MINISTERIO
DE LA PRESIDENCIA

SECRETARÍA DE ESTADO PARA LA FUNCIÓN PÚBLICA

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

Normalización en seguridad de las tecnologías de la información

Nipo: 000-10-073-0

Agosto de 2010

3ª edición internet

Nipo: 000-10-073-0

Catálogo general de publicaciones oficiales
http://www.060.es/te_ayudamos_a/Publicaciones_CGPO/index-ides-idweb.html

EQUIPO RESPONSABLE DEL PROYECTO
JEFE DEL PROYECTO:
Miguel A. Amutio Gómez
Jefe de Área de Planificación y Explotación - Ministerio de la Presidencia
EDICIÓN WEB:
Mª Paloma Balairón de la Poza
Analista Programador - Ministerio de la Presidencia

ÍNDICE

1. Conceptos básicos de normalización y organismos de normalización

Las normas son especificaciones técnicas, de carácter voluntario, consensuadas, elaboradas con la participación de las partes interesadas (fabricantes, usuarios y consumidores, laboratorios, administración, centros de investigación, etc.) y aprobadas por un organismo reconocido.

Estas normas tienen el carácter de acuerdos documentados y contienen las especificaciones técnicas o criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, asegurando de esta forma que los materiales, productos, procesos y servicios son apropiados para lograr el fin para el que se concibieron.

La normalización contribuye a simplificar y a incrementar la fiabilidad y eficiencia de los bienes y servicios que utilizamos, así como a mejorar el bienestar de la sociedad y redunda en el beneficio común.

Las normas son, por tanto, documentos de aplicación voluntaria, elaborados por las partes interesadas, por consenso y aprobados por un organismo reconocido.

En el ámbito internacional, ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) tienen por objeto favorecer el desarrollo de la normalización en el mundo, con vistas a facilitar los intercambios comerciales y las prestaciones de servicios entre los distintos países. Los trabajos desarrollados por ISO cubren prácticamente todos los sectores de la técnica, con excepción del campo eléctrico y electrotécnico, cuya responsabilidad recae en IEC. Los miembros de ISO o IEC son los organismos que representan la normalización de un país. Tan sólo un organismo de cada país puede ser miembro de estas organizaciones. La participación en los comités técnicos de ISO/IEC puede ser como miembro bien "P" (participante) o bien "O" (observador).

Los órganos de trabajo técnicos de ISO son los siguientes:

- *Comités Técnicos (CT)*: su función principal es el desarrollo de las normas internacionales y su revisión, en caso de que fuera necesario. Cada CT puede, si así lo cree conveniente debido a la amplitud de su campo de actuación, establecer subcomités y/o bien grupos de trabajo para cubrir temas específicos.
- *Subcomités (SC)*: tienen las mismas atribuciones que el CT y autonomía para realizar sus trabajos, con la única obligación de mantener informado al CT de sus actividades.
- *Grupos de Trabajo (GT)*: se crean para trabajos específicos emprendidos por el comité/subcomité.

Los documentos elaborados por ISO/IEC son, principalmente, de dos tipos:

- *Norma internacional (ISO/IEC)*: norma elaborada por los miembros participantes en un comité técnico, subcomité o grupo de trabajo y aprobada por votación entre todos los participantes.
- *Informe Técnico (TR)*: documento técnico elaborado para informar sobre los progresos técnicos de un tema determinado, dar recomendaciones sobre la ejecución de un trabajo y facilitar información y datos distintos a los que generalmente están contenidos en una norma.

En el ámbito europeo **CEN** (Comité Europeo de Normalización) contribuye a los objetivos de la Unión Europea y del espacio económico europeo con estándares técnicos de uso voluntario para facilitar el intercambio de bienes y servicios, eliminar barreras técnicas, fomentar la competitividad de la industria europea y ayudar a la creación del mercado interior europeo. Así, CEN produce normas en materias tales como el comercio libre, la seguridad de trabajadores y consumidores, la seguridad e interoperabilidad de las redes, la protección del medio ambiente, la explotación de los programas de investigación y desarrollo y la administración pública.

CEN emite principalmente:

- normas europeas (EN, European Standards),
- especificaciones técnicas (TS, Technical Specifications)
- informes técnicos (TR, Technical Reports).

Una norma europea (EN) conlleva la obligación de ser adoptada como una norma nacional idéntica y de anular las normas nacionales divergentes. Cuando se elaboran a solicitud de la Comisión Europea y, o bien de la Asociación Europea de Libre Comercio, se conocen como normas europeas mandatadas. Puede tratarse de normas que apoyan Directivas comunitarias o políticas comunitarias en diversas cuestiones, como políticas industriales o de seguridad de los consumidores, por ejemplo. Finalmente, una norma armonizada es una norma mandatada que ofrece soluciones técnicas necesarias para dar presunción de conformidad con los requisitos esenciales de una o varias Directivas, y sus referencias se han de publicar en el Diario Oficial de la Unión Europea.

En 1997 se creó **CEN/ISSS** (*Comité Europeen de Normalisation / Information Society Standardization System*) para centralizar las actividades de normalización europea en materia de tecnologías de la información y las comunicaciones. En particular, los talleres de CEN/ISSS producen los CEN Workshop Agreements (CWA).

En el ámbito nacional **AENOR**, la Asociación Española de Normalización y Certificación, asumió la responsabilidad internacional en ISO en 1987, en IEC en 1995 y es, por tanto, el comité miembro que representa los intereses españoles en el campo de la normalización ante dichas organizaciones y quien distribuye los productos de ISO/IEC, CEN/CENELEC, así como las normas UNE.

De la normalización en materia de seguridad de las tecnologías de la información se ocupan respectivamente, en el ámbito internacional de ISO/IEC el subcomité ISO/IEC JTC 1/SC 27, en el ámbito europeo de CEN el órgano CEN/ISSS, en el ámbito nacional de AENOR el subcomité espejo AEN/CTN 71/SC 27.

2. El papel de las normas en la seguridad de la información y de los sistemas de tecnologías de la información

El valor creciente de la información, de los servicios prestados por medios electrónicos y de los sistemas de tecnologías de la información que los soportan, su omnipresencia y su carácter de instrumento esencial para el desarrollo económico y social de nuestra sociedad y los riesgos que se dan, conducen todos ellos a la necesidad de adoptar políticas, procedimientos, prácticas y medidas organizativas y técnicas capaces de:

- Proteger la información y gestionar la seguridad de los sistemas respondiendo a las amenazas existentes.
- Garantizar las dimensiones esenciales de la seguridad como la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad.
- Satisfacer la confianza depositada en los productos y sistemas, en la información necesaria para la toma de decisiones y en las posibles expectativas en cuanto a oportunidades de innovación y adaptación.
- Satisfacer los posibles requisitos legales, sean éstos de carácter horizontal o sectorial.

La dependencia de los sistemas de información preocupa cada vez más a la sociedad ya que genera riesgos debidos a la propia complejidad de los sistemas, a posibles accidentes, errores o ataques, a la constante evolución en un entorno cambiante, o a un posible uso irresponsable de los mismos. La materialización de estos riesgos puede afectar a la propia continuidad de los servicios, sean internos o externos, a la protección de la información en general y, en particular, de los datos de carácter personal,

así como a la propia validez y eficacia de los actos que se apoyan en transacciones electrónicas, por ejemplo, de administración electrónica o comercio electrónico.

Los diversos actores afectados, particulares, administraciones públicas y empresas demandan seguridad y, en definitiva, confianza en el uso de los sistemas de tecnologías de la información.

Los pasos a dar para garantizar la seguridad de los sistemas de tecnologías de la información se orientan a la implantación de una gestión continua de la seguridad, a la adopción de medidas organizativas y técnicas que garanticen aspectos tales como la continuidad de su funcionamiento, la protección de la información, la validez de las transacciones electrónicas, la conformidad con el marco normativo y contractual correspondiente, con condiciones tecnológicas (normas) determinadas, el aseguramiento en cuanto a un uso adecuado y optimizado de los recursos, y, en general, la satisfacción de aquellos requisitos que contribuyen al logro de los objetivos de la organización.

Se pone de manifiesto, también, la necesidad o, en su caso, obligación de demostrar en la propia organización y ante terceros que se realiza una gestión competente, efectiva y continua de la seguridad en el marco de los riesgos detectados y de que se han adoptado aquellas medidas adecuadas y proporcionadas a los riesgos a los que está expuesta la organización.

En consecuencia, es necesaria la **existencia de un conjunto articulado, sistemático, estructurado, coherente y lo más completo posible de normas** que sirvan de vocabulario y lenguaje común, de unificación de criterios, de modelo, especificación y guía para su uso repetido que permitan satisfacer las necesidades y expectativas de la sociedad en materia de construcción, mantenimiento y mejora de la seguridad de la información y de los sistemas que la soportan, aportando a la vez racionalización, disminución de costes, mejoras en competitividad y calidad e incluso nuevas oportunidades.

En los últimos años, se ha producido un incremento de la atención a la seguridad de los sistemas de información, atención a la que no han sido ajenos los Organismos de normalización que están ampliado notablemente sus catálogos de normas disponibles en esta materia. Así, se viene desarrollando una colección significativa de normas en el campo de la seguridad de las tecnologías de la información, que refleja también la evolución de la normalización en general, en la medida en que, junto con el enfoque tradicional de desarrollo de normas centradas en aspectos de la tecnología, se viene produciendo el desarrollo de normas relacionadas con prácticas de gestión, servicios y gestión de riesgos.

Este incremento de la atención a la seguridad de la información y de las tecnologías asociadas, correlativo con el desarrollo de la sociedad de la información en general, y de la administración electrónica en particular, viene teniendo reflejo también en actuaciones de la OCDE y la Unión Europea.

Así, las ***Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad*** señalan que los Gobiernos deberían desarrollar políticas que recojan las buenas prácticas en la gestión de la seguridad y en la evaluación de riesgos. Este documento indica que pueden usarse normas de gestión de la seguridad de la información reconocidos internacionalmente, tales como las normas ISO y normas específicas de la industria, para establecer sistemas de gestión de la seguridad eficaces.

En la Unión Europea, la ***Comunicación de la Comisión de las Comunidades Europeas sobre Seguridad de las redes y de la información: Propuesta para un enfoque político europeo (COM(2001) 298 final)***, propone una serie de medidas y acciones. En particular, se refiere a que las administraciones públicas desarrollen una cultura de seguridad en el seno de la organización y establezcan políticas de seguridad hechas a medida para la institución de que se trate.

La Administración, en sus proyectos de seguridad, tiene presente la normalización en seguridad de las tecnologías de la información y tiene interés en el avance y madurez de las normas.

En particular, las normas se vienen teniendo presentes en instrumentos tales como los siguientes:

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

- Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v2).
- Herramienta PILAR, que soporta la realización del análisis y gestión de riesgos siguiendo la metodología MAGERIT v2.

3. Normas de seguridad de tecnologías de la información

3.1. Introducción

De una forma panorámica, los principales ámbitos de normalización son los relativos al sistema de gestión de seguridad de la información, a las técnicas y mecanismos, sean o no criptográficos, y a la evaluación de la seguridad de las tecnologías de la información y aspectos asociados, según se refleja en el gráfico siguiente, que también recoge la presencia de ámbitos que, de forma creciente, demandan una atención especializada, como la gestión de la identidad y privacidad y los servicios y controles de seguridad, aunque se apoyen, así mismo, en los tres ámbitos principales citados.

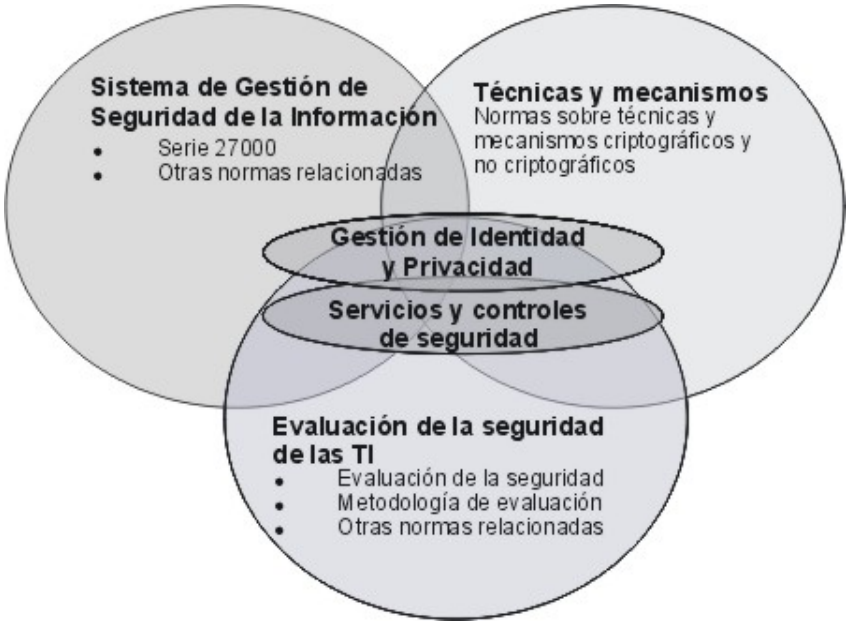

Figura 1: Panorámica general de ámbitos de normalización en ISO/IEC SC27

3.2 Normas de gestión de seguridad de la información

Perspectiva general

En 2004 se crea la serie 27000, con el objetivo de contribuir a la mejor identificación y ordenación de las normas de gestión de seguridad de la información, y satisfacer cuestiones tales como las siguientes:

- Proporcionar un marco homogéneo de normas y directrices.
- Proporcionar requisitos, metodologías y técnicas de valoración.
- Evitar el solapamiento de las normas y favorecer la armonización.
- Alinearse con los principios generalmente aceptados relativos al gobierno de las organizaciones.
- Ser consistente con las Directrices de Seguridad y de Privacidad de la OCDE.
- Usar lenguaje y métodos comunes.
- Facilitar la flexibilidad en la selección e implantación de controles.
- Ser consistente con otras normas y directivas de ISO.

Para conocer el estado de situación actualizado de la serie de normas ISO/IEC 27000 véase la página del subcomité ISO/IEC JTC1 SC27 en
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

Informes y normas UNE

En el ámbito de la normalización nacional, la creación de un cuerpo de normas e informes UNE viene tratando principalmente, hasta la fecha, la gestión de la seguridad de la información. Cabe destacar las siguientes normas:

Informes y normas UNE	
UNE ISO/IEC 27001:2007/M:2009	Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.
UNE ISO/IEC 2002 :2009	Código de buenas prácticas para la gestión de la seguridad de la información.
UNE 71504	Metodología de análisis y gestión de riesgos para los sistemas de información.

Para conocer el estado de situación actualizado de las normas UNE relativas a Tecnologías de la Información, Técnicas de seguridad véase www.aenor.es

3.3 Sistema de gestión de seguridad de la información

La aplicación de un sistema de procesos encaminado a gestionar la seguridad enfatiza la importancia de aspectos tales como los siguientes:

- La comprensión de los requisitos de seguridad de la información y la necesidad de establecer objetivos y una política para la seguridad de la información.
- La implantación y explotación de controles para gestionar los riesgos relativos a la seguridad de la información en el contexto general de los riesgos globales de la organización.
- El seguimiento del rendimiento del sistema.
- La mejora continua basada en la medida de los objetivos.
- Adopción del ciclo conocido como "Plan-Do-Check-Act" para especificar los requisitos del denominado Sistema de Gestión de Seguridad de la Información.

La norma UNE ISO/IEC 27001 especifica un sistema de gestión de seguridad de la información certificable y lo define como:

> "parte del sistema global de gestión, que sobre la base de un enfoque basado en los riesgos, se ocupa de establecer, implantar, operar, seguir, revisar, mantener y mejorar la seguridad de la información.
>
> Nota: El sistema de gestión incluye estructuras organizativas, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos."

La implantación de un SGSI permite a una organización lo siguiente:

- Conocer los riesgos.
- Prevenir, reducir, eliminar o controlar los riesgos mediante la adopción de los controles adecuados.
- Asegurar el cumplimiento de la legislación en materias tales como la protección de los datos de carácter personal, los servicios de la sociedad de la información o la propiedad intelectual, entre otras.

El **ciclo de vida del SGSI** se articula en UNE ISO/IEC 27001 según las cuatro etapas ya tradicionales en los sistemas de gestión en general, como los de gestión de calidad ISO 9001 o los de gestión medioambiental ISO 14001:

(1) **Implantación del SGSI**. Contempla actividades tales como la definición de la política de seguridad que incluye la definición del alcance y límites del sistema de gestión de seguridad de la información; el análisis y gestión de riesgos proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que estén expuestos; la evaluación de alternativas y la selección de los controles adecuados para el tratamiento de los riesgos, extraídos de forma justificada de la norma UNE ISO/IEC 27002 y, en su caso, de controles adicionales; la aprobación por la dirección de los riesgos residuales, la autorización por parte de la dirección de la implantación y explotación del sistema de gestión, así como la elaboración de la declaración de aplicabilidad, documento que recoge los controles relevantes y aplicables al sistema de gestión.

(2) **Explotación del SGSI**. Incluye actividades tales como la formulación y ejecución del plan de gestión de riesgos, la implantación de los controles seleccionados, la definición de cómo medir la efectividad de los controles seleccionados y la gestión de las operaciones y de los recursos necesarios del sistema de gestión.

(3) **Revisión del SGSI**. Incluye actividades tales como la revisión de los procedimientos y de los controles implantados para la detección temprana de errores, de brechas e incidentes de seguridad, para determinar si las actividades de seguridad de la información se comportan de conformidad con lo esperado y para ayudar a detectar eventos de seguridad, prevenir incidentes

y determinar si las acciones emprendidas para resolver una brecha de seguridad fueron efectivas; la realización de auditorías periódicas del SGSI para determinar la conformidad con la norma que especifica los requisitos del sistema de gestión, con los requisitos identificados en materia de seguridad de la información, la adecuada implantación y gestión de los controles y el funcionamiento conforme a lo esperado; la revisión de la valoración de los riesgos; la revisión del SGSI desde el punto de vista de la dirección para asegurar que el alcance permanece válido y para identificar posibles mejoras.

(4) **Mejora del SGSI**. Atendiendo a los resultados de las auditorías, a las aportaciones de los actores implicados, a los resultados de la medida de la efectividad, a la detección de amenazas y vulnerabilidades no tratadas adecuadamente y a los cambios que hayan podido producirse, debe mantenerse un proceso de mejora continua que incluya acciones tanto preventivas como correctivas.

La prestación **de servicios de certificación de conformidad con una norma que especifica los requisitos de un SGSI** tiene como **objetivo establecer la confianza en los sistemas de información**, potenciando la utilización del análisis de riesgos y de los controles necesarios para garantizar la satisfacción de los requisitos de seguridad.

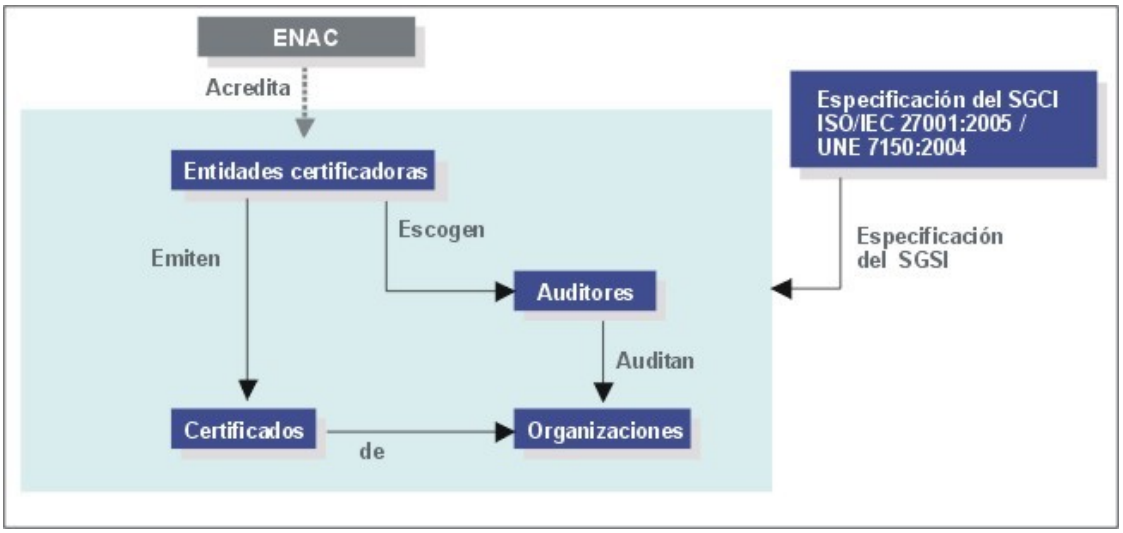

Figura 2. Esquema de los servicios de certificación de conformidad con una norma que especifica los requisitos de un SGSI

La certificación de un sistema de gestión de la seguridad de la información es un servicio voluntario de valor añadido para asegurar que la organización certificada ha implantado un SGSI de conformidad con un documento normativo específico para ello, como puede ser la norma UNE ISO/IEC 27001.

Figura 3 Esquema del procedimiento de certificación

Asimismo, el mantenimiento de la certificación requiere la realización de **auditorías de seguimiento** anuales y de una **auditoría de renovación** al tercer año.

Cabe esperar que diversas entidades presten estos los servicios de certificación de los sistemas de gestión de seguridad de la información de conformidad con la norma UNE ISO/IEC 27001 y que todas ellas se sometan al correspondiente procedimiento de acreditación de la Entidad Nacional de Acreditación (ENAC) como entidades certificadoras, de acuerdo con las normas correspondientes aplicables a los organismos certificadores de la conformidad en este campo (ISO/IEC 27006).

Relación con el Esquema Nacional de Seguridad:

Al menos para los sistemas que caigan en la categoría ALTA debería aplicarse un sistema de gestión de la seguridad de la información (SGSI) al objeto de poder satisfacer ciertos principios básicos [a) seguridad integral, b) gestión de riesgos, e) reevaluación periódica] y requisitos mínimos [Artículo 12. Organización e implantación del proceso de seguridad y Artículo 26. Mejora continua del proceso de seguridad]

El Esquema Nacional de Seguridad no exige específicamente que el SGSI sea un ISO/IEC 27001, si bien éste es aplicable. La certificación de conformidad con ISO/IEC 27001 NO es obligatoria en el Esquema.

3.4 Código de buenas prácticas para la gestión de la seguridad de la información

La norma UNE ISO/IEC 27002 aporta un conjunto de 133 controles y de recomendaciones, dirigido a los responsables de promover, implantar y mantener la seguridad, con vocación de ser útil en la mayor parte de las situaciones y organizaciones y de establecer una referencia común para el sector de la seguridad de los sistemas de información que favorezca el intercambio de productos, sistemas y servicios entre los proveedores, los clientes, los subcontratistas y otros actores.

Los **objetivos** principales de la norma ISO/IEC 27002 son los siguientes:

- **Identificar controles independientes de la tecnología** que sean de aplicación general para organizaciones pequeñas, medianas y grandes y aplicables a diferentes aplicaciones, sistemas y plataformas tecnológicas.
- **Facilitar la adopción de controles proporcionados al riesgo** en términos de políticas, prácticas, procedimientos, estructuras organizativas y funciones de software.
- **Atender la demanda relativa al desarrollo, implantación y medida de prácticas de seguridad efectivas**, que sirven tanto para la seguridad propia como para las relaciones con otras organizaciones, como referencia común para el desarrollo y la gestión de la seguridad y para la construcción de la confianza mutua en la seguridad de la información.
- **Proporcionar principios y recomendaciones de gestión en los que basar la política de seguridad** de la información en cualquier soporte, sin restringirse únicamente a los aspectos específicos de seguridad de tecnologías de la información y de las comunicaciones.

En cuanto a su aplicación práctica UNE ISO/IEC 27002, de forma general, concede gran énfasis a las siguientes cuestiones:

- La adopción de los controles proporcionados a los riegos detectados.
- La documentación de las políticas, los procedimientos y los controles.
- La identificación de las responsabilidades al nivel adecuado.
- La presencia de un control formalizado, en términos de formalización del control y de su periodicidad.
- La generación y conservación de evidencias.
- El tratamiento de los incidentes de seguridad.

En particular, ISO/IEC 27002 otorga al **análisis y gestión de riesgos** el papel clave para la identificación de los requisitos de seguridad, cuestión esencial, y para la **identificación y selección de los controles** y sobre su aplicación, en términos de su formalización y su periodicidad, **en el marco del principio de proporcionalidad**, que relaciona el valor de los activos y los riesgos a los que están expuestos, junto con el estado de la tecnología y los costes de la posible materialización de los riesgos,

así como de los controles que los contrarrestan; todo ello de acuerdo con la idea básica de que la seguridad es más barata si se incorpora, cuanto antes, en las fases de análisis y de diseño de los sistemas.

La norma ISO/IEC 27002 se estructura en introducción, objeto y campo de aplicación, términos y definiciones, estructura de la norma, valoración y tratamiento del riesgo, más once capítulos en los que se detallan los controles, lo cual lo convierte en un producto razonablemente compacto y manejable. Así mismo, como se ha expuesto más arriba, constituye una fuente de controles aplicables en un sistema de gestión de seguridad de la información.

La tabla que se incluye a continuación ofrece una visión panorámica de los contenidos de la norma ISO/IEC 27002.

Política de seguridad	Documento de política de seguridad. Revisión del documento de política de seguridad.
Organización de la seguridad	Infraestructura de organización de la seguridad. Seguridad en acceso de terceras partes.
Clasificación y control de activos	Responsabilidad de los activos. Clasificación de la información.
Seguridad ligada al personal	Antes del empleo. Durante el empleo. A la terminación del empleo o tras cambios en el mismo.
Seguridad física y del entorno	Áreas seguras. Equipamiento de seguridad.
Comunicaciones y gestión de explotación	Procedimientos operativos y responsabilidades. Gestión del servicio prestado por terceras partes. Planificación y aceptación de sistemas. Protección frente a software malicioso. Copias de seguridad. Gestión de seguridad de red. Manejo de soportes. Intercambio de información. Servicios de comercio electrónico. Registro de eventos.
Control de acceso al sistema	Requisitos de control de acceso. Gestión del acceso de usuarios. Responsabilidades del usuario. Control de acceso a servicios en red. Control de acceso al sistema operativo. Control de acceso a las aplicaciones. Informática móvil y teletrabajo.
Adquisición, desarrollo y mantenimiento de sistemas de información	Requisitos de seguridad de los sistemas de información. Procesamiento correcto de las aplicaciones. Uso de controles criptográfícos. Seguridad de los archivos del sistema. Seguridad en procesos de desarrollo y mantenimiento. Gestión de vulnerabilidades técnicas.
Gestión de incidentes de seguridad de la información.	Informe de incidentes y debilidades de seguridad de la información. Gestión de incidentes de seguridad de la información y mejoras.
Gestión de la continuidad	Aspectos de seguridad de la información en la gestión de la continuidad.
Conformidad	Conformidad con requisitos de carácter legal. Conformidad con políticas, normas y aspectos técnicos. Consideraciones de auditoría de sistemas de información.

La norma ISO/IEC 27002 apunta en su introducción algunos controles considerados esenciales, tales como los siguientes:

a) la protección de los datos de carácter personal y la intimidad de las personas

b) la salvaguarda de los registros de la Organización

c) la documentación de la política de seguridad de la información

d) la asignación de responsabilidades de seguridad de la información

e) la formación y capacitación para la seguridad de la información

f) el procesamiento correcto de las aplicaciones

g) la gestión de la vulnerabilidad

h) la gestión de la continuidad del negocio

i) la gestión de las incidencias de la seguridad de la información y sus mejoras

Relación con el Esquema Nacional de Seguridad:

La norma UNE ISO/IEC 27002 es un conjunto de controles de seguridad para sistemas de información genéricos orientados, inicialmente, al comercio electrónico.

Si bien numerosas medidas de seguridad del ENS coinciden con controles de UNE ISO/IEC 27002, el Esquema Nacional de Seguridad es más preciso y establece un sistema de protección proporcionado a los bienes protegidos lo que racionaliza la implantación de medidas de protección reduciendo la discrecionalidad. Mientras que la norma UNE ISO/IEC 27002 carece de este mecanismo de proporcionalidad, quedando, en su caso, a la mejor opinión del auditor que certifica la conformidad con la norma UNE ISO/IEC 27001.

Por otra parte, el Esquema Nacional de Seguridad contempla diversos aspectos de aplicación en el ámbito de la administración pública, por ejemplo, relativos a la firma electrónica, no recogidos en la norma UNE ISO/IEC 27002.

3.5 Técnicas y mecanismos

Destacan en este ámbito las técnicas y mecanismos criptográficos que tienen un protagonismo singular y creciente en la garantía de dimensiones de la seguridad tales como la confidencialidad, la integridad y la autenticación; forman parte de estructuras más complejas como servicios, aplicaciones e infraestructuras; y, de hecho, se han convertido en componentes clave sobre los que se sustentan piezas esenciales para los servicios de administración electrónica como puede ser la firma electrónica y el fechado electrónico.

En el campo de las técnicas y mecanismos criptográficos, las normas producidas por el SC27 ofrecen especificaciones relativas a cuestiones tales como las siguientes, sin ánimo de exhaustividad:

- Servicios de fechado electrónico (ISO/IEC 18014 *Time Stamping Services*). Se trata de una norma multiparte que, entre otras cuestiones, describe modelos, servicios y protocolos para el fechado electrónico.
- Algoritmos de cifrado simétricos, de bloque, de flujo y asimétricos (ISO/IEC 18033 *Encryption algorithms*).
- Funciones hash criptográficas (ISO/IEC 10118 *Hash functions*).
- Esquemas de firma digital que incorporan funcionalidades de autenticación e integridad (ISO/IEC 9796 *Digital signature schemes giving message recovery*).
- Autenticación de entidades (ISO/IEC 9798 *Entity authentication*); se trata de una norma multiparte que especifica diversos mecanismos de autenticación, utilizando, entre otras, técnicas de criptografía simétrica y asimétrica.
- Técnicas criptográficas basadas en curvas elípticas (ISO/IEC 15946 *Cryptographic techniques based on elliptic curves*); en particular, contienen especificaciones para sistemas de firma digital basados en curvas elípticas.
- Requisitos de módulos criptográficos.

- Gestión de claves (ISO/IEC 11770 *Key Management*). Trata de conceptos, modelos, servicios y mecanismos para la gestión de claves.
- Mecanismos de no repudio (ISO/IEC 13888 *Non repudiation*). Trata de modelos, mecanismos y de la utilización de técnicas de criptografía asimétrica para el no repudio.

3.6 La confianza en los productos y sistemas de tecnologías de la información

Los usuarios de productos y sistemas de tecnologías de la información necesitan confianza en que las soluciones que puedan desplegar satisfacen los objetivos de seguridad declarados por las mismas, en el sentido de que son capaces de hacer frente a las amenazas identificadas, de satisfacer las políticas de seguridad definidas en el marco de unos determinados supuestos o hipótesis de seguridad, así como de incorporar unos determinados requisitos funcionales y de aseguramiento que contribuyen a la satisfacción de los citados objetivos, como se resumen en la figura siguiente.

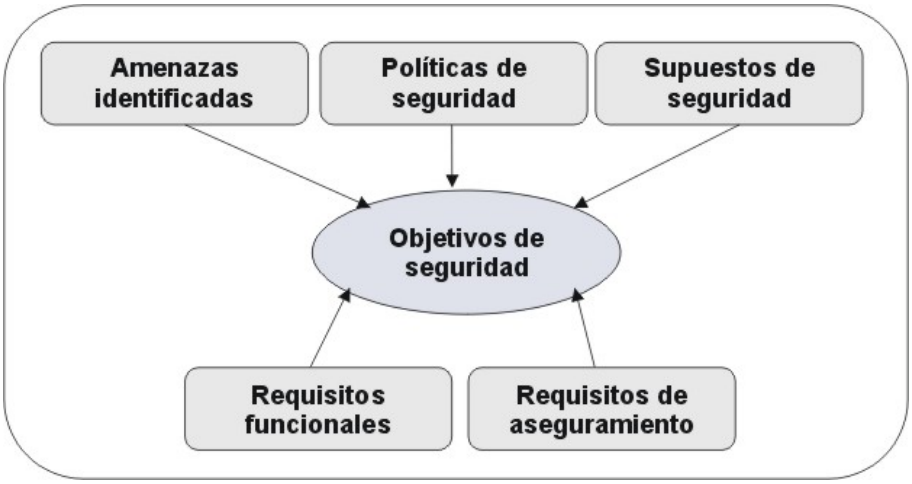

Figura 4: Relación de los objetivos de seguridad con amenazas, políticas, supuestos y requisitos funcionales y de aseguramiento

La utilización de productos y sistemas de tecnologías de la información cuya seguridad ha sido evaluada y, en su caso, certificada, es una de las salvaguardas principales para proteger la información y los sistemas que la manejan. Por *evaluación* se entiende el examen detallado a través del cual se confirma el nivel de seguridad demandado para un sistema de información o parte de él. La evaluación rigurosa e internacionalmente contrastada contribuye a dar confianza en la seguridad de los productos y sistemas de tecnologías de la información.

Un proceso de evaluación, ceñido a lo prescrito en ISO/IEC 15408 *Evaluation criteria for IT security*, persigue garantizar que las funciones de seguridad de tales productos y sistemas reúnen los requisitos declarados. Otra cuestión, que merece un tratamiento aparte, es que con una posterior certificación se garantizan los resultados de la evaluación y que ésta ha sido realizada de acuerdo con los procedimientos establecidos por un determinado Esquema.

Así, la evaluación facilita que el usuario pueda determinar si el producto satisface sus necesidades de seguridad, definidas habitualmente en función de los resultados del análisis de riesgos y de la expresión de una determinada orientación en materia de política de seguridad; a los desarrolladores les facilita la identificación de requisitos de seguridad, así como la evaluación de sus propios productos o sistemas; a los evaluadores les proporciona orientación a la hora de examinar el objeto evaluado frente a los requisitos que deben satisfacerse.

Destacan las siguientes normas:

- La norma ISO/IEC 15408 *Evaluation criteria for IT security*, consta de tres partes, y proporciona criterios para especificar medidas de seguridad y requisitos de seguridad de los productos y

sistemas de tecnologías de la información, facilitando una expresión precisa de los mismos, así como los criterios para evaluar su seguridad.

- La norma ISO/IEC 18045 *Methodology for IT security evaluation*, describe las acciones que debe llevar a cabo el evaluador y establece las pautas para realizar las evaluaciones correspondientes.
- La norma ISO/IEC TR 15446 *Guide for the production of Protection Profiles and Security Targets* proporciona orientación para la producción de perfiles de protección, que son conjuntos de requisitos de seguridad empaquetados e independientes de una implementación específica, orientados a satisfacer unas determinadas necesidades.

El SC27 viene desarrollando normalización en el campo de la evaluación de la seguridad de las tecnologías de la información, en estrecha colaboración con el proyecto de los Criterios Comunes de Evaluación de la Seguridad de las Tecnologías de la Información.

Sobre estos Criterios Comunes pivota el *Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información*. En este contexto, los certificados de la seguridad son expedidos por Organismos de Certificación reconocidos a productos o sistemas de TI, o a perfiles de protección, que hayan sido satisfactoriamente evaluados por Servicios de Evaluación, conforme a los Criterios Comunes (norma ISO/IEC 15408). El Arreglo especifica con detalle, entre otros aspectos, los requisitos que han de cumplir los Certificados de Criterios Comunes, los Organismos de Certificación y los Centros de Evaluación. España participó en la ratificación inicial del citado Arreglo el 23 de mayo de 2000 y desde el 17 de agosto de 2006 ha es participante acreditado para emitir certificados de seguridad de la tecnología de la información.

Puede consultarse más información sobre el Arreglo en: http://www.csae.map.es/csi/pg3433.htm

3.7 Catálogo de informes y normas ISO/IEC, así como proyectos de informes y normas

Los catálogos de informes y normas ISO/IEC, así como los proyectos de informes y normas pueden consultarse en: http://www.iso.org/iso/en/ISOOnline.frontpage

4. Organismos de normalización en la materia

4.1. ISO/IEC JTC 1/SC 27 – AEN/CTN 71/SC 27

El Subcomité ISO/IEC JTC 1/SC 27 Técnicas de Seguridad - Tecnología de la Información tiene por alcance y área de trabajo la normalización de métodos genéricos y técnicas para la seguridad de TI.

La actividad del SC27 se enmarca en la concepción de la Seguridad de la Tecnología de la Información como pieza fundamental para garantizar la confianza de individuos e instituciones en la sociedad de la información.

Los principios y técnicas comúnmente aceptadas de la Seguridad de Tecnología de la Información, sirven de cimiento y punto de referencia para la elaboración y el cumplimiento de las normativas. Dado el carácter de utilización extensiva e intensiva de los Sistemas de Información en la "aldea global", los principios y técnicas de la Seguridad, necesariamente deben gozar de un consenso lo más amplio posible, de ahí la importancia de que tengan una dimensión internacional, dotándoles así de una mayor eficacia.

La actividad del SC 27 incluye cuestiones tales como las siguientes:

- La identificación de requisitos genéricos (incluyendo requisitos metodológicos) de los servicios de seguridad para los sistemas de TI.

Relación con el Esquema Nacional de Seguridad:

Al menos para los sistemas que caigan en la categoría ALTA debería aplicarse un sistema de gestión de la seguridad de la información (SGSI) al objeto de poder satisfacer ciertos principios básicos [a) seguridad integral, b) gestión de riesgos, e) reevaluación periódica] y requisitos mínimos [Artículo 12. Organización e implantación del proceso de seguridad y Artículo 26. Mejora continua del proceso de seguridad]

El Esquema Nacional de Seguridad no exige específicamente que el SGSI sea un ISO/IEC 27001, si bien éste es aplicable. La certificación de conformidad con ISO/IEC 27001 NO es obligatoria en el Esquema.

3.4 Código de buenas prácticas para la gestión de la seguridad de la información

La norma UNE ISO/IEC 27002 aporta un conjunto de 133 controles y de recomendaciones, dirigido a los responsables de promover, implantar y mantener la seguridad, con vocación de ser útil en la mayor parte de las situaciones y organizaciones y de establecer una referencia común para el sector de la seguridad de los sistemas de información que favorezca el intercambio de productos, sistemas y servicios entre los proveedores, los clientes, los subcontratistas y otros actores.

Los **objetivos** principales de la norma ISO/IEC 27002 son los siguientes:

- **Identificar controles independientes de la tecnología** que sean de aplicación general para organizaciones pequeñas, medianas y grandes y aplicables a diferentes aplicaciones, sistemas y plataformas tecnológicas.
- **Facilitar la adopción de controles proporcionados al riesgo** en términos de políticas, prácticas, procedimientos, estructuras organizativas y funciones de software.
- **Atender la demanda relativa al desarrollo, implantación y medida de prácticas de seguridad efectivas**, que sirven tanto para la seguridad propia como para las relaciones con otras organizaciones, como referencia común para el desarrollo y la gestión de la seguridad y para la construcción de la confianza mutua en la seguridad de la información.
- **Proporcionar principios y recomendaciones de gestión en los que basar la política de seguridad** de la información en cualquier soporte, sin restringirse únicamente a los aspectos específicos de seguridad de tecnologías de la información y de las comunicaciones.

En cuanto a su aplicación práctica UNE ISO/IEC 27002, de forma general, concede gran énfasis a las siguientes cuestiones:

- La adopción de los controles proporcionados a los riegos detectados.
- La documentación de las políticas, los procedimientos y los controles.
- La identificación de las responsabilidades al nivel adecuado.
- La presencia de un control formalizado, en términos de formalización del control y de su periodicidad.
- La generación y conservación de evidencias.
- El tratamiento de los incidentes de seguridad.

En particular, ISO/IEC 27002 otorga al **análisis y gestión de riesgos** el papel clave para la identificación de los requisitos de seguridad, cuestión esencial, y para la **identificación y selección de los controles** y sobre su aplicación, en términos de su formalización y su periodicidad, **en el marco del principio de proporcionalidad**, que relaciona el valor de los activos y los riesgos a los que están expuestos, junto con el estado de la tecnología y los costes de la posible materialización de los riesgos,

así como de los controles que los contrarrestan; todo ello de acuerdo con la idea básica de que la seguridad es más barata si se incorpora, cuanto antes, en las fases de análisis y de diseño de los sistemas.

La norma ISO/IEC 27002 se estructura en introducción, objeto y campo de aplicación, términos y definiciones, estructura de la norma, valoración y tratamiento del riesgo, más once capítulos en los que se detallan los controles, lo cual lo convierte en un producto razonablemente compacto y manejable. Así mismo, como se ha expuesto más arriba, constituye una fuente de controles aplicables en un sistema de gestión de seguridad de la información.

La tabla que se incluye a continuación ofrece una visión panorámica de los contenidos de la norma ISO/IEC 27002.

Política de seguridad	Documento de política de seguridad. Revisión del documento de política de seguridad.
Organización de la seguridad	Infraestructura de organización de la seguridad. Seguridad en acceso de terceras partes.
Clasificación y control de activos	Responsabilidad de los activos. Clasificación de la información.
Seguridad ligada al personal	Antes del empleo. Durante el empleo. A la terminación del empleo o tras cambios en el mismo.
Seguridad física y del entorno	Áreas seguras. Equipamiento de seguridad.
Comunicaciones y gestión de explotación	Procedimientos operativos y responsabilidades. Gestión del servicio prestado por terceras partes. Planificación y aceptación de sistemas. Protección frente a software malicioso. Copias de seguridad. Gestión de seguridad de red. Manejo de soportes. Intercambio de información. Servicios de comercio electrónico. Registro de eventos.
Control de acceso al sistema	Requisitos de control de acceso. Gestión del acceso de usuarios. Responsabilidades del usuario. Control de acceso a servicios en red. Control de acceso al sistema operativo. Control de acceso a las aplicaciones. Informática móvil y teletrabajo.
Adquisición, desarrollo y mantenimiento de sistemas de información	Requisitos de seguridad de los sistemas de información. Procesamiento correcto de las aplicaciones. Uso de controles criptográfícos. Seguridad de los archivos del sistema. Seguridad en procesos de desarrollo y mantenimiento. Gestión de vulnerabilidades técnicas.
Gestión de incidentes de seguridad de la información.	Informe de incidentes y debilidades de seguridad de la información. Gestión de incidentes de seguridad de la información y mejoras.
Gestión de la continuidad	Aspectos de seguridad de la información en la gestión de la continuidad.
Conformidad	Conformidad con requisitos de carácter legal. Conformidad con políticas, normas y aspectos técnicos. Consideraciones de auditoría de sistemas de información.

La norma ISO/IEC 27002 apunta en su introducción algunos controles considerados esenciales, tales como los siguientes:

a) la protección de los datos de carácter personal y la intimidad de las personas

b) la salvaguarda de los registros de la Organización

c) la documentación de la política de seguridad de la información

d) la asignación de responsabilidades de seguridad de la información

e) la formación y capacitación para la seguridad de la información

f) el procesamiento correcto de las aplicaciones

g) la gestión de la vulnerabilidad

h) la gestión de la continuidad del negocio

i) la gestión de las incidencias de la seguridad de la información y sus mejoras

Relación con el Esquema Nacional de Seguridad:

La norma UNE ISO/IEC 27002 es un conjunto de controles de seguridad para sistemas de información genéricos orientados, inicialmente, al comercio electrónico.

Si bien numerosas medidas de seguridad del ENS coinciden con controles de UNE ISO/IEC 27002, el Esquema Nacional de Seguridad es más preciso y establece un sistema de protección proporcionado a los bienes protegidos lo que racionaliza la implantación de medidas de protección reduciendo la discrecionalidad. Mientras que la norma UNE ISO/IEC 27002 carece de este mecanismo de proporcionalidad, quedando, en su caso, a la mejor opinión del auditor que certifica la conformidad con la norma UNE ISO/IEC 27001.

Por otra parte, el Esquema Nacional de Seguridad contempla diversos aspectos de aplicación en el ámbito de la administración pública, por ejemplo, relativos a la firma electrónica, no recogidos en la norma UNE ISO/IEC 27002.

3.5 Técnicas y mecanismos

Destacan en este ámbito las técnicas y mecanismos criptográficos que tienen un protagonismo singular y creciente en la garantía de dimensiones de la seguridad tales como la confidencialidad, la integridad y la autenticación; forman parte de estructuras más complejas como servicios, aplicaciones e infraestructuras; y, de hecho, se han convertido en componentes clave sobre los que se sustentan piezas esenciales para los servicios de administración electrónica como puede ser la firma electrónica y el fechado electrónico.

En el campo de las técnicas y mecanismos criptográficos, las normas producidas por el SC27 ofrecen especificaciones relativas a cuestiones tales como las siguientes, sin ánimo de exhaustividad:

- Servicios de fechado electrónico (ISO/IEC 18014 *Time Stamping Services*). Se trata de una norma multiparte que, entre otras cuestiones, describe modelos, servicios y protocolos para el fechado electrónico.
- Algoritmos de cifrado simétricos, de bloque, de flujo y asimétricos (ISO/IEC 18033 *Encryption algorithms*).
- Funciones hash criptográficas (ISO/IEC 10118 *Hash functions*).
- Esquemas de firma digital que incorporan funcionalidades de autenticación e integridad (ISO/IEC 9796 *Digital signature schemes giving message recovery*).
- Autenticación de entidades (ISO/IEC 9798 *Entity authentication*); se trata de una norma multiparte que especifica diversos mecanismos de autenticación, utilizando, entre otras, técnicas de criptografía simétrica y asimétrica.
- Técnicas criptográficas basadas en curvas elípticas (ISO/IEC 15946 *Cryptographic techniques based on elliptic curves*); en particular, contienen especificaciones para sistemas de firma digital basados en curvas elípticas.
- Requisitos de módulos criptográficos.

- Gestión de claves (ISO/IEC 11770 *Key Management*). Trata de conceptos, modelos, servicios y mecanismos para la gestión de claves.
- Mecanismos de no repudio (ISO/IEC 13888 *Non repudiation*). Trata de modelos, mecanismos y de la utilización de técnicas de criptografía asimétrica para el no repudio.

3.6 La confianza en los productos y sistemas de tecnologías de la información

Los usuarios de productos y sistemas de tecnologías de la información necesitan confianza en que las soluciones que puedan desplegar satisfacen los objetivos de seguridad declarados por las mismas, en el sentido de que son capaces de hacer frente a las amenazas identificadas, de satisfacer las políticas de seguridad definidas en el marco de unos determinados supuestos o hipótesis de seguridad, así como de incorporar unos determinados requisitos funcionales y de aseguramiento que contribuyen a la satisfacción de los citados objetivos, como se resumen en la figura siguiente.

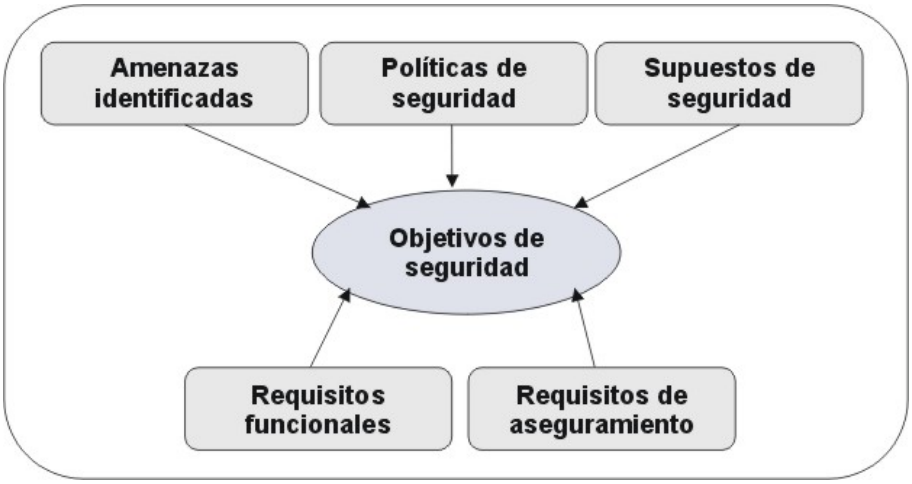

Figura 4: Relación de los objetivos de seguridad con amenazas, políticas, supuestos y requisitos funcionales y de aseguramiento

La utilización de productos y sistemas de tecnologías de la información cuya seguridad ha sido evaluada y, en su caso, certificada, es una de las salvaguardas principales para proteger la información y los sistemas que la manejan. Por *evaluación* se entiende el examen detallado a través del cual se confirma el nivel de seguridad demandado para un sistema de información o parte de él. La evaluación rigurosa e internacionalmente contrastada contribuye a dar confianza en la seguridad de los productos y sistemas de tecnologías de la información.

Un proceso de evaluación, ceñido a lo prescrito en ISO/IEC 15408 *Evaluation criteria for IT security*, persigue garantizar que las funciones de seguridad de tales productos y sistemas reúnen los requisitos declarados. Otra cuestión, que merece un tratamiento aparte, es que con una posterior certificación se garantizan los resultados de la evaluación y que ésta ha sido realizada de acuerdo con los procedimientos establecidos por un determinado Esquema.

Así, la evaluación facilita que el usuario pueda determinar si el producto satisface sus necesidades de seguridad, definidas habitualmente en función de los resultados del análisis de riesgos y de la expresión de una determinada orientación en materia de política de seguridad; a los desarrolladores les facilita la identificación de requisitos de seguridad, así como la evaluación de sus propios productos o sistemas; a los evaluadores les proporciona orientación a la hora de examinar el objeto evaluado frente a los requisitos que deben satisfacerse.

Destacan las siguientes normas:

- La norma ISO/IEC 15408 *Evaluation criteria for IT security*, consta de tres partes, y proporciona criterios para especificar medidas de seguridad y requisitos de seguridad de los productos y

sistemas de tecnologías de la información, facilitando una expresión precisa de los mismos, así como los criterios para evaluar su seguridad.

- La norma ISO/IEC 18045 *Methodology for IT security evaluation*, describe las acciones que debe llevar a cabo el evaluador y establece las pautas para realizar las evaluaciones correspondientes.
- La norma ISO/IEC TR 15446 *Guide for the production of Protection Profiles and Security Targets* proporciona orientación para la producción de perfiles de protección, que son conjuntos de requisitos de seguridad empaquetados e independientes de una implementación específica, orientados a satisfacer unas determinadas necesidades.

El SC27 viene desarrollando normalización en el campo de la evaluación de la seguridad de las tecnologías de la información, en estrecha colaboración con el proyecto de los Criterios Comunes de Evaluación de la Seguridad de las Tecnologías de la Información.

Sobre estos Criterios Comunes pivota el *Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información*. En este contexto, los certificados de la seguridad son expedidos por Organismos de Certificación reconocidos a productos o sistemas de TI, o a perfiles de protección, que hayan sido satisfactoriamente evaluados por Servicios de Evaluación, conforme a los Criterios Comunes (norma ISO/IEC 15408). El Arreglo especifica con detalle, entre otros aspectos, los requisitos que han de cumplir los Certificados de Criterios Comunes, los Organismos de Certificación y los Centros de Evaluación. España participó en la ratificación inicial del citado Arreglo el 23 de mayo de 2000 y desde el 17 de agosto de 2006 ha es participante acreditado para emitir certificados de seguridad de la tecnología de la información.

Puede consultarse más información sobre el Arreglo en: http://www.csae.map.es/csi/pg3433.htm

3.7 Catálogo de informes y normas ISO/IEC, así como proyectos de informes y normas

Los catálogos de informes y normas ISO/IEC, así como los proyectos de informes y normas pueden consultarse en: http://www.iso.org/iso/en/ISOOnline.frontpage

4. Organismos de normalización en la materia

4.1. ISO/IEC JTC 1/SC 27 – AEN/CTN 71/SC 27

El Subcomité ISO/IEC JTC 1/SC 27 Técnicas de Seguridad - Tecnología de la Información tiene por alcance y área de trabajo la normalización de métodos genéricos y técnicas para la seguridad de TI.

La actividad del SC27 se enmarca en la concepción de la Seguridad de la Tecnología de la Información como pieza fundamental para garantizar la confianza de individuos e instituciones en la sociedad de la información.

Los principios y técnicas comúnmente aceptadas de la Seguridad de Tecnología de la Información, sirven de cimiento y punto de referencia para la elaboración y el cumplimiento de las normativas. Dado el carácter de utilización extensiva e intensiva de los Sistemas de Información en la "aldea global", los principios y técnicas de la Seguridad, necesariamente deben gozar de un consenso lo más amplio posible, de ahí la importancia de que tengan una dimensión internacional, dotándoles así de una mayor eficacia.

La actividad del SC 27 incluye cuestiones tales como las siguientes:

- La identificación de requisitos genéricos (incluyendo requisitos metodológicos) de los servicios de seguridad para los sistemas de TI.

- El desarrollo de técnicas y mecanismos de seguridad (incluyendo los procedimientos de registro y las relaciones de los componentes de seguridad).
- El desarrollo de guías de seguridad (ejemplos, documentos interpretativos, análisis de riesgos).
- El desarrollo del soporte a la gestión, documentación y normas (ejemplo, terminología y criterios de evaluación).
- La normalización de algoritmos criptográficos para los servicios de integridad, autenticación y no repudio. Adicionalmente, incluye la normalización de algoritmos criptográficos de los servicios de confidencialidad para ser utilizados conforme a las políticas internacionalmente aceptadas.

Queda excluida de su actividad la inclusión de mecanismos en las aplicaciones, es decir, la normalización de cómo insertar los mecanismos de seguridad en las diversas aplicaciones (este aspecto queda a discreción de los desarrolladores).

El crecimiento continuo de los proyectos de informes y normas, acorde con el protagonismo creciente de la seguridad de la información y de las tecnologías asociadas, da lugar a que puedan identificarse áreas de actuación en la normalización de extensión suficiente como para que quepa plantearse la reorganización de la estructura preexistente de grupos de trabajo a fin de poder prestarles la cobertura y la atención proporcionada y adecuada a su relevancia. Fruto de esta reflexión el ISO/IEC JTC1 SC27 se reconfiguró en 2006 en torno a cinco grupos de trabajo, tras la creación y entrada en vigor de los grupos GT4 Servicios y controles de seguridad y GT5 Gestión de identidad y privacidad, con la consiguiente redistribución de la carga de trabajo que ha afectado especialmente al GT1 Requisitos, servicios de seguridad y guías.

El **SC27 se estructura en los siguientes cinco grupos de trabajo (GT)** que se citan a continuación con sus términos genéricos de referencia:

GT1: requisitos, servicios de seguridad y guías.

- Identificar los requisitos de los componentes de aplicaciones y sistemas
- Desarrollar normas para los servicios de seguridad (ejemplo, autenticación, control de acceso, integridad, confidencialidad, gestión y auditoría) utilizando técnicas y mecanismos desarrollados por el GT2.
- Desarrollar soporte interpretativo de documentos (ejemplo, guías de seguridad, glosarios, análisis de riesgos).
- Desarrollar normas para los sistemas de gestión de seguridad de la información.

GT2: mecanismos y técnicas de seguridad.

- Mecanismos relacionados con la autenticación, control de acceso, confidencialidad, no repudio, gestión de claves e integridad de datos.
- Técnicas criptográficas o no criptográficas.

GT3: criterios de evaluación de la seguridad.

- Normas para evaluar y certificar la seguridad de los sistemas, componentes y productos de TI. Esto incluye la consideración de redes de ordenadores, sistemas distribuidos, servicios de aplicación asociados, etc.
- Pueden distinguirse tres aspectos: criterios de evaluación, metodología para la aplicación de los criterios, procedimiento administrativo para la evaluación, certificación y esquemas de acreditación.

GT4: servicios y controles de seguridad.

- Desarrollar normas y recomendaciones para servicios y aplicaciones sobre los que se implantan controles y se logran los objetivos definidos por las especificaciones del sistema de gestión de seguridad de la información.

- El desarrollo de técnicas y mecanismos de seguridad (incluyendo los procedimientos de registro y las relaciones de los componentes de seguridad).
- El desarrollo de guías de seguridad (ejemplos, documentos interpretativos, análisis de riesgos).
- El desarrollo del soporte a la gestión, documentación y normas (ejemplo, terminología y criterios de evaluación).
- La normalización de algoritmos criptográficos para los servicios de integridad, autenticación y no repudio. Adicionalmente, incluye la normalización de algoritmos criptográficos de los servicios de confidencialidad para ser utilizados conforme a las políticas internacionalmente aceptadas.

Queda excluida de su actividad la inclusión de mecanismos en las aplicaciones, es decir, la normalización de cómo insertar los mecanismos de seguridad en las diversas aplicaciones (este aspecto queda a discreción de los desarrolladores).

El crecimiento continuo de los proyectos de informes y normas, acorde con el protagonismo creciente de la seguridad de la información y de las tecnologías asociadas, da lugar a que puedan identificarse áreas de actuación en la normalización de extensión suficiente como para que quepa plantearse la reorganización de la estructura preexistente de grupos de trabajo a fin de poder prestarles la cobertura y la atención proporcionada y adecuada a su relevancia. Fruto de esta reflexión el ISO/IEC JTC1 SC27 se reconfiguró en 2006 en torno a cinco grupos de trabajo, tras la creación y entrada en vigor de los grupos GT4 Servicios y controles de seguridad y GT5 Gestión de identidad y privacidad, con la consiguiente redistribución de la carga de trabajo que ha afectado especialmente al GT1 Requisitos, servicios de seguridad y guías.

El **SC27 se estructura en los siguientes cinco grupos de trabajo (GT)** que se citan a continuación con sus términos genéricos de referencia:

GT1: requisitos, servicios de seguridad y guías.

- Identificar los requisitos de los componentes de aplicaciones y sistemas
- Desarrollar normas para los servicios de seguridad (ejemplo, autenticación, control de acceso, integridad, confidencialidad, gestión y auditoría) utilizando técnicas y mecanismos desarrollados por el GT2.
- Desarrollar soporte interpretativo de documentos (ejemplo, guías de seguridad, glosarios, análisis de riesgos).
- Desarrollar normas para los sistemas de gestión de seguridad de la información.

GT2: mecanismos y técnicas de seguridad.

- Mecanismos relacionados con la autenticación, control de acceso, confidencialidad, no repudio, gestión de claves e integridad de datos.
- Técnicas criptográficas o no criptográficas.

GT3: criterios de evaluación de la seguridad.

- Normas para evaluar y certificar la seguridad de los sistemas, componentes y productos de TI. Esto incluye la consideración de redes de ordenadores, sistemas distribuidos, servicios de aplicación asociados, etc.
- Pueden distinguirse tres aspectos: criterios de evaluación, metodología para la aplicación de los criterios, procedimiento administrativo para la evaluación, certificación y esquemas de acreditación.

GT4: servicios y controles de seguridad.

- Desarrollar normas y recomendaciones para servicios y aplicaciones sobre los que se implantan controles y se logran los objetivos definidos por las especificaciones del sistema de gestión de seguridad de la información.

- Identificar los requisitos para la elaboración de normas sobre continuidad de negocio, cyber-seguridad y subcontratación.

GT5 gestión de identidad y privacidad.

- Desarrollar normas sobre gestión de la identidad de las personas, protección de datos personales y técnicas biométricas aplicadas a este ámbito.
- Identificar requisitos para el desarrollo de normas en materia de control de acceso.

Dentro de la concepción general de SC 27 expuesta anteriormente, el subcomité espejo español AEN/CTN 71/SC 27 actúa de acuerdo con objetivos tales como los siguientes:

- Apoyar la integración de los sectores público y privado de nuestro país en los procesos de normalización nacional e internacional en el campo de la seguridad de las tecnologías de la información.
- Apoyar el desarrollo de las normas de seguridad de las tecnologías de la información en los ámbitos nacional e internacional.
- Canalizar la normalización nacional e internacional en el campo de la seguridad de las tecnologías de la información hacia las políticas y directrices de tecnologías de la información de los sectores público y privado de nuestro país.
- Apoyar la difusión y uso de las normas de seguridad de las tecnologías de la información.

El Ministerio de la Presidencia participa mediante sus funcionarios como expertos, a través de la vocalía, en el subcomité espejo de ISO/IEC JTC 1/SC 27, que es en el ámbito español el subcomité AEN/CTN 71/SC 27 *"Técnicas de Seguridad - Tecnología de la Información*", encuadrado en la estructura del comité nacional AEN/CTN 71 "*Tecnología de la Información*", y en particular en el GT1: *Requisitos, servicios de seguridad y guías*, según las líneas expuestas más arriba.

4.2. CEN/ISSS

Las normas elaboradas por el Comité Europeo de Normalización cuentan con varias peculiaridades. La Directiva 98/34, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, otorga a la Comisión Europea el derecho a solicitar la elaboración de aquellas normas que puedan ser necesarias para la ejecución operativa de las Directivas comunitarias. Además, adquieren el carácter de norma armonizada cuando aportan una solución conforme con las disposiciones legales comunitarias y, en consecuencia, los Estados miembros están obligados a aceptar el cumplimiento de la norma. Dichas normas europeas armonizadas se notifican para una determinada Directiva en el Diario Oficial de la Unión Europea y, desde ese momento, la norma adquiere la capacidad de conferir presunción de conformidad a aquellos productos que la cumplen.

4.3. ISO/TMB Gestión de riesgos - AEN GET 13

ISO/TMB emprendió la elaboración de una norma de gestión de riesgos, de acuerdo con las siguientes orientaciones:

- Desarrollar un documento directriz de alto nivel que sirva de paraguas a las normas existentes en el campo de la gestión del riesgo.
- Ser coherente con los documentos existentes en la materia.
- No desarrollar una norma de sistema de gestión.
- Tener un lenguaje fácilmente comprensible que fomente su uso por los responsables organizativos.

- No desarrollar un documento que se vaya a utilizar para la certificación o para efectos contractuales.

Como resultado del trabajo realizado se han obtenido los siguientes resultados:

- ISO 31000 Risk management – Principles and guidelines
- ISO 73 Risk management - Vocabulary.
- ISO 31010 Risk management – Risk assessment techniques

En cuanto a España, en el BOE nº 298 de 14 de diciembre de 2005 se publicó la Resolución de 8 de noviembre de 2005, de la Dirección General de Desarrollo Industrial, por la que se autoriza a la Asociación Española de Normalización y Certificación (AENOR), para asumir funciones de normalización en el ámbito de la gestión de riesgos.

El GET 13 Gestión de riesgos se constituyó en la reunión celebrada el día 8 de febrero de 2006 (1/2006) como grupo espejo del correspondiente de ISO/TMB, con miembros procedentes de muy diversos sectores de actividad, tales como construcción, energía, transporte, salud, alimentación, riesgos laborales, tecnología, medio ambiente, prevención de accidentes, industria aeroespacial, líneas aéreas, tecnología de la información, de la Universidad, la Administración Pública y el Sector Privado.

La finalidad del GET 13 ha sido seguir el desarrollo de la normas citadas más arriba y de realizar la traducciones correspondientes.