas
  [firewall] cortafuegos
  [wap] punto de acceso inalámbrico
[pabx] centralita telefónica
[ipphone] teléfono IP

(1) Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

(2) Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.

(3) Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.

(4) Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.

(5) Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.

(6) Dícese de impresoras y servidores de impresión.

(7) Son los equipos que se instalan entre dos zonas de confianza.

(8) Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.

2.8 [COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[COM] Redes de comunicaciones
[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] comunicaciones radio [wifi] red inalámbrica [mobile] telefonía móvil [sat] por satélite [LAN] red local [MAN] red metropolitana [Internet] Internet

2.9. [Media] Soportes de información

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[Media] Soportes de información
[electronic] electrónicos [disk] discos [vdisk] discos virtuales [san] almacenamiento en red [disquette] disquetes [cd] cederrón (CD-ROM) [usb] memorias USB [dvd] DVD [tape] cinta magnética [mc] tarjetas de memoria [ic] tarjetas inteligentes [non_electronic] no electrónicos [printed] material impreso [tape] cinta de papel [film] microfilm [cards] tarjetas perforadas

2.10. [AUX] Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[AUX] Equipamiento auxiliar
[power] fuentes de alimentación [ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [wire] cable eléctrico [fiber] fibra óptica [robot] robots [tape] ... de cintas [disk] ... de discos [supply] suministros esenciales [destroy] equipos de destrucción de soportes de información [furniture] mobiliario: armarios, etc [safe] cajas fuertes

2.11. [L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

[L] Instalaciones
[site] recinto [building] edificio [local] cuarto [mobile] plataformas móviles [car] vehículo terrestre: coche, camión, etc. [plane] vehículo aéreo: avión, etc. [ship] vehículo marítimo: buque, lancha, etc. [shelter] contenedores [channel] canalización [backup] instalaciones de respaldo

2.12. [P] Personal

En este epígrafe aparecen las personas relacionadas con los sistemas de información.

[P] Personal
[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [sec] administradores de seguridad [des] desarrolladores / programadores [sub] subcontratas [prov] proveedores

2.13. XML

Los tipos de activos cabe esperar que evolucionen en el tiempo para adaptarse a la evolución tecnológica. Por ello se incluye a continuación una gramática de tipo XML que permita publicar periódicamente actualizaciones de los tipos antes descritos.

2.13.1. Sintaxis BNF

La notación se describe en el apéndice 1.

```
<magerit-extension>
  { tipos }*
</magerit-extension>

tipos ::=
  <classes under >
    { tipo }*
  </classes>

tipo ::=
  <class code>
    #name#
    [ descripción ]
    { tipo }*
  </tipo>
```

```
descripción ::=
  <description>
    #texto#
  </description>
```

Atributo	*Ejemplo*	*Descripción*
under	under=”X”	X identifica a un tipo de activos ya definido, indicando que los nuevos tipos de activos son refinamientos de X.
code	code=”X”	X es un identificador único que permite determinar unívocamente a qué tipo se refiere.

2.13.2. Esquema XSD

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified"
            version="2.0">
  <xsd:annotation>
    <xsd:documentation>version: magerit 3.0 (2011)</xsd:documentation>
    <xsd:documentation>date: 19.11.2011</xsd:documentation>
  </xsd:annotation>
  <xsd:element name="magerit-extension">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="classes" type="classesType"
                     minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:complexType name="classesType" mixed="true">
    <xsd:sequence>
      <xsd:element name="class" type="classType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="under" type="xsd:string" use="required"/>
  </xsd:complexType>
  <xsd:complexType name="classType" mixed="true">
    <xsd:sequence>
      <xsd:element name="description" type="xsd:string"
                   minOccurs="0"/>
      <xsd:element name="class" type="classType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="code" type="xsd:string" use="required"/>
  </xsd:complexType>
</xsd:schema>
```

3. Dimensiones de valoración

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos[2].

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

3.1. [D] Disponibilidad

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

La disponibilidad es una característica que afecta a todo tipo de activos.

A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

3.2. [I] Integridad de los datos

[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

3.3. [C] Confidencialidad de la información

[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

2 Como es el caso típico conocido como análisis de impacto (BIA) que busca determinar el coste de las paradas de los sistemas y desarrollar planes de contingencia para poner coto al tiempo de parada de la organización. En este caso se hace un análisis sectario de la disponibilidad.

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

3.4. [A] Autenticidad

[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio.

Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

3.5. [T] Trazabilidad

[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

3.6. XML

Las dimensiones de valoración cabe esperar que evolucionen en el tiempo para adaptarse a la evolución tecnológica. Por ello se incluye a continuación una gramática de tipo XML que permita publicar periódicamente actualizaciones de las dimensiones antes descritas.

3.6.1. Sintaxis BNF

La notación se describe en el apéndice 1.

```
<magerit-extension>
  { dimensiones }*
</magerit-extension>
```

```
dimensiones ::=
  <dimensions>
    { dimensión }*
  </dimensions>

dimensión ::=
  <dimension code >
    #nombre#
    [ descripción ]
  </dimension>

descripción ::=
  <description>
    #texto#
  </description>
```

Atributo	*Ejemplo*	*Descripción*
code	code=”X”	X es un identificador único que permite determinar unívocamente a qué dimensión se refiere.

3.6.2. Esquema XSD

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified"
            version="2.0">
  <xsd:annotation>
    <xsd:documentation>version: magerit 3.0 (2011)</xsd:documentation>
    <xsd:documentation>date: 19.11.2011</xsd:documentation>
  </xsd:annotation>
  <xsd:element name="magerit-extension">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="dimensions" type="dimensionsType"
                     minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:complexType name="dimensionsType" mixed="true">    <xsd:sequence>
      <xsd:element name="dimension" type="dimensionType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
  <xsd:complexType name="dimensionType" mixed="true">
    <xsd:sequence>
      <xsd:element name="description" type="xsd:string"
                   minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="code" type="xsd:string" use="required"/>
  </xsd:complexType>
</xsd:schema>
```

3.7. Referencias

- ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture”, 1989.

- ISO/IEC 27000
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”, December 2003.

  http://csrc.nist.gov/publications/fips/index.html
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

  http://www.cert.org/octave/

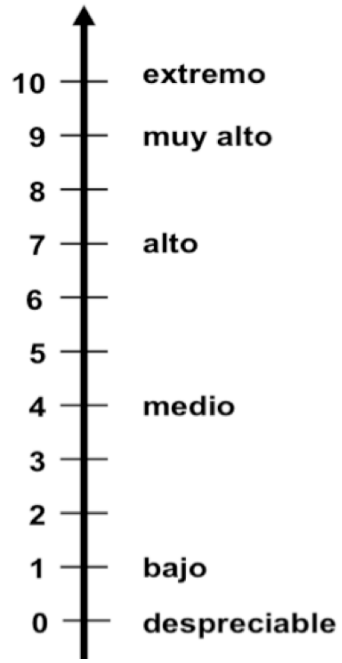
4. Criterios de valoración

Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos es sin embargo muy importante que

- se use una escala común para todas las dimensiones, permitiendo comparar riesgos,
- se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas[3] y
- se use un criterio homogéneo que permita comparar análisis realizados por separado

Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Las tablas siguientes pretenden guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos.

4.1. Escalas estándar

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

3 Así siempre es igual de relevante que un activo sea el doble de valioso que otro, independientemente de su valor absoluto. Por el contrario, sería extraño opinar que un activo vale dos más que otro sin explicitar su valor absoluto pues no es igual de relevante pasar de 0,1 a 2,1, que pasar de 1.000.000 a 1.000.002.

5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones

	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas

4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

4.2. XML

Los tipos de activos cabe esperar que evolucionen en el tiempo para adaptarse a la evolución tecnológica. Por ello se incluye a continuación una gramática de tipo XML que permita publicar periódicamente actualizaciones de los tipos antes descritos.

4.2.1. Sintaxis BNF

La notación se describe en el apéndice 1.

```
criterios ::=
  <criteria>
    { criterio }*
  </criteria>

criterio ::=
  <criterion code [ value ] >
    #texto#
    { criterio }*
  </criterion>
```

Atributo	*Ejemplo*	*Descripción*
value	value=”X”	X es un índice entre 0 y 10 de valoración cualitativa de activos.
code	code=”X”	X es un código único para identificar el criterio; en relación a la tabla previa, se identificará el epígrafe; por ejemplo, “7.4.c”

4.2.2. Esquema XSD

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified"
            version="2.0">
  <xsd:annotation>
    <xsd:documentation>version: magerit 3.0 (2011)</xsd:documentation>
    <xsd:documentation>date: 19.11.2011</xsd:documentation>
  </xsd:annotation>
  <xsd:element name="criteria">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="criterion" type="criterionType"
                     minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:complexType name="criterionType" mixed="true">
    <xsd:sequence>
      <xsd:element name="criterion" type="criterionType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="code" type="xsd:string" use="required"/>
    <xsd:attribute name="value" type="xsd:integer"/>
  </xsd:complexType>
</xsd:schema>
```

4.3. Referencias

- CCN-STIC-803 – Esquema Nacional de Seguridad – Criterios de Valoración.
- SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”, NIST, June 2004.
  http://csrc.nist.gov/publications/nistpubs/index.html
- HMG, “Residual Risk Assessment Method”, INFOSEC Standard No. 1. 2003.
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.
  http://www.cert.org/octave/

5. Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

5.1. [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen:
Natural (accidental)

5.1.1. [N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

5.1.2. [N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.1.3. [N.*] Desastres naturales

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad

Descripción:

otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...

Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]).

Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

Ver:

EBIOS:

03 – CONTAMINACIÓN
04 - SINIESTRO MAYOR
06 - FENÓMENO CLIMÁTICO
07 - FENÓMENO SÍSMICO
08 - FENÓMENO DE ORIGEN VOLCÁNICO
09 - FENÓMENO METEOROLÓGICO
10 - INUNDACIÓN

5.2. [I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

5.2.1. [I.1] Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	

5.2.2. [I.2] Daños por agua

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.2.3. [I.*] Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 04 - SINIESTRO MAYOR	

5.2.4. [I.3] Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 03 – CONTAMINACIÓN	

5.2.5. [I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

5.2.6. [I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

5.2.7. [I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN	

5.2.9. [I.8] Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	

5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: no disponible	

5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: como consecuencia del paso del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

5.2.12. [I.11] Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:

hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard").* Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "*TEMPEST protection",* queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

Origen:

Entorno (accidental)
Humano (accidental o deliberado)

Ver:

EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

5.3. [E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (accidental)

Ver correlación de errores y amenazas.

5.3.1. [E.1] Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.2. [E.2] Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.3. [E.3] Errores de monitorización *(log)*

[E.3] Errores de monitorización *(log)*	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: no disponible	

5.3.4. [E.4] Errores de configuración

[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	**Dimensiones:** 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

5.3.5. [E.7] Deficiencias en la organización

Obsoleta.

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible	

5.3.6. [E.8] Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.3.7. [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. **Ver:** EBIOS: no disponible	

5.3.8. [E.10] Errores de secuencia

[E.10] Errores de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos. **Ver:** EBIOS: no disponible	

5.3.9. [E.14] Escapes de información

Obsoleta: use E.19.

[E.14] Escapes de información	
Tipos de activos: •	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

5.3.10. [E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.11. [E.18] Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.12. [E.19] Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible	

5.3.13. [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. **Ver:** EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.16. [E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

5.3.17. [E.25] Pérdida de equipos

[E.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

5.3.18. [E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: **a**usencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

5.4. [A] Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (deliberado)

Ver correlación de errores y amenazas.

5.4.1. [A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: **Ver:** EBIOS: no disponible	

5.4.2. [A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

5.4.3. [A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - USURPACIÓN DE DERECHO	

5.4.4. [A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. **Ver:** EBIOS: 39 - ABUSO DE DERECHO	

5.4.5. [A.7] Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. **Ver:** EBIOS: no disponible	

5.4.6. [A.8] Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.4.7. [A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. **Ver:** EBIOS: no disponible	

5.4.8. [A.10] Alteración de secuencia

[A.10] Alteración de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. **Ver:** EBIOS: 36 - ALTERACIÓN DE DATOS	

5.4.9. [A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. **Ver:** EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

5.4.10. [A.12] Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. **Ver:** EBIOS: no disponible	

5.4.11. [A.13] Repudio

[A.13] Repudio	
Tipos de activos: • [S] servicios • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. **Ver:** EBIOS: 41 - NEGACIÓN DE ACCIONES	

5.4.12. [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. **Ver:** EBIOS: 19 - ESCUCHA PASIVA	

5.4.13. [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.14. [A.18] Destrucción de información

[A.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.15. [A.19] Divulgación de información

[A.19] Revelación de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación de información. **Ver:** EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

5.4.16. [A.22] Manipulación de programas

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

5.4.17. [A.23] Manipulación de los equipos

[A.22] Manipulación de los equipos	
Tipos de activos: • [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 25 - SABOTAJE DEL HARDWARE	

5.4.18. [A.24] Denegación de servicio

[A.24] Denegación de servicio	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

5.4.19. [A.25] Robo

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 3. [D] disponibilidad 4. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

5.4.20. [A.26] Ataque destructivo

[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. **Ver:** EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES	

5.4.21. [A.27] Ocupación enemiga

[A.27] Ocupación enemiga	
Tipos de activos: • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. **Ver:** EBIOS: no disponible	

5.4.22. [A.28] Indisponibilidad del personal

[A.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

5.4.23. [A.29] Extorsión

[A.29] Extorsión	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. **Ver:** EBIOS: no disponible	

5.4.24. [A.30] Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. **Ver:** EBIOS: no disponible	

5.5. Correlación de errores y ataques

Errores y amenazas constituyen frecuentemente las dos caras de la misma moneda: algo que le puede pasar a los activos sin animosidad o deliberadamente. Se pueden dar hasta tres combinaciones:

- amenazas que sólo pueden ser errores, nunca ataques deliberados
- amenazas que nunca son errores: siempre son ataques deliberados
- amenazas que pueden producirse tanto por error como deliberadamente

Para afrontar esta casuística, errores y amenazas se han numerado de tal manera que pueda establecerse este paralelismo. La siguiente tabla alinea errores con ataques mostrando cómo se correlacionan:

número	*error*	*ataque*
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización *(log)*	Manipulación de los registros de actividad
4	Errores de configuración	Manipulación de la configuración
5		Suplantación de la identidad del usuario
6		Abuso de privilegios de acceso
7	~~Deficiencias en la organización~~	Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Errores de [re-]encaminamiento	[Re-]encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico
13		Repudio
14	~~Escapes de información~~	Interceptación de información (escucha)
15	Alteración accidental de la información	Modificación deliberada de la información
18	Destrucción de información	Destrucción de información
19	Fugas de información	Revelación de información
20	Vulnerabilidades de los programas (software)	
21	Errores de mantenimiento / actualización de programas (software)	
22		Manipulación de programas
23	Errores de mantenimiento / actualización de equipos (hardware)	Manipulación de los equipos
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25	Pérdida de equipos	Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social (picaresca)

5.6. Nuevas amenazas: XML

Los amenazas cabe esperar que evolucionen en el tiempo para adaptarse a la evolución tecnológica. Por ello se incluye a continuación una gramática de tipo XML que permita publicar periódicamente actualizaciones de las amenazas antes descritas.

5.6.1. Sintaxis BNF

La notación se describe en el apéndice 1.

```
<magerit-extension>
  { amenazas }*
</magerit-extension>

amenazas ::=
  <threats under >
    { amenaza }*
  </ threats>

amenaza ::=
  <threat code [ tho ] [ thc ]>
    #name#
    [ descripción ]
    { amenaza }*
  </threat>

descripción ::=
  <description>
    #texto#
  </description>
```

Atributo	*Ejemplo*	*Descripción*
under	under=”X”	X identifica una amenaza ya definida, indicando que las nuevas amenazas son refinamientos de X.
code	code=”X”	X es un identificador único que permite determinar unívocamente a qué amenaza se refiere.
tho	tho=”H”	Origen (agente causante) de la amenaza. Puede ser N – Natural E – Entorno industrial H - Humano
thc	thc=”D”	Causa. Puede ser A – Accidental D - Deliberada

5.6.2. Esquema XSD

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified"
            version="2.0">
  <xsd:annotation>
    <xsd:documentation>version: magerit 3.0 (2011)</xsd:documentation>
    <xsd:documentation>date: 19.11.2011</xsd:documentation>
  </xsd:annotation>
  <xsd:element name="magerit-extension">
    <xsd:complexType>
```

```
      <xsd:sequence>
        <xsd:element name="threats" type="threatsType"
                     minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:complexType name="threatsType" mixed="true">
    <xsd:sequence>
      <xsd:element name="threat" type="threatType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="under" type="xsd:string" use="required"/>
  </xsd:complexType>
  <xsd:complexType name="threatType" mixed="true">
    <xsd:sequence>
      <xsd:element name="description" type="xsd:string"
                   minOccurs="0"/>
      <xsd:element name="threat" type="threatType"
                   minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="code" type="xsd:string" use="required"/>
    <xsd:attribute name="tho" type="threatOrigin"/>
    <xsd:attribute name="thc" type="threatCause"/>
  </xsd:complexType>
  <xsd:simpleType name="threatOrigin">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="N"/>
      <xsd:enumeration value="E"/>
      <xsd:enumeration value="H"/>
    </xsd:restriction>
  </xsd:simpleType>
  <xsd:simpleType name="threatCause">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="A"/>
      <xsd:enumeration value="D"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

5.7. Nivel de la amenaza: XML

Para que una fuente de información pueda proporcionar datos de inteligencia sobre la probabilidad de que una amenaza se materialice sobre un cierto tipo de activos.

5.7.1. Sintaxis BNF

La notación se describe en el apéndice 1.

```
<threat_announcement>
  { nivel_de_amenaza }*
</ threat_announcement >

nivel_de_amenaza ::=
  <tip class threat level >
    [ descripción ]
  </tip>

descripción ::=
  <description>
    #texto#
  </description>
```

Atributo	*Ejemplo*	*Descripción*
class	class=”C”	C identifica por su código a un tipo ya conocido de activos.
threat	threat=”T”	T identifica por su código a una amenaza ya conocida.
level	level=”A”	Nivel de la amenaza. Puede ser VR – muy raro (very rare) U – improbable (unlikely) P – posible (possible) VH – probable (very high) AC – prácticamente segura (almost certain)

5.7.2. Esquema XSD

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified"
            version="2.0">
  <xsd:annotation>
    <xsd:documentation>version: magerit 3.0 (2011)</xsd:documentation>
    <xsd:documentation>date: 19.11.2011</xsd:documentation>
  </xsd:annotation>
  <xsd:element name="threat-announcement">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="tip" type="tipType"
                     minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:complexType name="tipType" mixed="true">
    <xsd:sequence>
      <xsd:element name="description" type="xsd:string"
                   minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="asset" type="xsd:string" use="required"/>
    <xsd:attribute name="threat" type="xsd:string" use="required"/>
    <xsd:attribute name="level" type="levelType" use="required"/>
  </xsd:complexType>
  <xsd:simpleType name="levelType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="VR"/>
      <xsd:enumeration value="U"/>
      <xsd:enumeration value="P"/>
      <xsd:enumeration value="VH"/>
      <xsd:enumeration value="AC"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

5.8. Referencias

Existen numerosas fuentes que catalogan amenazas dentro del ámbito de las tecnologías de la información y las comunicaciones.

- ISO/IEC 27005
- EBIOS

- IT Baseline Protection Manual, Federal Office for Information Security (BSI), Germany. October 2003.

  http://www.bsi.de/gshb/english/etc/index.htm

- Managing Information Security Risks: The OCTAVE Approach, C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)

  http://www.cert.org/octave/

6. Salvaguardas

Las salvaguardas permiten hacer frente a las amenazas.

Las salvaguardas, especialmente las técnicas, varían con el avance tecnológico

- porque aparecen tecnologías nuevas,
- porque van desapareciendo tecnologías antiguas,
- porque cambian los [tipos de] activos a considerar,
- porque evolucionan las posibilidades de los atacantes o
- porque evoluciona el catálogo de salvaguardas disponibles.

En consecuencia, este catálogo de salvaguardas no entra en la selección de paquetes o productos a instalar, limitándose a establecer un paraguas taxonómico para ordenar y clasificar las diferentes concreciones materiales, tecnológicas, organizativas y procedimentales que sean de aplicación en cada momento..

6.1. Protecciones generales u horizontales

H	Protecciones Generales
H.IA	Identificación y autenticación
H.AC	Control de acceso lógico
H.ST	Segregación de tareas
H.IR	Gestión de incidencias
H.tools	Herramientas de seguridad
H.tools.AV	Herramienta contra código dañino
H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
H.tools.CC	Herramienta de chequeo de configuración
H.tools.VA	Herramienta de análisis de vulnerabilidades
H.tools.TM	Herramienta de monitorización de tráfico
H.tools.DLP	DLP: Herramienta de monitorización de contenidos
H.tools.LA	Herramienta para análisis de logs
H.tools.HP	Honey net / honey pot
H.tools.SFV	Verificación de las funciones de seguridad
H.VM	Gestión de vulnerabilidades
H.AU	Registro y auditoría

6.2. Protección de los datos / información

D	Protección de la Información
D.A	Copias de seguridad de los datos (backup)
D.I	Aseguramiento de la integridad
D.C	Cifrado de la información
D.DS	Uso de firmas electrónicas
D.TS	Uso de servicios de fechado electrónico (time stamping)

6.3. Protección de las claves criptográficas

K	Gestión de claves criptográficas
K.IC	Gestión de claves de cifra de información
K.DS	Gestión de claves de firma de información
K.disk	Gestión de claves para contenedores criptográficos
K.comms	Gestión de claves de comunicaciones
K.509	Gestión de certificados

6.4. Protección de los servicios

S	Protección de los Servicios
S.A	Aseguramiento de la disponibilidad
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.CM	Gestión de cambios (mejoras y sustituciones)
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.email	Protección del correo electrónico
S.dir	Protección del directorio
S.dns	Protección del servidor de nombres de dominio (DNS)
S.TW	Teletrabajo
S.voip	Voz sobre IP

6.5. Protección de las aplicaciones (software)

SW	Protección de las Aplicaciones Informáticas
SW.A	Copias de seguridad (backup)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
SW.CM	Cambios (actualizaciones y mantenimiento)
SW.end	Terminación

6.6. Protección de los equipos (hardware)

HW	Protección de los Equipos Informáticos
HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.op	Operación
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.end	Terminación
HW.PCD	Informática móvil
HW.print	Reproducción de documentos
HW.pabx	Protección de la centralita telefónica (PABX)

6.7. Protección de las comunicaciones

COM	Protección de las Comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.aut	Autenticación del canal
COM.I	Protección de la integridad de los datos intercambiados
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op	Operación
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.end	Terminación
COM.internet	Internet: uso de ? acceso a
COM.wifi	Seguridad Wireless (WiFi)
COM.mobile	Telefonía móvil
COM.DS	Segregación de las redes en dominios

6.8. Protección en los puntos de interconexión con otros sistemas

IP	Puntos de interconexión: conexiones entre zonas de confianza
IP.SPP	Sistema de protección perimetral
IP.BS	Protección de los equipos de frontera

6.9. Protección de los soportes de información

MP	Protección de los Soportes de Información
MP.A	Aseguramiento de la disponibilidad
MP.IC	Protección criptográfica del contenido

MP.clean	Limpieza de contenidos
MP.end	Destrucción de soportes

6.10. Protección de los elementos auxiliares

AUX	Elementos Auxiliares
AUX.A	Aseguramiento de la disponibilidad
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.AC	Climatización
AUX.wires	Protección del cableado

6.11. Seguridad física – Protección de las instalaciones

L	Protección de las Instalaciones
L.design	Diseño
L.depth	Defensa en profundidad
L.AC	Control de los accesos físicos
L.A	Aseguramiento de la disponibilidad
L.end	Terminación

6.12. Salvaguardas relativas al personal

Son aquellas que se refieren a las personas que tienen relación con el sistema de información.

PS	Gestión del Personal
PS.AT	Formación y concienciación
PS.A	Aseguramiento de la disponibilidad

6.13. Salvaguardas de tipo organizativo

Son aquellas que se refieren al buen gobierno de la seguridad.

G	Organización
G.RM	Gestión de riesgos
G.plan	Planificación de la seguridad
G.exam	Inspecciones de seguridad

6.14. Continuidad de operaciones

Prevención y reacción frente a desastres.

BC	Continuidad del negocio
BC.BIA	Análisis de impacto (BIA)
BC.DRP	Plan de Recuperación de Desastres (DRP)

6.15. Externalización

Es cada vez más flexible la frontera entre los servicios de seguridad prestados internamente y los servicios contratados a terceras partes. En estos casos es fundamental cerrar los aspectos de relación contractual:

- SLA: nivel de servicio, si la disponibilidad es un valor
- NDA: compromiso de secreto, si la confidencialidad es un valor
- Identificación y calificación del personal encargado
- Procedimientos de escalado y resolución de incidencias
- Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
- Asunción de responsabilidades y penalizaciones por incumplimiento

E	Relaciones Externas
E.1	Acuerdos para intercambio de información y software
E.2	Acceso externo
E.3	Servicios proporcionados por otras organizaciones
E.4	Personal subcontratado

6.16. Adquisición y desarrollo

NEW	Adquisición / desarrollo
NEW.S	Servicios: Adquisición o desarrollo
NEW.SW	Aplicaciones: Adquisición o desarrollo
NEW.HW	Equipos: Adquisición o desarrollo
NEW.COM	Comunicaciones: Adquisición o contratación
NEW.MP	Soportes de Información: Adquisición
NEW.C	Productos certificados o acreditados

6.17. Referencias

BSI
Federal Office for Information Security (BSI). “IT Baseline Protection Manual”, October 2003. Germany.
http://www.bsi.de/gshb/english/etc/index.htm

CC
Comon Criteria. Ver [ISO 15408].

Guías CCN-STIC
https://www.ccn-cert.cni.es/

ISO JTC 71/SC 27
Numerosas guías producidas por ISO concretan medidas de seguridad. Consulte el catálogo del comité 71 "TECNOLOGÍA DE LA INFORMACIÓN", subcomité SC 27 "TÉCNICAS DE SEGURIDAD".

ISO 15408
ISO/IEC 15408:2009, “Information technology — Security techniques — Evaluation criteria for IT security”.

ISO 27002
ISO/IEC 27002:2005, “Information technology — Security techniques — Code of practice for information security management”.
UNE-ISO/IEC 27002:2009, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”.

NIST 800-53
NIST, “Recommended Security Controls for Federal Information Systems”, National Institute of Standards and Technology, special publication SP 800-53 Rev.3, Aug. 2009.

RD 3/2010
Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

RD 1720/2007
Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Apéndice 1. Notación XML

Las descripciones de formatos XML se ajustan a la siguiente notación de tipo BNF[4]:

- las etiquetas XML se muestran como tales
- los atributos XML se explican en la sección “atributos”
- { ... }* denota que hay 0 o más
- { ... }+ denota que hay 1 o más
- | denota que son alternativas
- [...] denota que es opcional (0 o 1)
- #texto# es contenido literal: un nombre o una descripción
- lo demás es obligatorio

4 **BNF**: Backus-Naur Form. Es una forma de representar la gramática de un lenguaje. Una gramática BNF consiste en una serie de reglas de producción, donde el lado izquierdo se materializa en lo que se indica en el lado derecho. El lado derecho puede explicitar términos finales, o bien ser a su vez desarrollado mediante nuevas reglas de producción.

Apéndice 2. Fichas

Las siguientes secciones proporciona fichas para la captura de datos en un proyecto de análisis y gestión de riesgos.

Reproduzca las fichas siguientes, una por activo, del tipo que corresponda.

A2.1. [info] Activos esenciales: información

[info] Información	
código:	**nombre:**
descripción:	
propietario:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de la información, típicamente en las siguientes dimensiones de seguridad:

[I] integridad

[C] confidencialidad

[A] autenticidad de los datos

[T] trazabilidad de los datos, quién ha modificado qué

Valoración		
dimensión	***valor***	***justificación***
[I]		
[C]		
[A]		
[T]		

Las dependencias normalmente identifican servicios y personas que manejan esta información:

Dependencias de activos inferiores (hijos)	
activo:	**grado:**

¿por qué?:

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.2. [service] Activos esenciales: Servicio

[service] Servicio	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de los servicios que ofrece la Organización a otros, típicamente en las siguientes dimensiones:

[D] disponibilidad

[A] autenticidad de quién accede al servicio

[T] trazabilidad de quién accede al servicio, cuándo y que hace

Valoración		
dimensión	***valor***	***justificación***
[D]		
[A]		
[T]		

Las dependencias normalmente identifican equipamiento desplegado para prestar este servicio:

- aplicaciones (sw),
- equipos (hw),
- equipos de comunicaciones,
- soportes de información (media), etc.
- personas a cargo del servicio.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.3. [D] Datos / Información

[D] Datos / Información	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.3.	

Las dependencias normalmente identifican

- equipos que los hospedan
- líneas de comunicación por las que se transfieren
- soportes de información
- personas relacionadas: usuarios.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.4. [K] Claves criptográficas

[K] Claves criptográficas	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.4.	

Las dependencias normalmente identifican

- equipos que las hospedan
- soportes de información
- personas relacionadas: operadores, administradores y criptocustodios.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.5. [S] Servicios

[S] Servicios	
código:	**nombre:**
descripción:	

[S] Servicios
responsable:
tipo (marque todos los adjetivos que procedan) Ver Sección 2.5.

Las dependencias normalmente identifican

- personas relacionadas: usuarios, operadores y administradores.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.6. [SW] Aplicaciones (software)

[SW] Aplicaciones (software)	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.6.	

Las dependencias normalmente identifican

- personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

A2.7. [HW] Equipamiento informático (hardware)

[HW] Equipamiento informático (hardware)	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.7.	

Las dependencias normalmente identifican

- personas relacionadas con este equipo: operadores, administradores
- instalaciones que lo acogen

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

A2.8. [COM] Redes de comunicaciones

[COM] Redes de comunicaciones	
código:	**nombre:**

[COM] Redes de comunicaciones
descripción:
responsable:
ubicación:
número:
tipo (marque todos los adjetivos que procedan) Ver Sección 2.8.

Las dependencias normalmente identifican

- personas relacionadas: operadores, administradores
- instalaciones que lo acogen

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.9. [Media] Soportes de información

[SI] Soportes de información	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan)	

[SI] Soportes de información
Ver Sección 2.9.

Las dependencias normalmente identifican

- personas relacionadas: operadores, administradores
- instalaciones que lo acogen

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

A2.10. [AUX] Equipamiento auxiliar

[AUX] Equipamiento auxiliar	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.10.	

Las dependencias normalmente identifican

- personas relacionadas con este equipo: operadores, administradores

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

A2.11. [L] Instalaciones

[L] Instalaciones	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.11.	

Las dependencias normalmente identifican

- personas relacionadas con esta instalación: guardias, encargados de mantenimiento

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	grado:
¿por qué?:	

activo:	grado:
¿por qué?:	

A2.12. [P] Personal

[P] Personal	
código:	**nombre:**
descripción:	

[P] Personal
número:
tipo (marque todos los adjetivos que procedan) Ver Sección 2.12.

No suelen identificarse dependencias.

Apéndice 3. Modelo de valor

En este apéndice se describe un formato XML para el intercambio de modelos de activos entre herramientas. Este formato debe entenderse como de mínimos, en el sentido de que las herramientas pueden incorporar información adicional a la prescrita.

La información que se intercambia incluye

- identificación de los activos, con un código y un nombre descriptivo
- identificación de bajo qué tipo(s) cabe clasificar el activo
- identificación de las dependencias entre activos
- valoración de los activos en diferentes dimensiones

La notación se describe en el apéndice 1.

A3.1. Formato XML

```
modelo ::=
  <modelo>
  { dato }*
  { activo }*
  { dependencia }*
  { valoración }*
  </modelo>

dato ::=
  <dato clave texto />

activo ::=
  <activo código>
  #nombre#
  { tipo }+
  { dato }*
  </activo>

tipo ::=
  <tipo tipo />

dependencia ::=
  <dependencia superior inferior grado />

valoración ::=
  <valoracion activo dimension valor />
```

atributo	*ejemplo*	*descripción*
código	`codigo="X"`	Acrónimo que identifica unívocamente un activo en un modelo; es decir, que no pueden haber códigos repetidos.
clave	`clave="responsable"`	Aparece como características adicionales que informan sobre el modelo o activo. Típicamente aparecen claves como autor, organización, documentación relevante, clasificación, ubicación, fecha, versión, etc.
texto	`texto="JRP"`	Texto asociado a la clave en una característica.
tipo	`tipo="T"`	T es el código de alguno de los tipos definidos. Ver capítulo 2.
superior	`superior="X"`	X es el código de algún activo del modelo.

atributo	*ejemplo*	*descripción*
inferior	`inferior="X"`	X es el código de algún activo del modelo.
grado	`grado="valor"`	Un número real entre 0.0 y 1.0.
activo	`activo="X"`	X es el código de algún activo del modelo.
dimension	`dimension="D"`	D es el código de alguna de las dimensiones definidas. Ver capítulo 3.
valor	`valor="[clave]"` `valor="valor"`	Puede ser una clave simbólica o una cantidad real, positiva. Ver capítulo 4.

Apéndice 4. Informes

A lo largo del proyecto de análisis y gestión de riesgos se han identificado una serie de informes para los cuales se propone un índice a continuación. Frecuentemente, se puede extraer de estos informes un informe ejecutivo que excluye los detalles.

A4.1. Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Activos
   2.1. Árbol de activos (relaciones de dependencia)
   2.2. Valoración de los activos (valor propio)
      Indicando la razón de la valoración atribuida a cada activo en cada dimensión.
3. Descripción detallada
   Para cada activo:
   - clasificación (ver capítulo 2)
   - activos superiores e inferiores
   - valoración: valor propio y acumulado en cada dimensión

A4.2. Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Activos
   2.1. Árbol de activos (relaciones de dependencia)
   2.2. Valoración de los activos (valor propio)
      Indicando la razón de la valoración atribuida a cada activo en cada dimensión.
3. Amenazas por activo
   Para cada activo:
   - amenazas relevantes (ver capítulo 5)
   - degradación estimada en cada dimensión
   - frecuencia anual estimada
4. Activos por amenaza
   Para cada amenaza:
   - activos afectados
   - degradación estimada en cada dimensión
   - frecuencia anual estimada

A4.3. Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Se trabaja respecto de

- un catálogo de salvaguardas (ver capítulo 5)

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Salvaguardas (ver capítulo 5)
   Para cada salvaguarda, al nivel de detalle que se estime oportuno, indicación de su eficacia frente a los riesgos a los que se enfrenta.
   Si procede, muéstrese la evolución histórica y la planificación actual.

A4.4. Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Activos
   Para cada activo:
   1. Impacto acumulado
   2. Riesgo acumulado
   3. Impacto repercutido
   4. Riesgo repercutido
   Si procede, muéstrese la evolución histórica y el efecto de la planificación actual.

A4.5. Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir el riesgo sobre el sistema.

Se trabaja respecto de

- un catálogo de salvaguardas (ver capítulo 5)
- un umbral de eficacia

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Salvaguardas
   Para cada salvaguarda, al nivel de detalle que se estime oportuno, cuya eficacia sea inferior a un umbral determinado, indicación de su eficacia frente a los riesgos a los que se enfrenta.
   Si procede, muéstrese la evolución histórica y la planificación actual.

A4.6. Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

1. Marco de referencia
   - Política de seguridad de la organización
   - Relación de normas y procedimientos
2. Responsables y responsabilidades (a nivel de organización)
3. Programas de seguridad

   Por cada programa identificado:
   - objetivo genérico
   - prioridad o urgencia
   - ubicación temporal: ¿cuándo se llevará a cabo?
   - salvaguardas involucradas
   - unidad responsable de su ejecución
   - estimación de costes financieros
   - estimación de recursos
   - estimación de impacto para la organización

Cuando llega el momento para ser acometido, cada programa de seguridad debe detallar:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
  - costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas
  - costes de implantación inicial y mantenimiento en el tiempo
  - costes de formación, tanto de los operadores como de los usuarios, según convenga al caso
  - costes de explotación
  - impacto en la productividad de la Organización
- Una relación de subtareas a afrontar, teniendo en cuenta
  - cambios en la normativa y desarrollo de procedimientos
  - solución técnica: programas, equipos, comunicaciones y locales,
  - plan de despliegue
  - plan de formación

- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.