MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

II - Catálogo de Elementos

Madrid, 20 de junio de 2006
NIPO 326-05-047-X
Catálogo general de publicaciones oficiales
http://publicaciones.administracion.es

EQUIPO RESPONSABLE DEL PROYECTO MAGERIT versión 2

Director:
Francisco López Crespo
Ministerio de Administraciones Públicas

Miguel Angel Amutio Gómez
Ministerio de Administraciones Públicas

Javier Candau
Centro Criptológico Nacional

Consultor externo:
José Antonio Mañas
Catedrático
Universidad Politécnica de Madrid

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 de análisis y gestión.

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. Consulte las referencias.

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. Relación de tipos

[S] Servicios
Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios. Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios). Así se encuentran servicios públicos prestados por la Administración para satisfacer necesidades de la colectividad; servicios empresariales prestados por empresas para satisfacer necesidades de sus clientes; servicios internos prestados por departamentos especializados dentro de la Organización, que son usados por otros departamentos u empleados de la misma; etc. Al centrarse esta guía en la seguridad de las tecnologías de la información y las comunicaciones, es natural que aparezcan servicios de información, servicios de comunicaciones, servicios de seguridad, etc. sin por ello ser óbice para encontrar otros servicios requeridos para el eficaz desempeño de la misión de la organización.

`[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 (usuarios y medios de la propia organización)`
`[cont] contratado a terceros (se presta con medios ajenos)`
 	
`[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.

[D] Datos / Información

Elementos de información que, de forma singular o agrupados de alguna forma, representan el conocimiento que se tiene de algo.

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

Es habitual que en un análisis de riesgos e impactos, el usuario se limite a valorar los datos, siendo los demás activos meros sirvientes que deben cuidar y proteger los datos que se les encomiendan.

```
[vr] datos vitales (vital records) (1)
[com] datos de interés comercial (2)
[adm] datos de interés para la administración pública
[int] datos de gestión interna

[voice] voz
[multimedia] multimedia
[source] código fuente
[exe] código ejecutable
[conf] datos de configuración
[log] registro de actividad (log)
[test] datos de prueba

[per] datos de carácter personal (3)
  [A] de nivel alto
  [M] de nivel medio
  [B] de nivel básico

[label] datos clasificados (4)
  [S] secreto
  [R] reservado
  [C] confidencial
  [DL] difusión limitada
  [SC] sin clasificar
```

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 aquellos que tienen valor para la prestación de los servicios propios de la organización.
3. 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.
4. 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.

[SW] Aplicaciones (software)
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.

[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
  [file] servidor de ficheros
  [dbms] sistema de gestión de bases de datos
  [tm] monitor transaccional
  [office] ofimática
  [av] anti virus
  [os] sistema operativo
  [ts] servidor de terminales
  [backup] sistema de backup

[HW] Equipos informáticos (hardware)

Dícese de bienes 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.

```
[host] grandes equipos (1)
[mid] equipos medios (2)
[pc] informática personal (3)
[mobile] informática móvil (4)
[pda] agendas electrónicas
[easy] fácilmente reemplazable (5)
[data] que almacena datos (6)
[peripheral] periféricos
  [print] medios de impresión (7)
  [scan] escáneres
  [crypto] dispositivos criptográficos
[network] soporte de la red (8)
  [modem] módems
  [hub] concentradores
  [switch] conmutadores
  [router] encaminadores
  [bridge] pasarelas
  [firewall] cortafuegos
  [wap] punto de acceso wireless
[pabx] centralita telefónica
```

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 que, en caso de avería temporal o definitiva pueden ser reemplazados pronta y económicamente.
6. Son aquellos equipos en los que los datos permanecen largo tiempo. En particular, se clasificarán de este tipo aquellos equipos que disponen de los datos localmente, a diferencia de aquellos que sólo manejan datos en tránsito.
7. Dícese de impresoras y servidores de impresión.
8. Dícese de equipamiento necesario para transmitir datos: *routers*, módems, etc.

[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.

```
[PSTN] red telefónica
[ISDN] rdsi (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL
[pp] punto a punto
[radio] red inalámbrica
[sat] por satélite
[LAN] red local
[MAN] red metropolitana
[Internet] Internet
[vpn] red privada virtual
```

[SI] 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.

```
[electronic] electrónicos
  [disk] discos
  [san] almacenamiento en red
  [disquette] disquetes
  [cd] cederrón (CD-ROM)
  [usb] dispositivos 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
```

[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.

```
[power] fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado
[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
```

[L] Instalaciones
En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

[site] emplazamiento
[building] edificio
[local] local
[mobile] plataformas móviles
  [car] vehículo terrestre: coche, camión, etc.
  [plane] vehículo aéreo: avión, etc.
  [ship] vehículo marítimo: buque, lancha, etc.
  [shelter] contenedores
[channel] canalización

[P] Personal
En este epígrafe aparecen las personas relacionadas con los sistemas de información.
[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [des] desarrolladores [sub] subcontratas [prov] proveedores

2.2. Datos de carácter personal

La clasificación de los datos de carácter personal depende de la legislación aplicable en cada lugar y circunstancia. 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. Nº 298, de 14 de diciembre de 1999)
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (B.O.E. Nº 151, de 25 de junio de 1999)

Esta legislación establece los siguientes criterios:

Nivel básico

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. LOPD artículo 3. RD artículo 4.1.

Nivel medio

Datos de carácter personal relativos a la comisión de infracciones administrativas o penales, Hacienda Pública o servicios financieros. RD artículos 4.2 y 4.4.

Nivel alto

Datos de carácter personal relativos a ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales sin consentimiento de las personas afectadas. RD artículo 4.3.

2.3. Datos clasificados

La clasificación de datos es un procedimiento administrativo propio de cada organización o sector de actividad, que determina las condiciones de tratamiento de la información en función de la necesidad de preservar su confidencialidad.

La Comunidad Europea se rige por

- Decisión de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento

interno (2001/844/CE, CECA, Euratom)

- Decisión del Consejo de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo (2001/264/EC)

en la que se establecen los siguientes niveles:

Secreto (Très secret UE / EU Top Secret)

Esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros.

Si existe la probabilidad de que la puesta en peligro de materiales marcados TRÈS SECRET UE/EU TOP SECRET:

- amenace directamente la estabilidad interna de la UE o de alguno de sus Estados miembros o de países amigos;
- cause un perjuicio excepcionalmente grave a las relaciones con gobiernos amigos;
- ocasione directamente la pérdida generalizada de vidas humanas;
- ocasione un daño excepcionalmente grave a la capacidad de funcionar efectivamente o a la seguridad de las fuerzas de los Estados miembros o a las de otros contribuyentes, o haga que cese la efectividad de operaciones de seguridad o de inteligencia sumamente valiosas;
- ocasione un grave daño a largo plazo a la economía de la UE o de los Estados miembros.

Reservado (Secret UE)

Esta clasificación se aplicará únicamente a la información y al material cuya divulgación no autorizada pueda suponer un perjuicio grave para los intereses de la Unión Europea o de uno o más de sus Estados miembros.

Si existe la probabilidad de que la puesta en peligro de materiales marcados SECRET UE:

- cree tensiones internacionales;
- cause un perjuicio grave a las relaciones con gobiernos amigos;
- ponga vidas en peligro directamente o dañe gravemente el orden público o la seguridad o libertad individuales;
- ocasione un daño grave a la capacidad de funcionar efectivamente o a la seguridad de las fuerzas de los Estados miembros o a las de otros contribuyentes, o haga que cese la efectividad de operaciones de seguridad o de inteligencia sumamente valiosas;
- ocasione un considerable daño material a los intereses financieros, monetarios, económicos o comerciales de la UE o de uno de sus Estados miembros.

Confidencial (Confidentiel UE)

Esta clasificación se aplicará a la información y al material cuya divulgación no autorizada pueda suponer un perjuicio para los intereses esenciales de la Unión Europea o de uno o más de sus Estados miembros.

Si existe la probabilidad de que la puesta en peligro de materiales marcados CONFIDENTIEL UE:

- perjudique las relaciones diplomáticas, es decir, ocasione una protesta formal u otras sanciones;
- perjudique la seguridad o libertad individuales;
- perjudique la capacidad de funcionar efectivamente o a la seguridad de las fuerzas de los Estados miembros o las de otros contribuyentes, o disminuya la efectividad de operaciones de seguridad o de inteligencia valiosas;

- menoscabe notablemente la viabilidad financiera de organizaciones importantes;
- impida la investigación de delitos graves o facilite su comisión;
- menoscabe notablemente los intereses financieros, económicos y comerciales de la UE o de sus Estados miembros;
- ponga graves obstáculos al desarrollo o al funcionamiento de políticas prioritarias de la UE;
- interrumpa o perturbe notablemente actividades importantes de la UE.

Difusión limitada (Restreint UE)

Esta clasificación se aplicará a la información y al material cuya divulgación no autorizada pueda resultar desventajosa para los intereses de la Unión Europea o de uno o más de sus Estados miembros.

Si existe la probabilidad de que la puesta en peligro de materiales marcados RESTREINT UE:

- afecte desfavorablemente a las relaciones diplomáticas;
- causar considerable sufrimiento a individuos;
- dificulte el mantenimiento de la eficacia operativa o la seguridad de las fuerzas de los Estados miembros o de otros contribuyentes;
- ocasione pérdidas financieras o facilite ganancias o ventajas indebidas a individuos o empresas;
- quebrante el debido esfuerzo por mantener la reserva de la información facilitada por terceros;
- quebrante restricciones legales a la divulgación de información;
- dificulte la investigación o facilite la comisión de delitos;
- ponga en desventaja a la UE o a sus Estados miembros en negociaciones comerciales o en actuaciones de otra índole con terceros;
- ponga obstáculos al desarrollo o al funcionamiento efectivos de políticas prioritarias de la UE;
- menoscabe la adecuada gestión de la UE y sus operaciones.

2.3.1. Ley de secretos oficiales

La normativa europea citada anteriormente recoge la normativa española previa, Ley y Reglamento de Secretos Oficiales, que regula los procedimientos y medidas necesarias para la protección de las “materias clasificadas”.

- Ley 48/1978 de 7 de octubre, que modifica la Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Decreto 242/1969, de 20 de Febrero. por el que se desarrollan las disposiciones de la Ley 9/1968. de 5 de abril sobre Secretos Oficiales.
- Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales.

La ley 9 determina:

Artículo 2.

A los efectos de esta Ley podrán ser declaradas «materias clasificadas» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado.

Artículo 3.

Las «materias clasificadas» serán calificadas en las categorías de secreto y reservado en

atención al grado de protección que requieran.

Precisándose en el reglamento:

Articulo tercero, Materias clasificadas de «secreto» y de «reservado»

I. La clasificación de «secreto» se aplicará a todas las materias referidas en el artículo anterior que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado, o pudiera comprometer los Intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.

II. La clasificación de «reservado» se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a los referidos intereses fundamentales de la Nación, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

2.4. Sintaxis 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.

La notación se describe en el apéndice 1.

```
tipos ::=
  <tipos>
    { tipo }*
  </tipos>

tipo ::=
  <tipo código>
    #nombre#
    [ descripción ]
    { tipo }*
  </tipo>

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

Atributos

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

2.5. Referencias

Existen numerosas fuentes que identifican activos dentro del ámbito de las tecnologías de la información y las comunicaciones.

- GMITS, ISO/IEC IS 13335-1:2004, “Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management”.
- 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
- UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la

Gestión de la Seguridad de la Información". 2002.

- "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/

- GMITS, ISO/IEC TR 13335-5: 2001, "Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security"
- GMITS, ISO/IEC TR 13335-4: 2000, "Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards"
- GMITS, ISO/IEC TR 13335-3:1998, "Information technology - Security techniques - Guidelines for the management of IT security - Part 3: Techniques for management of IT security" Publicado como UNE 71501-3.
- MAGERIT, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997

  http://www.csi.map.es/csi/pg5m20.htm

- GMITS, ISO/IEC TR 13335-2:1997, "Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security" Publicado como UNE 71501-2.

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. Relación de dimensiones

[D] disponibilidad
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
¿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.

[I] integridad de los datos
Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
¿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.

[C] confidencialidad de los datos
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
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.

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.

[A_S] autenticidad de los usuarios del servicio
Aseguramiento de la identidad u origen.
¿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.

[A_D] autenticidad del origen de los datos
Aseguramiento de la identidad u origen.
¿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.

[T_S] trazabilidad del servicio
Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
¿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.

[T_D] trazabilidad de los datos
Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
¿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.

3.2. Sintaxis 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.

La notación se describe en el apéndice 1.

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

dimensión ::=
  <dimension código>
    #nombre#
    [ descripción ]
```

```
  </dimension>

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

Atributos

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

3.3. Referencias

- ISO/IEC 13335-1:2004, “Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management”, 2004.
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

  http://www.cert.org/octave/
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”, December 2003.

  http://csrc.nist.gov/publications/fips/index.html
- ISO/IEC 17799:2000, “Information technology -- Code of practice for information security management”, 2000.
- Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

  http://www.csi.map.es/csi/pg5m20.htm
- ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture”, 1989.

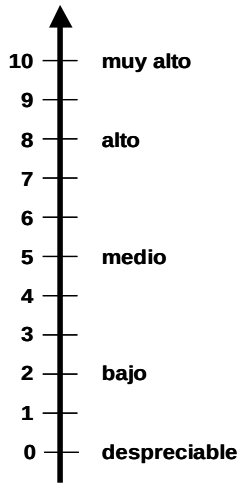
4. Criterios de valoración

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, permitiéndo 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; 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 5 niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:



valor		*criterio*
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a efectos prácticos

La tabla siguiente pretende guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos, habiéndose tomado en consideración los siguientes:

- seguridad de las personas
  - información de carácter personal[4]
- obligaciones derivadas de la ley, del marco regulatorio, de contratos, etc.
- capacidad para la persecución de delitos
- intereses comerciales y económicos
- pérdidas financieras
- interrupción del servicio

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.

4 La información de carácter personal se califica por dos vías: administrativa y valorada. La vía administrativa consiste en indicar a qué nivel pertenece el dato en cuestión; siendo esta una decisión cualitativa, las salvaguardas a emplear son independientes del valor que el dato en sí tenga para la organización. La vía valorada asigna un nivel a las consecuencias que para la organización tendría el deterioro del dato. De esta forma se distingue entre las obligaciones legales y los perjuicios para el servicio, sin obviar ninguno de estos aspectos, ambos importantes.

- orden público
- política corporativa
- otros valores intangibles

Lo más normal es que un activo reciba una simple valoración en cada dimensión en la que es valioso. Este planteamiento puede y debe ser enriquecido en el caso de dimensiones más complejas como es el caso de la disponibilidad, en la que las consecuencias varían dependiendo del tiempo que dure la interrupción. En estos casos, la dimensión no recibe una única calificación, sino tantas como escalones se hayan considerado relevantes. Los criterios que siguen se aplican en cada escalón, pudiendo variar el motivo[5].

4.1. Escala estándar

valor	*criterio*	
10	[olm]	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
	[iio]	Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información
	[si]	Seguridad: probablemente sea causa de un incidente excepcionalmente serior de seguridad o dificulte la investigación de incidentes excepcionalmente serios
	[ps]	Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas
	[po]	Orden público: alteración seria del orden constitucional
	[ir]	Probablemente cause un impacto excepcionalmente grave en llas relaciones internacionales
	[lbl]	Datos clasificados como secretos

5 Por ejemplo, una interrupción breve puede causar la desafección de los usuarios mientras que una interrupción larga puede llevar a penalizaciones por incumplimiento de obligaciones administrativas.

valor	*criterio*
9	[da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [adm] Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre [lg] Probablemente causaría causaría una publicidad negativa generalizada por por afectar de forma excepcionalmente grave a las relaciones ... [lg.a] a las relaciones con otras organizaciones [lg.b] a las relaciones con el público en general [lg.c] a las relaciones con otros paises [olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística [iio] Probablemente cause serios daños a misiones muy importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de enorme interés para la competencia [cei.b] de muy elevado valor comercial [cei.c] causa de pérdidas económicas excepcionalmente elevadas [cei.d] causa de muy significativas ganancias o ventajas para individuos u organizaciones [cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros [lro] Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación [si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios [ps] Seguridad de las personas: probablemente suponga la muerte de uno o más individuos [po] Orden público: alteración seria del orden público [ir] Probablemente cause un serio impacto en las relaciones internacionales [lbl] Datos clasificados como reservados
8	[ps] Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo, es probable que llegue a amenazar la vida de uno o más individuos) [crm] Impida la investigación de delitos graves o facilite su comisión [lbl] Datos clasificados como confidenciales

valor	*criterio*
7	[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones [adm] Administración y gestión: probablemente impediría la operación efectiva de la organización [lg] Probablemente causaría una publicidad negativa generalizada [lg.a] por afectar gravemente a las relaciones con otras organizaciones [lg.b] por afectar gravemente a las relaciones con el público en general [lg.c] por afectar gravemente a las relaciones con otros paises [olm] Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística [iio] Probablemente cause serios daños a misiones importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de alto interés para la competencia [cei.b] de elevado valor comercial [cei.c] causa de graves pérdidas económicas [cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones [cei.e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros [lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación [si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos [ir] Probablemente cause un impacto significativo en las relaciones internacionales [lbl] Datos clasificados como confidenciales
6	[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos [pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal [ps] Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo [po] Orden público: probablemente cause manifestaciones, o presiones significativas [lbl] Datos clasificados como de difusión limitada

valor	*criterio*
5	[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones [adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización [lg] Probablemente sea causa una cierta publicidad negativa [lg.a] por afectar negativamente a las relaciones con otras organizaciones [lg.b] por afectar negativamente a las relaciones con el público [olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local [iio] Probablemente dañe a misiones importantes de inteligencia o información [pi1] Información personal: probablemente afecte gravemente a un individuo [pi2] Información personal: probablemente quebrante seriamente leyes o regulaciones [lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación [ir] Probablemente tenga impacto en las relaciones internacionales [lbl] Datos clasificados como de difusión limitada
4	[pi1] Información personal: probablemente afecte a un grupo de individuos [pi2] Información personal: probablemente quebrante leyes o regulaciones [ps] Seguridad de las personas: probablemente cause daños menores a varios individuos [crm] Dificulte la investigación o facilite la comisión de delitos [lbl] Datos clasificados como de difusión limitada

valor	*criterio*
3	[da] Probablemente cause la interrupción de actividades propias de la Organización [adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización [lg] Probablemente afecte negativamente a las relaciones internas de la Organización [olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local) [iio] Probablemente cause algún daño menor a misiones importantes de inteligencia o información [cei] Intereses comerciales o económicos: [cei.a] de cierto interés para la competencia [cei.b] de cierto valor comercial [cei.c] causa de pérdidas financieras o merma de ingresos [cei.d] facilita ventajas desproporcionadas a individuos u organizaciones [cei.e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros [pi1] Información personal: probablemente afecte a un individuo [pi2] Información personal: probablemente suponga el incumplimiento de una ley o regulación [lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación [si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente [ps] Seguridad de las personas: probablemente cause daños menores a un individuo [po] Orden público: causa de protestas puntuales [ir] Probablemente cause un impacto leve en las relaciones internacionales [lbl] Datos clasificados como de difusión limitada
2	[lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización [cei] Intereses comerciales o económicos: [cei.a] de bajo interés para la competencia [cei.b] de bajo valor comercial [pi1] Información personal: pudiera causar molestias a un individuo [pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones [ps] Seguridad de las personas: pudiera causar daño menor a varios individuos [lbl] Datos clasificados como sin clasificar

valor	*criterio*	
1	[da]	Pudiera causar la interrupción de actividades propias de la Organización
	[adm]	Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización
	[lg]	Pudiera causar una pérdida menor de la confianza dentro de la Organización
	[olm]	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
	[iio]	Pudiera causar algún daño menor a misiones importantes de inteligencia o información
	[cei]	Intereses comerciales o económicos:
	[cei.a]	de pequeño interés para la competencia
	[cei.b]	de pequeño valor comercial
	[pi1]	Información personal: pudiera causar molestias a un individuo
	[lro]	Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación
	[si]	Seguridad: pudiera causar una merma en la seguridad o dificular la investigación de un incidente
	[ps]	Seguridad de las personas: pudiera causar daños menores a un individuo
	[po]	Orden público: pudiera causar protestas puntuales
	[ir]	Pudiera tener un impacto leve en las relaciones internacionales
	[lbl]	Datos clasificados como sin clasificar
0	[1]	no afectaría a la seguridad de las personas
	[2]	sería causa de inconveniencias mínimas a las partes afectadas
	[3]	supondría pérdidas económicas mínimas
	[4]	no supondría daño a la reputación o buena imagen de las personas u organizaciones

4.2. Sintaxis 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.

La notación se describe en el apéndice 1.

```
valoración ::=
  <valoracion>
    { nivel }*
  </valoracion>

nivel ::=
  <nivel valor código>
    { ítem }*
  </nivel>

ítem ::=
  <item>
    #descripción#
  </item>
```

Atributos

Atributo	*Ejemplo*	*Descripción*
valor	V=”X”	X es un índice entre 0 y 10 de valoración cualitativa de activos.
código	C=”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”

4.3. Referencias

- 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.

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema.	

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

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.

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.

[I.1] Fuego	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema.	

[I.2] Daños por agua	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	

[I.*] Desastres industriales	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
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.	

[I.3] Contaminación mecánica	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: vibraciones, polvo, suciedad, ...	

[I.4] Contaminación electromagnética	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electrónicos) ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ...	

[I.5] Avería de origen físico o lógico	
Tipos de activos: ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
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.	

[I.6] Corte del suministro eléctrico	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electrónicos) ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: cese de la alimentación de potencia	

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...	

[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.	

[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, ...	

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: ▯ [SI] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: como consecuencia del paso del tiempo	

[I.11] Emanaciones electromagnéticas	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [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.

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.

[E.1] Errores de los usuarios	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.	

[E.2] Errores del administrador	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: equivocaciones de personas con responsabilidades de instalación y operación	

[E.3] Errores de monitorización *(log)*	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [T_S] trazabilidad del servicio 2. [T_D] trazabilidad de los datos
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...	

[E.4] Errores de configuración

Tipos de activos:	**Dimensiones:**
[S] servicios [D] datos / información [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos

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.

[E.7] Deficiencias en la organización

Tipos de activos:	**Dimensiones:**
[P] personal	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.

[E.8] Difusión de software dañino

Tipos de activos:	**Dimensiones:**
[SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos

Descripción:
propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.

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

Tipos de activos:	**Dimensiones:**
[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio

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.

[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.	

[E.14] Escapes de información	
Tipos de activos: ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**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.	

[E.15] Alteración de la información	
Tipos de activos: ▯ [D] datos / información	**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.	

[E.16] Introducción de información incorrecta	
Tipos de activos: ▯ [D] datos / información	**Dimensiones:** 1. [I] integridad
Descripción: inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

[E.17] Degradación de la información	
Tipos de activos: ▯ [D] datos / información	**Dimensiones:** 1. [I] integridad
Descripción: degradación 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.	

[E.18] Destrucción de información	
Tipos de activos: ▯ [D] datos / información	**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.

[E.19] Divulgación de información	
Tipos de activos: • [D] datos / información	**Dimensiones:** 1. [C] confidencialidad

Descripción:
revelación por indiscreción.

Incontinencia verbal, medios electrónicos, soporte papel, etc.

[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.

[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.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware)	**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.

[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.

[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, ...	

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.

[A.4] Manipulación de la configuración	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos 7. [D] 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.	

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A_S] autenticidad del servicio 3. [A_D] autenticidad de los datos 4. [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.	

[A.6] Abuso de privilegios de acceso	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad

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.

[A.7] Uso no previsto	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
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.	

[A.8] Difusión de software dañino	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.	

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio
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.	

[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.	

[A.11] Acceso no autorizado	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio
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.	

[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”.	

[A.13] Repudio	
Tipos de activos: ▯ [S] servicios	**Dimensiones:** 1. [T_S] trazabilidad del servicio
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.	

[A.14] Interceptación de información (escucha)

Tipos de activos:	**Dimensiones:**
[D] datos / información [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	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.

[A.15] Modificación de la información

Tipos de activos:	**Dimensiones:**
[D] datos / información	1. [I] integridad

Descripción:
alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.16] Introducción de falsa información

Tipos de activos:	**Dimensiones:**
[D] datos / información	1. [I] integridad

Descripción:
inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.17] Corrupción de la información

Tipos de activos:	**Dimensiones:**
[D] datos / información	1. [I] integridad

Descripción:
degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.18] Destrucción la información

Tipos de activos:	**Dimensiones:**
[D] datos / información	1. [D] disponibilidad

Descripción:
eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.19] Divulgación de información	
Tipos de activos: ▯ [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación de información.	

[A.22] Manipulación de programas	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

[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.	

[A.25] Robo	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [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.	

[A.26] Ataque destructivo	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] 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.	

[A.27] Ocupación enemiga	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [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.	

[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, ...	

[A.29] Extorsión	
Tipos de activos: ▯ [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	

[A.30] Ingeniería social	
Tipos de activos: ▯ [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

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[6]:

número	*error*	*ataque*
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización *(log)*	
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 de la información	Modificación de la información
16	Introducción de información incorrecta	Introducción de falsa información
17	Degradación de la información	Corrupción de la información
18	Destrucción de información	Destrucción la información
19	Divulgación de información	Divulgación de información

6 Se deja en blanco la columna “ataque” cuando la amenaza es simplemente por error. Se deja en blanco la columna “error” cuando la amenaza siempre es deliberada.

número	*error*	*ataque*
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)	
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25		Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social

5.6. Amenazas por tipo de activos

Para completar la anterior presentación amenaza por amenaza, los siguientes cuadros agrupan las amenazas según el tipo de activo, indicando en qué dimensión puede afectarles significativamente. Nótese que debido a las dependencias entre activos, los activos inferiores soportan el valor de los activos superiores, siendo aquellos la vía por la que resultan perjudicados estos.

5.6.1. [S] Servicios

Las siguientes amenazas pueden materializarse sobre los activos de tipo [S], con consecuencias para la seguridad del sistema de información.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
E.1 E.2 E.4 E.24	E.1 E.2 E.4 E.9 E.10	E.2 E.4 E.9	E.2 E.4 E.9	E.2 E.3 E.4 E.9
A.4 A.7 A.24	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11	A.4 A.5 A.9 A.11	A.4 A.9 A.13

5.6.2. [D] Datos / Información

Las siguientes amenazas pueden materializarse sobre los activos de tipo [D], con consecuencias para la seguridad del sistema de información.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
E.1 E.2 E.3 E.18	E.1 E.2 E.3 E.15 E.16 E.17	E.2 E.3 E.14 E.19	E.2 E.4	E.2 E.3 E.4
A.4 A.18	A.4 A.11 A.15 A.16 A.17	A.4 A.11 A.14 A.19	A.4 A.11	A.4

5.6.3. [SW] Aplicaciones (software)

Las siguientes amenazas pueden materializarse sobre los activos de tipo [SW], con consecuencias para la seguridad del sistema de información.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
I.5				I.5
E.1 E.2 E.4 E.8 E.20 E.21	E.1 E.2 E.4 E.8 E.9 E.10 E.20 E.21	E.2 E.4 E.8 E.9 E.14 E.20	E.2 E.4 E.8 E.9	E.2 E.3 E.4 E.8 E.9
A.4 A.7 A.8	A.4 A.5 A.6 A.8 A.9 A.10 A.11 A.22	A.4 A.5 A.6 A.8 A.9 A.11 A.14 A.22	A.4 A.5 A.8 A.9 A.11 A.22	A.4 A.8 A.9 A.22

5.6.4. [HW] Equipos informáticos (hardware)

Las siguientes amenazas pueden materializarse sobre los activos de tipo [HW], con consecuencias para la seguridad del sistema de información.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7

[D]	[I]	[C]	[A_*]	[T_*]
E.2 E.4 E.23 E.24	E.2 E.4	E.2 E.4	E.2 E.4	E.2 E.4
A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.6 A.11	A.4 A.6 A.11 A.14 A.25 A.27	A.4 A.11	A.4

5.6.5. [COM] Redes de comunicaciones

Las siguientes amenazas pueden materializarse sobre los activos de tipo [COM], con consecuencias para la seguridad del sistema de información.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.8		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
E.2 E.4 E.24	E.2 E.4 E.9 E.10	E.2 E.4 E.9 E.14	E.2 E.4 E.9	E.2 E.4 E.9
A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11 A.12 A.14 A.25	A.4 A.5 A.9 A.11	A.4 A.9

5.6.6. [SI] Soportes de información

Las siguientes amenazas pueden materializarse sobre los activos de tipo [SI], con consecuencias para la seguridad del sistema de información.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10

[D]	[I]	[C]	[A_*]	[T_*]
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

5.6.7. [AUX] Equipamiento auxiliar

Las siguientes amenazas pueden materializarse sobre los activos de tipo [AUX], con consecuencias para la seguridad del sistema de información.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.9				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

5.6.8. [L] Instalaciones

Las siguientes amenazas pueden materializarse sobre los activos de tipo [L], con consecuencias para la seguridad del sistema de información.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.*				N.1 N.2 N.* I.1 I.2 I.*
A.7 A.26 A.27	A.11	A.11 A.27	A.11	

5.6.9. [P] Personal

Las siguientes amenazas pueden materializarse sobre los activos de tipo [P], con consecuencias para la seguridad del sistema de información.

[D]	[I]	[C]	[A_*]	[T_*]
E.7 E.28				
A.28	A.29 A.30	A.29 A.30	A.29 A.30	A.29 A.30

5.6.10. Disponibilidad

Las siguientes amenazas pueden materializarse sobre diferentes tipos de activos, con consecuencias para la disponibilidad del sistema de información.

	destrucción	***avería***		***saturación***	***carencia***
		física	***lógica***		
[S] servicios			E.1 E.2 E.3 A.4	A.7 E.24 A.24	
[D] datos / información	E.1 E.2 E.18 A.18		E.1 E.2 E.4 A.4		
[SW] aplicaciones (software)			I.5 E.1 E.2 E.4 E.20 E.21 A.4 E.8 A.8	A.7	
[HW] equipos informáticos (hardware)	N.1 N.2 N.* I.1 I.2 I.* I.3 I.7 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.7	I.4 E.2 E.4 A.4 E.23	A.7 E.24 A.24	I.6 A.25
[COM] redes de comunicaciones	N.1 N.2 N.* I.1 I.2 I.* I.3 I.7 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.7	I.4 E.2 E.4 A.4	A.7 E.24 A.24	I.6 I.8 A.25
[SI] soportes de información	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.7 I.10 A.26 A.27	N.2 I.2 I.3 I.4 I.5		A.7	I.6 A.25
[AUX] equipamiento auxiliar	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.2* I.3 I.4 I.5 I.7		A.7	I.6 I.9 A.25
[L] instalaciones	N.1 N.2 N.* I.1 I.2 I.* A.26 A.27	N.1 N.2 N.* I.1 I.2 I.*		A.7	
[P] personas			E.7		E.28 A.28

5.7. Sintaxis 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.

La notación se describe en el apéndice 1.

```
amenazas ::=
  <amenazas>
    { grupo }*
  </amenazas>

grupo ::=
  <grupo>
    { grupo | amenaza }*
    [ descripción ]
```

```
  </grupo>

amenaza ::=
  <amenaza código_amenaza>
    #nombre#
    { dimensión }+
    [ descripción ]
  </amenaza >

dimensión ::=
  <dimension código_dimensión>

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

Atributos

Atributo	*Ejemplo*	*Descripción*
código_amenaza	Z=”X”	X es un identificador único que permite determinar unívocamente a qué amenaza se refiere.
código_dimensión	D=”X”	X es un identificador único que permite determinar unívocamente a qué dimensión se refiere.

5.8. Referencias

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

- GMITS, ISO/IEC IS 13335-1:2004, “Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management”.
- 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/
- GMITS, ISO/IEC TR 13335-5: 2001, “Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security”
- GMITS, ISO/IEC TR 13335-4: 2000, “Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards”
- GMITS, ISO/IEC TR 13335-3:1998, “Information technology - Security techniques - Guidelines for the management of IT security - Part 3: Techniques for management of IT security” Publicado como UNE 71501-3.
- MAGERIT, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997

  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, “Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security” Publicado como UNE 71501-2.

6. Salvaguardas

Las salvaguardas permiten hacer frente a las amenazas. Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

[PR] procedimientos, que siempre son necesarios; a veces bastan procedimientos, pero otras veces los procedimientos son un componente de una salvaguarda más compleja. Se requieren procedimientos tanto para la operación de las salvaguardas preventivas como para la gestión de incidencias y la recuperación tras las mismas. Los procedimientos deben cubrir aspectos tan diversos como van del desarrollo de sistemas la configuración del equipamiento.

[PER] política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.

Soluciones técnicas, frecuentes en el entorno de las tecnologías de la información, que pueden ser

[SW] aplicaciones (software)

[HW] dispositivos físicos

[COM] protección de las comunicaciones

[FIS] seguridad física, de los locales y áreas de trabajo

La protección integral de un sistema de información requerirá una combinación de salvaguardas de los diferentes aspectos comentados, debiendo la solución final

1. estar equilibrada en los diferentes aspectos
2. tener en cuenta las salvaguardas adecuadas a cada tipo de activos
3. tener en cuenta las salvaguardas adecuadas a la dimensión de valor del activo
4. tener en cuenta las salvaguardas adecuadas a la amenaza a conjurar

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 determinar requisitos que deberán ser satisfechos por la solución práctica que se elija.

6.1. Salvaguardas de tipo general

Son aquellas que se refieren al buen gobierno de la seguridad con efectos beneficiosos sobre todo tipo de activos.

- Organización de la seguridad: roles, comités, ...
- Política corporativa de seguridad de la información
- Gestión de privilegios: adjudicación, revisión y terminación
- Procedimientos de escalado y gestión de incidencias
- Procedimientos de continuidad de operaciones: emergencia y recuperación

- Auditoría, registro (certificación) y acreditación del sistema

6.2. Salvaguardas para la protección de los servicios

ciclo de vida	*protección del valor*

• Especificación del servicio
• Desarrollo del servicio
• Despliegue del servicio
• Operación del servicio
• Terminación del servicio
	[A_S] →
	  • Control de acceso
	[T_S] →
	  • Registro de actuaciones
	  • Registro de incidencias
	[D] →
	  • Plan de continuidad

El control de acceso es un servicio de salvaguarda recurrente que se aplica en múltiples tipos de activos: acceso a los servicios, acceso a las aplicaciones, acceso al sistema operativo, acceso a los soportes de información, acceso físico a las instalaciones, etc. En todos ellos se requiere un sistema de identificación y autenticación que determine quién es el aspirante (sea persona u otro programa) y se coordine con el sistema de gestión de privilegios.

Los mecanismos de identificación y autenticación son múltiples y pueden combinarse de diferentes formas. Cabe destacar los siguientes:

- **contraseñas:** útil para sistemas que soportan poco riesgo, o como complemento a otros mecanismos
- **certificados digitales:** útil en sistemas expuestos a amenazas de repudio
- **dispositivos (tokens o tarjetas):** útil en sistemas que soportan riesgo elevado o requisitos de urgente disponibilidad
- **características biométricas:** útil para identificar personas, que no roles.

6.3. Salvaguardas para la protección de los datos / información

organización	*protección del valor*

• Carácter personal, si procede
  • documento de seguridad
• Clasificación, si procede
• Gestión de claves, si se emplea cifrado
	[A_D] →
	  • Control de acceso
	  • Firma electrónica
	[T_D] →
	  • Registro de actuaciones
	  • Registro de incidencias
	[D] →
	  • Copias de respaldo
	[I] →
	  • Detección y recuperación
	[C] →
	  • Cifrado (preventivo)
	  • Marcado (persecución)

6.4. Salvaguardas para la protección de las aplicaciones (software)

ciclo de vida	*protección del valor*

• Especificación funcional y no funcional
• Desarrollo
  • desarrollo seguro
  • protección del código fuente
• Aceptación y puesta en operación
• Explotación
  • gestión de cambios y configuración
  • gestión de incidencias
• Homologación / certificación / acreditación
	[I] →
	  • Protección frente a código dañino: virus, troyanos, puertas traseras, etc.
	[A_S, A_D] →
	  • Control de acceso
	[T_S, T_D] →
	  • Registro de actuaciones

6.5. Salvaguardas para la protección de los equipos (hardware)

seguridad física	*seguridad del sistema operativo*

• Inventario
• Control de entradas y salidas
• Destrucción
• Homologación / certificación / acreditación
	• Configuración
	  • equipos internos
	  • equipos que salen de los locales
	• Mantenimiento
	[I] →
	  • Protección frente a código dañino: virus, espías, etc.
	  • detección de intrusión
	• Registro de actuaciones
	• Gestión de privilegios
	• Control de acceso

6.6. Salvaguardas para la protección de las comunicaciones

ciclo de vida	*protección del valor*

• Planificación de capacidad
• Adquisición y mantenimiento
• Configuración
  • segregación de redes
  • configuración de *routers*
  • configuración de cortafuegos
• Gestión de claves, si se emplea cifrado
• Detección de intrusión
  • monitorización de uso
	• [D] → Plan de continuidad
	• [I] → Garantías de integridad
	• [C] → Cifrado
	• [A_S] → Control de acceso
	• [T_S] → Registro de actuaciones

6.7. Seguridad física

protección de las instalaciones

• Protección frente a accidentes naturales
  • terremotos, riadas, incendios, tormentas, etc.
• Protección frente a accidentes industriales
  • incendio, inundación, etc.
  • contaminación mecánica: polvo, vibraciones
  • contaminación electromagnética
• Protección frente a emanaciones electromagnéticas
• Protección del recinto: edificios, locales y áreas de trabajo
  • anuncio mínimo
  • barreras físicas
  • protección del cableado
• Control de acceso: entrada y salida de personas, equipos, soportes de información, etc.

6.8. Salvaguardas relativas al personal

ciclo de vida
• Especificación del puesto de trabajo • Selección de personal • Condiciones contractuales: responsabilidad en seguridad • Formación continua

6.9. Externalización

Es cada vez más flexible la frontera entre los servicios de seguridad prestados internamente y los servicios contratados a terceras partes:

- Desarrollo de aplicaciones o equipos
- Aplicaciones que ejecutan en otro lugar con acceso remoto (ASP – Application Service Provisioning)
- Mantenimiento de programas y equipos
- Seguridad gestionada: monitorización remota y gestión delegada de incidencias
- Prestación de servicios de comunicaciones
- Prestación de servicios de custodia de datos / información
- etc.

En todos 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

6.10. Referencias

- "Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades", MAP, 2004
  http://www.csi.map.es/csi/pg5c10.htm
- Centro Criptológico Nacional. Instrucción Técnica de Seguridad de las TIC (CCN-STIC-302). Interconexión de CIS que manejen información clasificada nacional en la Administración". Versión 1.2. Marzo de 2004.
- ISO/IEC TR 15446:2004, "Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets".
- GMITS, ISO/IEC IS 13335-1:2004, "Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management".
- "COBIT Security Baseline", ISACA, 2004.
  http://www.isaca.org/
- "IT Baseline Protection Manual", Federal Office for Information Security (BSI), Germany. October 2003.
  http://www.bsi.de/gshb/english/etc/index.htm
- "The Standard of Good Practice for Information Security", ISF. 2003
  http://www.isfsecuritystandard.com/index_ns.htm
- NIST Special Publication 800-53: "Recommended Security Controls for Federal Information Systems". 31 October, 2003.
  http://csrc.nist.gov/publications/index.html
- DoD Instruction 8500-2p, "Information Assurance (IA) Implementation". Feb. 2003.
- UNE-ISO/IEC 17799:2002, "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información". 2002.
- "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/
- GMITS, ISO/IEC TR 13335-5: 2001, "Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security"
- GMITS, ISO/IEC TR 13335-4: 2000, "Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards"
- ISO/IEC 15408, "Information technology — Security techniques — Evaluation criteria for IT security", 1999.
  `http://www.commoncriteriaportal.org/`
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- GMITS, ISO/IEC TR 13335-3:1998, "Information technology - Security techniques - Guidelines for the management of IT security - Part 3: Techniques for management of IT security" Publicado como UNE 71501-3.
- MAGERIT, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997
  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, "Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security" Publicado como UNE 71501-2.

Apéndice 1. Notación XML

Las descripciones de formatos XML se ajustan a la siguiente notación de tipo BNF[7]:

- 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

7 **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.

Para cada tipo de activo:

- [D] datos / información
- [S] servicios
- [SW] aplicaciones (software)
- [HW] equipamiento informático (hardware)
- [COM] redes de comunicaciones
- [SI] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones
- [P] personal

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

[D] Datos / información

[D] Datos / Información	
código:	**nombre:**
descripción:	
propietario:	
responsable:	

tipo (marque todos los adjetivos que procedan):

( ) [vr] datos vitales *(vital records)*

( ) [com] datos de interés comercial

( ) [adm] datos de interés para la administración pública

( ) [int] datos de gestión interna

( ) [source] código fuente

( ) [exe] código ejecutable

( ) [conf] datos de configuración

( ) [log] registro de actividad *(log)*

( ) [test] datos de prueba

( ) [per] datos de carácter personal

- ( ) [A] de nivel alto
- ( ) [M] de nivel medio
- ( ) [B] de nivel básico

( ) [label] datos clasificados

- ( ) [S] secreto
- ( ) [R] reservado
- ( ) [C] confidencial
- ( ) [DL] difusión limitada
- ( ) [SC] sin clasificar

Valoración de los datos / información, típicamente en las siguientes dimensiones de seguridad:

[I] integridad

[C] confidencialidad

[A_D] autenticidad de quién accede a los datos

[T_D] trazabilidad de quién accede a los datos, cuándo y qué hace

Valoración		
dimensión	***valor***	***justificación***
[I]		
[C]		
[A_D]		
[T_D]		

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[S] Servicios

[S] Servicios	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan): ( ) [anon] anónimos (sin requerir identificación del usuario) ( ) [pub] al público en general (sin relación contractual) ( ) [ext] a usuarios externos (bajo una relación contractual) ( ) [int] interno (usuarios y medios de la propia organización) ( ) [cont] contratado a terceros (se presta con medios ajenos) ( ) [www] world wide web ( ) [telnet] acceso remoto a cuenta local ( ) [email] correo electrónico ( ) [ftp] transferencia de ficheros ( ) [edi] intercambio electrónico de datos ( ) [dir] servicio de directorio ( ) [idm] gestión de identidades ( ) [ipm] gestión de privilegios ( ) [pki] PKI – infraestructura de clave pública	

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

[D] disponibilidad

[A_S] autenticidad de quién accede al servicio

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

Valoración		
dimensión	***valor***	***justificación***
[D]		
[A_S]		
[T_S]		

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[SW] Aplicaciones (software)

[SW] Aplicaciones (software)	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan): ( ) [prp] desarrollo propio *(in house)* ( ) [sub] desarrollo a medida (subcontratado) ( ) [std] estándar *(off the shelf)* ( ) [browser] navegador web ( ) [www] servidor de presentación ( ) [email_client] cliente de correo electrónico ( ) [app] servidor de aplicaciones ( ) [file] servidor de ficheros ( ) [dbms] sistema de gestión de bases de datos ( ) [tm] monitor transaccional ( ) [office] ofimática ( ) [av] anti virus ( ) [backup] sistema de backup ( ) [os] sistema operativo	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[HW] Equipamiento informático (hardware)

[HW] Equipamiento informático (hardware)	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	

tipo (marque todos los adjetivos que procedan):

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- ( ) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - ( ) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- ( ) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[COM] Redes de comunicaciones

[COM] Redes de comunicaciones	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan): ( ) [PSTN] red telefónica ( ) [ISDN] rdsi (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto ( ) [radio] red inalámbrica ( ) [sat] satélite ( ) [LAN] red local ( ) [MAN] red metropolitana ( ) [Internet] Internet ( ) [vpn] red privada virtual	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[SI] Soportes de información

[SI] Soportes de información	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan): ( ) [electronic] electrónicos ( ) [disk] discos ( ) [disquette] disquetes ( ) [cd] cederrón (CD-ROM) ( ) [usb] dispositivos 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	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[AUX] Equipamiento auxiliar

[AUX] Equipamiento auxiliar	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan): ( ) [power] fuentes de alimentación ( ) [ups] sistemas de alimentación ininterrumpida ( ) [gen] generadores eléctricos ( ) [ac] equipos de climatización ( ) [cabling] cableado ( ) [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	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[L] Instalaciones

[L] Instalaciones	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan): ( ) [site] emplazamiento ( ) [building] edificio ( ) [local] local ( ) [mobile] plataformas móviles ( ) [car] vehículo terrestre: coche, camión, etc. ( ) [plane] vehículo aéreo: avión, etc. ( ) [ship] vehículo marítimo: buque, lancha, etc. ( ) [shelter] contenedores ( ) [channel] canalización	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

[P] Personal

[P] Personal	
código:	**nombre:**
descripción:	
número:	
tipo (marque todos los adjetivos que procedan): ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores ( ) [adm] administradores de sistemas ( ) [com] administradores de comunicaciones ( ) [dba] administradores de BBDD ( ) [des] desarrolladores ( ) [sub] subcontratas ( ) [prov] proveedores	

Valoración (si procede)		
dimensión	***valor***	***justificación***

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

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

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.

3.1. 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.

4.1. 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

4.2. 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

4.3. 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.

4.4. 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.

4.5. 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.

4.6. 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.