ESTUDIO DE UNA ESTRATEGIA PARA LA IMPLANTACIÓN DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Curso de Doctorado
Plan 7440 Ingeniería en Automática y Electrónica Industrial, Ingeniería Informática y Sistemas Eléctricos

Periodo de investigación

Curso 2002/2003

Autor
Manuel Fernández Barcell
Universidad de Cádiz
Dpto. de Lenguajes y Sistemas Informáticos
manuel.barcell@uca.es

Índice

Índice de figuras

Índice de tablas

Resumen:

Para el cumplimiento del plan de acción eEurope 2005, planteamos una estrategia incremental de cinco niveles (desde el nivel más básico al más completo), para la implantación de un sistema de gestión de la seguridad en los sistemas de información (SGSI). En cada nivel estudiamos las normas y estándares que consideramos más adecuados y sus debilidades. En el nivel 1 damos consejos básicos de seguridad. En el nivel 2, lo basamos en las obligaciones legales emanadas del estudio de la Ley Orgánica 15/1999 (LOPD) y en el Real Decreto 994/1999 "Reglamento de Medidas de Seguridad de los Ficheros Automatizados" que contengan datos personales. En el nivel 3 analizamos las normas y estándares internacionales y nacionales y concluimos en la adopción de la norma española UNE ISO/IEC 17799:2000. Esta norma española es espejo de la norma internacional ISO 17799, que a su vez parte de la norma británica BS 7799. La Norma UNE 71501 IN facilita la comprensión de la seguridad de las TI (es espejo de la norma ISO/IEC TR 13335 "Information Technology - Guidelines for the management of IT security" GMITS). En el nivel 4 contemplamos las metodologías de análisis de riesgos, la británica CRAMM, la norteamericana OCTAVE y la española MAGERIT. En el nivel 5 comentamos las normas de certificación. Finalizamos con propuestas de líneas de trabajo para subsanar las debilidades detectadas.

1 Introducción

La necesidad de la seguridad en los actuales Sistemas de Información es una realidad no discutida pero no implementada.

Estadísticas de la C.E. indican 10.000 M € de pérdidas asegurables declaradas. A estos datos habría que sumarles las pérdidas conocidas y no declaradas por cuestiones de imagen, las conocidas no asegurables por el tipo de activo y las desconocidas. Podemos comentar la preocupación de las autoridades Comunitarias por esta situación, consciente de la importancia estratégica que para la Comunidad Europea tiene que los sistemas de información de las empresas, gobiernos e instituciones miembros, sean seguro. A modo de ejemplo, vamos a comentar dos iniciativas.

1. La Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre seguridad de las redes y de la información titulada "*Propuesta para un enfoque político europeo*"6 insta a los Estados miembros a fomentar el uso de mejores prácticas de seguridad, basadas en instrumentos existentes, tales como la norma UNE 17799 6 (norma equivalente a ISO/IEC IS 17799) "*Código de buenas prácticas para la gestión de la seguridad de la información"*, que constituye una referencia fundamental de los criterios y recomendaciones de seguridad.
2. El plan de acción "*eEurope 2005: una sociedad de la información para todos*"[1] 6. El objetivo de este plan es: "fomentar la seguridad de los servicios, aplicaciones y contenidos basados en una infraestructura de banda ancha ampliamente disponible". Establece, entre otros objetivos, que para el 2005, Europa deberá contar con "**Una infraestructura de información segura**". Para ello la Unión Europea ha puesto ya en marcha una estrategia global basada en las comunicaciones sobre seguridad de las redes[2] y ciberdelincuencia[3], y en la directiva 97/66/CE [4]. sobre protección de datos en relación con las comunicaciones electrónicas. El enfoque fue aprobado y desarrollado por la Resolución del

[1] Bruselas 28.5.2002 COM(2002) 263 final

[2] Seguridad de las redes y de la información: Propuesta para un enfoque político europeo, COM(2001) 298 de 6.6.2001.

[3] Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, COM(2000) 890 de 22.1.2001.

[4] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 30.1.1998

Consejo de 28 de enero de 2002[5] y por la reciente propuesta de decisión marco del Consejo relativa a los ataques de los que son objeto los sistemas de información [6].

Las acciones propuestas son:

- **Grupo operativo sobre ciberseguridad (CSTF).**. Los Estados miembros y el sector privado deben respaldar las actividades del CSTF. Se pretende que se convierta en un centro de competencia en materia de seguridad, p. ej., para desarrollar con los Estados miembros un concepto de sistema europeo de alerta en caso de ataque informático, facilitar el debate entre los distintos pilares y mejorar la cooperación transfronteriza.
- **Cultura de la seguridad.** Antes de finalizar 2005, debe construirse una "cultura de la seguridad" en el diseño e implementación de productos de información y comunicaciones. El sector privado debe elaborar buenas prácticas y normas y fomentar su aplicación sistemática. La Comisión tiene intención de apoyar estos proyectos y se esforzará por sensibilizar a todos los usuarios sobre los riesgos que pesan sobre la seguridad. 6
- **Comunicaciones seguras entre servicios públicos**. la Comisión y los Estados miembros examinarán la posibilidad de establecer un entorno de comunicaciones seguro para el intercambio de información de Estado clasificada.

El sexto programa marco de investigación, propone continuar con líneas de *investigación en materia de seguridad.* Las prioridades de investigación en materia de seguridad las estableces en las infraestructuras de redes y de información confiables, haciendo hincapié en las tecnologías emergentes (p. ej., banda ancha, arquitecturas inalámbricas o entorno inteligente) y detección de los puntos vulnerables y de las interdependencias en las infraestructuras. Se pretende también apoyar **la normalización** con el fin de **extender el uso de las normas abiertas** y de los **programas de fuente abierta**. Las actividades de investigación deben tener en cuenta igualmente el "factor humano" en la seguridad, p. ej., **normas básicas de seguridad** o facilidad de uso de los sistemas.

De las acciones y directivas comentadas en los párrafos anteriores, podemos establecer que para la Comunidad Europea, la seguridad de sus sistemas de información es una línea estratégica prioritaria. La estrategia deberá estar basada en:

- normas y estándares (internacionales y nacionales)
- el uso de programas de fuente abierto
- la creación de una cultura de la seguridad inexistentes en la actualidad

Podemos deducir por tanto, la necesidad de encontrar una estrategia de seguridad que permita facilitar a la pequeña y mediana empresa la consecución de los objetivos establecidos por la Comunidad Europea. Para lo cual debemos desarrollar tecnologías y metodologías propias , no dependientes de terceros.

En el apartado siguiente proponemos una estrategia basada en el estudio de los distintos Sistema de Gestión de la Seguridad de la Información existentes (ISMS *Information Security Management System*). Como consecuencia del análisis de esta estrategias pretendemos encontrar puntos débiles en las metodologías, tecnología y normas actuales que nos permitan definir propuestas de líneas de trabajo que mejoren las carencias actuales de los SGSI.

2 Estrategias para la seguridad de los sistemas de información

Para el cumplimiento los objetivos de la Comunidad Europea en materia de seguridad, es necesario que las administraciones, profesionales y empresas puedan organizar su política de seguridad.

Muchas organizaciones no abordan de modo serio una política de seguridad "formal" (según norma) por la complejidad de la misma. Las metodologías y normas existentes relacionadas con los SGSI no aclaran sus ámbitos de aplicación, resultando una amalgama de normas de compleja aplicación. Esto reduce su posible implantación a las grandes corporaciones. Un ejemplo de este caso sería la propuesta de ANEI [7]con su primer programa sectorial sobre *Gestión de la Seguridad de la Información* 6.

Pero si solo las grandes corporaciones pueden establecer políticas de seguridad adecuadas, no podremos contar con *una infraestructura segura* a nivel nacional y europeo.

[5] http://register.consilium.eu.int/pdf/es/01/st15/15152es1.pdf.

[6] http://europa.eu.int/comm/dgs/justice_home/index_es.htm, COM(2002) 173 final de 19.4.2002

[7] ANEI Asociación Nacional de Empresas de Internet http://www.a-nei.org/

Nuestra propuesta, para disminuir el rechazo inicial, es organizar la política de seguridad de una forma "escalonada", mediante una estrategia "incremental" 6. Las entidades deben mejorar su nivel de seguridad paso a paso. Esta estrategia se basa en un avance progresivo de la política de seguridad de una empresa o institución. De forma que empezamos por el mínimo. Una vez que la organización asume las medidas técnicas y organizativas de este nivel, está preparada para el siguiente paso de mejora. Así hasta alcanzar el máximo nivel exigido por las normas internacionales que permitan incluso una certificación del nivel alcanzado.

Los informes de Asociación Española de Empresas de Tecnologías de la Información SEDISI 6, nos indica que en España el nivel de implantación de medidas de seguridad es bajo o muy bajo, si exceptuamos las grandes corporaciones y algunos sectores muy concretos. Para que las medidas de seguridad tengan éxito, deben de ser asumidas completamente por los usuarios. Entendemos que es difícil pasar de la nada al estado perfecto. Por ello proponemos ir avanzando en los niveles de seguridad hasta alcanzar los objetivos ya mencionados.

Por tanto es necesario un sistemas de niveles "acumulativos". Es decir, lo comentado para el nivel 3, se añade a lo comentado en los niveles inferiores. Proponemos 5 niveles:

- Nivel 1.- Sistemas particulares- Autoprotección
- Nivel 2.- Sistemas pequeños- Cumplimiento de la legislación
- Nivel 3.- Sistemas medianos y grandes- Gestión de la seguridad de los sistemas de información
- Nivel 4: Gestión global de riesgos del sistema
- Nivel 5. Certificación

2.1 Nivel 1º: Sistemas particulares - Autoprotección

El primer nivel de seguridad correspondería a los sistemas personales que no tengan uso profesional. Un ejemplo sería el ordenador de casa, para uso personal. Estos sistemas no están sujeto a normativas legales. El R.D. 994/1999 indica que "El régimen de protección de los datos de carácter personal no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas"

Los objetivos del plan de acción *eEurope 2005* de "una infraestructura de información segura", "*Cultura de seguridad y normas básicas de seguridad*", nos indican que son necesarias iniciativas de concienciación de los usuarios sobre la importancia de la seguridad de sus sistemas de información. Estas acciones de concienciación sobre la importancia de la seguridad es clave en este nivel. Los usuarios personales no suelen considerar necesario tomar medidas de protección sobre la información que guardan en su ordenador. Si el ordenador no está conectado a internet, el riesgo de pérdida de información, o de falta de confidencialidad es una decisión que solo afecta al ámbito personal. La situación cambia radicalmente si el ordenador está conectado a internet. En este segundo caso, transciende el ámbito de el riesgo que personalmente quiera asumir el usuario, para afectar a todos los usuarios. La falta de protección a este nivel puede facilitar la expansión de virus, o los ataques de denegación de servicio, al ser utilizado el ordenador para ataque sobre servicios claves de la red. La falta de seguridad de los ordenadores de uso personal afectan de forma muy negativa a la seguridad total de la red. Es por tanto necesario garantizar la seguridad de los ordenadores de uso personal.

Los principios de seguridad que consideramos adecuados para este nivel son:

- La simplicidad: la primera salvaguarda es prestar atención para detectar el peligro y usar el sentido común para abortarlo
- Adecuación: proporcionada al bien a proteger. No matar mosquitos a cañonazos
- Centrarse en los puntos débiles. La cadena siempre se rompe por el eslabón más débil
- Economía: el coste de las medidas de seguridad debe ser inferior al costo del bien a proteger. No Infravalorar los costes de los riesgos, ni supervalorar los costes de las salvaguardas
- No inventar la rueda: parte del trabajo seguro que está hecho. Los sistemas incorporan muchas salvaguardas no utilizadas.
- Al final: todo problema de Seguridad termina con la instalación y uso de mecanismos de salvaguarda de varios tipos y complejidades.

Hay una serie de medidas de salvaguarda que consideramos imprescindibles a este nivel. Las clasificamos en "básica" y "avanzadas". Las básicas las consideramos de implantación obligatoria. Las avanzas serían de implantación deseadas.

Básicas

•Instalación de un sistema operativo seguro (control de acceso y permisos)

•Programa de antivirus actualizado

•Cortafuegos personales de libre distribución (seguridad perimetral)

•Programa detector de programas espías

•Programa de mantenimiento del registro de Windows (en el caso de utilizar este tipo de sistema operativo)

•Copias de seguridad

•Normas de uso del correo seguro (Políticas de adjuntos, no previsualización, no HTML, SSH)

•Normas de navegación segura (certificados, firma electrónica, SSL)

•Actualizaciones de los parches de seguridad de las aplicaciones instaladas

Avanzadas

•Sistemas de encriptación y autentificación *(GnuPGP*)

•Detector de vulnerabilidades (detectores de fallos de seguridad: *network security scanner*)

Las herramientas a utilizar en este caso son mayoritariamente de bajo coste y otras se pueden obtener de forma gratuita de sitios de distribución de *software* en Internet (ver anexo D).

Esto nos indica que no es la falta de herramientas de seguridad o su coste lo que hace que no se implemente una política de seguridad básica en los ordenadores de uso personal. Entendemos que es la falta de concienciación de los riesgos (¿a quién le va interesar lo que tengo en mi ordenador?), la no valoración de la información que almacena el sistema o del tiempo necesario para la recuperación de la información, unida a una falta de formación básica para entender estas herramientas.

Faltan a este nivel, herramientas autoconfigurables de dominio público, iniciativas de formación básica y concienciación, además de una guía básica de buenas costumbre de seguridad a nivel de ordenador personal. La colaboración de la Administración es fundamental para mejorar nuestro nivel de seguridad. En la educación obligatoria existen materias de informática. Deben de incluirse en ésta formación básica, las medidas de seguridad.

En el caso de la seguridad de equipos conectados a internet, hace falta el compromiso de colaboración de los proveedores de internet (ISP) para aportar herramientas y configuraciones seguras a sus clientes.

2.2 Nivel 2º: Sistemas pequeños- Cumplimiento de la legislación

El siguiente nivel, entendemos que corresponde a los sistemas de información de empresas o de personas físicas (profesionales). Estas instalaciones deben cumplir las normas del nivel 1º y como mínimo, las que por imperativo legal, les obligan a tener las leyes nacionales. En este apartado vamos a revisar la legislación nacional y las recomendaciones europea que existen en relación con la seguridad de los sistemas informáticos de este nivel.

Las herramientas a utilizar en este nivel son soluciones comerciales de bajo coste. No es un problema de inversión. La falta de cultura de seguridad hace que no se incorporen al uso cotidiano.

La seguridad es una necesidad muy reglamentada. En el apartado 2.2.1Legislación sobre seguridad informática, podemos comprobar lo acertado de esta aseveración.

El organismo en España encargado de velar por el cumplimiento de las leyes de protección de datos personal es la Agencia de protección de datos. Regulada por el título VI de LOPDCP 15/1999 y Estatutos de APD (R.D. 428/1993 de 26 de marzo BOE 106 de 4 de mayo de 1.993). Son funciones de la agencia: inspectora, ordenadora, de publicidad, sancionadora, inmovilizadora, reguladora, unificadora y de relaciones con el exterior.

En el sitio de la Agencia de Protección de Datos[8] en el apartado legislación, podemos encontrar los textos de las principales normas legales. También podemos encontrar "Guía práctica para ciudadanos" donde nos aclara los derechos básicos que tiene cualquier ciudadano en relación con la protección de sus datos personales. Por último señalar el apartado de "Recomendaciones e instrucciones" donde podremos encontrar recomendaciones sectoriales sobre el tema y las "Instrucciones" dictada por esta autoridad.

[8] https://www.agenciaprotecciondatos.org/

2.2.1 Legislación sobre seguridad informática

666 6

Comunidad EUROPEA

Estrategias europeas

- •Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales
- •Acuerdo de *Schengen* (14 junio de 1985)
- •Tratado de Niza, de 26 de febrero de 2002, modificativo de los Tratados Consultivos de la Unión Europea, introduciendo en los mismos la Carta de Derechos Fundamentales. (Entrada en vigor prevista para el año 2004, cuando sea ratificado por los 15 estados de U.E.).
- •Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las regiones sobre "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo"
- •Informe 'Bangemann'(94); Cumbres (Corfú94, ...)
- •eEurope 2005

Directivas europeas

- •Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- •Directiva 2002/58/CE, de 12 de julio de 2002 del Parlamento Europeo y Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

TELECOMUNICACIONES

- •Directiva 97/66/CE, del Parlamento Europeo
- •Directiva 2000/31/CE, del Parlamento Europeo y Consejo sobre determinados aspectos jurídicos de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.
- •Orden ECO/1758/2002, de 9 de julio, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos en materia de personal

Decisiones europeas

- •ITSEC (91), ITSEM (93), CC-SEC ...

En relación a estas estrategias, podemos comentar el nivel de cumplimiento en España. A modo de ejemplo el documento "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo"6. En este documento se expresan las medidas propuestas para paliar los problemas de seguridad de la red y de la información. Entre las que se cuentan: la concienciación, el desarrollo de un sistema europeo de alerta e información, el apoyo a la investigación y al desarrollo en materia de seguridad, la cooperación internacional o la creación de una legislación en materia de ciberdelincuencia. Podemos comentar el nivel de cumplimiento en España de algunas propuestas concretas como:

- •Los Estados miembros deberán poner en marcha una campaña de información y de educación sobre seguridad informática
- •Los Estados miembros deberán fomentar el uso de mejores prácticas basadas en medidas existentes como ISO/IEC 17799 Esta medida debería estar especialmente dirigida a las PYME. La Comisión prestará su apoyo a los Estados miembros en estos esfuerzos.
- •Los sistemas de educación de los Estados miembros deberán prestar mayor atención a los cursos sobre seguridad.

Las campañas institucionales sobre seguridad en España han sido y siguen siendo meramente testimoniales. No ha habido campaña de concienciación que pueda recibir ese nombre. Del segundo apartado entiendo que ni testimoniales. No existen ayudas a las PYMES para mejorar la seguridad de sus sistemas de información. De la tercera propuesta tampoco existen. Es necesaria la intervención gubernamental en todos los niveles de la Administración del Estado que fomenten, faciliten y formen en temas de seguridad informática, porque es una materia estratégica de primer orden para seguir perteneciendo al primer mundo.

Legislación estatal (España)

- •Constitución Española (diciembre 1978) Art. 18.4 la ley limitará el uso de la informática para garantizar el honor...
- •Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).6 6
- •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 personales.6 6
- •Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal. Derogada por la Ley Orgánica 15/1999
- •Real Decreto 1332/1994, 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre.
- •Real Decreto 428/1993, de 26 de marzo, Estatuto de la Agencia de Protección de Datos.
- •Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.
- •Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
- •Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- •Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
- •Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- •Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

TELECOMUNICACIONES

- •Ley 11/1998, de 24 de abril, General de Telecomunicaciones.
- •Real Decreto-Ley 1736/98, de 31 de julio, en el que se aprueba el Reglamento del Título III de la Ley General de Telecomunicaciones.
- •Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- •Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.

Comentarios sobre la legislación española

De todas estas leyes vamos a estacar las que mayor repercusión tienen en los Sistema de Gestión de la Seguridad de la Información

- •Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- •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 Personales.

2.2.2 Ley Orgánica 15/1999

Vamos a definir algunos términos utilizados en esta norma.. En el Anexo C de Definiciones de conceptos de la Ley Orgánica 15/1999 y del Real Decreto 1332/1994, podrá encontrar los términos para entender mejor estas leyes.

Datos accesibles al público

Los datos que figuren en censos, anuarios, bases de datos públicas, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, los títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Autoridad controladora del fichero

Significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuales operaciones se les aplicará (convenio 108 Consejo Europa).

Datos de carácter personal

Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada e identificable.

Responsable del fichero

Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad y contenido y uso del tratamiento.

Responsable de Seguridad

Persona o personas de la organización a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables en dicha organización.

Obligaciones de Seguridad de la L.O. 15/1999

- Art. 9: 1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Art. 9 (2): 2 En relación con la seguridad física la norma indica que no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
- Art. 43.3. h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. ¡falta grave!
- Artículo 45. Tipo de sanciones

  1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

  2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

  3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas
- Una obligación general para toda empresa o institución que solicita datos personales es que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

  a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

  b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

  c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

  d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

  e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

2.2.3 Real Decreto 994/1999 Reglamento de seguridad

Destacar 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 Personales sujetos al régimen de la Ley Orgánica 15/1999. El objetivo del Reglamento es establecer las medidas obligatorias técnicas y organizativas, necesarias para garantizar la seguridad de los ficheros, centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento.

El reglamento indica que hay que proteger la información en:

- Acceso en modo local
- Acceso a través de redes de comunicaciones
- Trabajos fuera del local de ubicación del fichero
- Los Ficheros temporales

El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento. Atendiendo al tipo de datos contenidos en su ficheros, deberá adoptar las diferentes medidas de seguridad recogidas en el Reglamento.

- Nivel básico: todos los ficheros con datos personales
- Nivel medio :datos relativos a solvencia patrimonial y crédito

•Nivel alto: datos de ideología, religión, creencias, etnia, salud, sexualidad

El Documento de Medidas de Seguridad es de carácter interno, no teniendo la obligación de ser presentado ante la Agencia, sino tan solo tenerlo disponible por si éste fuera requerido. Los niveles medio y alto exigen Auditorías.

Medidas de seguridad de nivel básico que establece el reglamento son:

•Documento de seguridad (art. 8) Políticas y reglamentos

•Funciones y obligaciones del personal (art. 9)

•Registro de incidencias (art. 10)

•Identificación y autenticación (art. 11)

•Control de acceso (art. 12)

•Gestión de soporte (art. 13)

•Copia de respaldo y recuperación (art. 14) semanal

El Documento de Seguridad indicado en el apartado uno debe contener al menos los siguientes apartados:

1. Ámbito de aplicación
2. Medidas, normas, procedimientos, reglas y estándares
3. Funciones y obligaciones
4. Estructura de los ficheros y sistemas que los tratan
5. Procedimiento de notificación ante incidencias
6. Procedimientos de copias de seguridad y de recuperación de los datos

Medidas de seguridad de nivel medio

Las medidas de seguridad de nivel medio son las siguientes

•Documento de seguridad (art. 15)

•Responsable de seguridad (art. 16)

•Auditoría (art. 17) cada dos años

•Identificación y autenticación (art. 18)

•Limitar el número de intentos

•Los controles periódicos que se deben realizar para verificar el cumplimiento de lo dispuesto

•Control de acceso físico (art. 19)

•Gestión de soportes (art. 20) La medidas que sea necesario adoptar cuando un soporte vaya a desechado o reutilizado. Impedir poder recuperar información borrada

•Registro de incidencia (art. 21)

•Pruebas con datos reales (art. 22) Está prohibido

Medidas de seguridad de nivel alto

•Distribución de soporte (art. 23) Cifrado de los soportes

•Registro de acceso (art. 24)

•Copias de respaldo (art. 25) Copia en lugar diferente a donde se encuentren los equipos.

•Telecomunicaciones (art. 26) Cifrado de la información.

Las medidas comentadas son acumulativas, es decir, la información de tercer nivel debe implementar las medidas de nivel tres, dos y uno.

El régimen de protección de los datos de carácter personal no será de aplicación:

1. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
2. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
3. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Tabla 1 Cuadro resumen de tipos de datos

	DATO	FICHEROS EN LOS QUE SE PUEDE ENCONTRAR
DATOS DE NIVEL ALTO	Ideología	Nómina
	Religión y creencias	Liquidación de renta
	Origen racial	Seguridad e higiene
	Salud	Salud del personal
	Vida sexual	Clientes de productos eróticos
	Datos recabados para fines policiales sin el consentimiento de las personas afectadas	
DATOS DE NIVEL MEDIO	Infracciones administrativas o penales	Clientes de abogados, gestores etc
	Hacienda Pública	Agencia Estatal de Administración Tributaria
	Servicios Financieros	Bancos
	Solvencia patrimonial y crédito	ASNEF
	Evaluación de la personalidad	Selección de personal
DATOS DE NIVEL BÁSICOS	Resto	Todos

Desde el pasado 26 de junio de 2002 la obligación de cumplir con las medidas expresadas en el reglamento, afecta a todas las empresas, administraciones o profesionales.

El reglamento, a nivel técnico, es difícil de cumplir de forma exhaustiva. Tampoco es fácil deducir la información precisa que requieren los documentos requeridos. Un ejemplo de ello es el denominado Documento de seguridad, que debe de tenerse en todos los casos. Podemos encontrar un ejemplo de documento de seguridad de cada uno de los niveles en la Agencia de Protección de Datos de la Comunidad de Madrid. [9] Esta referencia es muy valiosa porque no existe otros ejemplos de documentos "oficiales" 6.

La obligación legal de su cumplimiento, aunque la norma no sea de muy reciente creación, sigue siendo desconocida para la inmensa mayoría de las micro-pyme, y pymes de este país. La Agencia de Protección de Datos está siendo, por ahora, "generosa" y solo actúa en este tipo de empresas bajo demanda expresa. La aplicación estricta de la norma, debido a la cuantías de las sanciones, avocaría al cierre de muchos pequeños negocios. A modo de ejemplo comentar que un pobre video-club de barrio requiere las medidas de seguridad de máximo nivel.

2.3 Nivel 3º: Sistemas medianos y grandes - Gestión de la seguridad de los sistemas de información

Para la Gestión de la seguridad de los sistemas de información hay que tener en cuenta cada vez más normas legales y técnicas . Una forma de facilitar la gestión de la seguridad de sistemas de información es aplicar las normas internacionales existentes al respecto.

Algunas empresas podrán considerar importante la adecuación a una norma para obtener la certificación correspondiente porque su proceso de negocio (o clientes) lo demanden. Sin embargo, aunque esto pueda ser el caso para otras normas ISO (como la ISO 9000) no lo es tanto para la norma ISO/IEC 17799. ¿Por qué, entonces, puede ser necesario adecuarse a una norma como el ISO/IEC 17799?

La utilización de una norma de seguridad permite cerciorarse de que se cubren todos los aspectos de seguridad que debe abordar una organización, desde la especificación de una política de seguridad a la definición de necesidades de seguridad física o de recuperación de desastres. Claramente, una organización puede abogar por definir su política de seguridad y realizar su implementación sin seguir

[9] https://www.madrid.org/apdcm/

ninguna norma. El beneficio de utilizar una norma es el de acceder al conocimiento de expertos reflejado en una guía accesible a cualquier responsable de seguridad.

En este y siguientes niveles nos vamos a basar, además de las normas legales, en los estándares y recomendaciones internacionales.

2.3.1 Principios en Seguridad de la OCDE

Podemos empezar analizando los nueve Principios en Seguridad del de la OCDE (PARIS 2002) 6

- Principio 1: Concienciación
  - Los participantes deben ser conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.
- Principio 2: Responsabilidad
  - Todos los participantes son responsables de la seguridad de los sistemas de información y redes.
- Principio 3: Respuesta
  - Los participantes deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten la seguridad.
- Principio 4: Ética
  - Los participantes deben respetar los intereses legítimos de los otros.
- Principio 5: Democracia
  - La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.
- Principio 6: Evaluación de riesgos
  - Los participantes deben llevar a cabo evaluaciones de riesgo.
- Principio 7: Diseño e implementación de seguridad.
  - Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y redes.
- Principio 8: Administración de la Seguridad.
  - Los participantes deben adoptar una visión integral de la administración de la seguridad.
- Principio 9: Evaluación continua de la seguridad
  - Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad.

2.3.2 Nivel del análisis de riesgo

En relación con el análisis de riesgo, en el apartado 8 de UNE-71501-3 IN se establecen diversos niveles para su realización: mínimo, informal, detallado y combinado). Entendemos que el análisis descrito como combinado es el adecuado para este nivel. El nivel mínimo sería adecuado para el nivel anterior.

2.3.3 Instituciones de normalización

- Internacionales
  - ITU-T (recomendaciones -series-)
  - ISO/IEC (normas)
- Europeas
  - CEN/CENELEC
  - ETSI

2.3.4 Normas de Organismos internacionales

La implantación de la seguridad de la información, en la medida de lo posible, se consigue mediante un conjunto adecuado controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones *software*. Estas medidas de control sirven para asegurar que se cumplen los objetivos específicos de seguridad de la Organización. En el campo normativo voluntario de la gestión de la seguridad de las TI existen actualmente, como más relevantes, destacamos como fundamentales para este nivel las siguientes:

- La norma ISO/IEC 17799:2000 6 que ofrece las recomendaciones para realizar la gestión de la seguridad de la información, las versión española de esta norma es la norma espejo UNE-ISO/IEC 17799:2000.6
- La norma multiparte ISO/IEC 133356 6 6 6 6 conocidas como las GMITS donde se recogen las etapas del ciclo de gestión de la seguridad proporcionando orientaciones organizativas y técnicas, la versión española de esta norma multiparte es la UNE 71501 IN 2001. Generalmente cada Organización en base a los riesgos a que esté expuesta y los aspectos intrínsecos de su funcionamiento, define e implanta un Sistema propio para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de TI.
- BS 7799:1 "*Information Security Management*- Part 1: *Code of practice for information security management*" 6
- BS 7799-2 (*British Standards Institution*): buenas prácticas de gestión de seguridad. Para algunas organizaciones puede ser orientativa la norma Británica BS-7799-2 6, la cual fija requisitos para establecer, implementar y mantener un sistema de gestión de la seguridad de los sistemas de información (ISMS: *Information Systems Management System*). Aquellas organizaciones que quieran ser conformes a la norma BS-7799-2 deberán cumplir estrictamente los requisitos según se indican en su texto. Dada la riqueza de variantes presentes en el mundo real, para algunas organizaciones la norma resulta meramente orientativa.
- Norma ISO-OSI 7498-2: Arquitectura de Seguridad (Interconec. .S. Abiertos)
- Norma IS 17799-2 en preparación, para evaluar y certificar los Sistemas de Gestión de Seguridad que cumplan la IS 17799-1.
- Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad. (*Organisation For Economic Co-Operation And Development*. Paris 2002).6

Un cuadro-resumen de estas normas ordenadas separando las nacionales de las internacionales:

Normativas de Seguridad de la Información en España [10]

- UNE-ISO/IEC 17799:2002 "Código de buenas prácticas de la Gestión de la Seguridad de la Información" Traducción en castellano de la ISO/IEC 17799:2000 Equivale a la BS7799:1
- UNE 71501 IN "Guía para la Gestión de la Seguridad de TI" Equivale a ISO/TR 13335 parte 1, 2 y 3
  - Parte 1: Conceptos y modelos para la Seguridad de las TI ;
  - Parte 2: Gestión y planificación para la Seguridad de las TI
  - Parte 3: Técnicas para la Gestión de la Seguridad de las TI
- PNE 71502 (Proyecto de Norma Española) "Requisitos para la gestión de la seguridad de TI" Norma certificable actualmente en proyecto, en previsión para 2003, estará fundamente extraída de la BS7799-2:2002
- Metodologías: Magerit y Métrica V·36

Normativas de Seguridad de la Información internacionales

Normativas ISO desarrolladas por el comité JTC1/SC27 [11]

- ISO/IEC 17799:2000 "*Information Technology- Code of Practice for Information Security Management*"
- ISO/IEC TR 13335 "*Information Technology - Guidelines for the management of IT security*" (GMITS) -
  - Part 1: *Concepts and models for IT security*

[10] Disponibles en AENOR : www.aenor.es

[11] Otras normas ISO: listado completo en: http://www.din.de/ni/sc27/doc7.html

Disponibles en www.iso.ch

- Part 2: *Managing and planning IT security*
- Part 3: *Techniques for the management of IT security*
- Part 4: *Selection of safeguards*
- Part 5: *Management guidance on network security*

Reino Unido [12]

•BS7799:1 " *Information Security Management*- Part 1: *Code of practice for information security management*"

•BS7799-2:2002 "*Information Security Management*- Part2: *Specifications for an ISMS*" revisión 2 / 5 septiembre de 2002

•Metodología: CRAMM

Comentamos las normas que consideramos mas importantes para su aplicación en este nivel.

2.3.5 La Norma UNE 71501 IN

La Norma UNE 71501 IN se ha elaborado para facilitar la comprensión de la seguridad de las Tecnologías de la Información (TI), y proporcionar orientación sobre los aspectos de su gestión.

Los objetivos principales de esta norma son:

•Definir y describir los conceptos relacionados con la gestión de la seguridad de TI

•Identificar las relaciones entre la gestión de la seguridad de TI y la gestión de las TI en general

•Presentar varios modelos Útiles para explicar la seguridad de TI,

•Proporcionar orientación general sobre la gestión de la seguridad de TI, y proporcionar orientación en relación con la selección de salvaguardas.

La Norma UNE 7 150 1 IN está estructurada en varias partes:

•UNE 71501-1 IN que proporciona una visión general de los conceptos fundamentales y de los modelos utilizados para describir la gestión de la seguridad de TI. Sus contenidos van dirigidos a los responsables de la seguridad de TI y a quienes son responsables del plan global de seguridad de la organización.

•UNE 71501-2 IN que describe los aspectos de gestión y planificación de la seguridad de TI. Va dirigida a los directivos con responsabilidades relacionadas con los sistemas de TI de la organización. Pueden ser: directivos de TI responsables del diseño, desarrollo, pruebas, adquisición o explotación de sistemas de TI, o directivos responsables de actividades que hacen un uso sustancial de los sistemas de TI.

•UNE 71501-3 IN que describe técnicas de seguridad indicadas para quienes se encuentran implicados en actividades de gestión durante el ciclo de vida de un proyecto, como planificación, diseño, desarrollo, pruebas, implantación, adquisición o explotación.

UNE 71501-1 IN

Fundamento

Las organizaciones, tanto del sector público como del sector privado, dependen crecientemente de la información para el desarrollo de sus actividades. Así, la pérdida de autenticidad, confidencialidad, integridad y disponibilidad de su información y servicios puede tener para ellas un impacto negativo. En consecuencia, es necesario proteger la información y gestionar la seguridad de los sistemas de TI dentro de las organizaciones. Este requisito de proteger la información es particularmente importante, dado que numerosas organizaciones están conectadas a redes de sistemas de TI interna y externamente.

La gestión de la seguridad de TI es el proceso para alcanzar y mantener niveles apropiados de autenticidad, confidencialidad, integridad y disponibilidad. Las funciones de gestión de la seguridad de TI incluyen:

•Determinación de los objetivos, estrategias y políticas organizativas de la seguridad de TI,

•Determinación de los requisitos organizativos de la seguridad de TI,

•Identificación y análisis de amenazas a activos de la organización (análisis de riesgos),

•Como consecuencia del punto anterior, especificación de las salvaguardas apropiadas (gestión de riesgos),

[12] Disponibles en www.bsi-global.com

- Seguimiento de la implantación y operación de las salvaguardas necesarias para proteger la información y los servicios de la organización,
- Desarrollo e implantación de un plan de concienciación en la seguridad, y
- Detección y reacción ante incidentes.

La información es un activo organizativo. Puede existir en múltiples formas. Es vulnerable. Está sometida a una amplia variedad de amenazas. Debe ser protegida frente a impactos mediante la eliminación o minimización de los riesgos asociados. Se protege mediante el establecimiento de salvaguardas o elementos de control.

Aspectos de la gestión de la seguridad

La gestión de la seguridad de TI es una acción permanente, cíclica y recurrente. Vamos a comentar algunos de sus aspectos.

Gestión de la configuración

La gestión de la configuración es el proceso de seguimiento de los cambios en el sistema y puede hacerse formal o informalmente. El objetivo primordial de la gestión de la configuración, en relación a la seguridad, es garantizar que los cambios en el sistema no reducen la efectividad de las salvaguardas, ni la seguridad global de la organización.

Gestión de cambios

La gestión de cambios es el proceso que ayuda a identificar nuevos requisitos de seguridad cuando tienen lugar cambios en los sistemas de TI.

Análisis y gestión de riesgos

Persigue el equilibrio entre la naturaleza de los riesgos a los que están sometidos los datos y los tratamientos y el coste de las salvaguardas.

En el análisis y gestión de riesgos se identifican dos procesos:

- *El análisis de riesgos* es el proceso que permite la identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.
- *La gestión de riesgos* es el proceso que, basado en los resultados obtenidos en el análisis de riesgos, permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

MODELOS

Si bien existen diversos modelos para la gestión de la seguridad en TI, los modelos presentados en esta parte 1 de la Norma UNE71501 IN proporcionan los conceptos necesarios para su comprensión. Se presentan los siguientes modelos:

- Las relaciones entre elementos de seguridad
- Las relaciones en el análisis y gestión de riesgos
- La gestión del proceso de seguridad de TI

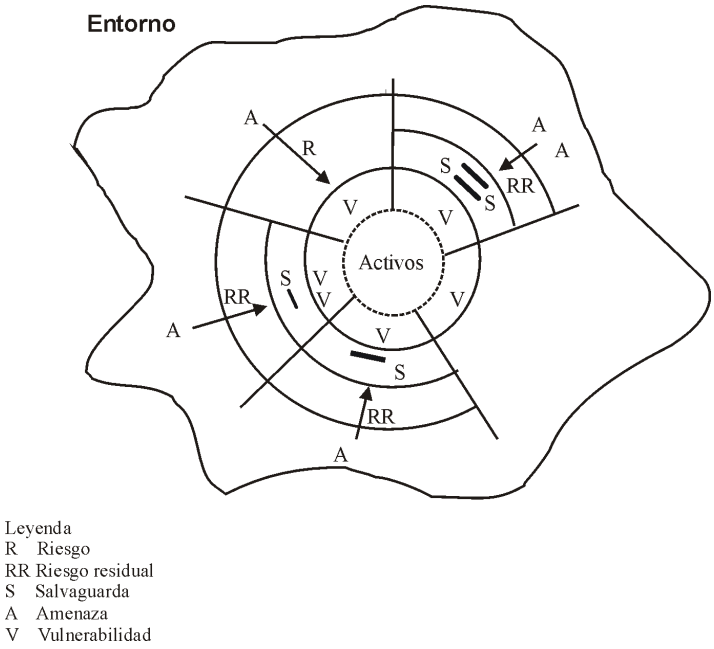

figura 2-1 relaciones entre elementos de seguridad. Fuente: AENOR

El modelo representa:

- •Un entorno sometido a amenazas que cambian constantemente y que son parcialmente conocidas,
- •Los activos de una organización,
- •Las vulnerabilidades de dichos activos,
- •Las salvaguardas seleccionadas para proteger los activos y para reducir las consecuencias de la posible materialización de las amenazas,
- •Las salvaguardas que reducen los riesgos, y
- •Los riesgos residuales aceptables para la organización.

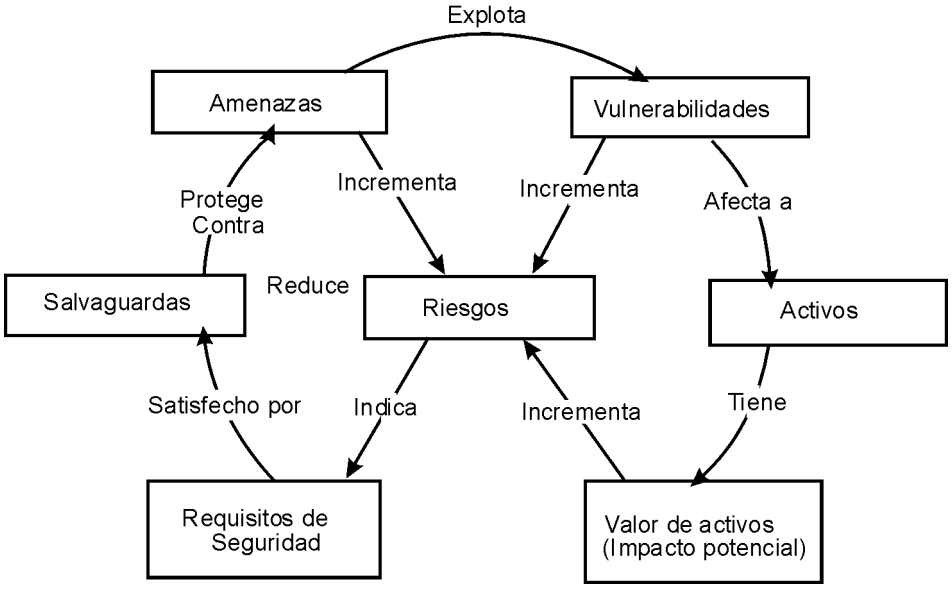

figura 2-2 Las relaciones en el análisis y gestión de riesgos Fuente: AENOR

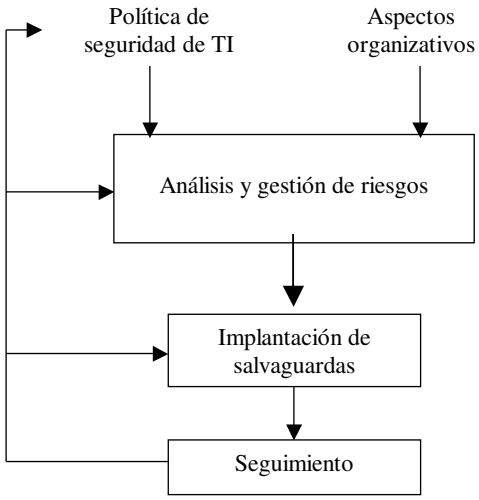

figura 2-3 La gestión del proceso de seguridad de TI

UNE 71501-2 IN

Trata sobre la gestión y las responsabilidades asociadas a un plan eficaz de seguridad de TI. Persigue familiarizar a los gestores con los principales procesos y funciones en la gestión de la seguridad de TI. La información proporcionada en esta parte puede no ser directamente aplicable a todas las organizaciones. En particular, las organizaciones pequeñas probablemente no dispongan de todos los recursos para llevar a cabo por completo algunas de las funciones descritas. descritas. En estos casos, es importante que los conceptos y funciones básicos sean adaptados de forma adecuada a la organización.

UNE 71501-3 IN

Examina diversas técnicas que son importantes para la gestión de la seguridad de TI. Estas técnicas están basadas en los conceptos y modelos aportados por la Norma UNE 71501-1 IN y en el proceso de gestión y responsabilidades tratados en la Norma UNE 71501-2 IN. La discusión en esta parte muestra las ventajas y desventajas de cuatro posibles estrategias para el análisis de riesgos. Se describe en detalle el enfoque combinado, y las diversas técnicas útiles para su implantación. Es el apartado mas concreto con unos anexos con ejemplos precisos.

2.3.6 PNE 71502 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (Proyecto de Norma Española)

No hay una norma ISO equivalente actualmente. Es equivalente a la norma Británica BS 7799-2:2002.

Los apartados son los siguientes:

1 OBJETO Y CAMPO DE APLICACIÓN (SGSI Controles Buenas Prácticas

2 NORMAS PARA CONSULTA

3 TÉRMINOS Y DEFINICIONES

- •Un SGSI comprende la estructura organizativa, los procedimientos, los procesos y los recursos para implantar la gestión de la seguridad de la información.
- •El sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.)
- •Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.

4 MARCO GENERAL DEL SGSI

- •Requisitos generales
- •Establecimiento del entorno de gestión (req. legales)
- •Selección de controles
- •Pasos para el establecimiento del entorno de gestión

- •Documentación
- •Control documental
- •Registros
- •Responsabilidades de la Dirección (Compromiso y Política)

Pasos para el establecimiento del entorno de gestión

- •FASE 1 Definición de la Política
- •FASE 2 Definición del alcance del SGSI
- •FASE 3 Desarrollo del Análisis de Riesgos
- •FASE 4 Gestión de Riesgos
- •FASE 5 Selección de controles a implantar y objetivos a cubrir
- •FASE 6 Preparar la relación de controles

5 IMPLANTACIÓN DEL SGSI

- •Implantación de los controles
- •Eficacia y calidad de los controles

6 EXPLOTACIÓN

- •Provisión de recursos materiales y humanos

7 REVISIÓN DEL SGSI

- •Auditorías y Revisión por Dirección

8 PROCESO DE MEJORA

PROCESO DE CERTIFICACIÓN

- •Reglamento en preparación (similar a otros)
- •Auditores con formación específica (legislación y tecnologías de información)

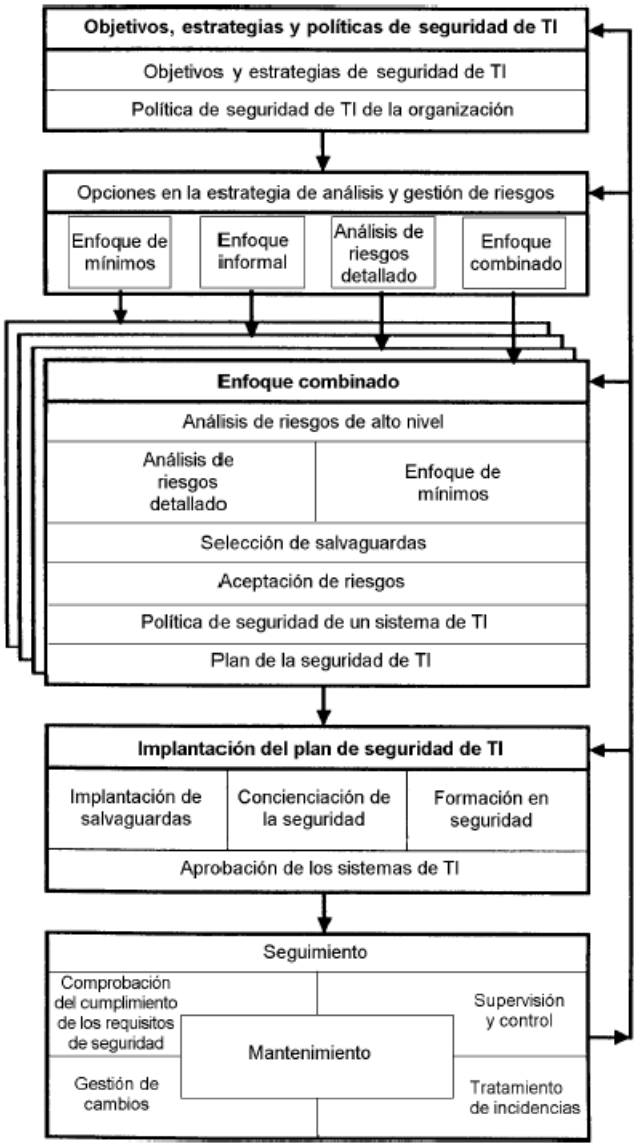

figura 2-4 PNE 71502

2.3.7 Norma UNE-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información

Basada en los tres conceptos fundamentales de confidencialidad, integridad y disponibilidad de la información, ya sea escrita, hablada o almacenada en un computador, la ISO/IEC 17799 6define las mejores prácticas para manejar la seguridad de la información, en términos de procesos, no de tecnología.

La ISO/IEC 17799 es una metodología estructurada, internacionalmente reconocida, orientada a la seguridad de la información que reconoce un proceso para evaluar, implantar, mantener y administrar la seguridad de la información.. La norma proporciona recomendaciones a los a los responsables la gestión de la seguridad de la información en las organizaciones.

Pretende proporcionar:

- •Una base para el desarrollo de normas de seguridad organizativas
- •Prácticas efectivas de gestión
- •Confianza en los acuerdos entre organizaciones.

Contiene10 secciones de salvaguardas

1. Política de seguridad

2. Aspectos organizativos para la seguridad
3. Clasificación y control de activos
4. Seguridad ligada al personal
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Desarrollo y mantenimiento de sistemas
9. Gestión de continuidad del negocio
10. Conformidad

además de 36 objetivos, 127 controles detallados:

La ISO/IEC 17799, que se basa en la norma BS 7799 debe ser utilizada como un documento de referencia, pues proporciona un completo conjunto de controles de seguridad.. A diferencia de ella, la BS 7799 especifica los requerimientos para establecer, implementar y documentar un Sistema de Gestión de Seguridad de Información (*Information Security Management System, ISMS*) y para que los controles de seguridad sean implementados de acuerdo a las necesidades particulares de cada organización.

Los pasos que debe seguir una organización que desea implementar una normativa de este tipo son: primero, establecer los requisitos de seguridad de la organización, identificando riesgos, amenazas, vulnerabilidades y posibilidades de impacto, principalmente. Luego, es necesario establecer principios y políticas para lo que queremos proteger. Además, se debe considerar un ítem de entrenamiento para que los empleados de la empresa comprendan cómo se debe establecer la norma. También, es clave definir un calendario de trabajo con tiempos determinados y el alcance de las políticas que se han de implementar.

La ISO/IEC 17799:2000 es un Código de Prácticas que no proporciona el necesario nivel de detalle para dar soporte a un esquema de certificación. En otros países se emplea la norma BS-7799-2.

Se trata del único estándar con aceptación mundial que satisface los requerimientos del mercado. Es una forma de reducir los costos de las primas de las pólizas de seguros; y mejora la efectividad de la seguridad de la información

Debe ser utilizada considerando el marco legal aplicable en cada país. Es importante señalar que el carácter de norma nacional idéntica a la Norma Internacional ISO/IEC 17799:2000, si se consideran apartados aislados, podríamos tener la visión que la norma incurre puntualmente en aspectos que pueden ser objeto de conflicto con la legislación aplicable en el marco español.

Pero si la norma se contempla en su totalidad, se verá que sí tiene en cuenta los mencionados aspectos, indicando el debido cumplimiento de la legislación aplicable en cada estado.

Recientemente las compañías dedicadas a la seguridad han lanzado una iniciativa que precisamente está orientada a concienciar a los responsables de la seguridad sobre la importancia del factor humano y las políticas de seguridad dentro de una organización [13].

2.3.8 La Norma BS 7799

BS 7799 permite definir y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS). Esta norma define los controles y las responsabilidades que más se adecuen a una organización, de acuerdo a su realidad, para administrar mejor la seguridad de la información. BSI, como fundadora de la norma BS 7799 es la principal entidad certificadora en dicho estándar.

Obtener la certificación BS 7799 es claramente un beneficio para las organizaciones de hoy, ya que representa una oportunidad para identificar las debilidades; permite al gerente general conocer y controlar la seguridad de la información de su compañía, además de una revisión permanente de la misma y de forma independiente del sistema de gestión de seguridad de la información que se tenga

Acerca de BSI (*British Standard*)

Fundada en 1901, BSI ha llevado más de 35,500 proceso de registro sobre 90 países. es miembro fundador de la Organización Internacional para la Estandarización (ISO), BSI facilitó y publicó el primer estándar para sistemas de administración de calidad, sistemas de administración ambiental, salud y administración de proyectos. También construyo la norma de seguridad BS 7799, base del estándar de buenas prácticas ISO/IEC 17799:2000. Actualmente cuenta con registro del 35% de la certificación de

[13] Puedes consultarla en http://www.humanfirewall.org/ y tiene un cuestionario que permite evaluar tu organización respecto de la iso17799

seguridad BS7799-2[14].

Por la proliferación de normativa legal en el ámbito nacional e internacional se hace necesario la elaboración de algún tipo de guía u orientación para poder aplicar prácticamente todas estas normas y recomendaciones.

2.4 Nivel 4º: Gestión global de riesgos del sistema

Como ya hemos comentado en el apartado anterior, de los niveles de riesgos establecidos el UNE 71501-3 IN, a este nivel le correspondería el análisis de riesgo detallado, con la ayuda de metodologías de análisis de riesgo. Existen muchas herramientas y metodologías disponibles para la medición de riesgos. Podemos enumerar

- •CRAMM 6
- •MAGERIT
- •OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*)
- •InfoSecure [15] metodología y herramientas de análisis de riesgo.
- •COBIT [16] (*Control Objetives For It*)
- •COBRA: Risk Consultant. *Software* de análisis de riesgo 6

Vamos a comentar las tres primeras.

2.4.1 CRAMM

Es el método de análisis y control de riesgos del Gobierno Británico (*CCTA Risk Analysis and Management Method*). CRAMM es un método estructurado y coherente para la identificación y la evaluación de riesgos en redes y sistemas de información. Abarca escenarios técnicos y no técnicos (por ejemplo, aspectos físicos de la seguridad de la tecnología de la información) y proporciona un método riguroso por etapas que permite programar adecuadamente las revisiones. Hay herramientas de software disponibles para CRAMM. La última versión es CRAMM Versión 5 de enero de 2003. Esta metodología se aplica con la norma BS 7799.

2.4.2 MAGERIT. Versión 1.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas

La versión 1.0 de MAGERIT 6 6 se presenta mediante un conjunto de guías:

- •Guía de Aproximación a la Seguridad de los Sistemas de Información,
- •Guía de Procedimientos, Guía de Técnicas,
- •Guía para Desarrolladores de Aplicaciones,
- •Guía para Responsables del Dominio Protegible,
- •Referencia de Normas legales y técnicas,
- •Arquitectura de la Información y especificaciones de la interfaz para el intercambio de datos.

MAGERIT, Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, fue elaborado con un doble objetivo: Estudiar los riesgos y recomendar las medidas. Es un método formal para investigar los riesgos que soportan los Sistemas de Información.

La estructura de MAGERIT permite realizar:

- •***El análisis de los riesgos*** para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de Información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.
- •***La gestión de los riesgos***, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir,

[14] (www.bsi-global.com)

[15] http://www.infosecuregroup.com/

[16] http://www.netconsul.com/

FUENTE: WWW.ISACA.ORG

impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

El Análisis y Gestión de Riesgos es el 'corazón' de toda actuación organizada de materia de seguridad. Influye, incluso, en las fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

Submodelos de MAGERIT

El modelo normativo de MAGERIT se apoya en tres submodelos:

- *Submodelo de Elementos de Seguridad*, con 6 entidades básicas: Activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.
- *Submodelo de Eventos de Seguridad*, con 3 tipos principales: Estático, dinámico organizativo y dinámico físico.
- *Submodelo de Procesos de Seguridad*, con 4 etapas tipificadas: Planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas.

Submodelo de Elementos

Activos. Se definen como los "recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección". Se pueden estructurar en las siguientes categorías: En el entorno del Sistema de Información necesario para su funcionamiento, en el sistema de información, la propia información, las funcionalidades de la organización y otros activos como, por ejemplo, la credibilidad de una persona jurídica o física, su intimidad, la imagen.

Amenazas. Se definen como "los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos". Las amenazas se pueden materializar y transformarse en agresiones. MAGERIT ve las amenazas como acciones capaces de modificar el "Estado de seguridad" del activo amenazado; acciones de tipo "evento", pues hay otras de tipo "decisión" humana.

Vulnerabilidad. Definida como la "ocurrencia real o frecuencia de materialización de una amenaza sobre un activo", la vulnerabilidad es una propiedad de la relación entre un activo y una amenaza. Ejerce entre ambos una función de 'mediación' en el cambio del 'estado de seguridad' del activo; siendo también el mecanismo de paso desde la amenaza a la agresión materializada. La vulnerabilidad tiene así dos aspectos: el estático, ligado a la función (forma parte del "estado de seguridad" del activo); y el dinámico, ligado al mecanismo (convierte la amenaza en agresión).

Impacto. Se define como "daño producido a la organización por un posible incidente" y es el resultado de la agresión sobre el activo, o visto de manera más dinámica, "la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento". El impacto puede ser cuantitativo (si representa pérdidas cuantitativas monitorizables directas o indirectas); cualitativo con pérdidas orgánicas (por ejemplo, de fondo de comercio, daño de personas); y cualitativo con pérdidas funcionales (o de los subestados de seguridad).

Riesgo. Se ha definido como la "posibilidad de que se produzca un impacto dado en la organización". Su importancia como resultado de todo el análisis organizado sobre los elementos anteriores (activos, amenazas, vulnerabilidades e impactos) queda velada por su apariencia como indicador resultante de la combinación de la vulnerabilidad y el impacto que procede de la amenaza actuante sobre el activo. Este riesgo calculado permite tomar decisiones racionales para cumplir el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con el umbral de riesgo, un nivel determinado con ayuda de la política de seguridad de la Organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un riesgo residual que se considera asumible.

Salvaguardas. Para reducir el riesgo se necesita la mejora de salvaguardas existentes o la incorporación de otras nuevas. MAGERIT distingue entre la llamada Función o Servicio de Salvaguarda y la llamada Mecanismo de Salvaguarda. Se define la función o servicio de salvaguarda como "reducción del riesgo"; y el mecanismo de salvaguarda como "dispositivo, físico o lógico, capaz de reducir el riesgo". Una función o servicio de salvaguarda es así una acción para reducir un riesgo de tipo actuación u omisión (es una acción fruto de una decisión, no de tipo evento). Esa actuación se concreta en un mecanismo de salvaguarda que opera de dos formas: la salvaguarda preventiva ejerce como acción sobre la vulnerabilidad y la salvaguarda curativa actúa sobre el impacto.

En resumen:

- •Activo: dominio de elementos afectables por el riesgo y la seguridad
- •Amenazas: Factores de Riesgo sobre los activos del dominio
- •Vulnerabilidad: probabilidad de que se materialice cada amenaza en cada activo
- •Impacto: consecuencia de que se materialice cada amenaza en cada activo
- •Riesgo: composición de Impactos en los activos y de vulnerabilidades a las amenazas
- •Salvaguardas: medidas técnicas y/u organizativas para reducir el riesgo bajo un umbral aceptable

Submodelo de Eventos

Refleja las relaciones generales entre las 6 entidades reseñadas en el Submodelo de Elementos.

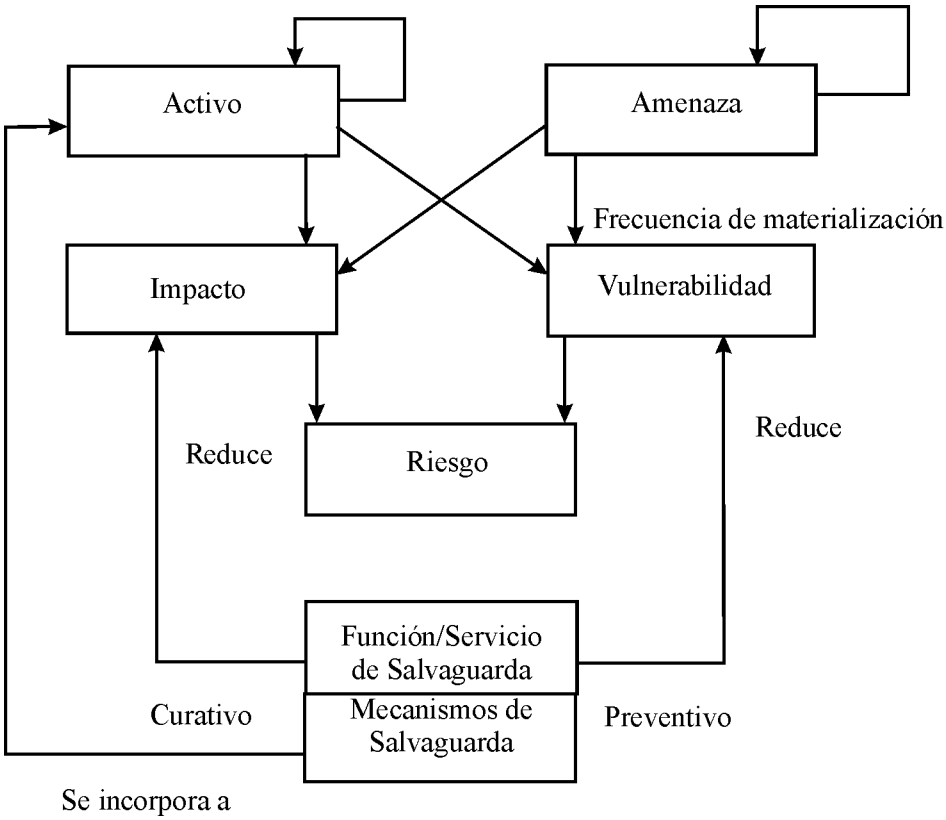

figura 2-5 Relaciones entre elementos

Submodelo de Procesos

El Submodelo de Procesos de MAGERIT está dividido en etapas, compuestas por actividades y éstas se desglosan en tareas (y en caso necesario en subtareas).

El Submodelo de Procesos de MAGERIT comprende 4 etapas:

1. Planificación del Proyecto de Riesgos. Como consideraciones iniciales para arrancar el proyecto de análisis y gestión de riesgos, se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.

2. Análisis de riesgos. Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.

3. Gestión de riesgos. Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

4. Selección de salvaguardas. Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del AGR, para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a

diversos niveles.

Herramientas:

- Herramienta RIS2K *Magerit*. La utilización de esta herramienta RIS2K, que data de 1998, es únicamente recomendable a efectos de demostración o de aplicación a entornos o situaciones no muy complejas. Para los demás usos, conviene emplear otros instrumentos de mayor flexibilidad y potencia, como las hojas de cálculo de propósito general.
- La herramienta CHINCHON versión 1.3 , elaborada por D. José Antonio Mañas, Profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid. CHINCHON es una herramienta que sigue la metodología MAGERIT. La entrada se escribe en XML y realiza un análisis de la posición de riesgo, sirviendo de apoyo a su gestión. Los derechos de propiedad intelectual pertenecen al autor, quien ha puesto la herramienta en el dominio público.

Seguridad para el desarrollo de aplicaciones

Para poder construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con MÉTRICA V 3 6. MAGERIT permite añadir durante el desarrollo del Sistema la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfaces tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

La Guía para Desarrolladores de Aplicaciones. Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica.

Productos y servicios complementarios

"Los Criterios de seguridad, normalización y conservación" 6 recogen los requisitos, criterios, y recomendaciones relativos a la implantación de las medidas de seguridad organizativas y técnicas para asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en el diseño, desarrollo, implantación y explotación de las aplicaciones que la Administración General del Estado utiliza para el ejercicio de sus potestades. Estos Criterios pueden ser complemento de MAGERIT y útiles para otras organizaciones que no pertenecen a las Administraciones Públicas. Podemos encontrar criterios de normalización, seguridad, y conservación aplicables a muchos entornos. Aconsejamos la consulta de este documento.

2.4.3 OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*)

OCTAVE 6 es una metodología estadounidense desarrollada por el Centro de Coordinación CERT del Instituto de Ingeniería del Software de la Universidad Carnegie-Mellon. Un segundo método está en desarrollo el OCTAVE-S, dirigido a pequeñas organizaciones.

2.5 NIVEL 5º Certificación

El siguiente nivel correspondería a la Certificaciones de productos. Entendemos que este es el nivel superior, después de implantar un Sistema de Gestión de la Seguridad de la Información según una norma estándar, lo que procede es Certificar que cumple con dicha norma. No está disponible todavía la norma para la certificación de la norma UNE 17799. Comentamos en este apartado la norma ISO/IEC 15408 (Criterios Comunes), para certificación de componentes.

2.5.1 Normas de evaluación y certificación

Son el conjunto de normas que sirven para evaluar o certificar que, instalaciones, normas, o programas poseen certificaciones de seguridad. Nos encontramos con normas de diversos ámbitos:

- Estadounidenses
  - TCSEC-Trusted Computer SECurity (libro naranja)
- Europeos
  - ITSEC/ITSEM
- Internacionales
  - ISO/IEC 15408-1 (CC v2.1)

Un poco de historia

Common Criteria es el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos IT y ampliamente aceptado por la comunidad internacional.

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (*Trusted Computer System Evaluation Criteria*) y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas mas flexibles y adaptables a la constante evolución de los sistemas de IT.

De ahí la comisión europea, en el año 1.991 publicó el ITSEC (*Information Technology Security Evaluation Criteria*), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canada, igualmente se desarrollaron en 1.993 los criterios CTCPEC (*Canadian Trusted Computer Product Evaluation*) uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publico los *Federal Criteria* como una aproximación a unificar los criterios europeos y americanos.

Tal escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general, y en esa labor ISO comienza a trabajar a principios de los años 90. Esta tarea fue asignada al grupo de trabajo 3 (WG 3) del subcomité 27 (SC 27) del Comité Técnico ISO/IEC JTC 1 dedicado a Tecnologías de la Información.

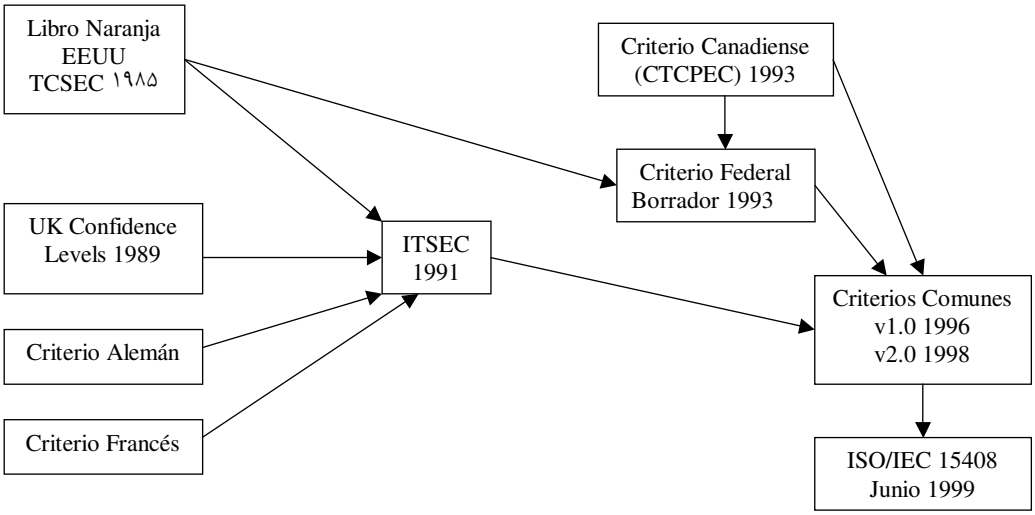

figura 2-6 Evolución de los criterios comunes

La culminación del proceso ocurrió en Junio de 1999, cuando ISO estableció el *Common Criteria* versión 2.0 como estándar, estableciéndolo como ISO 15408 con el título de "*Evaluation Criteria for Information Technology Security*" (ISO-IEC 15408).

Es el resultado de una laboriosa e intensa negociación entre países para obtener un acuerdo de reconocimiento mutuo de las certificaciones de seguridad de productos IT realizadas entre un grupo de 14 países entre los que figura España como firmante del acuerdo a través del Ministerio de Administraciones Publicas[17].

Estos 14 países signatarios de los acuerdos de *Common Criteria*, llegaron a este arreglo porque permitiría establecer un único criterio con el que evaluar la seguridad de los productos de IT, contribuyendo a aumentar la confianza de los usuarios en los mismos.

Vamos a ver con un poco de más detalles cada una de las normas anteriores.

2.5.2 CRITERIOS EVALUACIÓN EEUU: TCSEC (*Trusted Computer SECurity*)

El propósitos de estos criterios de evaluación son:

- •Suministrar normas de seguridad a los fabricantes.
- •Definir métricas de evaluación y certificación.
- •Establecer condiciones para la adquisición de sistemas.

[17] (http://www.map.es/csi/pg3432.htm)

Los requisitos establecidos son:

- •Funciones a implementar
- •Adecuación de las implementaciones

Las divisiones establecidas

- •D, C, B, A

Las clases establecidas son:

- •D protección mínima
- •C1, C2 protección discrecional
- •B1, B2, B3 protección preceptiva
- •A1 protección verificada

2.5.3 ESTÁNDAR EUROPEO DE EVALUACIÓN Y CERTIFICACIÓN

En es estándar Europeo de Certificación y Evaluación podemos distinguir entre:

- •Los criterio de evaluación: ITSEC *Information Technology SECurity*
- •La metodología: ITSEM.

Una característica de esta norma Europea es la existencia de un esquema nacional de evaluación y certificación. Cada país tiene su autoridad de Evaluación y Certificación.

Criterios de Evaluación ITSEC (*Information Technology SECurity*)

Los Criterios de Evaluación ITSEC se fijan sobre los Objetivo de seguridad, las Funciones de seguridad y los Mecanismos de seguridad sobre el Objeto a evaluar (TOE).

Los aspectos de la evaluación se realizan sobre:

- •La funcionalidad. Establece 10 niveles funcionales de F1-F10(Conjunto de funciones de seguridad: F-DX, F-DC, F-DI, F-AV, F-IN, F-B3, F-B2, F-B1, F-C2, F-C1).
- •La confianza. Establece 7 niveles de garantía (Efectividad y Corrección: E0, E1, E2, E3, E4, E5, E6).

Metodología ITSEM

Las partes implicadas que se reconocen en esta metodología son:

- •El patrocinador del producto que queremos certificar
- •El Productor
- •Las Instalaciones de evaluación
- •La Comisión nacional de certificación

Funciones de la Comisión nacional de certificación

- •Las funciones de las comisiones nacionales de Certificación son las siguientes:
- •Acreditación de instalaciones
- •Supervisión de la evaluación
- •Revisión Informes Técnicos
- •Emisión de certificados
- •Publicación de certificados

Acuerdo de reconocimiento mutuo de certificados (Nov. 1997)

Organismos de certificación reconocidos:

- •Reino Unido
- •Francia
- •Alemania

2.5.4 ISO/IEC 15408 (Criterios Comunes[18])

La Norma internacional ISO 15408, también conocida como "*Common Criteria*" 6 establece unos criterios de evaluación y certificación de la seguridad en Tecnologías de la Información. Quedan fuera de su marco de normalización los siguientes aspectos:

- •Medidas administrativas

[18] ISO/IEC 15408 http://www.commoncriteria.org/

•Medidas físicas

•Marco legal de la evaluación

•Calidad intrínseca de los algoritmos de cifrado

Justificación

Muchos sistemas y productos de Tecnologías de la Información están diseñados para satisfacer y realizar tareas específicas y puede ocurrir, normalmente por razones económicas, que determinados aspectos de seguridad se encuentren delegados en funciones de seguridad de otros productos o sistemas de propósito general sobre los cuales ellos trabajan como pueden ser sistemas operativos, componentes *software* de propósito específico o plataformas *hardware*.

Por tanto, las medidas de salvaguarda dependen del correcto diseño y funcionamiento de los servicios de seguridad que implementan otros sistemas o productos IT más genéricos.

Sería deseable por tanto, que éstos estuvieran sometidos a evaluación para conocer en que medida nos ofrecen garantías y podemos depositar confianza en ellos. Muchos clientes y consumidores de sistemas y productos IT carecen de los conocimientos necesarios o recursos suficientes para juzgar por ellos mismos si la confianza que depositan en estos sistemas o productos IT es adecuada y desearían no obtener esa certeza solamente en base a la información que proporcionan los fabricantes o las especificaciones de los desarrolladores.

La norma ISO/IEC 15408 define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT. Ello permite la equiparación entre los resultados de diferentes e independientes evaluaciones, al proporcionar un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto en base al conjunto de requisitos de seguridad y garantía que satisface respecto a esta norma obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

Por tanto, la norma ISO/IEC 15408 proporciona una guía muy útil a diferentes perfiles relacionados con las tecnologías de la seguridad.

Desarrolladores de productos o sistemas de tecnologías de la información (fabricantes).Pueden ajustar sus diseños y explicar lo que ofrecen.

Los evaluadores de seguridad, que juzgan y certifican en que medida se ajusta una especificación de un producto o sistema IT a los requisitos de seguridad deseados. Es decir, puede certificar lo que asegura.

Los usuarios que pueden conocer el nivel de confianza y seguridad que los productos de tecnologías de la información y sistemas le ofrecen y puede explicar lo que quiere.

1. Los usuarios pueden comparar sus requerimientos específicos frente a los estándares de *Common Criteria* para determinar el nivel de seguridad que necesitan.
2. Los usuarios pueden determinar mas fácilmente cuando un producto cumple una serie de requisitos. Igualmente, *Common Criteria* exige a los fabricantes de los productos certificados publicar una documentación exhaustiva sobre la seguridad de los productos evaluados.
3. Los usuarios pueden tener plena confianza en las evaluaciones de *Common Criteria* por no ser realizadas por el vendedor, sino por laboratorios independientes. La evaluación de *Common Criteria* es cada vez mas utilizada como condición necesaria para concurrir a concursos públicos. Por ejemplo, el Departamento de Defensa Americano ha anunciado planes para utilizar exclusivamente productos certificados *por Common Criteria*.
4. Debido a que *Common Criteria* es un estándar Internacional, proporciona un conjunto común de estándares que los usuarios con operaciones internacionales pueden utilizar para escoger productos que se ajusten localmente a las necesidades de seguridad.

En definitiva, proporcionando un conjunto de estándares en seguridad como los recogidos por *Common Criteria*, se crea un lenguaje común entre los fabricantes y los usuarios, que ambos pueden entender. Los fabricantes utilizarán este lenguaje para contar a sus clientes potenciales las características de sus productos evaluadas en *Common Criteria*, e igualmente habilita a los usuarios a identificar y comunicar adecuadamente sus necesidades de seguridad. Se proporcionan unos medios y mecanismos objetivos que nos permitirán tomar decisiones en base algo más sólido que las meras percepciones.

Diferentes partes del Estándar

El ISO/IEC 15408 se presenta como un conjunto de tres partes diferentes pero relacionadas. A continuación, describimos cada una de ellas:

Parte 1. Introducción y modelo general. IS 15408-1:1999(2002) *Introduction and general model*

Define los principios y conceptos generales de la evaluación de la seguridad en tecnologías de la información y presenta el modelo general de evaluación. También establece cómo se pueden realizar especificaciones formales de sistemas o productos IT atendiendo a los aspectos de seguridad de la información y su tratamiento.(la estructura y lenguaje comunes para expresar los requisitos de seguridad de productos o sistemas de TI).

- PP –*protection profile* –perfil de protección
  - lo que se quiere: requisitos para una categoría de productos
- ST –*security target* –objetivo de seguridad
  - fabricante: lo que ofreceré: especificaciones de un producto
- TOE –*target of evaluation* –objetivo de evaluación
  - una implementación de ST

Parte 2. Requisitos Funcionales de Seguridad IS 15408-2: 1999(2002) *Security functional requirements*

Este tipo de requisitos definen un comportamiento deseado en materia de seguridad de un determinado producto o sistema IT.

Parte 3. Requisitos de Garantías de Seguridad IS 15408-3:1999(2002) *Security assurance requirements*

Este tipo de requisitos establecen los niveles de confianza que ofrecen funciones de seguridad del producto o sistema. Trata de evaluar que garantías proporciona el producto o sistema en base a los requisitos que se satisfacen a lo largo del ciclo de vida del producto o sistema.

Evolución del estándar

Las normas que se están elaborando para el futuro inmediato son:

- IS 15292:2001(2005) *Protection profile registration procedures*
- WD 18045 *Methodology for IT security evaluation*

Niveles de garantía

- *Common Criteria* o ISO/IEC 15408, proporcionan también unos niveles de garantía (EAL) como resultado final de la evaluación. EAL –*Evaluated Assurance Level*
- EAL0: sin garantías
- EAL1: probado funcionalmente
- EAL2: probado estructuralmente
- EAL3: probado y chequeado metódicamente
- EAL4: diseñado, probado y revisado metódicamente
- EAL5: diseño y pruebas semi-formales
- EAL6: diseñado, probado y verificado semi-formalmente
- EAL7: diseñado, probado y verificado formalmente Constituyen la base para el reconocimiento mutuo

Organización de los requisitos de Seguridad

Los CC establecen unos criterios de evaluación basados en un análisis riguroso del producto o sistema IT a evaluar y los requisitos que este satisface. Para ello, establece una clasificación jerárquica de los requisitos de seguridad. Se determinan diferentes tipos de agrupaciones de los requisitos siendo sus principales tipos los que vemos a continuación:

- Clase: Conjunto de familias comparten un mismo objetivo de seguridad.
- Familia: un grupo de componentes que comparten objetivos de seguridad pero con diferente énfasis o rigor.
- Componente: un pequeño grupo de requisitos muy específicos y detallados. Es el menor elemento seleccionable para incluir en los documentos de perfiles de protección (PP) y especificación de objetivos de seguridad (ST).

2.5.5 Metodología abierta para la verificación de la seguridad (OSSTMM)

Existe una metodología de código abierto para la verificación de la seguridad de los sistemas. Esta metodología es de ISECOM 6 (*Institute for security and Open methodologies*) La metodología se conoce por las siglas OSSTMM – (*Open Source Security Testing Methodology Manual*).

Isecom es una organización internacional, sin ánimo de lucro, que tiene como objetivo desarrollar conocimientos y herramientas relacionadas con la seguridad, ofreciéndolas bajo una licencia de código abierto que permite su libre utilización.

OSSTMM es el estándar más completo existente en la actualidad con una metodología para la verificación de la seguridad de los sistemas y las redes que disponen de una conexión a Internet.

Esta metodología, se encuentra en constante evolución y es fruto de la colaboración de más de 150 colaboradores de todo el mundo. Gracias a este número de colaboradores, el documento incorpora los más recientes cambios y nuevos desarrollos relacionados con la seguridad informática.

La OSSTMM es una metodología para la realización de las verificaciones de seguridad en Internet. Se trata del principal proyecto existente en la actualidad para definir una metodología formal que permita verificar la seguridad informática de los equipos, desarrollado de una forma independiente y totalmente abierto. Otros proyectos en los que se está trabajado son la metodología para la programación segura y la "*Hacker High School*".

El disponer de una metodología de trabajo estandarizada significa que permita garantizar el nivel de pruebas que se realizan en el momento de verificar la seguridad. No pretende especificar una lista de pruebas concretas a realizar, sino los elementos que deben verificarse, tanto desde el exterior como el interior.

Un aspecto importante a señalar es que la OSSTMM ha sido diseñada para cubrir los aspectos técnicos establecidos por diversas legislaciones. Así, en el caso concreto de España, la OSSTMM incluye los requerimientos establecidos tanto por la ley de protección de datos y la LSSICE.

Es un proyecto interesante pero que no es adecuado para la elaboración de los planes de seguridad que por normativa legal hay que realizar.

Son mas recomendable la norma ISO 17799 ayudada de la metodología Magerit. La metodología OSSTMM esta orientada a evaluar la seguridad de un sistema. Esta orientada a realizar una auditoría de seguridad de los sistemas.

2.5.6 Metodología del *Computer Security Resource Center* (CSRC-NIST)

El *Computer Security Resource Center* (organismo que depende del NIST, *National Institute of Standards and Technology* del departamento de comercio de los Estados Unidos) ha publicado su metodología para la verificación de la seguridad de los sistemas y de las políticas de seguridad 6.

Este documento está dividido en cuatro secciones: una introducción a la metodología, la descripción de los métodos de verificación y el conjunto de seguridad, la definición de los métodos y objetivos de las pruebas de seguridad y, en la última sección, que elementos deben tener prioridad cuando se realizan las verificaciones con unos recursos limitados.

3 Discusión

Como comentábamos en la introducción de este trabajo, una vez analizadas las distintas normas y estándares, nivel a nivel, vamos a comentar las carencias detectadas para encontrar líneas de trabajo. En general, podemos afirmar con rotundidad que el nivel de cumplimiento de plan de acción eEurope 2005 es muy bajo en España.

En el nivel 1º

En relación con la creación de una cultura de seguridad, establecida en el plan de acción eEurope 2005, podemos afirmar que no existen campañas institucionales para concienciar a los usuarios de la importancia de la seguridad de los sistemas personales.

Podemos considerar que la única iniciativa nacional con cierta difusión es el Centro de alerta temprana de virus 6, donde podemos encontrar además de información sobre virus, alguna información sobre seguridad. La existencia de este sitio no es conocida. No se ha realizado la suficiente difusión entre el gran público como para que tenga una incidencia positiva en la mejora de la seguridad en España. Sus campañas se han limitado a los virus informáticos. Para subsanar esta carencia sería necesario aumentar la difusión de la existencia de este sitio y mejorar su contenido además de realizar una verdadera campaña de concienciación de la importancia de la seguridad en los sistemas de información a todos los niveles. Esta línea de trabajo le corresponde a la Administración, y no requiere mas que voluntad política para hacerlo.

De la falta de concienciación sobre la importancia de los sistemas de gestión de la seguridad no existe solo entre el gran público. Alcanza a capas de más alto nivel de formación y responsabilidad. Podemos comentar la carencia de asignaturas específicas sobre seguridad en la mayoría de los planes de estudios de las Diplomaturas de Informática en España. Cuando existen alguna asignatura de seguridad suelen tratar sobre criptografía. Podemos poner como ejemplo de este caso nuestra propia Universidad. Por tanto, además de la falta de concienciación, hace falta más formación en materia de seguridad a todos los niveles. Las medidas de concienciación y formación son administrativas y no proporcionan líneas de trabajo.

Un usuario no profesional o doméstico necesita utilizar una serie de programas amplio para garantizar la seguridad.(antivirus, cortafuegos, detector de intrusos, filtros de contenidos, configuración segura de su sistema operativo, actualizaciones de los parches de seguridad de las aplicaciones, limpiado y mantenimiento del registro de Windows...). Independientemente del costo, (puede elegir entre versiones gratuitas no totalmente operativas o de pago), requieren actualmente unos conocimientos amplios de informática, imposible de exigir a todos los usuarios. Un camino puede ser exigir una certificación de formación mínima para la adquisición y utilización de los ordenadores si van a estar conectados a internet., o que los ISP no proporcionaran conexión a un ordenador hasta comprobar (por medio de auditoria remota de seguridad) que el sistema cumple con unos mínimos. Es claro que estas medidas se enfrentan a intereses comerciales y que son de implantación poco probable.

Otra posibilidad es el desarrollo de herramientas de seguridad de código abierto y gratuitos, con "inteligencia" para aprender del entorno y con capacidad de auto-configuración. Estas características son requeridas para evitar la necesidad de un nivel de formación alto y continuo de todos los usuarios de ordenadores. El conjunto de herramientas abarcaría a las relacionadas como básicas en el nivel 1º.

Nivel 2º

En este nivel, el principal objeto de discusión son las características técnicas del reglamento de seguridad, el grado de facilidad de su cumplimiento, y la utilidad real en relación con la mejora de la seguridad de los sistemas de información.

El reglamento de seguridad (Real decreto 994/1999) establece la obligación de elaborar un documento de seguridad, pero no establece ningún modelo. Hay algunos ejemplo no oficiales 6 6. Son necesarios la elaboración de documentos de seguridad específicos para sectores concretos (abogados, médicos, gestorías, pequeño comercio...). Esto facilitaría muchísimo la realización de documentos de seguridad. Esta es una línea de trabajo.

El reglamento no especifica las medidas concretas a nivel técnico que hay que tomar en cada caso, dejando cierta ambigüedad. Por ejemplo indica en varios de sus apartados "*..se tomarán las adecuadas medidas técnicas que garantices*....". Esto deja indefenso al técnico que haya realizado el documento de seguridad. Si hay un ataque el técnico siempre es culpable, por definición. Algunos preceptos legales son técnicamente muy difícil de cumplir. El reglamento no está basado en estándares que permita certificaciones. Es necesario la modificación del Reglamento de Seguridad con la visión de los técnicos informáticos.

El reglamento de seguridad no requiere estar calificado para realizar las preceptivas auditorias de seguridad. Es necesario que se requiera una titulación oficial informática de nivel universitario o acreditación certificada por organismo oficial para la realización de las auditorias.

Los colegios profesionales (médicos, abogados, gestores administrativos..) deben de realizar campañas entre sus asociados, así como los gremios y asociaciones empresariales para la difusión de la obligación de cumplimiento del reglamento de seguridad.

Estas dos últimas consideraciones requieren una solución por parte de la Administración. No son objeto de investigación.

Faltan herramientas que comprueben que las medidas contenidas en el documento de seguridad están realmente implementadas. Para un adecuado análisis de riesgos necesitamos también dispositivos que comprueben de modo automático las vulnerabilidades de un sistema concreto y las amenazas reales que son aplicables. Sí existen herramientas de análisis de seguridad pero enfocadas a ataques sobre puertos. Pero son parciales y poco configurables. No se adaptan a las medidas del documento de seguridad. Es necesario el desarrollo de estas herramientas con las características ya mencionadas.

Dada la existencia de una normativa legal de obligado cumplimiento, serán necesario elementos probatorios cuando existan denuncias expresas. No hay criterios de actuaciones para la obtención de

pruebas de delitos informáticos. Proponemos como línea a seguir la definición de metodologías de Análisis Forense y de diseños de dispositivos que permitan el desarrollo de Análisis Forense.

Nivel 3º

Analizadas las distintas normas sobre sistemas de gestión de seguridad, podemos resumir que el ciclo de vida para la gestión de la seguridad de un sistema de información responde a los siguientes pasos:

1. Determinar los objetivos y la estrategia de seguridad, de acuerdo con las funciones de nuestra organización y los requisitos necesarios que sean necesarios garantizar. Establecer la política de seguridad de la INFORMACIÓN.
2. Análisis y gestión de riesgos. Así conoceremos el contexto de nuestro problema, nuestros activos, nuestros puntos débiles y las medidas de seguridad de las que disponemos. Además, también lograremos determinar la relación de medidas de seguridad que a menor costo minimizan nuestros posibles daños. Analizamos la rentabilidad de las posibles soluciones a implantar.
3. Establecer la planificación de la seguridad a implantar.
4. Adecuar la organización a las nuevas responsabilidades y asignar tareas dentro del organigrama.
5. Implantar las medidas seleccionadas
6. Concienciar y entrenar al personal en el uso de las nuevas medidas
7. Monitorización y supervisión de los mecanismos de seguridad implantados y atender a los posibles eventos o incidentes
8. Revisión y auditoria de la situación para ver si se siguen garantizando los requisitos de seguridad o es necesario un nuevo análisis de riesgos.

Esta metodología es cíclica y continua, siempre en constante revisión, puesto que las amenazas a la seguridad son algo dinámico y las tecnologías de protección y prevención están en constante evolución.

En los casos de empresa medianas y grandes es fundamental el establecimiento formal de políticas de seguridad, mediante la difusión y seguimiento de las buenas prácticas establecidas por la ISO/IEC 17799:2000.

La norma ISO/IEC 17799 y su espejo nacional UNE 17799 de buenas prácticas de seguridad, no tienen actualmente norma internacional de certificación. La existencia de esa norma certificadora actuaría de aliciente para que muchas empresas que no consideran prioritario la implantación de dicha norma en la actualidad, se lo plantearan aunque fuese solo por motivos de imagen ante el mercado. Es necesaria la pronta publicación de la norma certificadora con el objetivo de mejorar la situación de seguridad de las empresas e instituciones. La experiencia de las certificaciones de calidad demuestra que no solo las grandes empresas, sino que también la mediana y pequeña han ido obteniendo certificaciones de calidad para mejorar su imagen ante sus clientes potenciales. Tampoco existe una norma UNE certificadora de estos sistemas. Es cierto que existe la BS 7799-2, que permite certificaciones, pero al ser una norma nacional Británica no tiene el mismo efecto.

Desde el punto de vista de una pequeña empresa aplicar las medidas técnicas para cumplir con la norma BS 7799-2 sería una tarea que cualquier administrador de seguridad podría llevar a cabo sin mayor dificultades.

En cualquier caso, es importante destacar el hecho de que las medidas de seguridad puedan implementarse con *software* libre 6. Esto permite llevar a cabo implementaciones de la política de seguridad sin que sea necesario considerar el coste del *software* y sin que aparezcan problemas de escalabilidad. El primero de los problemas es al que habitualmente se enfrentan las pequeñas empresas por el elevado coste del *software* asociado a la seguridad, el segundo de los problemas es también común en empresas grandes debido al elevado número de sistemas a asegurar. El *software* libre ofrece, por tanto, una solución válida al entorno de seguridad de cualquier organización permitiendo la adecuación e implementación de políticas de seguridad basadas en estándares internacionales.

Existen herramientas de análisis de vulnerabilidades como *nessus*, *satan* 6 o *tripewire* 6 , principalmente dedicadas a vulnerabilidades de redes. No existen herramientas que analicen la seguridad de los sistemas en relación con las normas estándares de seguridad. Tampoco encontramos herramientas con capacidad de aprendizaje.

Otra carencia encontrada es la inexistencia de herramientas de “entrenamiento” de los usuarios en relación con las amenazas potenciales de un sistema. Se necesitan simuladores de ataques,

parametrizables para comprobar la reacción del sistema de seguridad y sobre todo del cumplimiento de los usuarios de las políticas de seguridad.

Por la proliferación de normativa legal en el ámbito nacional e internacional se hace necesario la elaboración de algún tipo de guía u orientación para poder aplicar prácticamente todas estas normas y recomendaciones. Es necesario el desarrollo de documentos de seguridad sectoriales, como el documento de Criterios de seguridad normalización y conservación del MAP6, que contengan todos los aspectos relacionados en las normas internacionales de seguridad para ese sector.

Existen soluciones llave en mano por parte de algunos proveedores, para implantar un sistema se seguridad más integrales, pero solo son accesible, por su elevado costo , a las muy grandes corporaciones en las que la seguridad es fundamental (ej: banca), pero que no están al alcance de la mediana empresa.

Nivel 4º

MAGERIT, es otra metodología, pero para el análisis y la gestión de riesgos de la seguridad de los sistemas de información. Por tanto, para el establecimiento de la política de seguridad, es necesario utilizar previamente MAGERIT y luego, para elaborar el documento formal de seguridad que recoge los requisitos de protección, es recomendable el estándar ISO 17799, o su norma espejo UNE-ISO/IEC 17799-1.

Existen herramientas para el análisis de riesgo como CHINCHON que suministrándoles la información que solicita puede facilitar el análisis de riesgos. La otra línea, en la que no encontramos desarrollos, es la de aplicaciones y dispositivos que de modo automático capten los datos necesarios del sistema, propongan salvaguardas, las implementen y vuelvan al punto de inicio. Proponemos aplicaciones con capacidad de aprendizaje y autoadaptable a cada entorno.

Nivel 5º

Los *Common Criteria* o ISO 15408, están más orientados a la evaluación de *software* y *hardware* que a la evaluación de sistemas. Son una buena guía para ver como establecer requisitos de seguridad respecto a atributos de la seguridad como la confidencialidad, disponibilidad, integridad, autenticación. A día de hoy, y dado su elevado costo, no se utiliza para certificar instalaciones.

Esta norma. es importante para que los fabricantes puedan certificar el nivel de seguridad que ofrecen sus productos. Desde el punto de vista del usuario es interesante porque sabe hasta que nivel de seguridad puede pedirle al producto que compra y por tanto no incorporar eslabones ni más débiles ni más fuertes de lo necesario a su cadena de seguridad. Pero en si misma no mejora los sistemas de gestión de seguridad.

Disponemos de acuerdos internacionales de reconocimientos de certificaciones nacionales según 6 "*A R R E G L O sobre el Reconocimiento de los Certificados de Criterios Comunes*" en el campo de la Seguridad de las Tecnologías de la Información.

La metodología OSSTMM esta orientada a evaluar la seguridad de un sistema y a realizar una auditoría de seguridad de los sistemas. Resaltar que es un *software* libre. Esta última es la característica más destacable. Permite certificar sistemas y certifica a profesionales para que puedan emitir certificaciones. Estas certificaciones tiene reconocimiento internacional, pero ajenos a los organismos oficiales de certificación. Esto implica que son más económicos y más independientes de intereses comerciales. Contribuciones a esta metodología o desarrollos de metodologías similares pero en otras áreas de la seguridad de sistemas es una línea de futuro.

La Metodología CSRC-NIST es principalmente para evaluar la seguridad de redes.

4 Elección de una línea de trabajo

En este apartado queremos resumir las líneas de trabajo que podemos obtener del apartado anterior y concretar cuales entran dentro de nuestro enfoque de trabajo futuro y cuales descartamos.

En el nivel 1 hemos apuntado como línea de trabajo para cumplir con el plan de acción eEurope 2005 y demás directivas, está la necesidad de campañas de concienciación sobre la importancia de la seguridad informática así como de mayor formación a nivel de la enseñanza obligatoria como de las de nivel universitario. Las medidas de concienciación y formación son administrativas y no proporcionan líneas de trabajo. Si entendemos como línea de trabajo el desarrollo de herramientas de seguridad de código abierto y gratuitos, con "inteligencia" para aprender del entorno y con capacidad de auto-configuración.

En el nivel 2 descartando las medidas de índole administrativas, encontramos la necesidad de desarrollo de herramientas que compruebe de forma automática la correcta implantación de las medidas incluidas en el documento de seguridad, activando alarmas en caso necesario a los responsables. No estamos hablando simplemente de desarrollar una aplicación que no existe, sino de dotarlas autoconfiguración. mediante capacidades de aprendizaje. Tendríamos que crear un sistema nuevo de aprendizaje basado en las distintas tendencias actuales, adaptado a este entorno.

En el nivel 3: Otra carencia encontrada es la inexistencia de métodos de "entrenamiento" de los usuarios en relación con las amenazas potenciales de un sistema. Se necesitan "simuladores" de ataques, parametrizables para comprobar la reacción del sistema de seguridad y sobre todo del cumplimiento de los usuarios de las políticas de seguridad.

En el nivel 4: desarrollar nuevos sistemas de análisis forense que permitan descubrir los riesgos sobre los activos de un sistema concreto. En el nivel 5 no encontramos líneas de trabajo. Normalmente las certificaciones están en manos de ciertos organismos que son los que tiene autoridad para certificar.

5 Conclusiones

El Comité Técnico ISO que trata sobre seguridad en las tecnologías de la Información es el JTC 1 / SC 27. El número de estándares publicados son de 47. El comité está dividido en tres grupos de trabajo.

Tabla 2 Grupos de trabajo del comité técnico JTC1/SC 27

Grupos de trabajo	Título
JTC 1/SC 27/WG 1	Requirements, security services and guidelines
JTC 1/SC 27/WG 2	Security techniques and mechanisms
JTC 1/SC 27/WG 3	Security evaluation criteria

De los 47 estándares publicados relacionados con temas de seguridad, la inmensa mayoría corresponden al grupo 2 de mecanismos y técnicas. Podemos encontrar 6 del grupo 1 y 3 del tercero. Las relacionadas con la criptografía y las firmas digitales y autentificación son la mayoría de las normas. Del mismo modo encontramos que en términos de investigación, se repiten las proporciones en los apartados de seguridad. Por tanto podemos afirmar que proporcionalmente hay poca investigación en relación con las metodologías de los sistemas de gestión de seguridad. Las líneas de trabajo apuntadas en el apartado de discusión, son un claro ejemplo de las posibilidades de este campo en investigación.

No existe una metodología ni estándar para la realización del análisis forense. Es necesario el desarrollo de un cuerpo metodológico normalizado (una metodología) de Análisis Forense del tipo de la metodología OSSTMM.

No hay ninguna guía de procedimientos disponible para que las informaciones obtenidas por medio del análisis forense puedan tener carácter probatorio ante un tribunal.

Hay una carencia de dispositivos neutros que permitan el análisis forense de ordenadores. Se propone el diseños de dispositivos que permitan el desarrollo de Análisis Forense.

Es necesario desarrollar "aplicaciones informáticas soporte", de *software* libre, (herramientas) que faciliten la implantación de Sistemas de Gestión de Seguridad de la Información según Norma Internacional ISO17799 y el cumplimiento del reglamento de seguridad.

Existe normas y estándares relacionados con los sistemas de seguridad, pero no se indican a que nivel o tamaño de empresa corresponde cada uno. En este trabajo hemos establecido una clasificación de los mismos atendiendo al nivel y tamaño de la organización. Por tanto, una estrategia de implantación progresiva de las medidas de seguridad facilita los sistemas de gestión de la seguridad de la información.

La implantación de un estándar como UNE ISO/IEC 17799 no garantiza el completo cumplimiento de las obligaciones exigidas en el reglamento de seguridad.

6 Referencias:

[1] ISO/IEC 15408 (Criterios Comunes) parte 1, 2 y 3 [consulta 11junio de 2003] http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF

[2] ISO/IEC 17799:2000 *Information Security Management, Code of Practice for Information Security Management. International Standard*. [consulta 11 junio de 2003] http://www.iso17799software.com/

[3] BS 7799-1:1999 *Information security management –Part 1: Code of practice for information security management. British Standard*.

[4] BS 7799-2:2002 *Information Security Management. Part 2 Specification for information security management systems. British Standard*.

[5] UNE ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información (*Information technology – Code of practice for information security managment*)

[6] ISO/IEC 13335-1 IT- *Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for managing and planning IT security*

[7] ISO/IEC 13335-2 IT- *Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security*

[8] ISO/IEC 13335-3 IT- *Security techniques - Guidelines for the management of IT security - Part 3: Techniques for the management of IT security*

[9] ISO/IEC 13335-4 IT- *Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards*

[10] ISO/IEC 13335-5 IT- *Security techniques - Guidelines for the management of IT security - Part 5: Management guidance on network security*

[11] UNE 71501-1 IN Parte 1: Conceptos y modelos para la seguridad de TI

[12] UNE 71501-2 IN Parte 2: Gestión y planificación de la seguridad de TI

[13] UNE 71501-3 IN Parte 3: Técnicas para la gestión de la seguridad de TI

[14] INFORMATION TECHNOLOGY *Baseline Protection* Manual [consulta 4 junio de 2003] http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

[15] Guía de seguridad informática (SEDISI) [consulta: 11 junio de 2003] http://www.sedisi.es/06_index.htm ,

[16] MAGERIT V.1.0 Metodología de análisis y gestión de riesgos de los sistemas, 1997 Ministerio de Administraciones Públicas Boletín Oficial del Estado ISBN 84-340-0960-9; [consulta 6 de junio de 2003] http://www.map.es/csi/pg5m20.htm

I. Guía de aproximación a la seguridad de los sistemas de información
II. Guía de procedimientos
III. Guía técnica
IV. Guía para desarrolladores de aplicaciones
V. Guía para responsable del dominio protegible
VI. Arquitectura de la información y especificaciones de la interfaz para intercambio de datos
VII. Referencia de normas legales y técnicas CD-ROM

[17] LORTAD Reglamento de seguridad. E. Del Peso Navarro – M. A. Ramos González, Diaz de Santos, 1999 ISBN 84-7978-412-1

[18] LORTAD análisis de la ley. E. Del peso – M. A. Ramos González, Díaz de Santos, 1998 ISBN 84-7978-343-5 2º edición.

[19] Ley de protección de datos. La nueva Lortad. Del peso navarro, E, Díaz de Santos, 2000 ISBN 84-7978-446-6

[20] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre seguridad de las redes y de la información: Propuesta para un enfoque político europeo [consulta: 4 de junio de 2003]. y http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_es.pdf

[21] 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 [consulta 5 de junio de 2003] http://www.map.es/csi/pg3415.htm

[22] Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal [consulta 5 de junio de 2003] https://www.agenciaprotecciondatos.org/datd1.htm

[23] Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas en el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio. .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3417.htm

[24] Legislación sobre ficheros de tratamiento automatizado de datos de carácter personal. .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3419.htm

[25] Legislación sobre protección de datos de carácter personal (Disposiciones generales). .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3418.htm

[26] PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (Otras disposiciones). .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3426.htm

[27] PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (Aprobación de Documentos de seguridad en aplicación del reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. .[consulta 4 de junio de 2003] http://www.csi.map.es/csi/pg3425.htm

[28] Evaluación y certificación de la seguridad de las tecnologías de la información. MAP.[consulta 11 junio de 2003] http://www.csi.map.es/csi/pg3432.htm

[29] Adopting a multi-annual programme (2003-2005) for the monitoring of eEurope, dissemination of good practices and the improvement of network and information security (MODINIS). Brussels, 26.07.2002 COM(2002) 425 final 2002/0187 (CNS). .[consulta 4 de junio de 2003] http://www.map.es/csi/pdf/modenis_en.pdf

[30] A R R E G L O sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información. .[consulta 4 de junio de 2003] http://www.map.es/csi/pdf/acuerdo.pdf

[31] Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook .[consulta 4 de junio de 2003] ; http://csrc.nist.gov/publications/nistpubs/800-12/

[32] Estrategia para la Seguridad de los Sistemas de Información. Madrid 22 de octubre del 2002. Julián Marcelo Cocho. Universidad Politécnica de Valencia. [consulta: junio 2003] http://www.grupodoxa.com/html/grupodoxa/pdf/estrategias.pdf

[33] eEurope 2005: Una sociedad de la información para todos. junio de 2002. Bruselas, 28.5.2002 COM(2002) 263 final [consulta: 5 junio 2003] http://www.guiafc.com/documentos/2002-COM-263.pdf

[34] Documentos de seguridad. Agencia de Protección de Datos de la Comunidad de Madrid [consulta: 6 de junio 2003] https://www.madrid.org/apdcm/contenidos/documento_box00.html

[35] Estándares Internacionales de seguridad en sistemas de información. I Consecri (Congreso Nacional de Seguridad en Sistemas Teleinformáticos y Criptografía). Arturo Ribagorda Garnacho. Catedrático de Universidad. Universidad Carlos III Madrid. [Consulta: 6 de junio de 2003] http://www.consecri.com.ar/pdf/Consecri%2025-09-01/Exposiciones/05%20-%20Est%E1ndares%20internacionales%20de%20seguridad%20en%20Sist%20Inf.pdf

[36] Certificación de la Seguridad. José A. Mañas jmanas@dit.upm.es Dpto. de Ingeniería de Sistemas TelemáticosUniversidad Politécnica de Madrid. [Consulta: 6 junio 2003] http://jungla.dit.upm.es/~pepe/ec/2003/02-certificacion.pdf

[37] eEurope 2005: Propuesta de Reglamento de la Agencia de Seguridad de la Información y de las Redes Europeas presentada por la Comisión. (COM(2003) 63 final (Febrero 2003) (en inglés) [consulta 14 de junio de 2003] http://www.csi.map.es/csi/pdf/nisa_en.pdf

[38] REDI Revista Electrónica de Derecho Informático.[Consulta 6 junio de 2003] http://v2.vlex.com/es/ppv/doctrina/fuente_29

[39] Guías de la OCDE para la seguridad de los sistemas de información y redes Hacia una cultura de seguridad. *Organisation For Economic Co-Operation And Development*. (Paris 2002).[consulta 7 junio 2003]http://www.oecd.org/pdf/M00033000/M00033189.pdf

[40] CRAMM del Gobierno Británico (CCTA *Risk Analysis and Management Method*).[consulta 7

junio de 2003] http://www.cramm.com/ y Para obtener más información, consulte: http://www.crammusergroup.org.uk/

[41] Recomendaciones de seguridad. Chelo Malagon Poyato (chelo.malagon@rediris.es) Francisco Monserrat Coll (francisco.monserrat@rediris.es) David Martinez Moreno (david.martinez@rediris.es) 15 de diciembre de 2000. Versi on 0.1 [consulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/recomendaciones.pdf

[42] Documentación sobre seguridad en la Comunidad RedIRIS [consulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/

[43] Definición de una política de seguridad José R. Valverde JRValverde@es.embnet.org onsulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html

[44] Gestión de la seguridad de la información. Noviembre 2002, Mario López de Ávila Muñoz. [consulta 8 junio 2003] www.a-nei.org/documentos/PS17799.pdf

[45] Adecuándose a la norma ISO/IEC 1799 mediante software libre * José Fernando Carvajal Vión Grupo de Interés en Seguridad de ATI (ATI-GISI) carvaco@ati.es Javier Fernández-Sanguino Peña Grupo de Interés en Seguridad de ATI (ATI-GISI) jfs@computer.org 28 de octubre de 2002 [consulta 9 junio de 2003] http://www.ibiblio.org/pub/Linux/docs/LuCaS/Presentaciones/200211hispalinux/jfs2/linux-iso17799.pdf y en http://www.opensource.org.mx/lucas/Presentaciones/200211hispalinux/jfs2/linux-iso17799.html

[46] Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades. Ministerios de Administraciones Públicas. Madrid, febrero de 2003. [consulta 10 junio 2003] http://www.map.es/csi/pg5c10.htm.

[47] Magerit V1.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas. Consejo Superior de Informática y para el impulso de la Administración electrónica [Consulta 9 de junio de 2003]. http://www.map.es/csi/pg5m20.htm

[48] CHINCHON - Análisis del Riesgo. D. José Antonio Mañas, Profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid. [Consulta 9 junio de 2003] http://jungla.dit.upm.es/~pepe/chinchon/README.htm

[49] MÉTRICA. Versión 3. Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Ministerio de Administraciones Publicas 2002. CSIAE.[Consulta 9 de junio de 2003] http://www.map.es/csi/metrica3/index.html

[50] Cuarto informe anual situación de la protección de las personas en lo que respecta al tratamiento de datos personales y a la protección de la vida privada en la comunidad y en terceros países relativo al año 1999. 5019/02/es WP 46. [consulta: 11 junio de 2003] http://www.aece.org/docs/recogida.datos.internet.wp29.pdf

[51] COBRA ISO 17799 COMPLIANCE & SECURITY RISK ANALYSIS [consulta 11 junio de 2003] http://www.iso17799software.com/download.htm

[52] Alerta-antivirus centro de atención temprana de virus y seguridad informática. Ministerio de Ciencia y Tecnología. [consulta 11 junio 2003] http://www.alertaantivirus.es/index.html

[53] ISECOM *Institute for security and Open methodologies OSSTMM* - Open Source Security Testing Methodology Manual [consulta 11 junio de 2003] http://www.isecom.org/

[54] Metodología del *Computer Security Resource Center* (CSRC-NIST) [consulta 12 junio de 2003] http://csrc.nist.gov/

[55] El Comité técnico del Consejo Superior de Informática de Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados (CITAD) [consulta 12 junio de 2003] http://www.map.es/csi/fr340001.htm

[56] OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*) [consulta 12 junio de 2003] URL: http://www.cert.org/octave/

[57] Documento de seguridad. Manual Práctico. Martín Manent González. Derecho.com 2003 .ISBN 84-95996-05-7

[58] Las Tecnologías de la Sociedad de la Información en la Empresa Española, 2002. SEDISI. [Consulta 8 junio de 2003] http://www.sedisi.es/05_index.htm

[59] SSITAD – seguridad y legislación. Ministerio de Administraciones Públicas, [consulta 14 junio de 2003] http://www.csi.map.es/csi/pg6000.htm

[60] Adopción de un programa plurianual (2003-2005) para el seguimiento del Plan eEurope, la difusión de las mejores prácticas y la mejora de las redes y la seguridad de la información (MODINIS)". Propuesta de Decisión del Consejo (COM(2002) 425 final) (Julio 2002) (en inglés) [consulta 14 de junio de 2003] http://www.csi.map.es/csi/pdf/modenis_en.pdf

[61] La protección de datos personales. La solución en entornos Microsoft. D. Gonzalo Gallo Ruiz, D. Iñigo Coello de Portugal Martínez del Peral, D. Fernando Parrondo García, D. Héctor Sánchez Montenegro. 2003 [consulta 12 junio 2003] http://www.microsoft.com/spain/technet/seguridad/otros/libro_lopd.asp

[62] I Programa sectorial ANEI de gestión de la Seguridad de la Información. Mario López de Ávila Muñoz. 2002 [consulta 6 junio de 2003. http://www.a-nei.org/documentos/PS17799.pdf

[63] Satan 1.1.1 Dan Farmer and Wietse Venema [consulta 6 junio de 2003] http://www.trouble.org/satan/ plataformas: Linux, Solaris

[64] Tripwire 2.3.1-2 Tripwire, Inc. info@tripwire.com [consulta 6 de junio de 2003] http://www.tripwire.org plataforma: Linux

Anexo A: Estándares internaciones ISO

El Comité Técnico ISO que trata sobre seguridad en las tecnologías de la Información es el **JTC 1 / SC 27**. El número de estándares publicados son de 47. El comité está dividido en tres grupos de trabajo

Grupos de trabajo	Título
JTC 1/SC 27/WG 1	*Requirements, security services and guidelines*
JTC 1/SC 27/WG 2	*Security techniques and mechanisms*
JTC 1/SC 27/WG 3	*Security evaluation criteria*

Relación de estándares: Fuente: http://www.iso.ch/

NORMA	DESCRIPCIÖN
ISO/IEC 7064:2003	Information technology -- Security techniques -- Check character systems
ISO 8372:1987	Information processing -- Modes of operation for a 64-bit block cipher algorithm
ISO/IEC 9796-2:2002	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2000	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:1999	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2002	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-1:1997	Information technology -- Security techniques -- Entity authentication -- Part 1: General
ISO/IEC 9798-2:1999	Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms
ISO/IEC 9798-3:1998	Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999	Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:1999	Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 9979:1999	Information technology -- Security techniques -- Procedures for the registration of cryptographic algorithms
ISO/IEC 10116:1997	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO/IEC 10118-1:2000	Information technology -- Security techniques -- Hash-functions -- Part 1: General
ISO/IEC 10118-2:2000	Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-3:2003	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998	Information technology -- Security techniques -- Hash-functions -- Part

NORMA	DESCRIPCIÖN
ISO/IEC 7064:2003	Information technology -- Security techniques -- Check character systems
	4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:1996	Information technology -- Security techniques -- Key management -- Part 1: Framework
ISO/IEC 11770-2:1996	Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:1999	Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 13335-1:1996	Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
ISO/IEC TR 13335-2:1997	Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security
ISO/IEC TR 13335-3:1998	Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
ISO/IEC TR 13335-4:2000	Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
ISO/IEC TR 13335-5:2001	Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
ISO/IEC 13888-1:1997	Information technology -- Security techniques -- Non-repudiation -- Part 1: General
ISO/IEC 13888-2:1998	Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 13888-3:1997	Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 14516:2002	Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services
ISO/IEC 14888-1:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General
ISO/IEC 14888-2:1999	Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Identity-based mechanisms
ISO/IEC 14888-3:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms
ISO/IEC 14888-3:1998/Cor 1:2001	
ISO/IEC 15292:2001	Information technology - Security techniques - Protection Profile registration procedures
ISO/IEC 15408-1:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC 15408-2:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
ISO/IEC 15408-3:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO/IEC 15816:2002	Information technology -- Security techniques -- Security information objects for access control
ISO/IEC 15945:2002	Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General

NORMA	DESCRIPCIÖN
ISO/IEC 7064:2003	Information technology -- Security techniques -- Check character systems
ISO/IEC 15946-2:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures
ISO/IEC 15946-3:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment
ISO/IEC TR 15947:2002	Information technology -- Security techniques -- IT intrusion detection framework
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management
ISO/IEC 18014-1:2002	Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework
ISO/IEC 18014-2:2002	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
ISO/IEC 21827:2002	Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®)

Anexo B: Glosario según la Norma UNE 71501 IN

activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

amenaza: Evento que puede desencadenar un incidente en la Organización, produciendo daños o pérdidas materia- les o inmateriales en sus activos.

análisis de riesgos: Proceso que permite la identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

autenticidad: Característica que se refiere a la comprobación y confirmación de la identidad real de los activos (procesos, sistemas, información) y/o actores (usuarios) y/o de la autorización por parte de los autorizadores, así como la verificación de estas tres cuestiones.

confidencialidad: Característica que evita el acceso o la divulgación de activos del dominio (información) a individuos, entidades o procesos no autorizados. Concierne sobre todo a activos de tipo información, y a menudo se relaciona con la intimidad o "privacidad", cuando esa información se refiere a personas físicas, contemplada en la LOPD, Ley Orgánica de Protección de Datos 15/1999

controles básicos: Conjunto mínimo de salvaguardas establecidas para un sistema o una organización

disponibilidad: Característica que previene contra la denegación no autorizada de acceso a los activos. La disponibilidad se asocia a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información.

fiabilidad: Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

gestión de riesgos: Proceso basado en los resultados obtenidos en el análisis de riesgos, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados reduciendo de esta manera al mínimo su potencialidad o sus posibles perjuicios.

impacto: Consecuencia sobre un activo de la materialización de una amenaza.

integridad: Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio. La integridad está vinculada a la fiabilidad funcional del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél) y suele referirse (aunque no siempre) a activos de tipo información. Por ejemplo, son típicos los problemas causados por la amenaza de un virus (llegado con un disquete externo o a través de la red) a la integridad de los datos almacenados en el disco duro de un ordenador personal.

política de seguridad de TI: Conjunto de normas reguladoras, reglas y prácticas, que determinan el

modo en que los activos, incluyendo la información considerada como sensible, son gestionados, protegidos y distribuidos dentro de una organización.

responsabilidad: Propiedad de una entidad que garantiza que las acciones de ésta (como violaciones o intentos de violación de la seguridad) queden asociadas inequívocamente a ella.

riesgo: Es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (conjunto de activos) o en toda la organización.

riesgo residual: Es el riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

salvaguarda: Acción, procedimiento **o** dispositivo, físico o lógico que reduce el riesgo.

seguridad de TI: Conjunto de aspectos relacionados con la autenticidad, confidencialidad, integridad y disponibilidad.

vulnerabilidad: Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.

Anexo C: Definiciones de conceptos de la Ley Orgánica 15/1999 y del Real Decreto 994/1999

Tanto la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, Real Decreto 994/1999, de 11 de junio de Medidas de Seguridad, recogen en su articulado definiciones de conceptos que facilitan la comprensión de estas leyes.

Datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.

Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Datos accesibles al público: datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

Recurso: cualquier parte componente de un sistema de información.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Soporte: objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se pueden grabar o recuperar datos.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Anexo D: sitios de seguridad

En estas direcciones hay antivirus el línea

www.pandasoftware.es (*panda active scan*)

http://es.trendmicro-europe.com/enterprise/products/housecall.php

www.trendmicro.es (products housecall)

http://www.zonavirus.com/Antivirus_on_line.asp lista de antivirus *on line*

http://www.ravantivirus.com/scan/indexn.php

http://scan.sygatetech.com/prestealthscan.html

http://www.bitdefender.com/scan/licence.php

SNORT http://www.snort.org/

http://www.spychecker.com/

http://www.hormiga.org/hack/scaners.htm

NESSUS: http://www.nessus.org/

NMAP: http://www.insecure.org/nmap/ y http://www.insecure.org/links.html

Landguard: http://www.gfi.com/lannetscan/index.htm

Shadow Security Scanner: http://www.safety-lab.com/en/

RETINA: www.eeye.com

http://www.securityfocus.com/ Excelente sitio de seguridad

Centro de Alertas del MAP http://www.map.es/csi/pg7060.htm

Servicio de seguridad IRIS-CERT http://www.rediris.es/cert

Para detección de problemas de seguridad en centros de Red-IRIS y actuación coordinada para resolverlos Universidad Politécnica de Cataluña http://escert.upc.es

Sitio con listas de distribución e información sobre la ISO 17799

http://www.ictnet.es/ICTnet/cv/comunidad.jsp?area=tecInf&cv=sgsi

www.microsoft.com/spain/seguridad
ISO 17799 Directory www.iso-17799.com
Information Systems Auditand Control Association www.isaca.org
National Institute of Standards and Technology www.nist.gov
Disaster Recovery Journal www.drj.com
Business Continuity Institute www.thebci.org
Contingency Planning Exchange Inc www.cpeworld.org
Contingency Planning World www.business-continuity-world.com
Disaster Recovery Institute International www.drii.org
Globalcontinuity www.globalcontinuity.com
www.agenciaprotecciondatos.org
www.delitosinformaticos.com
www.ips.es
www.ipsca.com
http://www.criptonomicon.com/

Anexo E: Direcciones de interés de Criterios Comunes

Common Criteria
http://www.commoncriteria.org
Consejo Superior de Informática, SISTAD
http://www.map.es/csi/pg6000.htm
Perfiles de Protección Evaluados
http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html
http://niap.nist.gov/cc-scheme/PPRegistry.html
Productos Comerciales Evaluados
http://www.commoncriteria.org/epl/index.html