

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 **UPNET** (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 **IIFP** (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

Antonio Carbonell Novella, Juan Manuel Cuevas Lavela, Juan Antonio Esteban Iriarte, José Javier Llerena Martínez, Francisco López Crespo, Rafael Martín Cocho, Celestino Moreno Alfonso, José Molina Bertrán, Olga Pallas Codina, Fernando Piera Gómez (Presidente del Consejo), Ramón Puigjáner Trepat, Moisés Robles Giner, Miquel Sánchez Grífio, Asunción Yturbe Herranz

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

Comisión y autoridades

Jorge Llúcar

Traducciones

Grupo de Lengua e Informática de ATI <<http://www.ati.es/gt/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>, <flopez@ati.es>

Arquitectura

José Luis González (DACP-UPC) <jordit@ac.upc.esc>
Víctor Vilaplana Xifera (Univ. de Zaragoza) <victor@unizar.es>

Andalucía STIC

Martín Tourino, Manuel Palao (ASIA) <marinatourino@marinatourino.com>, <m.palao@palao.com>

Baleares

Coral Celero Muñoz, Mario G. Plattini Vethuis (Escuela Superior de Informática, UCLM)

<coral.celero@uclm.es>, <mplattini@eii.ucm.es>

Derecho y Tecnologías

Isabel Hernández Colomos (Fac. Derecho de Donostia, UPV) <iherando@legaltek.net>

Iñaki Díaz Fernández de Mora (Avanza & Davara) <idavara@dvara.com>

Escuela Universitaria de la Informática

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

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

Gestión del Conocimiento

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

Inteligencia Artificial

Fernando Beltrán de la Fuente (DSIC-UPV) <fbeltran@dsic.upv.es>

<fbeltran@ibarber@dsic.upv.es>

Interacción Persona-Computador

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

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

Internet

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

Llorenç Panés Casas (Indra) <pages@at.es>

Lengua e Informática

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

Lenguajes informáticos

Antonio Martín López (UJI, Carlos III) <amarin@it.uic3.es>

Libertades e Informática

Alfonso Escalona (FIR-Univ. de La Laguna) <aescalan@ull.es>

Lingüística computacional

Xavier González Gurvart (Univ. de Vigo) <xgg@uvigo.es>

Manuel Poblete (Univ. de Alicante) <mpoblete@dsi.ua.es>

Mundo estudiantil

Adolfo Vázquez Rodríguez (Ramón de Estudiantes del IEEE-UCM) <a.vazquez@ieee.org>

Profesionales informáticos

Rafael Fernández Calvo (ATI) <rfernandezcalvo@ati.es>

Miquel Sarriés Grífio (Ayto. de Barcelona) <msarries@ati.es>

Datos y servicios telemáticos

Luis Guijarro Coloma (DCOM-UPV) <lguijarro@dcn.upv.es>

Redes y servicios telemáticos

Josep Soley Pareta (DACP-UPC) <pareta@ac.upc.es>

Sistemas de Tiempo Real

Alejandro Alonso, Juan Antonio de la Puent (DIT-UPM) <ajalonso.juanpuente@dit.upm.es>

Sociedad Informática

Jesús M. González Barahona, Pedro de las Heras Quirós (GSYC-URJC) <job.pheras@gsic.escet.urjc.es>

Tecnología de Objetos

Jesús García Molina (DIS-UM) <jmolina@correo.um.es>

Gustavo Rossi (LIFIP-Universidad Autónoma) <gustava@sol.info.unlp.edu.ar>

TIC y Educación

Juan Manuel Díodoro Beard (UC3M) <dodero@ic3m.es>

Francesc Riverà (PalmCAT) <frivera@waradoo.es>

Tecnologías y Empresas

Pablo Hernández Medrano (Bluemat) <pablomm@bluemat.biz>

TIC y Empresas

Valentín Masró Maldonado, Antonio Guevara Plaza (Univ. de Málaga) <agrayo, guevara>@cc.uma.es>

TIC y Turismo

Andrés Aguayo Guevara Plaza (Univ. de Málaga) <agrayo, guevara>@cc.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 copyleft 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, 3^{er} dcha., 28006 Madrid

Tlfn. 914029391; fax. 913093685 <novatica@at.es>

Composición, Edición y Redacción ATI Valencia

Av. Reino de Valencia 23, 46005 Valencia

Tlfn. fax. 963353397 <secreta@at.es>

Asociación de Redactores ATI Cataluña

Via Laietana 41, 1^{er}, 08003 Barcelona

Tlfn. 934125235; fax. 934127713 <secregen@at.es>

Redacción ATI Andalucía

Isaac Newton, s/n, Ed. Sadiel,

19002 Granada, Tfno. fax. 954460779 <secreand@at.es>

Redacción ATI Aragón

Lagasca 9, 3^{er} planta Zaragoza,

Tlfn. fax. 976235181 <secreara@at.es>

Redacción ATI Asturias-Cantabria

<gp.astucant@at.es>

Redacción ATI Galicia-La Mancha

<gp-clmancia@at.es>

Redacción ATI Canarias

Recinto Ferial s/n, 36540 Silleda (Pontevedra)

Tlfn. 986581413; fax. 986580162 <secregal@at.es>

Suscripciones y Ventas

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

Publicidad

Padilla 66, 3^{er} dcha., 28006 Madrid

Tlfn. 914029391; fax. 913093685 <novatica.publicidad@at.es>

Imprenta

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

Periodico: ISSN 1515-1975 - ISSN 0211-2124; CODEN NOVAEC

Issue: Fernando Agresta / © ATI 2004

Nº 172, noviembre-diciembre 2004, año XXX

sumario

> 02

editorial

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

Las claves

Rafael Fernández Calvo

> 05

monografía

Criptografía - Una tecnología clave

(En colaboración con **Upgrade**)

Editores invitados: Arturo Ribagorda Garnacho, Javier Areito Bertolín, Jacques Stern

Presentación

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

Arturo Ribagorda Garnacho, Javier Areito Bertolín, Jacques Stern

> 06

Una breve panorámica de la Criptografía

Arturo Ribagorda Garnacho, Javier Areito Bertolín

> 08

Un Canal de Comunicaciones Anónimo

Joan Mir Rubio, Joan Borrell Viader, Vanesa Daza Fernández

> 10

Aplicación del Doble Cifrado a la Custodia de Claves

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

Reconstrucción de la secuencia de control en Generadores

con Desplazamiento Irregular

Slobodan Petrović, Amparo Fuster Sabater

> 17

Cifrado de imágenes usando Autómatas Celulares con Memoria

Luis Hernández Encinas, Ascensión Hernández Encinas, Sara Hoya White, Ángel Martín del Rey, Gerardo Rodríguez Sánchez

> 21

Aplicaciones de la Criptografía de Curva Elíptica

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

> 24

Hacia una herramienta de formación por ordenador para la enseñanza de la Criptografía

Vasilios Katos, Terry King, Carl Adams

> 28

Analísisis científico del Ciberterrorismo

Ivo Desmedt

> 33

secciones técnicas

Gestión del Conocimiento

Gestión del conocimiento 'informal' basada en redes P2P

> 38

Alfredo Picón Cabezudo, Teodoro Mayo Muñiz, Alonso Álvarez García

Libertades e informática

Las herramientas prohibidas: tratamiento de los Ciberdelitos en la Ley Orgánica 15/2003, de modificación del Código Penal

> 44

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: ique 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

> 64

Referencias autorizadas

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"

normas de publicación para autores

Diciembre 2004

Novática agradece su contribución desinteresada a los miles de autores que han elegido y elegirán sus páginas para presentar sus aportaciones al avance profesional y tecnológico de la Informática.

Periodicidad: **Novática** tiene periodicidad bimestral y aparece los meses de febrero, abril, junio, septiembre, octubre y diciembre, salvo retrasos debidos a causas de fuerza mayor. El cierre de la edición es habitualmente un mes antes de la fecha de distribución (dos meses para los artículos del bloque monográfico).

Normas de revisión: todos los artículos serán sometidos a un proceso de "revisión por iguales" (*peer review*), o revisión por personas especializadas en la materia objeto del artículo, excepto los expresamente solicitados por **Novática** a sus autores. En el caso de las monografías, serán los editores invitados y su equipo los que realicen la revisión y decidan sobre su publicación o no. Excepto en el caso de las monografías, los artículos deberán ser enviados a la oficina de Coordinación Editorial (Novática-ATI. Calle Padilla 66, 3^a dcha., 28006 Madrid, <novatica@ati.es> (ver "Soportes" más abajo). Una vez aprobados por el revisor(es), serán publicados tan pronto como sea posible, si bien la publicación no está garantizada pues razones de exceso de material pueden hacerla imposible. Los autores serán informados del resultado de la revisión y de la publicación o no de los artículos remitidos.

Tamaño y formato de los artículos: los artículos deberán tener un máximo de 4.500 palabras, lo que equivale a entre 8 y 10 páginas DIN A4 a doble espacio (fuente Times New Roman, tamaño 12), incluyendo resumen, palabras clave, figuras, bibliografía y notas. Sólo en casos excepcionales se aceptarán artículos superiores a dicho tamaño. Salvo excepciones, los artículos no deberán incluir más de cinco ecuaciones ni más de doce referencias bibliográficas o notas, y deberán incorporar título, resumen (máximo 20 líneas), palabras clave (un máximo de 10), nombre, dos apellidos y afiliación del autor/a (es/as), así como su dirección postal y electrónica, y números de teléfono y fax. **Nota importante:** título, resumen y palabras clave deberán enviarse en español e inglés.

Soportes: los artículos deberán ser enviados a **Novática** en formato digital, preferentemente mediante correo electrónico o, si no se tiene acceso a éste, mediante disquete a través de correo postal. En caso de envío por correo electrónico, si el fichero tiene un tamaño superior a los 250KB, es preciso enviar el fichero comprimido con ZIP e indicando qué procesador de texto entre los citados a continuación se ha utilizado. En ambos casos (correo electrónico o disquete) el artículo debe ser enviado en formato Word, OpenOffice, RTF o HTML. En todos los casos el artículo habrá de enviarse también en formato PDF para asegurar la fidelidad al original en el proceso de edición.

Además, también en todos los casos, es preciso además enviar las figuras por separado, con la mayor resolución posible (mínimo 600 ppi), teniendo en cuenta que solamente se publicarán en blanco y negro.

Lengua: aunque **Novática** admite artículos escritos en todas las lenguas reconocidas por la Constitución española y los Estatutos de las diferentes Comunidades Autónomas, dado que el ámbito de difusión de la revista conlleva su publicación en castellano, como lengua oficial común, los autores deberán presentar sus artículos en castellano y, si así lo desean, en otra lengua oficial de su elección. **Novática** enviará a los socios y suscriptores que lo soliciten una copia de la versión original de aquellos artículos que hayan sido escritos en una lengua oficial que no sea el castellano.

Copyright: **Novática** da por supuesto que un autor acepta las presentes normas al enviar su original y que, en caso de que esté destinado a ser publicado en otro medio ajeno a ATI (o ya haya sido publicado) debe de aportar la autorización del editor del mismo para su reproducción por **Novática** (incluida la autorización para realizar traducciones). **Novática** por tanto no asume ninguna responsabilidad sobre derechos de propiedad intelectual si un texto se ha publicado en otro medio de comunicación, sea inadvertidamente o no, por parte del autor. Todo autor que publique un artículo en **Novática** debe saber que autoriza su reproducción, citando la procedencia, salvo que el autor utilice de forma explícita una modalidad de © o copyright, que lo impida. Asimismo, se entiende que el autor acepta que, además de en **Novática**, su artículo podrá ser también publicado y distribuido de forma electrónica, en su totalidad o parcialmente, en los medios habituales de difusión de ATI (servidor WWW, listas de distribución Internet, etc.) o en aquellos medios en los que ATI y **Novática** participen, como, por ejemplo, **UPGRADE** o **OPENET**.

Estilo: si bien **Novática** respeta totalmente el estilo y contenido de cada artículo, da por supuesta la autorización del autor para retocar su ortografía, léxico, sintaxis, titulación y paginación, a fin de facilitar su comprensión por el lector y de subsanar posibles errores. Cualquier cambio que afecte al contenido será consultado con el autor.

socios institucionales de ati

Según los Estatutos de ATI, pueden ser socios institucionales de nuestra asociación "las personas jurídicas, públicas y privadas, que lo soliciten a la Junta Directiva General y sean aceptados como tales por la misma".

Mediante esta figura, todos los profesionales y directivos informáticos de los socios institucionales pueden gozar de los beneficios de participar en las actividades de ATI, en especial congresos, jornadas, cursos, conferencias, charlas, etc. Asimismo los socios institucionales pueden acceder en condiciones especiales a servicios ofrecidos por la asociación tales como Bolsa de Trabajo, cursos a medida, mailings, publicidad en Novática, servicio ATInet, etc.

Para más información dirigirse a <info@ati.es> o a cualquiera de las sedes de ATI. En la actualidad son socios institucionales de ATI las siguientes empresas y entidades:

AGROSEGURO
AIGÜES DEL TER LLOBREGAT
AJUNTAMENT DE L'HOSPITALET DE LLOBREGAT
AYUNTAMIENTO DE TERRASSA
ALMIRALL PRODESFERMA, S.A.
ATOS ORIGIN, SAE
BARCELONESA DE DROGAS DE PRODUCTOS QUÍMICOS
Barcelonesa de Gestión Administrativa, S.L.
BBR INGENIERIA DE SERVICIOS, S.L.
BT TELECOMUNICACIONES, S.A.
BURKE FORMACIÓN, S.A.
CÁLCULO, S.A.
CARGILL España, S.A.
CCS PROFESIONALES, S.L.
CENTRO ESTUDIOS VELÁZQUEZ, S.A. (C.E. ADAMS)
CHOICE, S.A.
CLASE 10 SISTEMAS, S.L.
CLINICA PLATÓ FUNDACIÓN PRIVADA
COOPERS & LYBRAND AUDITORÍA Y CONSULTORÍA
CONSULTORES SAYMA, S.A.
Departament d'Ensenyament de la Generalitat de Catalunya
DEPTO. INFORMÁTICA - ESC. POLITÉCNICA (CÁCERES)
DIMENSIÓN INFORMÁTICA, S.L.
DOXA CONSULTORES, S.L.
EDITORIAL BELLADONA S.L.
ENDESA INGENIERIA DE TELECOMUNICACIONES (SEVILLA)
EPISER, S.L.
ESPECIALIDADES ELÉCTRICAS S.A. (ESPELTA)
ESTEVE QUÍMICA, S.A.
FINCONSUM - Financiación al Consumo
FUNDACION SAN VALERO
GRUPO CORPORATIVO GFI INFORMÁTICA, S.A.
GRUPO INFORMÁTICO ITEM, S.A.
GS y C, Gabinete Sistemas y Consultoría, S.L.
INFORMATION BUILDERS IBÉRICA, S.A.
INQA TEST, S.L.
INSERT SISTEMAS, S. A.
INSTITUT D'ESTUDIS CATALANS
INVERAMA, S.A.
ISC INGENIERÍA DE SISTEMAS Y COMUNICACIONES
IN2 INGENIERÍA DE INFORMACIÓN
KRITER, S.A.
LATIN WALK, S.L.
LABORATORIOS SERONO, S.A.
META4 SPAIN, S.A.
METASINCRO, S.L.
NÁCAR, Tecnologías de la información, S.L.U.
NTR - NET TRANSMIT & RECEIVE, S.L.
ONDATA INTERNATIONAL, S.L.
OCCIDENTAL HOTELES MANAGEMENT, S.A.
ORGANISMO AUTÓNOMO INFORMÁTICA Y
COMUNICACIONES DE LA COMUNIDAD DE MADRID
PAUTA FORMACIO S.L.
RÁPIDA SISTEMAS INTEGRALES, S.A.
RD SISTEMAS, S.A.
RENAULT FINANCIACIÓN
SADIEL, S.A.
SARA LEE DE ESPAÑA, S.A.
SCATI LABS, S.A. (ZARAGOZA)
SERES ESPAÑA, S.A.
SERTECNET VALENCIA
SERVEIS INFORMÀTICS
SISTEMAS TÉCNICOS LOTERÍAS DEL ESTADO (STL)
SOCIEDAD DE REDES ELECTRÓNICAS Y SERVICIOS, S.A.
SOLUCIONES INFORMÁTICAS PARA EL COMERCIO, S.L.
STRATESYS CONSULTING ADP&M, S.L.
SYSDATA, S.L.
T-SYSTEMS
TATUM SISTEMAS
TCP SISTEMAS DE INGENIERÍA, S.L.
TRANSBAIX LLOBREGAT, S. A. (Grupo Seur)
TRW ISCS, S.L.
UNIVERSIDAD ANTONIO DE NEBRIJA
UNIVERSIDAD DE EXTREMADURA (Dpto. de Informática)
UNIVERSITAT OBERTA DE CATALUNYA
WAPETON NUEVAS TECNOLOGÍAS, S.A.