

EDITORIAL

De nuevo se acerca el congreso internacional de COMMON Europe. El CEC 2010 se celebrará del 12 al 15 de junio en Stratford-on-Avon, una ciudad pequeña pero con gran encanto y mucha historia. El comité técnico ha preparado una agenda muy completa con contenidos para todos los gustos (gestión de sistemas, desarrollo de aplicaciones, domino, AIX, redes, etc.). Además contará con una exposición en la que tradicionalmente encontramos los productos más novedosos.

El congreso contará con ponentes internacionales de máximo nivel. Auténticos expertos en la materia llegados directamente desde los laboratorios de IBM, que nos explicarán con detalle las nuevas funcionalidades, y analistas independientes que nos darán la visión de dichos productos en relación con las necesidades reales de las empresas.

Así mismo, habrá una sala dedicada a los Business Partners y a los miembros de la Academic Initiative, en la que habrá charlas dirigidas especialmente a estos colectivos, los partners y los estudiantes de iSeries.

Contenido:

Editorial	1
Supercomputación para un mundo más inteligente	3
Noticias cortas	5
Eventos	12

“Creo sinceramente que se dan pocas oportunidades de obtener tanta información actualizada a un precio tan competitivo.”

Sabemos que corren tiempos difíciles, en los que hay que mirar con lupa cualquier gasto. Sin embargo, creo sinceramente que se dan pocas oportunidades de obtener tanta información actualizada a un precio tan competitivo, y por ello quiero animaros a que os planteéis asistir o, en su defecto, enviar a alguien de vuestro equipo que pueda sacar buen provecho de un evento de este calibre.

Nos vemos, espero, en Stratford-on-Avon.

Olga Miralles i Mulleras
Presidenta
COMMON Europe España

**Be part of the biggest AS/400
(IBM i) community in Europe!**



Supercomputación para un mundo más inteligente

“Hace pocos días IBM anunció en Alemania la construcción de la primera máquina que superará el Petaflop en Europa”

Si los 6,700 millones de habitantes del planeta utilizásemos un ordenador personal sin descanso las 24 horas del día, tardaríamos 46 años en hacer lo que el superordenador más potente del mundo, ubicado en Estados Unidos, puede realizar en un solo día. Su anuncio, hace apenas 8 meses, supuso un hito en el mundo de la tecnología, al ser la primera máquina capaz de superar la barrera de 1 Petaflop (1.000 billones de operaciones por segundo). Hace pocos días IBM anunció en Alemania la construcción de la primera máquina que superará el Petaflop en Europa. Ese récord quedará muy atrás en el año 2.012, cuando entre en funcionamiento Sequoia, un superordenador 20 veces más potente, anunciado a principios de febrero por IBM, que ofrece más capacidad de proceso que la suma de los 500 ordenadores más potentes del mundo (la actual lista Top500).

La imparable evolución de la tecnología ha hecho que hoy dispongamos de superordenadores incluso en el salón de nuestra casa: es significativo que hace apenas 6 años, una PlayStation 3 hubiera podido formar parte de la lista Top500.

El desarrollo de superordenadores cada vez más potentes es necesario para dar respuesta a los retos científicos actuales. Por ejemplo, en el terreno sanitario, son capaces de crear modelos de las proteínas de los distintos órganos humanos para analizar sus interacciones con diversos tipos de fármacos. Utilizando tan sólo una pequeña parte de la potencia de la máquina más potente del mundo, los investigadores podrían realizar en una tarde ensayos clínicos simulados en 27 millones de pacientes.



El futuro cercano de la supercomputación nos permitirá resolver, de forma mucho más precisa, modelos matemáticos complejos que permitirán simular una realidad, la interacción de la misma con su entorno y predecir su evolución en el tiempo. Es difícil imaginar los avances que puede llevar su aplicación, por ejemplo, al campo de la genética, al estudio de las proteínas y sus interacciones a nivel molecular, o a la investigación de la propagación de epidemias o incendios. La predicción de riesgos asociados a la climatología (terremotos, tsunamis, tornados) o al sector financiero (gestión de activos en tiempo real) podría dar un salto cualitativo.



En España existen ya varios centros de supercomputación. Sin duda un entorno de vanguardia en este campo se encuentra en el Centro Nacional de Supercomputación de Barcelona, que desarrolla junto a IBM el proyecto MareIncognito. Su objetivo es definir las características y el diseño de superordenadores con capacidad de cálculo superior a 10 Petaflops. Estas máquinas multiplicarán por cien la potencia de su superordenador MareNostrum, el más potente de España, y permitirán abordar temas tan complejos como el origen del universo, la calidad de los alimentos o la eficiencia de las fuentes y procesos energéticos. Otros proyectos de supercomputación interesantes acaban de arrancar recientemente en Madrid, el País Vasco y Canarias.

Es indudable que esta ciencia pone a nuestro alcance la posibilidad de construir un planeta más inteligente. Sus avances presentes y futuros permitirán abordar nuevos problemas y también dar respuesta a los retos científicos actuales, algo que sin duda redundará en el beneficio de la humanidad.

Publicado en El Mundo el 31.03.09

“Es indudable que esta ciencia pone a nuestro alcance la posibilidad de construir un planeta más inteligente”

Nieves Delgado.
Vicepresidenta de la división de Sistemas y Tecnología de IBM España, Portugal, Grecia e Israel

Esta revista es un medio de comunicación de nuestra asociación. Las opiniones en ella expresadas son las de sus autores y no coinciden, necesariamente, con las del Comité Ejecutivo de la Asociación.

NOTICIAS CORTAS

Estas son las diez razones para que la Administración libere software

Permite reducir el déficit, favorece la competitividad y contribuye al desarrollo de una economía sostenible basada en el conocimiento sostenien desde Cenatic, la fundación pública que ha elaborado un decálogo con el que se anima a la Administración a liberar software .

El [Centro Nacional de Referencia de Aplicación de las TIC basadas en Fuentes Abiertas \(Cenatic\)](#) ha publicado un [argumentario](#) que expresa los motivos que deben llevar a las administraciones públicas a **liberar el software considerado de fuentes abiertas** y ponerlo a disposición de toda la sociedad.

Las **diez razones** para que la Administración libere software son las siguientes:

1. Permite **mayor eficiencia presupuestaria** al ahorrar costes en el mantenimiento y en la evolución del software.
2. Cumple las recomendaciones de la Ley 11/2007, del **Real Decreto de Interoperabilidad**, y de las directivas europeas de la ISA.
3. **Favorece la transparencia**, la interoperabilidad, la independencia y la sostenibilidad de las aplicaciones de las Administraciones Públicas.
4. **Desarrolla el ecosistema del sector TIC**, garantizando la independencia de proveedores y su disponibilidad futura.
5. Pone conocimiento y activos a disposición de las empresas.
6. Contribuye a la **reducción del déficit público**, y fomenta el desarrollo de una economía basada en el conocimiento y la innovación.
7. **Mejora la competitividad** al fomentar la cooperación entre administraciones, universidades, centros de I+D+i y empresas, extendiendo buenas prácticas de compartición de conocimiento y fortaleciendo la innovación abierta.
8. Facilita la **adaptación a las necesidades concretas de las administraciones**, en materia lingüística, legislativa, de accesibilidad e imagen.
9. Garantiza la **privacidad** y la seguridad en el tratamiento de la información.
10. Permite **compartir, reutilizar y colaborar**

Enormes retos tecnológicos

“La administración pública española se enfrenta a enormes retos tecnológicos en la actualidad, como son hacer efectivo el acceso electrónico de los ciudadanos a los servicios públicos, permitir la reutilización

“Permite reducir el déficit, favorece la competitividad y contribuye al desarrollo de una economía sostenible basada en el conocimiento ‘”

de información y la interoperabilidad entre administraciones, así como crear los canales necesarios para la participación de la ciudadanía... y ninguno de ellos es fácil", afirma **Manuel Velardo**, director de Proyectos y Servicios de Cenatic. En su opinión, la mejor forma de conseguirlo en un entorno de ajuste presupuestario es la que establece el reciente Esquema Nacional de Interoperabilidad: *"compartir, reutilizar y colaborar"*.

*"El nuevo escenario se caracteriza por un **entorno propicio a la compartición de soluciones**, la reutilización de sistemas y la colaboración entre instituciones, y en este escenario, los sistemas de fuentes abiertas son una herramienta necesaria"*, comenta Manuel Velardo, quien además afirma que las administraciones españolas ya son conscientes de ello, ya que según los datos que manejan en Cenatic *"el **50 por ciento de los grandes sistemas instalados en la Administración utilizan software libre**, el 46 por ciento del software desarrollado por las comunidades autónomas es de fuentes abiertas, y el 80 por ciento de los grandes ayuntamientos españoles tienen iniciativas de software libre"*.

Compartir, reutilizar y colaborar

*"Europa ha invertido ya **1.200 millones de euros en software**, pero aún podría obtenerse un mayor rendimiento de todos estos activos si se logra que las administraciones liberen el software con el que ya cuentan"*, comenta Velardo. *"La liberación o publicación de software es la razón de ser del software libre, y sólo de esta manera es posible acceder a los beneficios de los que hablamos en el argumentario que acabamos de publicar"*.

*"Desde Cenatic entendemos que para alcanzar los beneficios de la liberación de software no es suficiente con su publicación web, sino que es necesario un **correcto modelo de explotación y comunidad** que, promovido por las propias administraciones públicas y con la imprescindible participación del tejido empresarial TIC local y las comunidades de desarrollo, garantice la sostenibilidad del software liberado a través de la transferencia de conocimiento y la correcta gestión de contribuciones"*, añade.

Impulso al software de fuentes abiertas

Cenatic es el proyecto estratégico del Gobierno de España cuya misión es fomentar y difundir las TIC de fuentes abiertas en todos los ámbitos de la sociedad.

Entre sus objetivos está ayudar a que la Administración española aproveche al máximo las oportunidades y ventajas que el software libre y las tecnologías abiertas pueden aportarles. Para ello, cuentan con el conocimiento necesario para asesorar en los procesos de liberación de software, compartición y reutilización entre administraciones públicas, y apoyar de esta manera a sus responsables tecnológicos en la toma de decisiones. El [documento](#) que Cenatic ha presenta-

"Cenatic es el proyecto estratégico del Gobierno de España cuya misión es fomentar y difundir las TIC de fuentes abiertas en todos los ámbitos de la sociedad"

do es parte de este proceso de asesoramiento, dentro del proyecto Comunidad de Conocimiento Compartido.

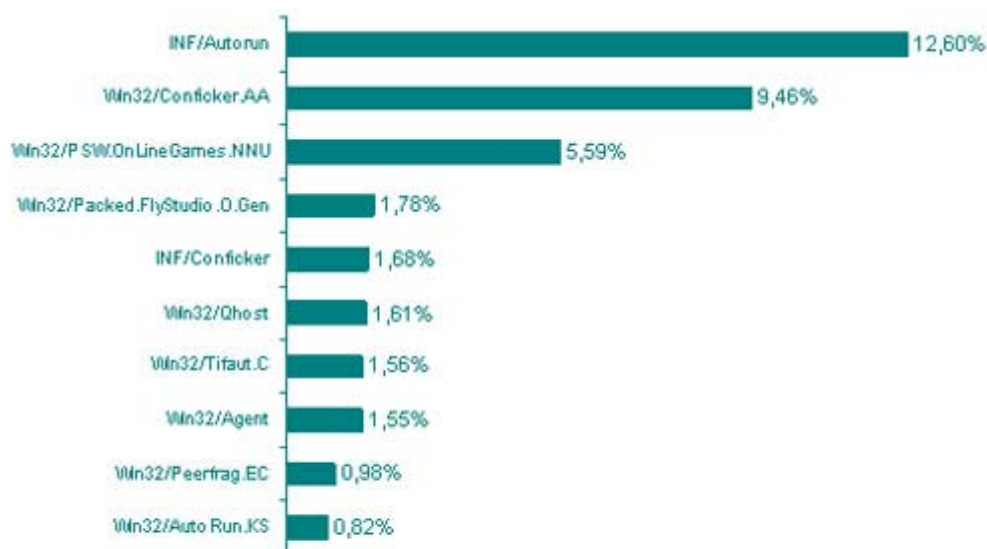
La desarticulación de dos grandes botnets, principal tema de seguridad en marzo

Autorun, Conficker y OnlineGames siguen dominando el ranking mensual sobre amenazas más detectadas en España durante el mes de marzo realizado por ESET .

ESET ha publicado su **informe sobre las amenazas más detectadas en España** durante el mes de marzo, que continúa presidido por Autorun, Conficker y OnlineGames, los tres códigos maliciosos más prevalentes en nuestro país durante el último año.

A pesar de que las tres formas de malware dominantes siguen siendo las mismas, ESET ha constatado un aumento en el porcentaje de detección de aquellas amenazas que utilizan la **función de autoarranque de Windows (Autorun)** cuando el usuario introduce un medio extraíble (como memorias USB, teléfonos móviles o dispositivos MP3), mientras que, por otra parte, ha bajado el número de amenazas destinadas a robar contraseñas de juegos online. En meses anteriores, por el contrario, las tres amenazas mantenían niveles de detección similares entre sí, y muy superiores a los del resto de integrantes del ranking.

El **cuadro de las amenazas más detectadas** durante el mes de marzo en España queda de la siguiente forma:



Códigos maliciosos más detectados en España / Marzo 2010

“Autorun, Confickerr y OnlineGames siguen dominando el ranking mensual sobre amenazas más detectadas en España durante el mes de marzo realizado por ESET”

Botnets desarticuladas y los atentados de Moscú

El mes de marzo se inició con el **desmantelamiento de dos de las redes de ordenadores zombies, o botnets**, más grandes conocidas hasta la fecha, como fueron Waledac y Mariposa. Esta última estaba controlada por tres usuarios españoles y se calcula que controlaba a **13 millones de ordenadores** zombies. Las botnets siguen siendo una amenaza en auge aunque mucha gente aun desconoce su existencia y funcionamiento.

Para **Josep Albors**, responsable del departamento técnico de Ontinet.com, "hay tres cosas que pueden interesar a los ciberdelincuentes que crean y gestionan las botnets: el **procesador del equipo** atacado, que puede ser usado en beneficio de la botnet para ejecutar procesos no autorizados por el usuario; la cantidad de **memoria en el disco duro** de la máquina, que puede ser usada para almacenar todo tipo de ficheros sin que el usuario lo sepa; y la **conexión a Internet** de nuestro ordenador, como posible vía de salida para el envío de spam, códigos maliciosos o ataques de denegación de servicio".

Por otro lado, aprovechando la [ceremonia de los Oscar](#), los creadores de malware siguieron haciendo uso de técnicas de posicionamiento en buscadores para colocar sus creaciones entre los primeros resultados en las búsquedas de información sobre el evento realizadas por los usuarios. Esta técnica también se ha utilizado en la última parte del mes en relación a los [atentados en el metro de Moscú](#).

Navegadores, sistemas operativos y falsos antivirus

Los navegadores de Internet también han visto como han aparecido parches críticos para [solucionar graves vulnerabilidades](#). Primero fue **Microsoft** quien informó de una vulnerabilidad en las versiones 6 y 7 de su navegador Internet Explorer, lanzando un parche fuera del ciclo habitual de actualizaciones para solucionarla.

Pero no fue la única compañía en hacerlo. Durante marzo también se detectaron varios agujeros de seguridad en los **navegadores Opera y Firefox**. La fundación Mozilla publicó una actualización relativamente rápida para solucionar las vulnerabilidades que afectaban a su navegador, distribuyendo los [parches en la versión 3.6.2](#) del mismo.

Marzo fue también el mes en el que **Apple** decidió lanzar una gran [actualización para su sistema operativo, Mac OS X](#), que solucionaba hasta 65 fallos de seguridad, alguno de ellos de una antigüedad considerable. Con la popularización de los dispositivos de Apple, cada vez son más los creadores de malware que se fijan en ellas y esperamos ver más ataques a las mismas durante los próximos meses.

Por último, los falsos antivirus siguen con su campaña de propagación y engaño a los usuarios, destacando este mes casos curiosos como aquellos que usan [nombres de conocidas firmas de seguridad](#) para propiciar que los usuarios descarguen sus creaciones, y otros que aluden a aumentar la [seguridad en redes sociales](#) para conseguir sus objetivos.

"Autorun, Confickerr y OnlineGames siguen dominando el ranking mensual sobre amenazas más detectadas en España durante el mes de marzo realizado por ESET"

Los diez mandamientos de la seguridad para los usuarios de teléfonos móvil

Tomar conciencia de que los móviles son equipos informáticos que pueden ser atacados es la clave para mantener un elevado nivel de seguridad. ESET ofrece un decálogo a los usuarios para que protejan mejor sus teléfonos .

El mercado de la telefonía móvil ha evolucionado en los últimos años para pasar de ofrecer a los usuarios un simple terminal desde el que poder hacer llamadas a pequeños equipos informáticos que, además, permiten establecer conexiones telefónicas. Convertidos en auténticos **ordenadores personales**, los actuales equipos de telefonía móvil deben ser tratados como tales, y también desde el punto de vista de la seguridad.

Decálogo para un móvil seguro

Dado que estos *'pequeños ordenadores'* se han vuelto más comunes y con unas características más sofisticadas, se han convertido también en víctimas potenciales a los ataques. [ESET](#) ha elaborado un decálogo de **hábitos básicos de seguridad** para que los usuarios mantengan la protección e integridad de los datos que almacena y transmiten a través de sus teléfonos móviles:

1. **Active el acceso a su dispositivo mediante PIN.** Si su terminal lo permite, establezca también un código para el desbloqueo del mismo, de forma que se impida su uso por parte de terceros, así como el acceso a los datos almacenados en caso de pérdida o robo.
2. **Realice una copia de seguridad de los datos de su terminal.** Le permitirá tener a salvo los datos de agenda, fotos, vídeos, documentos almacenados, descargas realizadas, etc., y poder restaurarlos en caso de que el teléfono sea infectado.
3. **Active las conexiones por bluetooth, infrarrojos y WiFi sólo cuando vaya a utilizarlas,** de forma que no se conviertan en puertas abiertas constantemente a posibles atacantes. Si su modelo lo permite, establezca contraseñas para el acceso a su terminal a través de estas conexiones. Además, para evitar rastreos, establezca la conexión Bluetooth de manera que no se muestre públicamente el teléfono, lo que se conoce como "modo oculto".
4. Asegúrese siempre de que los **equipos a los que se conecta están limpios** y no le transmitirán archivos infectados.
5. No inserte tarjetas de memoria en su terminal sin haber comprobado antes que están libres de ficheros infectados.
6. **Descargue sólo aplicaciones de sitios de confianza o de las tiendas oficiales** (como Apple Store, Ovi de Nokia, etc.) y certificadas por los fabricantes.

“Dato que estos *'pequeños ordenadores'* se han vuelto más comunes y con unas características más sofisticadas, se han convertido también en víctimas potenciales a los ataques”

“es clave que sea consciente de que su teléfono puede ser vía de infección para otros equipos y también objetivo de los cibercriminales, dado el creciente uso que hacemos de estos aparatos para realizar cada vez más actividades online”

7. **No acceda a los enlaces facilitados a través de mensajes SMS/MMS no solicitados** y que impliquen la descarga de contenidos en su terminal.
8. **Desconéctese siempre de los servicios web** que requieran contraseña antes de cerrar su navegador web.
9. Instale un software antivirus que le permita la detección proactiva de amenazas en su terminal, de forma que impida su ejecución y transmisión a otros equipos.
10. **Conozca y apunte el número IMEI** (*International Mobile Equipment Identity*, Identidad Internacional de Equipo Móvil) de su teléfono. Este número, único para cada móvil en todo el mundo, permite a las operadoras desactivar el teléfono en caso de robo, incluso si se le cambia la tarjeta SIM. Para ver ese código, marque ***#06#** . El teléfono le devolverá el código IMEI.

*“Como en otros ámbitos de la seguridad informática, la principal vía de infección del equipo suele ser siempre el propio usuario, bien por mostrarse confiado o bien por desconocimiento, de forma que es clave que sea consciente de que su teléfono puede ser vía de infección para otros equipos y también objetivo de los cibercriminales, dado el creciente uso que hacemos de estos aparatos para realizar cada vez más actividades online”, reflexiona **Fernando de la Cuadra**, director de Educación de Ontinet.com, distribuidor exclusivo de ESET en España.*

CONTACTOS

* Si estás interesado en recibir la **revista de Contact Center**, remítenos un correo electrónico a info@common-es.org con los siguientes datos: empresa, nombre y apellidos de la persona que desea recibir la revista, cargo que desempeña en su compañía y la dirección completa de la misma.

* Si quieres recibir información o estás interesado en celebrar una presentación en el **IBM FORUM** puedes ponerte en contacto con Carmen Torres en carmentorres@es.ibm.com o llamar al 91 397 7358. También tienes información en <http://www.ibm.com/es/events/centers/madrid>.

Os recordamos que el IBM FORUM **ofrece un 10% de descuento a los miembros de Common** que utilicen cualquiera de los servicios del IBM Forum de Madrid

PROXIMOS EVENTOS COMMON

12—15 de Junio. COMMON EUROPE CONGRESS 2010

Stratford Upon Avon/ UK

Este año el Common Europe Congress se celebrará en UK, Stratford upon Avon del 12 al 15 de Junio.

Toda la información con al agenda y precios está en la página web de Common Europe www.comeur.org.

Los que tengan intención de asistir a este evento, hay precios especiales. Se ha ampliado la fecha de inscripción hasta el 21 de Abril.

En nuestra página web www.common.es encontrarás más información sobre estas sesiones.

“En nuestra página web www.common.es encontrarás más información sobre estas sesiones”



C/ Goiri, 30—7º D
 28039 Madrid
 Teléfono: 913.116.114
 Correo: info@common.es
 www.common-es.org

EDICION:

Common Europe España

COMITÉ EJECUTIVO**PRESIDENTE**

OLGA MIRALLES
 EMAIL: olgam@common.es

VICEPRESIDENTE

SANTIAGO PICAZO
SAYTEL SERVICIOS INFORM
 EMAIL: spicazo@common.es

SECRETARIO

ROSARIO RODRÍGUEZ MEGO
IBM ESPAÑA
 EMAIL : charormego@common.es

TESORERO

GUILLERMO ANDRADES
CPI SOFTWARE
 EMAIL: gab@common.es

VOCALES

DEBORA CLAP
CLAP SOLUCIONES INFORM
 EMAIL: debora@common.es

**COORDINACION Y EDICION**

Juan José Casado

SECRETARIA

Alicia Santos

FINES DE LA ASOCIACION:

- Promover entre sus miembros el intercambio de informaciones y experiencias sobre todas las cuestiones relacionadas con la informática.
- Desarrollar coloquios seminarios y reuniones para el estudio de los sistemas de información, que permitan un mejor aprovechamiento de los equipos y materiales existentes en el mercado
- Canalizar las experiencias de los miembros de la Asociación a fin de obtener mejoras en beneficio de los Miembros usuarios
- Establecer relaciones con otras Asociaciones o grupos profesionales, nacionales e internacionales, con actividades iguales o similares
- Realizar cualesquiera otras actividades que, de acuerdo con los objetivos antes enumerados, ayuden a la consecución de los fines previstos.