

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 **Upgrade**, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UPENET** (*UPGRADE European Network*)

<<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**, **AIZ** y **ASTIC**.

CONSEJO EDITORIAL

Antoni Carbonell Nogueras, Juan Manuel Cueva Lovelle, Juan Antonio Esteban Iriarte, José Javier Larralde Izáñez, Josep Crespo, Juan Manuel Cocho, Celestino Martín Alcañiz, Josep Molas i Bertrán, Olga Pallás Codina, Fernando Píera Gómez (Presidente del Consejo), Ramon Puigjaner Trepal, Moisés Robles Giner, Miquel Sàrries Grifó, Asunción Yturbe Herranz

Coordinación Editorial

Rafael Fernández Calvo <r/calvo@ati.es>

Composición y autoedición

Jorge Llácer

Traducciones

Grupo de Lengua e Informática de ATI <<http://www.ati.es/gl/lengua-informatica/>>

Administración

Tomas 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>, <flc@ati.es>

Arquitecturas

Jordi Tubella (DAC-UPC) <jordi@ac.upc.es>

Victor Viñals Yuferra (Univ. de Zaragoza) <victor@unizar.es>

Audiovisual

Marina Tourino, Manuel Palao (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>, <mpiattini@inf-cr.uclm.es>

Derecho e tecnologías

Isabel Hernando Gil (Fac. Derecho de Donostia, UPV) <ihernando@legaltel.net>

Isabel Davara Fernández de Marcos (Davara & Davara) <isdavara@davara.com>

Enseñanza Universitaria de la Informática

Joaquín Ezpeleta Mateo (CPS-UZAR) <ezpeleta@posta.unizar.es>

Cristóbal Pareja Flores (DSIP-UCM) <cpareja@sisip.ucm.es>

Gestión del Conocimiento

Joan Baiget Solé (Cap Gemini Ernst & Young) <joan.baiget@ati.es>

Informática y Filosofía

Josep Corco (UIC) <jcorco@unica.edu>

Esperanza Marcos (ESCET-URJC) <cucca@escet.urjc.es>

Informática Gráfica

Miguel Chover Selles (Universitat Jaume I de Castellón) <mchover@lsi.uji.es>

Roberto Vivó (Eurographics, sección española) <rvivo@dsic.upv.es>

Ingeniería del Software

Javier Dolado Gossens (Fac. Ingeniería de la UPV) <gdolado@si.ehu.es>

Luis Fernández (PRIS-El-UEM) <luferm@dpri.ssi.ueu.es>

Inteligencia Artificial

Federico Barber, Vicenle Botti (DSIC-UPV)

<fbotti@barber@dsic.upv.es>

Interacción Persona-Computador

Julio Abascal González (FI-UPV) <julio@si.ehu.es>

Jesús Lóres Vidal (Univ. de Lleida) <jesus@eup.udl.es>

Internet

Alonso Álvarez García (TID) <alonso@ati.es>

Llòrenç Pagès Cassà (Tindra) <pages@ati.es>

Lenguaje e Informática

M. del Carmen Ugarte (IBM) <cugarte@ati.es>

Lenguajes Informáticos

Andrés Marín López (Univ. Carlos III) <amarin@it.uc3m.es>

J. Angel Velázquez (ESCET-URJC) <a.velazquez@escet.urjc.es>

Libertades e Informática

Alonso 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@disi.ua.es>

Mundo estudiantil

Adolfo Vázquez Rodríguez (Rama de Estudiantes del IEEE-UCM)

<a.vazquez@ieee.org>

Profesión Informática

Rafael Fernández Calvo (ATI) <r/calvo@ati.es>

Miquel Sàrries Grifó (Ayto. de Barcelona) <msarries@ati.es>

Redes y servicios telemáticos

Luis Guiparí Coloma (DCOM-UPV) <lguipar@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@icc.uma.es>

Sistemas de Tiempo Real

Alejandro Alonso, Juan Antonio de la Puente

(DIT-UPM) <[@dit.upm.es](mailto:galonso@puente)>

Software Libre

Jesús M. González Barahona, Pedro de las Heras Quirós

(GSYC-URJC) <[@gsyc.escet.urjc.es">jmb.pheras">@gsyc.escet.urjc.es](mailto:jmb.pheras)>

Tecnología de Objetos

Jesus Garcia Molina (DIS-UM) <jmolina@correo.um.es>

Gustavo Rossi (LPIA-UNLP, Argentina) <gustavo@sol.info.unlp.edu.ar>

Tecnologías para la Educación

Juan Manuel Dodero Beardo (UC3M) <dodero@inf.uc3m.es>

Francisco Riviere (PalmCAT) <friviere@wanadoo.es>

Tecnologías y Empresa

Pablo Hernández Medrano (Bluematt) <pablohm@bluematt.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)

<[@icc.uma.es">aguayo_guevara">@icc.uma.es](mailto:aguayo_guevara)>

Las opiniones expresadas por los autores son responsabilidad exclusiva de los mismos. **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; se ruega enviar a **Novática** un ejemplar de la publicación.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid

Padilla 66, 3º, dcha., 28006 Madrid

Tfn. 914029391; fax. 913093685 <novatica@ati.es>

Composición, Edición y Redacción ATI Valencia

Av. del Reino de Valencia 23, 46005 Valencia

Tfn./fax. 963303092 <secretari@ati.es>

Administración y Redacción ATI Cataluña

Via Laietana 41, 1º, 1ª, 08003 Barcelona

Tfn. 934125235; fax. 934127713 <secretgen@ati.es>

Redacción ATI Aragón

Isaac Newton, s/n, Ed. Sadiel,

Isa. Carluja 41092 Sevilla, Tfn./fax. 954460779 <secretand@ati.es>

Redacción ATI Asturias

Lapazca 9, 3-B, 50006 Zaragoza,

Tfn./fax. 976235181 <secretara@ati.es>

Redacción ATI Asturias-Cantabria <go-astucant@ati.es>

Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>

Redacción ATI Galicia

Recinto Ferial s/n, 36540 Silleda (Pontevedra)

Tfn. 986581413; fax. 986580162 <secretgal@ati.es>

Subscripciones y Ventas

<<http://www.ati.es/novatica/interes.html>>, o en ATI Cataluña o ATI Madrid

Publicidad

Padilla 66, 3º, dcha., 28006 Madrid

Tfn. 914029391; fax. 913093685 <novatica.publicidad@ati.es>

Imprenta

Ortiz S.A., Juan de Austria 66, 08005 Barcelona.

Depósito legal: B.15.154-1975 -- ISSN: 0211-2124; CODEN NOVACE

Portada: Antonio Crespo Foix / © ATI 2004

Diseño: Fernando Agresta / © ATI 2004

Nº 172, noviembre-diciembre 2004, año XXX

sumario

editorial

> 02

Nueva Junta Directiva General de ATI

La vía agropiscícola a las patentes de software

A vueltas con el canon privado sobre soportes digitales

en resumen

> 05

Las claves

Rafael Fernández Calvo

monografía

Criptografía - Una tecnología clave

(En colaboración con **Upgrade**)

Editores invitados: *Arturo Ribagorda Garnacho, Javier Areitio Bertolín, Jacques Stern*

Presentación

Criptografía: la clave de la seguridad de la información en el siglo XXI

> 06

Arturo Ribagorda Garnacho, Javier Areitio Bertolín, Jacques Stern

Una breve panorámica de la Criptografía

> 08

Arturo Ribagorda Garnacho, Javier Areitio Bertolín

Un Canal de Comunicaciones Anónimo

> 10

Joan Mir Rubio, Joan Borrell Viader, Vanesa Daza Fernández

Aplicación del Doble Cifrado a la Custodia de Claves

> 15

Mónica Breitman Mansilla, Carlos Gete Alonso, Paz Morillo Bosch, Jorge L. Villar Santos

Reconstrucción de la secuencia de control en Generadores

con Desplazamiento Irregular

> 17

Slobodan Petrovic, Amparo Fúster Sabater

Cifrado de imágenes usando Autómatas Celulares con Memoria

> 21

Luis Hernández Encinas, Ascensión Hernández Encinas, Sara Hoya White,

Ángel Martín del Rey, Gerardo Rodríguez Sánchez

Aplicaciones de la Criptografía de Curva Elíptica

> 24

María de Miguel de Santos, Carmen Sánchez Ávila, Raúl Sánchez Reillo

Hacia una herramienta de formación por ordenador para la enseñanza

> 28

de la Criptografía

Vasilios Katos, Terry King, Carl Adams

Análisis científico del Ciberterrorismo

> 33

Ivo Desmedt

secciones técnicas

Gestión del Conocimiento

Gestión del conocimiento 'informal' basada en redes P2P

> 38

Alfredo Picón Cabezado, Teodoro Mayo Muñoz, Alonso Álvarez García

Libertades e informática

Las herramientas prohibidas: tratamiento de los Ciberdelitos

> 44

en la Ley Orgánica 15/2003, de modificación del Código Penal

Carlos Sánchez Almeida

Redes y servicios telemáticos

SRMSH: un mecanismo multinivel de control de la congestión

con detección y recuperación de pérdidas

> 50

Oscar Martínez Bonastre, Carlos Palau Salvador

Seguridad

Firmas y documentos electrónicos: ¡que viene el lobo!

> 55

Petr Švédá, Václav Matyáš Jr.

Tecnología de Objetos

La documentación de frameworks frente a las dificultades de sus usuarios

> 58

Guillermo Jiménez Díaz, Mercedes Gómez Albarrán

Referencias autorizadas

> 64

sociedad de la información

Breve historia de la prensa española especializada

en Tecnologías de la Información

> 70

Alfonso González Quesada

asuntos interiores

Coordinación editorial - Fé de erratas / Programación de Novática

> 76

Normas de publicación para autores / Socios Institucionales

> 77

Monografía del próximo número: "XML"

Novática disponible en la Intranet de ATI

Recordamos que en la Intranet de ATI, en <http://intranet.ati.es/novatica/>, se encuentran disponibles, en formato PDF, las versiones digitales completas de todos los números de nuestra revista a partir del 138 (feb.-mar. 1999), además de los números 0 y 1.

El acceso está restringido a los socios de ATI únicamente, con la única condición de que estén registrados en ATInet. Para registrarse hay que ponerse en contacto con info@ati.es.

Revista austríaca se une a UPENET (UPGRADE European Network)

El pasado mes de noviembre se incorporó a **UPENET** (**UPGRADE** European Network) la revista **OCG Journal**, editada por OCG (Österreichische Computer Gesellschaft, <http://www.ocg.or.at/>). OCG es una asociación austríaca miembro de CEPIS (Council of Professional Informatics Societies, <http://www.cepis.org>).

OCG Journal se convierte así en la quinta revista miembro de **UPENET** junto a **Novática**, la italiana **Mondo Digitale**, la chipriota **Pliroforiki** ("Informática" en griego) y la polaca **Pro Dialog**.

Hay grandes probabilidades de que otras revistas de sociedades miembro de CEPIS se incorporen en los próximos meses. Con ello se ampliará aún más el alcance de esta red, en la que **Novática** tiene un papel muy relevante como editora de **UPGRADE**, revista en torno a la cual se articula **UPENET**.

Es importante señalar que las revistas que forman parte de esta red, entre ellas la nuestra, podrán publicar artículos aparecidos en **UPGRADE** y en las revistas participantes en la misma.

Más información sobre **UPENET** puede encontrarse en <http://www.upgrade-cepis.org/pages/upenet.html>.

Con motivo de la incorporación de **OCG Journal**, CEPIS ha distribuido un comunicado de prensa cuyo texto completo puede encontrarse, en inglés, en <http://www.cepis.org/news.html>.

Lista electrónica de UPGRADE

Recordamos que **UPGRADE** tiene una lista cuyo objetivo es distribuir noticias sobre esta revista digital europea publicada, desde su creación en octubre de 2000, por **Novática** en nombre de CEPIS (Council of European Professional Informatics Societies). En <http://www.upgrade-cepis.org/pages/editinfo.html#newsletter> se encuentra información sobre sus características y sobre cómo darse de alta en ella.

fé de erratas

Novática nº 171

El artículo "Diseño de suelos (CUPCAM 2003, problema G, solución)" de **Juan Céspedes Prieto**, **Antonio Fernández Anta** y **Ángel Herranz Nieva**, publicado en la sección "programar es crear" del nº 171 (septiembre-octubre 2004, pp. 74-75), contenía numerosos errores en las ecuaciones de la página 74, debido a problemas de composición no imputables a los autores y por los que pedimos disculpas a ellos y a nuestros lectores.

Dichos errores se han subsanado en la versión digital disponible tanto en <http://www.ati.es/novatica/2004/171/nv171sum.html> como en la Intranet de ATI, en <http://intranet.ati.es/novatica/>.

Monografías para 2005

Por acuerdo de los Consejos Editoriales de **Novática** y **UPGRADE** los temas de las monografías de los primeros números de 2005 de ambas revistas serán las siguientes, salvo imprevistos o causas de fuerza mayor:

Nº 173 (enero-febrero): "XML". Editores invitados: **Carlos Delgado Kloos** (Universidad Carlos III de Madrid), cdk@it.uc3m.es; **Charles McCathieNevile** (W3C, World Wide Web Consortium), charles@w3.org.

Nº 174 (marzo-abril): "IPv6". Editores invitados: **Jordi Domingo Pascual** (Universitat Politècnica de Catalunya), jordi.domingo@ac.upc.es; **Matthew Ford** (BT Exact), matthew.ford@bt.com.

Nº 175 (mayo-junio): "Web Semántica". Editores invitados: **Asunción Gómez Pérez** (Universidad Politécnica de Madrid), asun@fi.upm.es; **V. Richard Benjamins** (Intelligent Software Components, S.A.), rbenjamins@isoco.dot.com.

En próximas fechas se anunciarán los temas de las restantes monografías de 2005.