XXX aniversario
novática
UPGRADE Revista de la Asociación de Técnicos de Informática

Nº 176, julio-agosto 2005, año XXXI

sumario

Monografía del próximo número: "*Computación ubicua*"

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática). ***Novática*** edita también **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (**UP**GRADE ***E**uropean **NET**work*)

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2** y **ASTIC.**

Consejo Editorial
Antoni Carbonell Nogueras, Juan ManuelCueva Lovelle, Juan Antonio Esteban Iriarte,Francisco López Crespo, Celestino Martín Alonso, Josep Molas i Bertrán, Olga Pallás Codina, Fernando Piera Gómez (Presidente del Consejo), Ramón Puigjaner Trepat, Miquel Sàrries Griñó, Asunción Yturbe Herranz

Coordinación Editorial
Rafael Fernández Calvo <rfcalvo@ati.es>

Composición y autoedición
Jorge Llácer Gil de Ramales
Traducciones
Grupo de Lengua e Informática de ATI <http://www.ati.es/gt/lengua-informatica/>
Administración
Tomás Brunete, María José Fernández, Enric Camarero, Felicidad López

Secciones Técnicas: Coordinadores

Administración Pública electrónica
Gumersindo García Arribas, Francisco López Crespo (MAP)
<gumersindo.garcia@map.es>, <fllc@ati.es>
Arquitecturas
Enrique F. Torres Moreno (Universidad de Zaragoza) <enrique.torres@unizar.es>
Jordi Tubella Morgadas (DAC-UPC) <jordi@ac.upc.es>
Auditoría SITIC
Marina Touriño Troitiño, Manuel Palao García-Suelto (ASIA)
<marinatourino@marinatourino.com>, <manuel@palao.com>
Bases de datos
Coral Calero Muñoz, Mario G. Piattini Velthuis
(Escuela Superior de Informática, UCLM)
<Coral.Calero@uclm.es>, <mpiattin@inf-cr.uclm.es>
Derecho y Tecnología
Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV)<ihernando@legaltek.net>
Elena Davara Fernández de Marcos (Davara & Davara) <edavara@davara.com>
Enseñanza Universitaria de la Informática
Joaquín Ezpeleta Mateo (CPS-UZAR) <ezpeleta@posta.unizar.es>
Cristòfol Pareja Flores (DSIP-UCM) <cpareja@sip.ucm.es>
Gestión del Conocimiento
Joan Baiget Solé (Cap Gemini Ernst & Young) <joan.baiget@ati.es>
Informática y Filosofía
Josep Corco Juvinyà (UIC) <jcorco@unica.edu>
Esperanza Marcos Martínez (ESCET-URJC) <cuca@escet.urjc.es>
Informática Gráfica
Miguel Chover Sellés (Universitat Jaume I de Castellón) <chover@lsi.uji.es>
Roberto Vivó Hernando (Eurographics, sección española) <rvivo@dsic.upv.es>
Ingeniería del Software
Javier Dolado Cosín (DLSI-UPV) <dolado@si.ehu.es>
Luis Fernández Sanz (PRIS-EI-UEM) <lufern@dpris.esi.uem.es>
Inteligencia Artificial
Federico Barber Sánchis, Vicente Botti Navarro (DSIC-UPV)
<{vbotti, fbarber}@dsic.upv.es>
Interacción Persona-Computador
Julio Abascal González (FI-UPV) <julio@si.ehu.es>
Jesús Lores Vidal (Univ. de Lleida) <jesus@eup.udl.es>
Internet
Alonso Álvarez García (TID) <alonso@ati.es>
Llorenç Pagés Casas (Indra) <pages@ati.es>
Lengua e Informática
M. del Carmen Ugarte García (IBM) <cugarte@ati.es>
Lenguajes Informáticos
Andrés Marín López (Univ. Carlos III) <amarin@it.uc3m.es>
J. Ángel Velázquez Iturbide (ESCET-URJC) <a.velazquez@escet.urjc.es>
Libertades e Informática
Alfonso Escolano (FIR-Univ. de La Laguna) <aescolan@ull.es>
Lingüística computacional
Xavier Gómez Guinovart (Univ. de Vigo) <xgg@uvigo.es>
Manuel Palomar (Univ. de Alicante) <mpalomar@dlsi.ua.es>
Mundo estudiantil
Adolfo Vázquez Rodríguez (Rama de Estudiantes del IEEE-UCM)
<a.vazquez@ieee.org>
Profesión Informática
Rafael Fernández Calvo (ATI) <rfcalvo@ati.es>
Miquel Sàrries Griñó (Ayto. de Barcelona) <msarries@ati.es>
Redes y servicios telemáticos
Luis Guijarro Coloma (DCOM-UPV) <lguijar@dcom.upv.es>
Josep Solé Pareta (DAC-UPC) <pareta@ac.upc.es>
Seguridad
Javier Areitio Bertolín (Univ. de Deusto) <jareitio@eside.deusto.es>
Javier López Muñoz (ETSI Informática-UMA) <jlm@lcc.uma.es>
Sistemas de Tiempo Real
Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM)
<{aalonso,jpuente}@dit.upm.es>
Software Libre
Jesús M. González Barahona, Pedro de las Heras Quirós
(GSYC-URJC) <{jgb,pheras}@gsyc.escet.urjc.es>
Tecnología de Objetos
Jesus García Molina (DIS-UM) <jmolina@correo.um.es>
Gustavo Rossi (LIFIA-UNLP, Argentina) <gustavo@sol.info.unlp.edu.ar>
Tecnologías para la Educación
Juan Manuel Dodero Beardo (UC3M) <dodero@inf.uc3m.es>
Tecnologías y Empresa
Pablo Hernández Medrano (Bluemat) <pablohm@bluemat.biz>
TIC para la Sanidad
Valentín Masero Vargas (DI-UNEX) <vmasero@unex.es>
TIC y Turismo
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga)
<{aguayo, guevara}@lcc.uma.es>

Las opiniones expresadas por los autores son responsabilidad exclusiva de losmismos. ***Novática*** permite la reproducción de todos los artículos, a menos que lo impida la modalidad de © o *copyright* elegida por el autor, debiéndose en todo caso citar su procedencia y enviar a ***Novática*** un ejemplar de la publicación.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Ciudad de Granada 131, 08018 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Asturias-Cantabria <gp-astucant@ati.es>
Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
Suscripción y Ventas
<http://www.ati.es/novatica/interes.html>, o en ATI Cataluña o ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica.publicidad@ati.es>
Imprenta
Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix / © ATI 2005
Diseño: Fernando Agresta / © ATI 2005

¿Dónde nacen las normas voluntarias y las recomendaciones relativas a la seguridad de la información?

Paloma García López
AENOR (Asociación Española de Normalización y Certificación)

<pgarcial@aenor.es>

Resumen: *las normas se elaboran en el seno de los comités técnicos de normalización que forman parte de la estructura de los organismos de normalización. Dichos comités están formados por una composición equilibrada de todas las partes interesadas en el campo de aplicación que corresponda al comité. En el ámbito de la seguridad de la información, a nivel internacional el principal comité responsable es el JTC1/SC27 "Técnicas de Seguridad"; su homólogo a nivel español es el CTN71/SC27, que lleva el mismo nombre. En el plano concreto de las normas relativas a la seguridad de la información, se ha apostado por la tendencia, apoyada e impulsada por el comité internacional, de abordar este tema desde el punto de vista de la gestión de la seguridad. En este sentido, se ha puesto en marcha el denominado Modelo de Gestión 27000, Modelo de Gestion de la Seguridad de la Información, del que daremos información ampliada en este artículo.*

Palabras clave: *CEN/ISSS, comité, consenso, CTN71/SC27, JTC1/SC27, modelo de gestión, normas voluntarias, organismo de normalización, seguridad de la información, SGSI, Sistema de Gestión de la Seguridad de la Información.*

Autora

Paloma García López es Ingeniero Industrial por la Universidad Politécnica de Madrid. Desde 1999 desarrolla su actividad laboral en AENOR (Asociación Española de Normalización y Certificación), siendo actualmente Jefe del Servicio de Telecomunicaciones y Tecnologías de la Información en la División de Normalización; coordina la actividad nacional de normalización de los productos y servicios de este sector y participando activamente en las iniciativas europeas e internacionales del sector. Actualmente es la responsable del comité nacional AEN/CTN71, Tecnologías de la Información, y del SC27, Técnicas de seguridad, que forma parte de la estructura del primero.

1. Introducción

Aunque pueda estar en la mente de muchas personas el que los documentos conocidos como normas internacionales han sido 'hallados' por casualidad y firmados por un autor anónimo que nunca se llegará a identificar, esto no tiene nada que ver con la realidad de cómo se elaboran, en la actualidad, las normas en los organismos de normalización oficialmente reconocidos, ya sean éstos de carácter nacional, europeo o internacional.

Concretamente en lo referente al marco internacional que se ocupa de los aspectos relacionados con las Tecnologías de la Información, en adelante TI, existe un comité conjunto constituido entre los dos organismos internacionales de normalización, **ISO** (Organización Internacional de Normalización) e **IEC** (Comisión Electrotécnica Internacional, que se centra en los aspectos eléctricos de cada campo). Este comité conjunto Nº1 es el denominado **JTC1** (*Joint Technical Committee 1*), en este órgano participan 68 países, entre ellos España, a través de **AENOR** (Asociación Española de Normalización y Certificación) que asumió su responsabilidad internacional en ISO en 1987 y en IEC en 1995, representando los intereses españoles en el campo de la normalización internacional ante dichas organizaciones.

Dentro de ISO, existe también el Comité ISO/TC 68 "Servicios financieros" que en la actualidad cuenta con un alto potencial de desarrollo en lo que a normas internacionales en el campo de la seguridad se refiere, en particular las relacionadas las con tecnologías de protección de datos, seguridad de los sistemas de transferencia, soluciones de autenticación para el consumidor, etc. El subcomité (SC) responsable del ámbito de la seguridad dentro de la estructura del TC68 es el SC 2 "Gestión de la seguridad y operaciones generales en banca" de cuya estructura y proyectos en marcha hablaremos más adelante.

Aunque queda fuera del alcance de este artículo, es importante mencionar otro ámbito de normalización donde puntualmente se elaboran documentos normativos relativos a TI, que se denominan Recomendaciones, es la Unión Internacional de Telecomunicaciones, **UIT**, organismo responsable de la normalización internacional en materia de telecomunicaciones y que participa en muchos de los proyectos del JTC1.

En el ámbito del Comité ISO/IEC/JTC 1 se considera la especificación, diseño y desarrollo de sistemas y herramientas que tratan la información en sus distintos aspectos: captura, representación, proceso, seguridad, transmisión, intercambio, presentación, direccionamiento, organización, almacenamiento y recuperación.

Este órgano de trabajo está estructurado en una serie de subcomités dedicado cada uno de ellos a un aspecto específico de las TI; en concreto el que ocupa el número 27 es el responsable de todos los aspectos de seguridad, denominándose **JTC1/SC27** "Técnicas de Seguridad". En la actualidad cuenta con más de 40 países miembros, entre ellos, cómo no podía esperarse otra cosa, España. La relación entre los organismos antes citados se muestra en la **figura 1**.

En el JTC1 existe también un órgano denominado I*nformation Technology Task Force* (ITTF) responsable de la planificación cotidiana y coordinación del trabajo técnico del mismo, y de la aplicación de los Estatutos y los Procedimientos de ISO e IEC

2. ISO/IEC/JTC1/SC 27 "Técnicas de Seguridad", cuna de las normas internacionales de seguridad de TI

El anteriormente presentado SC27 es un subcomité englobado en la estructura del JTC1, en el que **expertos de los países miembros** del mismo trabajan conjuntamente para llegar a un contenido consen-suado en el aspecto de que se trate. Normalmente el trabajo se desarrolla en grupos de trabajo formados por expertos en el asunto objeto de la futura norma internacional. De esta manera, y siempre asumiendo la voluntariedad en que nacen las normas, partiendo de una propuesta de trabajo inicial se desarrolla un texto que va superando una serie de fases formales de aprobación, básicamente una fase de encuesta pública seguida, al menos, de una fase de voto formal al texto presentado. Finalmente el contenido es aprobado formalmente por los organismos de normalización miembros del JTC1 cómo órgano superior (en el caso español los servicios técnicos de AENOR), finalizando el proceso con la publicación por ISO e IEC de una norma internacional que es fruto del consenso mundial y está dotada de la transparencia en el proceso que garantizan las etapas que ha ido superando.

El **alcance** de este subcomité incluye:

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

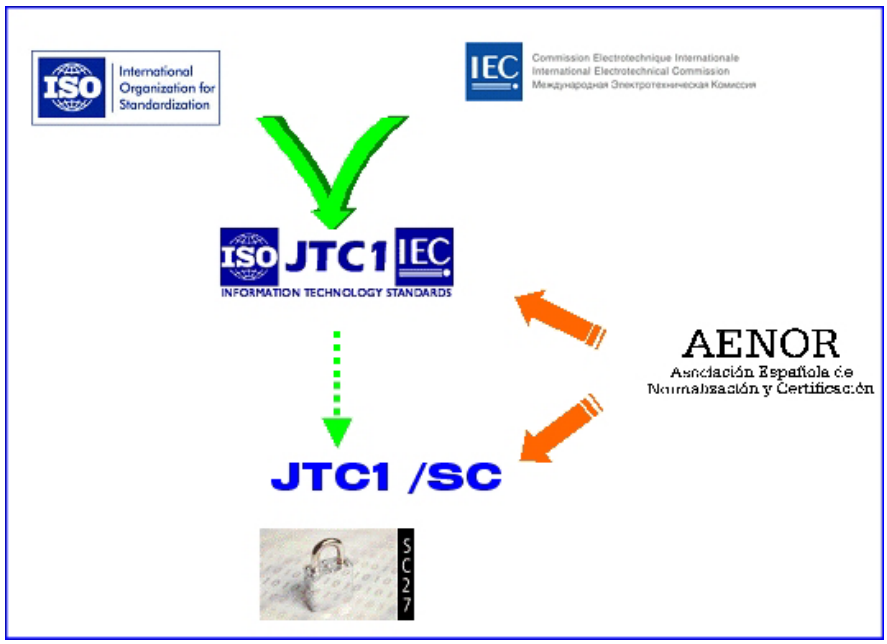

Figura 1. Organismos involucrados en la normalización de los aspectos relacionados con las Tecnologías de la Información.

- El desarrollo de técnicas y mecanismos de seguridad (incluyendo los procedimientos de registro y las relaciones de componentes de seguridad).
- El desarrollo de documentación de apoyo y normas (por ejemplo, terminología y criterio de evaluación de seguridad).

Y excluye la inclusión de mecanismos en las aplicaciones.

2.1. Estructura del SC 27

El Subcomité ISO/IEC JTC 1/SC se estructura en 3 grupos de trabajo (WG, *Working Groups*), que se muestran en la **figura 2**. En la **tabla 1** se muestra con un mayor grado de detalle el campo de actividad de cada uno de los grupos de trabajo. Es importante destacar, en lo relativo a las normas producidas en el seno del JTC1/SC27, la puesta en marcha del denominado Modelo de Gestión 27000, el Modelo de Gestion de la Seguridad de la Información, que es un nuevo modelo de gestión, los Sistemas de Gestión de de la Seguridad de la Información (SGSI), siglas españolas que se corresponden con sus homólogas inglesas ISMS (*Information Security Management Systems*).

La apuesta de abordar las seguridad de la información en las organizaciones desde el punto de vista de la gestión de la seguridad comenzó hace ya tiempo a nivel internacional en el Comité Técnico Conjunto ISO/IEC/JTC1, cuando en el año 2000 se publicó la Norma ISO/IEC 17799:2000 "Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información".

Hace pocos meses que finalizó la revisión formal de esta norma en el SC27/WG1, que se inició en el año 2003, acogiéndose al procedimiento de revisión temprana, dado que las normas internacionales pueden tener un periodo de vigencia de hasta cinco años antes de su revisión. Esta norma formará parte próximamente del catálogo de ISO e IEC y paralelamente comenzará su adopción como norma UNE-ISO/IEC 17799, como ya se hizo con la anterior edición, para incluirla en el catálogo de AENOR a lo largo de este año.

El optar por la revisión temprana del texto se corresponde con la situación de creciente demanda detectada en el sentido de disponer de un conjunto de normas internacionales que haga posible contar con un modelo de gestión de la seguridad de la información que alcance la penetración en las organizaciones y en la sociedad de que gozan en la actualidad los modelos de gestión de la calidad y gestión medioambiental internacional-mente aceptados. Se trata además un sistema de gestión totalmente integrable con estos dos sistemas y que supone un paso más en la gestión global de las organizaciones, pues proporciona directrices claras sobre cómo gestionar la seguridad de los sistemas de información, partiendo del supuesto de que la información de que disponen las entidades es un activo clave en su negocio.

Junto con la publicación en breve de dicha norma internacional, en su nueva versión revisada, se ha puesto en marcha en el SC27/WG1 la elaboración de un conjunto de normas y un proyecto de renumeración de todo este conjunto para convertirlo en un modelo coherente, anunciado como **Modelo de Gestión Serie 27000**. A tal fin se ha reservado el rango de numeración 27000 a 27010 para las normas sobre Gestión de la Seguridad de la Información.

En la **tabla 2** se muestra un cuadro con los proyectos actualmente en desarrollo de dicho modelo, con su numeración prevista y con la duración del periodo de permanencia

WG 1	• **Identificación de los requisitos de los componentes de aplicaciones y sistemas.** • **Elaboración de normas para los servicios de seguridad (ejemplo, autenticación, control de acceso, integridad, confidencialidad, gestión y auditoria) utilizando técnicas y mecanismos desarrollados por el WG2.** • **Desarrollo de un soporte interpretativo de documentos (ejemplo, guías de seguridad, glosarios, documentos sobre análisis de riesgos).**
WG 2	• **Mecanismos relacionados con la autenticación, control de acceso, confidencialidad, no repudio, gestión de claves e integridad de datos.** • **Técnicas criptográficas o no criptográficas.**
WG 3	• **Elaboración de 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.** • **Se distinguen tres aspectos básicos:** • **criterios de evaluación** • **metodología para la aplicación de los criterios** • **procedimiento administrativo para la evaluación, certificación y esquemas de acreditación.**

Tabla 1. Ámbitos de actividad de los Grupos de Trabajo del Subcomité ISO/IEC JTC 1/SC.

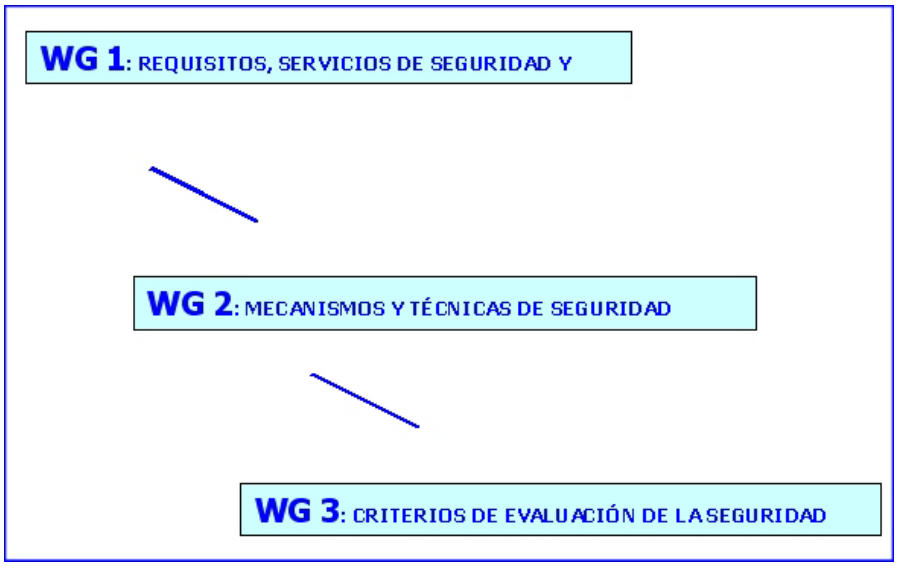

Figura 2. Grupos de Trabajo del Subcomité ISO/IEC JTC 1/SC.

3. ISO/TC 68 "Banca y Servicios Financieros Relacionados con las Operaciones Bancarias"

Como ya se adelantó al comienzo de este artículo, este comité internacional, creado en 1948 y que cuenta en la actualidad con 59 países miembros y 15 representaciones del sector bancario y finnaciero (VISA, MASTERCARD, ECMA, SWIT, BIS/BRI...), tiene dentro de su campo de actividad un importante capítulo dedicado a la seguridad, con un futura carga de trabajo en el plano de la seguridad de las tecnologías de la información, derivada del desarrollo y crecimiento de las comunicaciones electrónicas. La estructura del TC 68 se muestra en la **figura 3**.

El SC2 es el más directamente encargado de la normalización de los aspectos de gestión de la seguridad dentro del campo de aplicación del TC68 y está compuesto por 9 gru-

de la antigua numeración, cuando se trate de normas anteriormente publicadas, para lo que se ha acordado una transición que en todos los casos finaliza en abril del 2007.

Las referencias que figuran en la **tabla 2** con las siglas NP (*New Proposal*), WD (*Working Draft*), FCD (*Final Committee Draft*), FDIS (*Final Draft International Standard*), se corresponden con distintos estados de desarrollo del proyecto de norma antes de su publicación definitiva como norma internacional. Los proyectos de norma internacional en fase NP, WD o FCD son fases tempranas de elaboración en las que el texto no ha pasado la fase de aprobación del órgano técnico correspondiente (grupo de trabajo en primer nivel y subcomité en siguiente nivel), por lo que su contenido puede varias sustancialmente hasta final del proceso.

La fases DIS (*Draft International Standard*) y FDIS corresponden a etapas de encuesta y voto por los organismos nacionales de normalización miembros del Comité de ISO/IEC responsable de la norma.

Como ejemplo del activo seguimiento que a nivel nacional se está haciendo de todo este trabajo internacional es importante destacar que la futura Norma Internacional **ISO/IEC 27004** sobre métricas y mediciones para la gestión de los sistemas de seguridad de la información fue una propuesta española respaldada por un documento elaborado en un grupo de trabajo del órgano nacional espejo del JTC1/SC27, el CTN71/SC27 "Técnicas de Seguridad", que forma parte de la estructura de comités de normalización de AENOR. Para el desarrollo de esta norma, AENOR presentó la candidatura de un miembro del subcomité nacional para ser editor del proyecto, candidatura que fue aprobada conjuntamente con la candidatura de editor presentada por Estados Unidos.

Históricamente	Octubre 2004	Abril 2005	Abril 2007
-	Referencia reservada para futura norma		**ISO/IEC 27000**
-	ISO/IEC FCD 24743 Information Security Management Systems (ISMS) requirements	ISO/IEC FDIS 27001 Information Security Management Systems (ISMS) requirements	**ISO/IEC 27001**
ISO/IEC 17799: 2000	ISO/IEC 17799: 2000 (en revisión)	ISO/IEC 17799: 2005	**ISO/IEC 27002**
-	Referencia reservada para futura norma		**ISO/IEC 27003**
-	ISO/IEC 1º WD 24742 Information technology. Security	ISO/IEC WD 27004	**ISO/IEC 27004**

Tabla 2. Proyectos actualmente en desarrollo del Modelo de Gestión Serie 27000.

Figura 3. Órganos técnicos del TC 68.

pos de trabajo (WG), de los que el WG9 es responsabilidad compartida con el SC6, dada la también alta implicación de este subcomité en los aspectos de seguridad. En la **figura 4** se muestran dichos grupos de trabajo.

4. Panorama nacional: AEN/CTN 71/SC27 "Técnicas de Seguridad de TI"

Como miembro español en los organismos internacionales de normalización, AENOR es responsable de coordinar la participación de expertos españoles en estos grupos de trabajo; para ello tiene constituida toda un estructura de más de 170 comités nacionales de normalización, en su mayoría espejo de los órganos internacionales.

En el ámbito que nos ocupa, el comité que cuenta en su campo de actividad con todos los aspectos relativos a las Tecnologías de la Información es el comité nacional AEN/CTN 71, estructurado de igual manera que su homólogo en ISO/IEC en subcomités y con idéntica numeración. El SC27 es el específicamente dedicado a la seguridad de las TI, que cuenta con los tres grupos de trabajo espejo de los internacionales además de un grupo horizontal a los anteriores enfocado a las métricas de seguridad, línea de actividad que a propuesta española ha comenzado a desarrollarse en el JTC17/SC27 desde su última reunión plenaria el pasado mes de abril. Las correspondencias entre ISO y AENOR en dichos ámbitos se muestran en la **figura 4**.

Desde el subcomité nacional, en el que participan más de 40 entidades, se hace un seguimiento muy activo de toda la documentación recibida desde el organismo internacional, para emitir el voto español cuando así se requiere. Aunque la mayoría de las comunicaciones para la elaboración del trabajo técnico se realizan por vía electrónica, se mantiene un calendario de reuniones del JTC 1 /SC 27 a las que asisten varios vocales del subcomité, tanto a las reuniones de los grupos de trabajo como a las reuniones plenarias del JTC1/SC27 que se celebran normalmente con una periodicidad anual y cada año en un continente.

Las reuniones de los grupos de trabajo (WG) vienen teniendo lugar en abril y octubre de cada año, y en ellas se toman las decisiones de carácter técnico. En la semana siguiente a la reunión de octubre tiene lugar la reunión penaria donde se toman decisiones de gestión y de carácter más horizontal: asignación de responsabilidades, coordinación y consolidadción de calendarios de reuniones, revisión de planes de trabajo, identificación de áreas donde puede requerirse normalización, petición de contribuciones técnicas a los organismos nacionales, aprobación de subdivisiones o cambio de fase de los proyectos — por ejemplo, su publicación como norma internacional (IS) —, nombramiento de editores de proyecto, etc...

Para la representación de la postura nacional, los miembros asistentes a las reuniones internacionales conforman la delegación española y son acreditados por AENOR como expertos nacionales para asistir a dichas reuniones.

En estos momentos se cuenta además con varios miembros del subcomité nacional que son editores internacionales de normas en los diferentes WGs del JTC1/SC27.

El próximo año, durante los días 8 al 17 de mayo, se celebrará en Madrid la reunión plenaria del comité internacional JTC1/SC27, que ya fue acogida en Madrid en el año 1999 con una gran éxito de organización y avances de trabajo.

5. Panorama europeo para la normalización de los aspectos relativos a la seguridad de las TI

Para finalizar la intención informativa de este artículo, vamos a resumir a continuación los principales órganos de trabajo dónde se desarrollan actividades de normalización de aspectos relativos a la seguridad de las TI en el marco europeo.

A mediados de 1997 el Comité Europeo de Normalización (**CEN**) creó el denominado **CEN/ISSS** (Information Society Standardization System) con objeto de encuadrar en su campo de actuación todas las actividades relacionadas con las Tecnologías de la Información y las Comunicaciones, en adelante TIC, y que hasta la fecha no tenían un espacio dedicado en la estructura existente.

No se trata sólo de un nuevo comité de normalización, pues su aportación recae en el nuevo sistema de trabajo que propone para dar respuesta a las necesidades de un nuevo mercado denominado, entre otras muchas formas, "Sociedad de la Información" y para el que los métodos de normalización tradicional como única herramienta no dan una respuesta acorde al ritmo impuesto por este nuevo mercado.

El CEN/ISSS se posiciona, dentro del marco de la normalización europea, como un

WG 4 Directrices para la seguridad de la información en banca
WG 6 Marco general para la seguridad de TI en instituciones financieras
WG 8 Gestión de la Infraestructura de Clave Pública (PKI) para servicios financieros
WG 10 Seguridad de la información biométrica
WG 11 Algoritmos de cifrado usados en aplicaciones bancarias
WG 12 Seguridad en banca para el público general
WG 14 Esquema de sintaxis criptográfica para servicios financieros
WG 11 Algoritmos de cifrado usados en aplicaciones bancarias
WG 9 Requisitos para mensajes de autenticación

Figura 4. Grupos de trabajo del SC2.

> Las normas se elaboran en el seno de los comités técnicos de normalización que forman parte de la estructura de los organismos de normalización

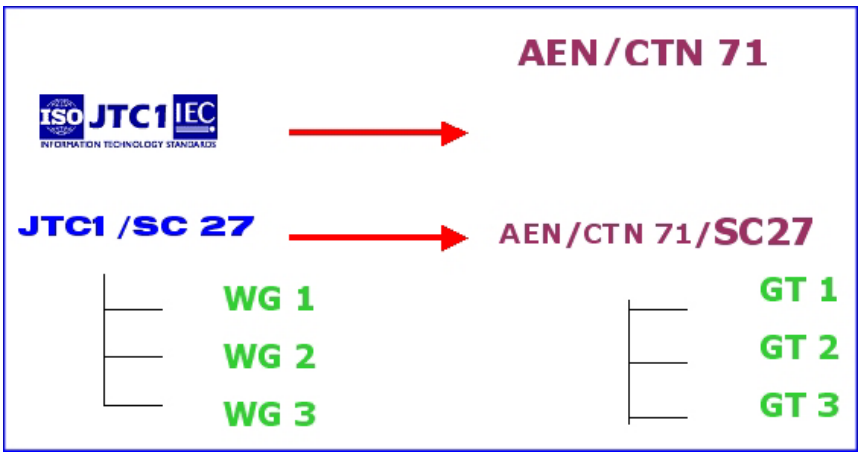

Figura 5. Correspondencias entre ISO y AENOR en lo relativo a Tecnologías de la Información y Seguridad de la Información.

servicio abierto que dota de un enfoque ágil dirigido al mercado de las nuevas tecnologías al ya totalmente arraigado sistema tradicional de hacer las cosas en lo que a normalización se refiere, combinando las especificaciones 'informales' (o mejor, "no del todo formales") con una garantía de seguridad ofrecida por un consenso que reside en los participantes en cada iniciativa. Este mecanismo de consenso es abierto, transparente y ha sido recientemente redefinido para acercarle, más si cabe, a los intereses de la industria y de los consumidores.

Los órganos de trabajo, denominados ***Workshops*** (WS), o talleres de trabajo, proporcionan a los sectores participantes la oportunidad de encontrarse con otros agentes en una situación muy similar a la suya, pudiendo desarrollar un resultado basado en el consenso y validado en un amplio entorno.

Estos talleres de trabajo han sido concebidos con un grado tal de flexibilidad que asegure al entorno particular de cualquiera de ellos el satisfacer los objetivos de todos los miembros del grupo, estando siempre presentes los valores fundamentales de estos grupos: flexibilidad, adaptabilidad, mínima burocracia, apertura a nuevas ideas y resultados prácticos, y efectivos ligados a una eficiente utilización de los recursos

Los documentos producidos en estos talleres de trabajo son los denominados CWAs (*CEN Workshop Agrements*, es decir "Acuerdos de trabajo de CEN"), respondiendo este nombre a su filosofía de elaboración, que no contempla todas las fases obligatorias de información pública y consenso que poseen las normas europeas. Además del desarrollo de estos documentos, el CEN/ISSS proporciona otros servicios de valor añadido como son multitud de actividades de I+D, consorcios y foros de debate públicos a nivel europeo, elaboración de estudios estadísticos en el ámbito europeo sobre determinados aspectos de la Sociedad de la Información, etc...

Desde los comienzos del CEN/ISSS se han creado más de 40 *workshops*. Se han publicado 72 CWAs y están formalmente registrados más de 1.500 participantes.

En lo referente a seguridad de las TI, en la **figura 5** se muestran los *workshops* que tienen o han tenido actividad relativa a algún aspecto de seguridad de TI.

6. Conclusion

Cómo conclusión de toda la información suministrada en este artículo, es importante que quede clara la idea que se proponía al inicio del mismo, y es cómo a través de la participación directa en los órganos y grupos de trabajo de normalización, desde su ámbito nacional al internacional tenemos la vía de influencia en futuras normas y especificaciones técnicas que naciendo en el espíritu de la voluntariedad marcarán con toda certeza la forma futura de hacer las cosas en lo referente a los aspectos de seguridad de la información, que son clave para la buena marcha de los negocios hoy en día.

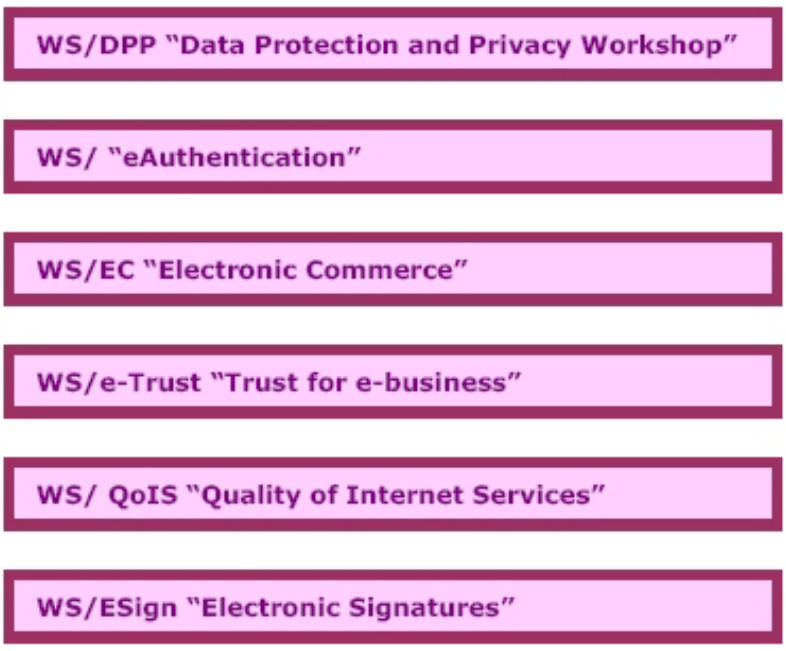

Figura 6. *Workshops* de CEN/ISSS involucrados en algún aspecto de seguridad de TI.

Apéndices (todos los documentos citados en estos apéndices se encuentran disponibles en el depto. de publicaciones de AENOR, <http://www.aenor.es/>).

1. Normas elaboradas por el JTC1/SC27

Referencia ISO/IEC	WG	Título
8372:1987	2	*Information processing, modes of operation for a 64-bit block cipher algorithm*
9796 **9796-2:2002** **9796-3:2000**	2	*Digital signature schemes giving message recovery* *Part 2: Integer factorization based mechanisms* *Part 3: Discrete logarithm based mechanisms*
9797 **9797-1:1999** **9797-2:2002**	2	*Message Authentication Codes (MACs)* *Part 1: Mechanisms using a block cipher* *Part 2: Mechanisms using a dedicated hash-function*
9798 **9798-1:1997** **9798-2:1999** **9798-3:1998** **9798-4:1999** **9798-5:1999**	2	*Entity authentication* *Part 1: General* *Part 2: Mechanisms using symmetric encipherment algorithms* *Part 3: Mechanisms using digital signature techniques* *Part 4: Mechanisms using a cryptographic check function* *Part 5: Mechanisms using zero knowledge techniques*
9979:1999	1	*Procedures for the registration of cryptographic algorithms*
10116:1997	2	*Modes of operation for an n-bit block cipher algorithm*
10118 **10118-1:2000** **10118-2:2000** **10118-3:1998** **10118-4:1998**	2	*Hash-functions* *Part 1: General* *Part 2: Hash-functions using an n-bit block cipher algorithm* *Part 3: Dedicated hash-functions* *Part 4: Hash-functions using modular arithmetic*
11770 **11770-1:1996** **11770-2:1996** **11770-3:1999**	 1 2 2	*Key Management* *Part 1: Framework* *Part 2: Mechanisms using symmetric techniques* *Part 3: Mechanisms using asymmetric techniques*
TR 13335 **13335-1:1996** **13335-2:1997** **13335-3:1998** **13335-4:2000** **13335-5:2001**	1	*Guidelines for the management of IT Security* *Part 1: Concepts and models for IT Security* *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*
13888 **13888-1:1997** **13888-2:1998** **13888-3:1997**	2	*Non-repudiation* *Part 1: General* *Part 2: Mechanisms using symmetric techniques* *Part 3: Mechanisms using asymmetric techniques*
TR 14516:2002	1	*Guidelines for the use and management of Trusted Third Party services*
14888 **14888-1:1998** **14888-2:1999** **14888-3:1998**	2	*Digital signatures with appendix* *Part 1: General* *Part 2: Identity-based mechanisms* *Part 3: Certificate-based mechanisms*
15292:2001	3	*Protection Profile registration procedures*
15408 **15408-1:1999** **15408-2:1999** **15408-3:1999**	3	*Evaluation criteria for IT security* *Part 1: Introduction and general model* *Part 2: Security functional requirements* *Part 3: Security assurance requirements*
15816:2002	1	Security information objects for access control
15945:2002	1	*Specification of TTP services to support the application of digital signatures*
TR 15947:2002	1	*IT intrusion detection framework*
17799:2000	1	*Code of practice for information security management*
18014 **18014-1:2002**	2	*Time-stamping services* *Part 1: Framework*

2. Documentos europeos elaborados en el CEN/ISSS relativos a la seguridad de TI

Referencia CWA	Título
CWA 14162	*Datatyping for Electronic Data Interchange*
CWA 14228	*Summaries of some Frameworks, Architectures and Models for Electronic Commerce*
CWA 14708	*The practical use of Electronic signatures in E-Commerce: a Guide for SMEs*
CWA 14911	*Cyber Identity: Specification of a Top Level Service (TLS) for verifying Identifiers*
CWA 14921	*Web services - Utilization Guidelines for selected areas of Application*
CWA 14167 (Multipart)	*Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*
CWA 14169	*Secure Signature-creation devices "EAL 4+"*
CWA 14170	*Security requirements for signature creation applications*
CWA 14171	*General guidelines for electronic signature verification*
CWA 14172 (Multipart)	*EESSI Conformity Assessment Guidance*
CWA 14355	*Guidelines for the implementation of Secure Signature-Creation Devices*
CWA 14365 (Multipart)	*Guide on the Use of Electronic Signatures*
CWA 14890 (Multipart)	*Application Interface for smart cards used as Secure Signature Creation Devices*
CWA 14357	*Quality of Internet Service*
CWA 14842-1	*Electronic commerce - Shop presentation and transactions - Part 1: Regulatory and self-regulatory requirements*
CWA 14842-2	*Electronic commerce - Shop presentation and transactions - Part 2: Business process requirements*
CWA 14842-3	*Electronic commerce - Shop presentation and transactions - Part 3: ICT security requirements*
CWA 14174-3	*Financial transactional IC card reader (FINREAD) - Part 3: Security requirements*
CWA 14722-3	*Embedded financial transactional IC card reader (embedded FINREAD) - Part 3: Functional and Security Specifications*
CWA 15262	*Inventory of Data Protection Auditing Practices*
CWA 15263	*Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization*
CWA 15292	*Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)*
CWA 15264 (Multipart) **-1** **-2** **-3**	 *Architecture for a European interoperable eID system within a smart card infrastructure* *Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services* *User Requirements for a European interoperable eID system within a smart card infrastructure*

3. Normas nacionales elaboradas por el CTN71/SC27

Referencia UNE	Título
NE 71501-IN:2001	Guía para la gestión de la seguridad de TI Parte 1: Conceptos y modelos para la seguridad de TI *(ISO/IEC TR 13335-1: 1996)*
NE 71501-IN:2001	Parte 2: Gestión y planificación de la seguridad de TI *(ISO/IEC TR 13335-2: 1997)*
NE 71501-IN:2001	Parte 3: Técnicas para la gestión de la seguridad de TI *(ISO/IEC TR 13335-3: 1998)*
NE-ISO/IEC17799:2002	Código de buenas practicas para la Gestión de la Seguridad de la Información
NE 71502 :2004	Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)
NE-CWA 14169:2004*	Dispositivos seguros de creación de firma (EAL4+)

* Elaborada en grupo de trabajo conjunto entre CTN71 y CTN133 "Telecomunicaciones".