novática
Revista de la Asociación de Técnicos de Informática

***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), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

**<http://www.ati.es/novatica/>**
**<http://www.ati.es/reicis/>**

**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**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.



**Coordinación Editorial, Redacción Central y Redacción ATI Madrid**
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
**Composición, Edición y Redacción ATI Valencia**
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
**Administración y Redacción ATI Cataluña**
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
**Redacción ATI Andalucía** <secreand@ati.es>
**Redacción ATI Galicia**<secregal@ati.es>
**Suscripción y Ventas** <novatica.subscripciones@atinet.es>
**Publicidad** Plaza de España 6, 2ª planta, 28008 Madrid
Tlnf 914029391; fax.913093685 <novatica@ati.es>
**Imprenta:** Derra S.A., Juan de Austria 66, 08005 Barcelona.
**Depósito legal:** B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
**Portada:** "Mineral, vegetal, animal" - Concha Arias Pérez / © ATI
**Diseño:** Fernando Agresta / © ATI 2003

Nº 223, mayo-junio 2013, año XXXIX

# sumario



**Tema del próximo número:**
**"Eficiencia energética en centros de proceso de datos"**

## El "caso Snowden" y la seguridad de las redes de telecomunicación

Una de las noticias más relevantes de los últimos meses ha sido el "caso Snowden".

Como es bien sabido, su protagonista ha sido Edward Snowden, un joven profesional informático, ahora exiliado en Rusia, que estuvo empleado en las dos principales agencias de espionaje[1] estadounidenses, la CIA (*Central Intelligence Agency*) y la NSA (*National Security Agency*). En el mes de mayo, Snowden filtró al periódico británico The Guardian detalles de los programas de vigilancia e intrusión masivas sobre las redes de telecomunicaciones de todo el mundo llevados a cabo por la citada NSA en colaboración con sus homólogas británica GCHQ (*Government Communications Headquarters*) y alemana BND (*Bundesnachrichtendienst*); también, según analistas bien informados, con otras agencias de espionaje de países aliados de los EEUU.

Este asunto puede ser contemplado desde muchos puntos de vista, por ejemplo sus aspectos políticos, su impacto sobre la privacidad, el difícil equilibrio entre libertad y seguridad e incluso la opinión que se pueda tener sobre Snowden (¿un traidor a su patria?, ¿un oportunista ansioso de notoriedad?, ¿un defensor de los derechos a la intimida y a la libertad de expresión?). Sin embargo, en este editorial vamos a concentrarnos sobre todo en lo que se refiere a la ruptura por los citados organismos de los sistemas cifrados de seguridad usados para proteger la privacidad de los ciudadanos en el uso de las diversas herramientas de telecomunicación disponibles.

Según The Guardian, los métodos utilizados "*incluyen medidas ocultas para asegurar el control por parte de la NSA de la definición de los estándares internacionales de cifrado, el uso de superordenadores para romper el cifrado por la 'fuerza bruta' y – el secreto mejor guardado de todos – la colaboración con las mismas empresas tecnológicas y proveedores de servicios de Internet. Mediante esta colaboración clandestina, estas agencias habían introducido vulnerabilidades secretas – conocidas como puertas traseras o puertas trampa – en programas comerciales de cifrado*". Y sigue diciendo lo siguiente: "*La NSA hace modificaciones al software y a los dispositivos comerciales de encriptado para poder 'explotarlos' … y obtiene detalles técnicos de sistemas criptográficos comerciales de seguridad de la información a través de sus relaciones con las empresas del sector*".

Estamos hablando de esas mismas empresas que comercializan programas y dispositivos que se ofrecen en el mercado como garantes de la seguridad de ordenadores y redes de de telecomunicaciones. Son empresas que además nos aseguran que nuestros correos electrónicos, nuestras conversaciones telefónicas, nuestros datos bancarios o médicos están cuidadosamente protegidos y no pueden ser descifrados ni por gobiernos ni por delincuentes (en el primer caso a menos que exista una orden judicial que lo permita), puesto que usan protocolos de seguridad de enorme utilización mundial como HTTPS y Secure Sockets Layer (SSL). Sobre ellos, y sobre Voice-Over-IP, han puesto en especial su atención las agencias de espionaje antes citadas y probablemente algunas más con capacidad tecnológica y financiera para hacerlo pero que han tenido la suerte de no ser mencionadas por Snowden.

Se da además la circunstancia de que estos protocolos, programas y dispositivos han sido "hackeados" y ha habido intrusiones masivas en las comunicaciones, principalmente mediante el sistema PRISM, no solamente con el fin, comprensible en alguna medida, de proteger a la gran potencia imperial estadounidense de las amenazas terroristas sino también para fines mucho menos justificables como el espionaje industrial y la interceptación de las comunicaciones de gobernantes y organizaciones de países amigos y aliados, entre ellos la presidenta del Brasil o los comisarios de la Unión Europea.

Existe consenso en la comunidad de Internet sobre que la interoperabilidad global y el carácter abierto de la Red son el fundamento de su utilidad para el avance social y económico del planeta, a la vez que constituyen un elemento esencial para la confianza de los usuarios en la inviolabilidad de sus comunicaciones a través de la misma. Esta confianza está siendo quebrada por la conducta de las citadas agencias de espionaje sin que el principal gobierno implicado, el de los EEUU, haya mostrado su intención de cambiar de conducta.

Por ello es necesario que haya una reacción seria no sólo de los gobiernos y organismos espiados sino, también y sobre todo, de la sociedad civil a través de organizaciones de defensa de los derechos humanos, organizaciones profesionales del mundo de la informática y las telecomunicaciones, de usuarios de Internet, etc.

La gravedad de los hechos denunciados así lo justifica.

***La Junta Directiva de ATI***

### Reacciones sobre este asunto

- Comunicado de la Internet Society: "*Internet Society Responds to Reports of the U.S. Government's Circumvention of Encryption Technology*", <http://www.internetsociety.org/sites/default/files/Internet%20Security%20Statement%20090913.pdf>.
- Comunicado de Privacy International: "*Governments break silence on surveillance as activists launch human rights principles*", <https://www.privacyinternational.org/press-releases/governments-break-silence-on-surveillance-as-activists-launch-human-rights-principles>.

### Nota

[1] La palabra "espionaje" ha sido convenientemente sustituida en los últimos años por "inteligencia", más tranquilizante y políticamente correcta.

# IFIP TC6
# *Latin American Tutorials in Networking* (LATIN 2013)

Ramon Puigjaner Trepat
*Vicepresidente de IFIP; Catedrático Emérito de la Universitat de les Illes Balears; ex-presidente de ATI*
<putxi@uib.cat>

Durante las semanas del 10 y del 17 de junio se celebraron en San José (Costa Rica) y San Salvador (El Salvador) dos sesiones de cursos tutoriales organizados por el Working Group 6.9 (WG6.9: *Communications Networks for Developing Countries*) de la IFIP. En San José se contó con la colaboración de la Universidad de Costa Rica y en San Salvador con la de la Universidad Tecnológica de El Salvador.

En ambos casos, esas universidades proporcionaron toda la infraestructura logística (salas, soporte para la proyección de transparencias, alimentación, etc.) necesaria. En ambos casos se contó con la financiación parcial del *Development Countries Support Committee* (DCSC) de la IFIP y el Centro Latinoamericano de Estudios en Informática (CLEI).

En la sesión celebrada en Costa Rica se impartieron los tutoriales:

- *Introduction to Networking* (9 horas) por el Prof. Augusto Casaca del Instituto Superior Técnico de Lisboa (PT).
- *Social Media Mining* (9 horas) por el Prof. Ricardo Baeza-Yates, VP de Yahoo! Research para Europa, Oriente Medio y América Latina en Barcelona y Profesor a tiempo parcial de la Universitat Pompeu Fabra de Barcelona.
- *Network Security* (6 horas) por el Prof. Tomáš Vaník de la Czech Technical University de Praga (CZ).
- Además, a pesar de no estar programado el Prof. Augusto Casaca impartió una versión reducida del tutorial *Internet of Things* (4 horas) que debía impartir en San Salvador.

A esta sesión de tutoriales asistieron 28 personas al tutorial sobre *Introduction to Networking*, 61 personas al de *Social Media Mining*, 34 personas al de *Network Security*, y 33 personas al de *Internet of Things* procedentes de distintas universidades y empresas, mayoritariamente costarricenses y más especialmente de la zona de San José.

En la sesión celebrada en San Salvador se impartieron los tutoriales:

- *Introduction to Networking* (9 horas) por el Prof. Augusto Casaca del Instituto Superior Técnico de Lisboa (PT).
- *Quality of Service* (QoS) (9 horas) por el Prof. Ramon Puigjaner, catedrático emérito de la Universitat de les Illes Balears.
- *Internet of Things* (6 horas) por el Prof. Augusto Casaca del Instituto Superior Técnico de Lisboa (PT).

A esta sesión asistieron las mismas 45 personas entre estudiantes y profesores de la Universidad Tecnológica de El Salvador y de la Universidad Gerardo Barrios de San Miguel (SV) a los tres tutoriales programados.

## en resumen Soporte al negocio y práctica profesional: El sueño del buen editor

Llorenç Pagés Casas
*Coordinación Editorial de* ***Novática***

Pienso que el sueño de todo editor es conseguir que cada uno de los números de su revista abarque un espectro de temas y contenidos ampliamente variado de tal forma que pueda interesar a toda su tipología de lectores.

De acuerdo con este pensamiento, creo que este número cumple perfectamente con el "sueño" que he descrito.

Soporte al negocio y práctica profesional; herramientas avanzadas y herramientas básicas; artículos de autores de talla mundial y pequeños relatos de experiencias de los lectores.

Estas dualidades diversas, relacionadas con temas y contenidos, quedan perfectamente cubiertas en este número mediante dos grandes bloques: Monografía y Visiones, respectivamente.

Efectivamente, en nuestra monografía titulada "*Minería de procesos*" cuyos editores invitados han sido ***Antonio Valle Salas*** (Socio Director de G2) y ***Anne Rozinat*** (Socia cofundadora de Fluxicon) encontramos la descripción de una prometedora disciplina, de muy reciente aparición, cuyo objetivo es promover técnicas de ayuda al análisis de los procesos empresariales basadas en potentes herramientas informáticas.

Se trata probablemente de la última y más moderna tendencia dentro de ese sinfín de posibilidades que el tratamiento informático ha ido permitiendo con vistas a la mejora de la toma de decisiones empresariales. Con la particularidad de que en ***Novática 223*** hemos podido contar con información y argumentaciones de algunos de los mejores especialistas mundiales, miembros "fundacionales" de este movimiento (una visita a la página que corresponde de la Wikipedia acaba corroborando que este nuestro "sueño" se ha hecho aquí realidad).

Por su parte, el bloque "Visiones sobre lenguajes de programación" se encuentra mucho más centrado en las interioridades de nuestra práctica profesional, a partir del análisis de esos "engranajes básicos de construcción" que para nosotros suponen los lenguajes de programación.

Este bloque se inicia con un magnífico y pormenorizado análisis a cargo de ***Jesús J. García Molina*** sobre cómo la "metáfora de objetos" se ha ido introduciendo en los lenguajes de programación modernos y finaliza con algunos breves relatos de experiencias personales que nos han enviado nuestros lectores. Mientras que, en la mitad del bloque, el lector encontrará un estudio detallado a cargo de ***Óscar Belmonte Fernández*** y ***Carlos Granell Canut*** sobre los resultados de la encuesta sobre el uso de los lenguajes de programación que promovimos hace pocos meses y que recibió un número bastante significativo de respuestas.

Por último, señalemos que, como viene siendo habitual, las aportaciones de nuestros coordinadores de secciones técnicas en sus "Referencias autorizadas" nos han acabado de ayudar a configurar un número rico en temas y perspectivas.

Como conclusión, siendo éste uno de nuestros números soñados, esperamos y deseamos que contribuya también al "sueño" de nuestros lectores de encontrar aquí los contenidos que más puedan interesarles.