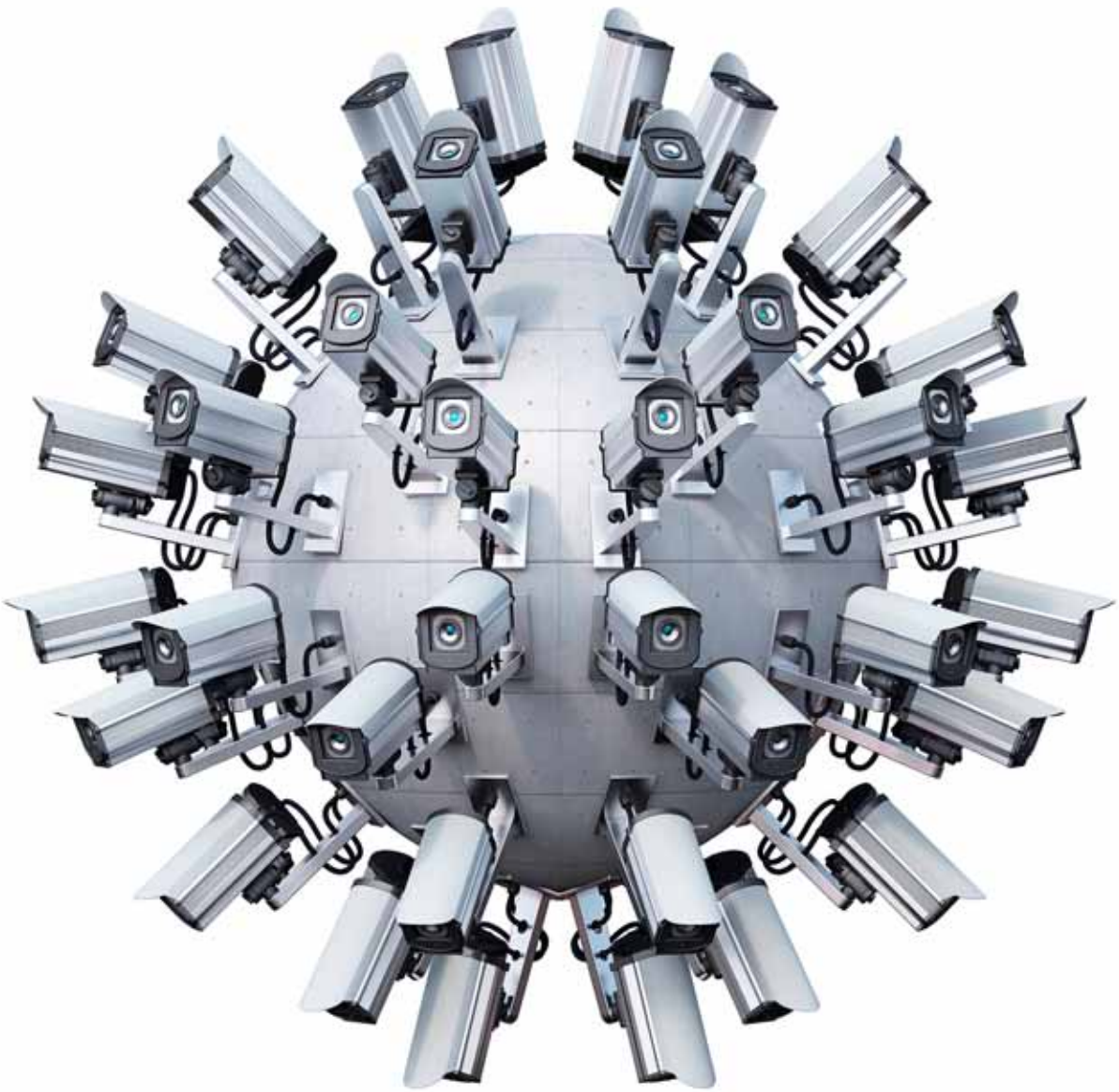
AESPECIAL

SEGURIDAD



CON LOS OJOS BIEN ABIERTOS

Las empresas confían en que la nueva Ley de Seguridad Privada, aprobada ya por el Consejo de Ministros, beneficie a un sector que sufre el descenso de contratos con la Administración y la caída de los precios.

EN 2012, LAS COMPAÑÍAS FACTURARON UN 10% MENOS QUE EL AÑO ANTERIOR, ROZANDO LOS 2.900 MILLONES DE EUROS PÁGS. 2-3 LOS SERVICIOS GIRAN EN TORNO A LA UNIÓN DE VIGILANCIA FÍSICA Y ELECTRÓNICA Y LAS ÚLTIMAS TECNOLOGÍAS DE IMAGEN PÁG. 4 FORMAS DE COMBATIR EL CIBERCRIMEN, UN TIPO DE DELITOS QUE CUESTA A ESPAÑA 19.000 MILLONES AL AÑO PÁGS. 6-8

Personal de seguridad en las oficinas centrales de Securitas, en Madrid.

EN 2012, LA FACTURACIÓN DEL SECTOR CAYÓ UN 10%, HASTA QUEDARSE POR DEBAJO DE LOS 2.900 MILLONES DE EUROS

UN BLINDAJE PARA EL FUTURO

LAS COMPAÑÍAS ESTÁN SATISFECHAS CON LA NUEVA LEY DE SEGURIDAD PRIVADA, ACTUALMENTE EN TRÁMITE PARLAMENTARIO, QUE RECONOCE AL VIGILANTE COMO AGENTE DE LA AUTORIDAD Y POTENCIA SU COLABORACIÓN CON LAS FUERZAS PÚBLICAS

POR MARÍA JOSÉ GÓMEZ-SERRANILLOS

Era necesaria porque los tiempos y, con ellos, las necesidades, han evolucionado. Es la sensación generalizada en torno a la nueva Ley de Seguridad Privada, cuyo proyecto de ley aprobó el Consejo de Ministros el pasado junio y que se encuentra en trámite parlamentario. El sector llevaba años demandando la reforma de la ley, vigente desde 1992, y está satisfecho con el nuevo marco. "Incorpora el reconocimiento del vigilante de seguridad como agente de la autoridad y potencia la colaboración entre éstos y las fuerzas de Seguridad del Estado", subraya Ángel Córdoba, presidente de la patronal Aproser. "La norma es más abierta que la anterior. También contempla la ampliación de las zonas de acción de los vigilantes a espacios como las calles aledañas a tiendas y centros comerciales que disponen de seguridad. Antes, su marco de vigilancia se limitaba al interior de los espacios", explica. Uno de los casos más recientes de esta ampliación se dio en la pasada festividad de San Juan en las playas de Cádiz, donde el Ayuntamiento contrató seguridad privada para actuar junto a la Policía Local y Nacional.

EN LOS ÚLTIMOS AÑOS LOS PRECIOS DE LOS SERVICIOS SE HAN REDUCIDO EN TORNO A UN 15%. LAS FIRMAS SE VEN OBLIGADAS A AJUSTAR EL PRESUPUESTO SIN PERDER CALIDAD

Con la nueva legislación a las puertas, el sector mira adelante en un momento delicado por la caída del negocio y por unas presiones sobre el precio cada vez mayores. Según Aproser, en 2011 la facturación fue de 3.215 millones de euros, lo que supuso una caída del 5% frente a 2010 y del 25% en relación al inicio de la crisis, en 2008. "Estimamos que la caída llegó al 10% en 2012 respecto al año anterior", apunta Córdoba.

Las compañías se enfrentan al desplome de los contratos con la Administración y a una exigencia cada vez mayor del cliente por seguir contratando seguridad de calidad, pero a un coste muy ajustado. "Los precios han caído en torno a un 15% en los últimos años", apunta Luis Posada, consejero delegado de la sueca Securitas, presente en España desde 1992. "Los servicios en la Administración, uno de los clientes tradicionales, se han reducido entre un 20% y un 25%", añade. "Estamos haciendo un gran esfuerzo por adecuar la tarifa de los servicios a los clientes, sin que se resienta la eficacia. Además, nos estamos adaptando a la nueva mentalidad de las compañías sobre seguridad: la cobertura debe combinar vigilancia física con sistemas tecno-

lógicos. Antes se basaba la seguridad sólo en la vigilancia física", explica. Securitas tiene una facturación anual de 510 millones de euros en España y una plantilla de 17.000 empleados. El metro de Barcelona, el aeropuerto de Barajas y El Corte Inglés son algunos de sus clientes.

Las españolas Eulen Seguridad y Grupo Norte intentan igualmente reenfocar sus negocios para no perder clientes. Estas compañías juegan con la ventaja de pertenecer a grupos con otras divisiones de negocio como servicios de limpieza y catering, que pueden equilibrar áreas más afectadas por la caída de las ventas. Alberto García, director de Grupo Norte, explica que la estrategia actual de la firma vallisoletana es la expansión nacional, para pasar de ser una empresa focalizada en Castilla y León a tener presencia en Madrid, Galicia, Castilla-La Mancha y Barcelona. "Conseguimos crecer cuatro millones de euros el pasado año, hasta los 26 millones", subraya. Entre otras, la compañía presta servicio a las plantas españolas de Leche Pascual y Campofrío.

PROSEGUR, LÍDER DEL NEGOCIO EN ESPAÑA, INVIRTIÓ 288 MILLONES DE EUROS EN LA COMPRA DE NUEVE EMPRESAS EN MERCADOS COMO ALEMANIA, BRASIL Y CHINA DURANTE 2012

Ya consolidada en el mercado español y con unas ventas de 312 millones en 2012, Eulen Seguridad está focalizando gran parte de sus esfuerzos en los otros 13 países donde tiene presencia, que aportan el 25% del negocio. "Nuestra intención es alcanzar el 50% en 2015. Chile y México son mercados que están funcionando muy bien, y estamos empezando a trabajar en los países árabes, prestando servicios en plataformas petroleras y barcos de defensa", explica Emilio García, director de la compañía.

Desde hace años, el negocio exterior es un pilar clave en la estrategia del líder nacional, Prosegur, con 943 millones de euros en España el pasado ejercicio. La compañía ha comprado varias empresas en los últimos años en Alemania, Brasil, India, Singapur y China. "En 2012, Prosegur adquirió nueve firmas por un importe que ascendió a los 288 millones de euros", señalan desde la empresa. Con una trayectoria de más de 35 años de historia, Prosegur tiene una plantilla de 150.000 empleados en 16 países. Una de sus señas de identidad es su esfuerzo por ofrecer continuamente los últimos sistemas tecnológicos.

La unión de fortalezas también es clave para el grupo Seguriber Umano, nacido de la unión de ambas firmas en 2012. La compañía ingresó 148 millones de euros el pasado año y cuenta con 5.240 empleados. Dada la fuerte atomización del sector en España, integrado por casi 1.500 compañías, las sinergias de este tipo permiten duplicar y fortalecer capacidades, aseguran desde la firma. ■

PROTECCIÓN CON SELLO DE GARANTÍA

Garantizar la calidad del servicio y frenar el intrusismo del que siempre ha adolecido la profesión son los fines principales que persigue la Especificación Técnica, promovida recientemente por la patronal Aproser y desarrollada por Aenor. Su presidente, Ángel Córdoba, explica que "se trata de una certificación que distingue a las firmas de seguridad que cumplen la legalidad vigente". Teniendo en cuenta la prácticas dudosas de muchas empresas del sector, ligadas a la falta de licencia, la carencia de contratos de sus vigilantes o los salarios dudosos, esta certificación supone un reconocimiento a las compañías que se desmarcan de estos abusos. "Las 12 empresas integrantes de Aproser ya cuentan con ella, y está abierta a cualquiera que desee tenerla con el fin de demostrar su buen hacer", añade Córdoba. "Con ella se protege tanto las condiciones laborales de los vigilantes de seguridad, como al cliente, ya que se le ofrecen unos servicios adecuados y profesionales", subraya Córdoba. La patronal ha estado trabajando durante dos años en esta garantía, detectando los puntos de mejora, y ha confiado su desarrollo a Aenor, certificadora líder del mercado español.

LAS TECNOLOGÍAS DE LA IMAGEN HAN REVOLUCIONADO LOS DISPOSITIVOS QUE CONTRATAN LAS EMPRESAS

ESPECIALIZARSE ABRE PUERTAS

LA CRISIS LLEVA A LAS COMPAÑÍAS DEL SECTOR A CONJUGAR MÁS QUE NUNCA LA VIGILANCIA FÍSICA Y ELECTRÓNICA, ASÍ COMO A ACUMULAR EXPERIENCIA EN ÁREAS CONCRETAS DE ACTIVIDAD COMO ESTRATEGIA PARA DIFERENCIARSE DE LA COMPETENCIA

POR ANA ROMERO

Los responsables de las empresas de seguridad buscan productos y servicios con los que satisfacer a una clientela empresarial que, apurada por la crisis, mira cada céntimo que gasta. Las compañías apuestan por combinar sistemas de seguridad tradicionales –vigilancia física– con dispositivos tecnológicos.

Juan Jerez y Rafael Villarías, directores de Sistemas en Eulen y Grupo Norte, respectivamente, explican que las firmas tratan de ofrecer productos integrales, que dan apoyo al servicio del vigilante y mitigan el coste del trabajo presencial, tratándose de opciones complementarias, no sustitutivas. En este contexto, ¿ha habido recientemente algún avance técnico que haya cambiado el desarrollo de las labores de vigilancia? El caldo de cultivo en el que evolucionan las propuestas de las empresas son el actual mundo de redes de comunicación y la tendencia a la integración de los sistemas, con un peso creciente de los centros de procesado de datos. Los responsables de Seguriber Umano opinan que en los últimos años se han producido dos hitos importantes: la mejora de la red de transmisión de comunicaciones y el uso de la imagen. Jerez puntualiza que las tecnologías audiovisuales aplicadas a la seguridad constituyen el motor de la innovación en el sector. En el terreno de la identificación, se están acabando las contraseñas y los códigos de acceso. "Es tiempo de tarjetas inteligentes sin contacto y de sistemas biométricos de reconocimiento del iris, la huella dactilar o el rostro", recuerda el experto de Eulen.

TYCO DESARROLLA UN SISTEMA BASADO EN LA RADIOFRECUENCIA Y DIRIGIDO AL NEGOCIO DE LA DISTRIBUCIÓN, MIENTRAS QUE GRUPO NORTE APUESTA POR DAR SERVICIO A NUCLEARES

Es tiempo de tarjetas sin contacto y sensores biométricos, como el de la imagen./ A. D.

La especialización para ofrecer servicios adecuados a determinados sectores empresariales es otra de las apuestas de las firmas para diferenciarse de la competencia. Así, por ejemplo, Ricardo Arroyo, director general de Tyco, explica que una de las últimas iniciativas que desarrolla el grupo es un sistema de seguridad basado en la radiofrecuencia y dirigido al negocio de la distribución. "Se trata de un chip de control del producto que combina la seguridad y la información de control del almacén", indica.

Grupo Norte, que tiene experiencia en hospitales y centros de transformación eléctrica, entre otros sectores, también pone el foco en prestar servicio a centrales nucleares, área en la que se inició con un contrato con Enusa, empresa dedicada al suministro de uranio enriquecido. Por su parte, Grupo Segur también está avanzando posiciones ofreciendo servicios a las áreas aeroportuaria y energética, entre otras.


Seguridad para tu empresa.
Tranquilidad para ti.
Sólo cuando lo que más te importa está protegido, puedes sentir verdadera **tranquilidad**. En Prosegur te ofrecemos las mejores soluciones integrales de seguridad para tu **empresa**. Y tú sólo tendrás que preocuparte de disfrutar cada instante de tu vida.
PROSEGUR
www.prosegur.com

EL CIBERCRIMEN CUESTA A ESPAÑA 19.000 MILLONES DE EUROS CADA AÑO

LA LLAVE DE LA CONFIANZA

LOS ATAQUES A EMPRESAS Y ADMINISTRACIONES SE MULTIPLICAN POR EL AUGE DE LAS TIC, MIENTRAS LA FORMACIÓN INTERNA Y LOS SISTEMAS DE PROTECCIÓN SE REVELAN COMO LAS ÚNICAS VÍAS PARA MINIMIZAR LOS RIESGOS

Los servicios en la nube mejoran la competitividad de las empresas, pero entrañan riesgos de seguridad. / S. PANTELIC

POR **RUBÉN FOLGADO**

Si en la Edad Media los señores feudales se protegían con murallas de varios metros de altura, los ciudadanos y las empresas de la *era Google* se ven obligados a luchar contra enemigos invisibles que incluso son capaces de alterar el curso bursátil de una compañía tan sólo saboteando un perfil de Twitter. El fenómeno de internet ha cambiado radicalmente la manera de entender las relaciones profesionales, pero esa maraña de conexiones y datos ha abierto una gigantesca puerta al intrusismo y al cibercrimen. Según el Centro Nacional de Inteligencia (CNI), España pierde cada año 19.000 millones de euros a causa de los ciberataques y la mayor parte de estos números rojos se debe a robos sufridos por empresas y usuarios privados.

UNO DE LOS MAYORES PELIGROS SON LAS FUGAS INTERNAS, EN LAS QUE LOS PROPIOS EMPLEADOS DE LA COMPAÑÍA FILTRAN DATOS POR CARECER DE SISTEMAS DE CONTROL

"El mayor problema al que se enfrentan compañías y administraciones es su exceso de confianza, porque todas, grandes y pequeñas, pueden ser atacadas", explica Fernando de la Cuadra, director de Educación de Eset España, uno de los mayores proveedores de seguridad informática. "La diferencia que existe es que ahora nos damos cuenta de que nos están espiando. Estas situaciones se han dado siempre, pero ahora el espionaje es casi siempre digital", agrega.

La modernización que ha vivido la economía española ha ido acompañada de una explosión tecnológica sin precedentes que, en muchas ocasiones, no ha obedecido a una planificación meditada. "Muchas compañías se adaptan cada vez más rápido a las nuevas tecnologías, pero no cuentan con el tiempo necesario para implementar los sistemas de seguridad más adecuados", asegura Jorge Hormigos, ingeniero y experto en seguridad de Trend Micro, compañía que ha firmado un acuerdo con Interpol para apoyar programas mundiales sobre ciberseguridad. El responsable recalca que "en la actualidad se dan muchos casos de espionaje industrial porque algunas empresas están muy interesadas en conocer la propiedad intelectual de la competencia".

La adopción del *cloud computing* ha obligado a realizar un esfuerzo extra para que los datos sensibles no acaben en manos indeseadas. "Hay empresas que optan por la nube pero gestionando ellas mismas todos los datos. Otras, en cambio, ceden la custodia de sus datos a terceros. En ese caso hay que asegurarse del nivel de protección que ofrece la empresa que los alojará, ya que puede variar mucho o incluso estar amparada bajo una legislación diferente", agrega Hormigos.

Aunque los ataques desde el exterior son cada vez más virulentos, las principales fugas de información parten desde el interior de las organizaciones. "Es fundamental disponer de controles de seguridad adecuados contra las fugas internas, conocidas como ataques internos, en los que un empleado o una subcontrata acceden a datos y se los llevan sin permiso ni control", explica Marcos Gómez, subdirector de Operaciones del Instituto Nacional de Tecnologías de la Comunicación (Inteco). Gómez destaca las herramientas DPL (*data loss prevention*, prevención de pérdida de datos en inglés), que avisan a la compañía sobre los intrusos que, por error o intencionadamente, sustraen información con un alto valor.

VIGILANCIA ESPECIALIZADA · INNOVACIÓN & TECNOLOGÍA · CONSULTORÍA & DESARROLLO

Un paso más
en soluciones de seguridad

Le ofrecemos una solución de seguridad que se adapta a su negocio integrando diferentes medios de protección y respuesta durante las 24 horas del día. Invertimos en recursos tecnológicos y de diseño de sistemas de seguridad para reforzar nuestra capacidad de proponer soluciones óptimas que abarquen seguridad física, tecnología, vigilancia presencial, control de alarmas y servicios de consultoría e investigación.

Entrepeñas, 27 · 28051 · Madrid · Tel: 91 277 60 00 · **info@securitas.es** · **www.securitas.es**

El auge de las redes sociales ha ayudado a los cibercriminales a crear toda una ingeniería para ganarse la atracción de los usuarios. "Uno de los mayores inconvenientes es que los empleados creen que el ordenador del trabajo es suyo y en realidad pertenece a la empresa. Hay que ser más cautos", subraya de la Cuadra. Otra tendencia que también complica la monitorización y el control de todos los datos que circulan en las empresas es el auge del *bring your own device* (Byod), que supone el uso de móviles y tabletas personales para que el empleado siga conectado a su compañía aunque no se encuentre en ella. "Es muy complicado proteger toda la información sensible que se transfiere con estos dispositivos porque son personales", añade de la Cuadra.

Por estos motivos, los expertos señalan la importancia de la formación continuada de los empleados. "Una mala gestión de los datos y no contar con los mecanismos adecuados de control puede desembocar en un riesgo más probable de materializarse, por eso es muy importante contar con la formación adecuada", explica Gómez, de Inteco. "Hay que pensar que los empleados son usuarios y potenciales objetivos, por eso deben tener una formación continuada para evitar abrir *puertas* en sus equipos", agrega de la Cuadra.

Las estrategias de los piratas virtuales pasan por el clásico *phishing* –recabar datos bancarios o de tarjetas de crédito a través de correos electrónicos engañosos– y llegan hasta el envío masivo de supuestas multas de la Policía Nacional por haber visitado páginas con contenido sexual. Precisamente, el Cuerpo Nacional de Policía (CNP) ha presentado el Plan Policía 3.0, con el que pretende transformar la operatividad de la organización gracias al uso intensivo de las nuevas tecnologías e incluyendo al cibercrimen como uno de los ejes de actuación.

LOS ATAQUES EN ESPAÑA SE HAN MULTIPLICADO POR NUEVE EN SÓLO DOS AÑOS, MIENTRAS LOS EXPERTOS ASEGURAN QUE ES NECESARIO CREAR UN ÓRGANO CAPAZ DE LIDERAR TODA LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

"Los ataques en España han pasado de 458 en 2010 a casi 4.000 en 2012, y en las administraciones públicas se han triplicado. Esto es algo que compromete la competitividad del sistema y la protección del ciudadano", afirma Gianluca D'Antonio, presidente de Isms Forum, una organización que agrupa a las principales compañías de seguridad informática. "Las competencias de la ciberseguridad están repartidas entre muchos departamentos del Gobierno, además de las comunidades autónomas, y se necesita un líder claro para abordar la estrategia", concluye.

UNA 'LIBERTAD' SIN FRONTERAS

Estados Unidos enarbola desde su fundación la bandera de la libertad, pero el escándalo del supuesto espionaje cometido sistemáticamente por su Gobierno ha puesto contra las cuerdas la máxima del país de las oportunidades. La colaboración del gabinete de Obama con gigantes tecnológicos como Apple, Facebook o Google evidencia la falta de control que existe sobre la información que circula por internet. Millones de usuarios y empresas españolas comparten o alojan información personal en servidores de estas compañías sin tener consciencia sobre cómo ha podido ser utilizada. "Hay que leer minuciosamente la política de privacidad de los contratos con empresas extranjeras. La única manera de asegurar una protección de datos correcta es dejarlos en manos de empresas amparadas bajo la jurisdicción española", asegura Fernando de la Cuadra, responsable de Formación de Eset España. "El problema de las filtraciones sólo se soluciona con tecnologías alternativas a las norteamericanas. La mayoría de las herramientas de seguridad con las que se trabaja en Europa tiene base estadounidense y la UE tiene capacidad para desarrollar sus propios productos", agrega Gianluca D'Antonio, presidente de Isms Forum.

En los últimos meses las principales potencias mundiales están moviendo ficha para marcar sus estrategias. EEUU incluso ha acusado públicamente al Gobierno chino de atacar varios servidores y empresas para obtener información sensible. La UE aprobó a principios de año su propio plan, mientras que España presentó en mayo el borrador de la Estrategia Nacional de Seguridad, que dedica un apartado al crimen digital. Además, el ministro de Justicia ha presentado el anteproyecto del Código Procesal Penal, en el cual se contempla la posiblidad de que los jueces autoricen a los cuerpos de seguridad a instalar software malicioso en los sistemas de delincuentes sospechosos.