

EMPRESAS

Acuerdo sobre el ERE de 20 días

RENAULT La dirección y los sindicatos han alcanzado un acuerdo sobre el Expediente de Regulación de Empleo (ERE) con carácter suspensivo de 20 días para la factoría de Carrocería-Montaje de Valladolid, que se aplicará a 2.088 trabajadores entre septiembre y febrero.

Ampliación de capital

ZELTIA Noscira, filial del grupo Zeltia, ha finalizado una ampliación de capital en la que ha captado 2,86 millones de euros, que destinará a financiar las actividades de la compañía durante 2012. Zeltia pasa así de controlar un 70,8% a ostentar un 73,32% del capital de Noscira.

Recompra del 20% en manos de Yahoo!

ALIBABA La empresa china de Internet ha recomprado la mitad de la participación que posee Yahoo! en su capital por 7.600 millones de dólares (5.792 millones de euros). La estadounidense Yahoo! tenía algo más del 40% de Alibaba y ahora conserva un 23%.

Nuevo concepto de tienda en Japón

INDITEX El grupo ha estrenado el nuevo concepto de tienda global en su establecimiento de Ginza, el área más elitista de Tokio. Inditex ha procedido a la redecoración de la tienda, que se inauguró en 2003. En Japón, Inditex cuenta con 84 establecimientos, 78 de ellos de Zara.

Contrato para una planta en México

ACCIONA La compañía ha logrado el contrato para diseñar y construir la primera parte de la planta de tratamiento de aguas residuales El Caracol (México), con una inversión de 47 millones de euros. El contrato incluye la operación y el mantenimiento de la planta durante 23 años.

Acuerdo para la aplicación del ERE

ASSIGNIA La compañía ha alcanzado un acuerdo con los sindicatos sobre la aplicación de un Expediente de Regulación de Empleo (ERE), que afectará a 139 trabajadores (el 11,3% de la plantilla total), de los que 115 son de Assignia en España y el resto, de su filial EOC.

Las empresas refuerzan su inversión en tecnología para frenar a los 'hackers'

SEGURIDAD INFORMÁTICA/ Las grandes organizaciones destinan ya más de un millón de dólares diarios a mejorar sus tecnologías de la información. Desde el sector, insisten en que "no hay alternativa".

E. Arrieta. Madrid

Cada semana, las grandes organizaciones de EEUU, China e India invierten un millón de dólares en proteger la información confidencial en sus filiales extranjeras. En estos países, la inversión en tecnologías de la información supera ya el millón de dólares diario, según cifras de McAfee.

En Europa, y en especial en España, estas cuantías son menores, pero igualmente suponen una parte importante del presupuesto. Sólo en Reino Unido, el cibercrimen les costó a las empresas británicas 21.000 millones de libras (25.983 millones de euros) en 2011.

"Hasta ahora, las empresas han percibido la seguridad de sus sistemas como un gasto, cuando, en realidad, la pérdida de información o la caída de su servicio puede costarles mucho más", declara Gunter Junk, director de EMEA de la empresa de seguridad informática Sophos. "No hay otra alternativa que tomarse en serio la protección de los sistemas que, en definitiva, computan o almacenan la información más crítica de una compañía", insiste.

Más riesgos

La amenaza es real y se extiende conforme se profesionalizan los ciberdelincuentes, ya sean *hacktivistas* (activistas políticos que operan en la Red) o *hackers* con ambiciones económicas.

Los riesgos aumentan también a medida que los trabajadores emplean un mismo dispositivo (PC, móvil o tableta) para trabajar y para un uso de entretenimiento, como por ejemplo acceder a Facebook o navegar por Internet. Según el organismo Inteco, dependiente del Ministerio de Industria, el *malware* orientado



Los 'piratas' de Anonymous han protagonizado varios ataques informáticos.

Microsoft advierte de un fallo en Internet Explorer

Microsoft ha advertido sobre un fallo de seguridad en su navegador web Internet Explorer. La compañía insta a los clientes a descargar un software para reducir el riesgo de infección, como medida provisional. El fallo afecta a cientos de millones

de usuarios. La herramienta de seguridad es gratuita y se conoce como el kit de herramientas Enhanced Mitigation Experience Toolkit (Emet), que está disponible a través de la página web de Microsoft. Internet Explorer fue el segundo navegador

más utilizado del mundo el mes pasado, con una cuota del 33%, por detrás de Chrome (de Google), con el 34%, informa Europa Press. La Unión Europea estaría preparando una investigación sobre posibles prácticas anticompetitivas en el sector.

a la comisión de fraude está presente en más de un tercio de los equipos de los hogares españoles. Y, precisamente, entre el 93% y el 94% del *malware* en un ordenador procede de haber entrado en una página web infectada.

El debate que se abre aquí es cómo alcanzar el equilibrio entre la eficiencia (los dispositi-

vos móviles permiten una mayor agilidad) y la seguridad de la información corporativa. Esta nueva amenaza, conocida en el sector como BYOD (*bring your own device*), se puede solventar a través de software de seguridad y de un control de los dispositivos por parte de los departamentos de Sistemas.

"El 78% de las empresas tienen BYOD sin saberlo o sin haberlo permitido de forma explícita. Se trata de una tendencia que es necesario abordar cuando antes pero que no tiene sentido prohibir, puesto que no va a desaparecer", opina Santiago Cordero, director de Consultoría y Preventa de T-Systems España.

Makro invierte 75 millones en tres aperturas este año

J.B. Valencia

La cadena de *cash and carry* Makro ha destinado este año unos 75 millones de euros a la apertura de nuevos establecimientos. La compañía ha abierto ya uno en Madrid y en las próximas semanas abrirá los de Elche (Alicante) y Alcalá de Guadaíra (Sevilla). Cada uno de ellos con una inversión de veinticinco millones de euros, según explicó ayer el director general, José María Cervera, durante un encuentro en Valencia para celebrar el 40º aniversario de la empresa.

El directivo destaca que, con estas aperturas, la empresa registra este año una creación de empleo neto del 10%, hasta 3.450 personas, aunque en los años anteriores también venía creciendo entre un 2% y un 5%.

Makro, que el año pasado facturó 1.289 millones de euros, tiene actualmente 34 centros en España y con la ampliación de este año da, de momento, por cerrado su plan de aperturas.

El grupo ha aumentado también el peso de la marca propia, que el año pasado aumentó del 21% al 23% de sus ventas.

Exportación

Cervera reveló que Makro tiene en Valencia su centro de exportación de productos alimentarios de España para el resto de sus tiendas europeas. La división se denomina Valencia Trading Office y se creó en el año 2010. El pasado ejercicio tuvo un volumen de ventas de 44 millones de euros y las expectativas para este ejercicio son las de duplicar ese nivel. Trabajan en ella actualmente 27 personas y está en proceso de ampliación de plantilla. Esta división arrancó para exportar cítricos, pero pronto amplió su gama a otras frutas y también a las verduras.

Nuevos riesgos

● **Movilidad:** el hecho de que los trabajadores usen sus PC o móviles para trabajar sin un control previo de la empresa, abre una puerta a los *hackers*.

● **Cloud computing:** esta modalidad será segura siempre que las empresas verifiquen la profesionalidad y las condiciones que les ofrece su proveedor tecnológico, como constatan desde Arsys.

● **Crimen organizado:** ciertas mafias han creado en la Red un negocio que ya genera más dinero que las drogas y del que cualquier empresa o particular puede ser víctima.

● **Hacktivismo:** este movimiento tiene como principios el anonimato y la libre distribución de información por la Red. Entre estos grupos se encuentran Anonymous o Luzsec, pero no son los únicos, recuerdan desde ISMS Forum.

Al mismo tiempo, Bruselas prepara ya la que será la norma en materia de protección de datos dentro de dos años.

Mientras, desde ISMS Forum Spain (Asociación Española para el Fomento de la Seguridad de la Información), reclaman a la Administración una campaña de concienciación ciudadana y "más apoyo público a las pymes para poner en marcha sus estrategias de seguridad", en palabras del presidente de ISMS, Gianluca D'Antonio. "El tardío reconocimiento de la importancia estratégica de disponer de un ciberespacio seguro ha provocado, entre otras cosas, que el Gobierno no haya creado aún un sistema de ciberseguridad nacional completo", critican desde esta asociación.