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>
Cristóbal 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

Paloma García López[1], Stefanos Gritzalis[2], Javier López Muñoz[3]

[1] AENOR (Asociación Española de Normalización y Certificación); [2] Universidad del Egeo (Grecia); [3] Universidad de Málaga

<pgarcial@aenor.es>, <sgritz@aegean.gr>, <jlm@lcc.uma.es>

Presentación
La normalización en Seguridad TIC: una tarea colectiva internacional y multisectorial

Editores invitados

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.

Stefanos Gritzalis es titulado en Física y en Automatización Eléctrónica y un Doctorado en Informática por la Universidad de Atena (Grecia). Actualmente es Profesor Asociado y responsable del Dpto. de Ingeniería de Sistemas de Información y Comunicación de la Universidad del Egeo (Grecia), así como Director del Laboratorio de Seguridad de Información y Comunicación (Info-Sec Lab). Ha participado en varios proyectos de I+D nacionales y europeos financiados por la Unión Europea en el área de de Seguridad de Información y Comunicación. Entre estos programas se incluyen SNOCER (FP6 SME-1), CRL Study (DG Enterprise), KEYSTONE (DG XIII), COSACC (DG XIII), EUROMED-ETS (DG XIII), ERMIS (DG XVI) y PD4/5 (DG XIII). Sus publicaciones científicas incluyen siete libros sobre diversos temas TIC y más de noventa artículos para revistas y conferencias nacionales e internacionales. Ha pertenecido a comités de programa u organización de conferencias informáticas nacionales e internacionales y es revisor de varias revistas científicas. Fue miembro de la Junta Directiva de la Sociedad Informática de Grecia (*Greek Computer Society*). Es socio de ACM y de IEEE.

Javier López Muñoz es Doctor Ingeniero en Informática, adscrito al Área de Ingeniería Telemática del Depto. de Lenguajes y Ciencias de la Computación de la Universidad de Málaga. Desarrolla su actividad docente como Profesor Titular en la ETS de Ingeniería Informática y su labor investigadora dentro del grupo GISUM (Grupo de Ingeniería del Software) de esta universidad, donde coordina el subgrupo de Seguridad. Su actividad investigadora está centrada en el en el área de Seguridad en Redes de Comunicación y en Comercio Electrónico, habiendo realizando parte de esa labor de investigación en varios centros universitarios de EE.UU. especializados en la materia. En GISUM, es responsable técnico de varios proyectos de investigación relacionados con los aspectos prácticos de Seguridad de las TIC, entre los que destaca el proyecto internacional Global PKI de la *Telecommunications Advancement Organization* de Japon. Asimismo, es Director Técnico del Proyecto IST CASENET del V Programa Marco de la Unión Europea. Es socio de ATI, representante de ATI en el TC11 (*Security and Protection in Information Processing Systems*) de IFIP, coeditor de la sección técnica de Seguridad de ***Novática*** y frecuente colaborador de esta revista, como autor y editor invitado de diversas monografías.

1. Introducción

Más a menudo de lo que en principio nos pudiera parecer, trabajamos con documentos conocidos como normas internacionales o con documentos directamente basados en esas normas. De hecho, una parte considerable de la investigación realizada en universidades, empresas y centros de investigación, nacionales e internacionales, tiene como fundamento la existencia previa de tales normas. Lejos de poder parecer que las normas son simples documentos "hallados" por casualidad y firmados por un autor anónimo que nunca se llegará a identificar, en realidad se elaboran en el senoa través de **los organismos de normalización** oficialmente reconocidos.

El carácter multisectorial que con el paso del tiempo han ido adquiriendo los documentos elaborados en el ámbito de la **normalización voluntaria** va aumentando su dimensión en el sentido de que cada vez es mayor el número de sectores que va tomando conciencia de esta actividad como base para poder ofrecer a los usuarios y clientes servicios y productos de mejor calidad.

En lo referente al marco internacional que se ocupa de los aspectos relacionados con las **Tecnologías de la Información y la Comunicación (TIC)**, existe un comité conjunto constituido entre los dos organismos internacionales de normalización, ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*, que se centra en los aspectos eléctricos de cada campo). El comité conjunto Nº1 es el denominado JTC1 (*Joint Technical Committee 1*).

En el alcance 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.

Tal órgano está estructurado en una serie de Subcomités dedicado cada uno de ellos a un aspecto específico de las Tecnologías de la Información, en concreto el que ocupa el número 27, es el responsable de todos los aspectos de seguridad, denominándose JTC1/SC27 "Técnicas de Seguridad".

El acercamiento de las **actividades de Normalización y Certificación (N+C)** a las organizaciones y al ciudadano es cada vez mayor en el ámbito de dichas tecnologías, concretamente en todo lo relativo a la seguridad de la información, y no únicamente en lo referente a requisitos de fabricación y puesta en el mercado de productos sino también a la normalización de la gestión de la información que las organizaciones llevan a cabo con el objetivo de asegurar la información que manejan.

De todo ello haremos un recorrido a lo largo de este monográfico, que se centra en mostrar el mundo de la normalización y estandarización desde la perspectiva de la seguridad TIC. Si durante muchos años el área de la seguridad ha sido en sí misma un área 'oscura' en comparación con otras de las Tecnologías de la Información, más aún lo ha sido la elaboración de las normas que han regido los principios de esas técnicas de seguridad que hoy encontramos implanta-

Nota del Editor de *Novática*: por razones de espacio no se han incluido en esta monografía de ***Novática*** los artículos " *Common Criteria International Standards*" de ***Miguel Bañón*** y "*International Standardization of Information and IT Security - Current and Future SC27 Activities*" de ***Ted Humphreys***. Estos artículos han sido publicados en el número 4/2005 de **UP**GRADE, en inglés, y aparecerán en próximos números de ***Novática***, en castellano.

das en muchas aplicaciones y sistemas informáticos y de comunicaciones. Este monográfico pretende poner luz a dichos procesos de elaboración de las normas de seguridad.

2. El contenido de esta monografía

El monográfico consta de siete artículos (ver **Nota del Editor** en la página anterior) que recorren los asuntos que, en el marco antes descrito, hemos entendido de mayor interés para el lector.

El primer bloque de los artículos se centra plenamente en acercar al lector a los organismos de normalización. Así, en primer lugar, ***Paloma García López***, en su artículo "*¿Dónde nacen las normas voluntarias y las recomendaciones relativas a la seguridad de la información?*" proporciona una introducción al mundo de la normalizacióny estandarización, detallando y aclarando las estructuras de los organismos nacionales e internacionales involucrados, desde el **origen y la forma de elaboración** de las normas relativas a la seguridad de las tecnologías de la información que se manejan en la actualidad por los distintos colectivos, presentando el panorama y los principales documentos existentes a nivel internacional, europeo y por último la situación nacional y el posicionamiento y participación de España en estos desarrollos, dedicando una apartado especial aasí como los procesos de elaboración de las normas.

A continuación, el artículo "*CEN/ISSS y su contribución a la estandarización europea en Seguridad de las Tecnologías de la Información*", de ***Luc Van den Berghe***, presenta la perspectiva de dicho organismo y muestra el esfuerzo del mismo para ofrecer el entorno donde poder desarrollar los estándareslos documentos y especificaciones allá donde se identifica un área de interés.

Hay un segundo bloque compuesto por una serie de artículos de carácter más general en los que se dan las claves de futuro y los requisitos de los diferentes colectivos a los que hay que dar una respuesta para permitir el desarrollo, avance y penetración de la, en tantas ocasiones referenciada, Sociedad de la Información, entramos en detalle en una serie de aspectos, con una enorme proyección de futuro.

A continuaciónEn este bloque, ***José A. Mañas Argemí***, con su artículo "*Medidas y métricas de seguridad para los Sistemas de Información*", entra en la manera en que vamos a medir el **grado de seguridad** que hemos implantado en una organización, tanto desde el punto de vista de requisitos técnicos como desde las **medidas de gestión** con las que se cuenta argumenta cómo las métricas aparecen como elementos imprescindibles para conocer el estado actual de la seguridad, mejorarlo y gestionar gastos e inversiones.

Le sigue ***Marina Touriño Troitiño***, que en "*Auditoría de Seguridad de las TI desde la perspectiva de la normalización*" muestra cómo la auditoría de la seguridad de la información y el marco normativo son mundos que confluyen y se mejoran mutuamente para contribuir a la expansión de la seguridad que requiere la Sociedad de la Información. La autora argumenta cómo las métricas aparecen como elementos imprescindibles para conocer el estado actual de la seguridad, mejorarlo y gestionar gastos e inversiones.

El siguiente artículo, "*Legislación, estándares y recomendaciones relativos a la firma electrónica*", elaborado por ***Josep Lluís Ferrer Gomila*** y ***Apol·lònia Martínez Nadal***, pone de manifiesto la consonancia existente entre la legislación de la Unión Europea y las recomendaciones técnicas, aunque también constatan la falta de alineación, en ocasiones, de la norma jurídica. Marina Touriño, en "*Auditoría de Seguridad de las TI desde la Perspectiva de la Normalización*", muestra cómo la auditoría de la Seguridad de la información y el marco normativo son mundos que confluyen y se mejoran mutuamente para contribuir a la expansión de la Seguridad que requiere la Sociedad de la Información.

En un último bloque, ***David Chadwick***, a través de "*El estándar X.509 para gestión de privilegios*", proporciona un visión genérica de las Infraestructuras de Administración de Privilegios (*Privilege Management Infrastructures*, PMIs) y su evolución desde la edición de 2001 del estándar X.509 hasta la nueva edición de 2005, que aparecerá en breve.

El monográfico lo cierran ***Spyros Kokolakis*** y ***Costas Lambrinoudakis***, con el trabajo "*Estándares de seguridad de las TIC para aplicaciones en el ámbito sanitario*", que es una interesante contribución sobre las normas de seguridad aplicadas a la telemedicina o *e-Health*, que es en estos momentos un **campo emergente** en la intersección entre la informática médica, salud pública y los negocios; se refieren a los servicios de salud y la información que se entrega o se mejora a través de Internet y sus tecnologías relacionadas. Muestrancómo el campo de la Salud Pública ha sido siempre pionera en el uso de normas y estándares de seguridad especialmente desarrollados y adaptados para esa controvertida área de aplicación de las Tecnologías de la Información.

Debemos señalar que en la presentación de esta monografía no hemos incluido las habituales "referencias útiles" dado que los artículos que la componen contienen una gran cantidad y calidad de ellas.

Para finalizar, agradecemos a los autores sus interesantes contribuciones y a los editores de ***Novática*** y **UP**GRADE la oportunidad que nos han ofrecido de editar esta monografía.