

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, AI2 y ASTIC.

## CONSEJO EDITORIAL

Antoni Carbonell Nogueras, Juan Manuel Cueva Lovelle, Juan Antonio Esteban Iriarte, José Javier Garralda Bahar, Francisco López Crespo, Julián Marcelo Cocho, Celestino Martín Alonso, Josep Molas i Bertrán, Olga Pallas Codina, Fernando Pierra Gómez (Presidente del Consejo), Ramón Puigjaner Trepal, Moisés Robles Giner, Miquel Sàrries Griño, Asunción Yturbe Herranz

**Coordinación Editorial**  
Rafael Fernández Calvo <rfcalvo@ati.es>  
**Composición y autoedición**  
Jorge López  
**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 Aribas, Francisco López Crespo (MAP) <gumersindo.garcia@map.es>, <flcc@ati.es>  
**Arquitecturas**  
Jordi Tubella (DAC-UPC) <jordit@ac.upc.es>  
Victor Vibalbaterra (Univ. de Zaragoza) <victor@unizar.es>  
**Auditoría STIC**  
Marina Touriño, 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 Hernández Collazos (Fac. Derecho de Donostia, UPV) <ihernando@legalete.net>  
Isabel Davara Fernández de Marcos (Davara & Davara) <idavara@davara.com>  
**Escuela Universitaria de la Informática**  
Joaquín Ezpeleta Mateo (CPS-UZAR) <ezpeleta@posta.unizar.es>  
Cristóbal Pareja Flores (DSIP-UCM) <cpajef@sisip.ucm.es>  
**Gestión del conocimiento**  
Joan Baiget Solé (Cap Gemert Ernst & Young) <joan.baiget@ati.es>  
**Informática y Filosofía**  
Jesús Corco (UC) <jcorco@unica.edu>  
Esperanza Marcos (ES CET-URJC) <cuca@es cet.urjc.es>  
**Informática Gráfica**  
Miguel Chover Solés (Universitat Jaume I de Castellón) <chover@lsi.uji.es>  
Roberto Vivó (Eurographics, sección española) <rvivo@dsic.upv.es>  
**Ingeniería del Software**  
Javier Dolado Cosín (ULS-UPV) <dolado@si.ehu.es>  
Luis Fernández (PSE-UEM) <luferrn@pse.asi.uem.es>  
**Inteligencia Artificial**  
Federico Barber, Vicente Botti (DSIC-UPV) <fvotti, fbarber@dsic.upv.es>  
**Interacción Persona-Computador**  
Julio Abascal González (FI-UPV) <julio@si.ehu.es>  
Jesús Lorés Vidal (Univ. de Lleida) <jesus@eup.udl.es>  
**Internet**  
Alonso Álvarez García (TID) <alonso@ati.es>  
Llorenç Panis Casas (Indra) <pages@ati.es>  
**Lengua e Informática**  
M. del Carmen Ugarte (IBM) <cuarte@ati.es>  
**Lenguajes Informáticos**  
Andrés Marín López (Univ. Carlos III) <amarin@it.uc3m.es>  
J. Ángel Velázquez (ES CET-URJC) <a.velazquez@es cet.urjc.es>  
**Librerías e Informática**  
Alfonso Escosido (FRU-UV de La Laguna) <aescosid@uill.es>  
**Lingüística computacional**  
Xavier Gómez Guinovart (Univ. de Vigo) <xgg@uvigo.es>  
Manuel Palomar (Univ. de Alicante) <mpalomar@dsi.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 Griño (Ayto. de Barcelona) <msarries@ati.es>  
**Redes y servicios telemáticos**  
Luis Guisjar Coloma (DCOM-UPV) <lguisjar@dc om.upv.es>  
Jesús Pareja Flores (DAC-UPC) <pareja@ac.upc.es>  
**Seguridad**  
Javier Areitio Bertolin (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) <jalonso, jpuente@dit.upm.es>  
**Software Libre**  
Jesús M. González Barahona, Pedro de las Heras Quirós (GSYC-URJC) <jlob.oheras@gsync.es cet.urjc.es>  
**Tecnología de Objetos**  
Jesús María Molina (DIS-UM) <jmolina@correo.um.es>  
Gustavo Rpgsi (LFFIA-UNLP, Argentina) <gustavo@sol.info.unlp.edu.ar>  
**Tecnologías para la Educación**  
Juan Manuel Dodero Beardo (UC3M) <ddodero@inf.uc3m.es>  
Francisco Riviere (PalmCAT) <friviere@wanadoo.es>  
**Tecnología y Empresa**  
Pablo Hernández Medrano (Bluemat) <pablohm@bluemat.biz>  
**TIC para la Salud**  
Valentín Masero Vargas (DI-UNEX) <vmasero@unex.es>  
**TIC y Turismo**  
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga) <aguayo, guevara@iccc.uma.es>

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  
Tlf. 91 4029391, fax 91 3093685 <novatica@ati.es>  
**Composición, Edición y Redacción ATI Valencia**  
Av. del Reino de Valencia 23, 46005 Valencia  
Tlf. fax 963330892 <secregen@ati.es>  
**Administración y Redacción ATI Cataluña**  
Via Laietana 41, 1º, 1ª, 08003 Barcelona  
Tlf. 934 125235, fax 934 127115 <secregen@ati.es>  
**Redacción ATI Andalucía**  
Isaac Newton, s/n, Ed. Sadiel,  
Isla Cartuja 41092 Sevilla, Tlf./fax 954460779 <secreand@ati.es>  
**Redacción ATI Aragón**  
Lagasca 9, 3-B, 50006 Zaragoza  
Tlf./fax 976261511 <secreara@ati.es>  
**Redacción ATI Asturias-Cantabria**  
Redacción ATI Castilla-La Mancha <clp.mancha@ati.es>  
**Redacción ATI Galicia**  
Recinto Ferrol s/n, 36340 Silleda (Pontevedra)  
Tlf. 986581413, fax 986580162 <secregal@ati.es>  
**Subscripción y Ventas**  
<<http://www.ati.es/novatica/interes.html>>, o en ATI Cataluña o ATI Madrid  
**Publicidad**  
Padilla 66, 3º dcha., 28006 Madrid  
Tlf. 91 4029391, fax 91 3093685 <novatica.publicidad@ati.es>  
**Imprenta**  
Derra S.A., Juan de Austria 66, 08005 Barcelona  
**Distribución legal** B, 15, 154, 1975 - ISSN: 0211-2124, CODEN NOVAEC  
**Distribución** Antonio Crespo Foley © ATI 2004  
**Diseno** Fernando Agresta / © ATI 2004

**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 Bertolin, Jacques Stern

#### Presentación

**Criptografía: la clave de la seguridad de la información en el siglo XXI** > 06

Arturo Ribagorda Garnacho, Javier Areitio Bertolin, Jacques Stern

**Una breve panorámica de la Criptografía** > 08

Arturo Ribagorda Garnacho, Javier Areitio Bertolin

**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** > 17

con Desplazamiento Irregular

Slobodan Petrovic, Amparo Fúster Sabater

**Cifrado de imágenes usando Automatas 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

Maria 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 Cabezudo, 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** > 50

con detección y recuperación de pérdidas

Oscar Martínez Bonastre, Carlos Palau Salvador

### Seguridad

**Firmas y documentos electrónicos: ¡que viene el lobo!** > 55

Petr Švéda, 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