economistas
Consejo General
RASI Auditores de Sistemas de la Información
Σ economistas y titulados mercantiles

Julio 2013

actualidad RASI

REVISTA RASI · Auditores de Sistemas de la Información

Contenido

Nuevo Consejo General de Economistas

De acuerdo con la disposición transitoria segunda de la Ley 30/2011, sobre la creación (…) Página 4

Consejo Editorial

EDITA: CGE - RASI

COORDINADORA: Sara Argüello

COMITÉ DE REDACCIÓN
Valentí Pich, Carlos Puig, Carlos Alonso de Linaje, Abel Bonet, José A. Canalejas, Esteban García, Alejandro García, Josep Puigvert, Miguel Ángel Sánchez, Joaquim Altafaja y Yazomary García.

Las opiniones expresadas en las colaboraciones firmadas no se corresponden, necesariamente, con los puntos de vista del Consejo Editorial

ENTREVISTA

Página 5

¿Qué diferencias prácticas supone el concepto "Accountability" para los responsables y encargados de tratamiento en relación a la LOPD?

No existe una definición única y universalmente aceptada del concepto de "accountability" (…)

José Luis Rodríguez Álvarez

Tribunas de opinión

Nuevo Reglamento Europeo de Protección de Datos

Joaquim Altafaja Diví, CISA, CISM, CGEIT

Desde su publicación como propuesta el pasado 25 de enero de 2012, mucho hemos oído hablar del nuevo Reglamento Europeo (…) Página 10

Peritaje Forense Informático

Pedro Sánchez

Estamos en un siglo en el que podemos decir que todo o gran parte de nuestro trabajo se basa en el funcionamiento de la informática (…) Página 13

Responsabilidad penal de las personas jurídicas

Yazomary García García

La reforma del Código Penal en España como consecuencia de la Ley 5/2010, de 22 de junio de 2010 que entró en vigor (…) Página 17

Tuenti apuesta por la privacidad y la seguridad como estrategia de negocio

Javier Tamayo

Allá por enero de 2012, la Vicepresidenta de la Comisión Europea y responsable de la Agenda Digital, **Neelie Kroes,** ya apuntó (…) Página 19

SEEEEEEEEEEOOOOOOOOOO

Carlos Alonso de Linaje

Internet nos ha cambiado la vida de un modo u otro a todos nosotros. El conocimiento se ha democratizado residiendo (…) Página 22

RASI: trabajando para conseguir que la economía digital y el uso de las TIC encuentren su lugar entre los servicios profesionales

La culminación del proceso de unificación del Consejo General de Colegios de Economistas y del Consejo Superior de Titulares Mercantiles, ha llevado a la desaparición de los mismos y a la creación del nuevo Consejo General de Economistas. Lo mismo ha sucedido con los órganos especializados de los anteriores Consejos, aprobándose en la primera reunión del Pleno del nuevo Consejo General, celebrada el 24 de mayo, la creación de distintos órganos especializados y grupos de trabajo, entre los que se encuentra RASI, Registro de Auditores de Sistemas de la Información.

RASI es un órgano técnico especializado del Consejo General de Economistas, que desempeña una labor, cada vez más significativa, de fomento de la Sociedad de la Información entre nuestros profesionales, mediante la promoción del uso de las Tecnologías de la Información y la Comunicación, especialmente en las Pymes, para las que, máxime en momentos como el actual, su imagen y reputación cobra especial relevancia, no sólo en el mundo offline sino también en el digital.

RASI Auditores de Sistemas de la Información

Valentí Pich
Presidente del Consejo General de Economistas

Uno de los puntos más fuertes de nuestra organización colegial es agrupar actualmente a 70.000 profesionales en nuestros Colegios, y no menos importante, la posibilidad de hacerlo con aquellas personas que superen los nuevos planes de estudio de Bolonia relacionados con la Economía y la Empresa, adaptados al Espacio Europeo de Educación Superior, esto es, a la totalidad de los futuros profesionales del ámbito de la Economía en el conjunto de sus actividades.

RASI presta servicios de formación e información a sus miembros sobre todos aquellos aspectos relacionados con el cumplimiento normativo de profesionales y despachos con implicaciones IT, Seguridad de la Información, Cloud Computing, Social Media, Internet y el uso profesional de las nuevas tecnologías, siendo precisamente en relación con estas áreas donde encontramos, hoy en día, algunas de las profesiones más comentadas, analizadas y buscadas por los recién licenciados o graduados.

En este número de "ActualidadRASI", el cuarto ya, encontraréis una entrevista, en relación con el Reglamento Europeo de Protección de Datos que se aprobará próximamente. A continuación, cinco artículos de profesionales en el ámbito de la Protección de datos, Responsabilidad Penal de personas jurídicas, Peritaje informático, Redes sociales y Posicionamiento en internet; una recopilación de consultas planteadas por nuestros miembros y un repaso de las actividades realizadas por RASI desde el último número de nuestra revista.

Te invitamos a formar parte de este registro y a afrontar con nosotros los retos que se nos presentan derivados de la dinámica evolución de las nuevas tecnologías

Desde RASI trabajamos con determinación con objeto de conseguir que la economía digital y el uso de las TIC encuentren en el mercado de los servicios profesionales aquel espacio que le corresponde. Te invitamos a formar parte de este registro, ahora más que nunca, y a afrontar con nosotros los retos que se nos presentan derivados de la dinámica evolución de las nuevas tecnologías.

Más servicios para todo el colectivo

Queridos compañeros:

Uno de los principales objetivos del nuevo Consejo General es el de incrementar el número de servicios a proporcionar a sus miembros. En esta línea, y, dada la importancia que actualmente ocupan las Tecnologías de la Información y la Comunicación (TIC), hemos entendido que resulta fundamental poner el RASI a disposición de todo el colectivo unificado.

El Registro de Auditores de Sistemas de Información (RASI) presta soporte a los auditores en la evaluación de diversos aspectos de los sistemas de información y promueve una importante actividad formativa –presencial y on line– en áreas de cumplimiento normativo con implicaciones TIC, como son, entre otras, la protección de datos, la prevención de blanqueo de capitales y las regulaciones de entidades financieras y sociedades de inversión.

Ya en el año 2003, concretamente el 23 de junio, se publicó la Resolución del Instituto de Contabilidad de Auditoría de Cuentas, relativa a la Norma Técnica de Auditoría sobre *Auditoría de Cuentas en Entornos Informatizados*, cuyo objeto es "establecer las reglas y suministrar una guía respecto a los procedimientos a seguir cuando se realice una auditoría en un entorno informatizado." Por lo tanto, no estamos hablando de un concepto nuevo en auditoría, como son los sistemas de información, pero sí podemos afirmar que éstos han tenido una evolución enorme en los últimos tiempos.

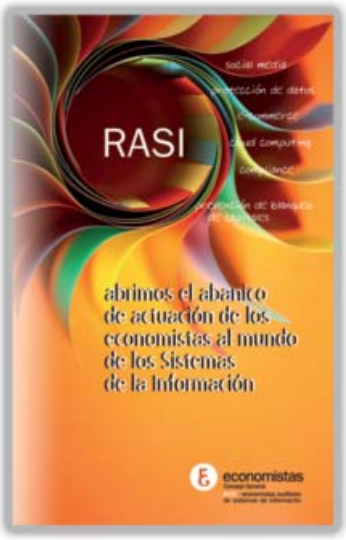
Así pues, el auditor tendrá que evaluar de qué manera dicho entorno informatizado afecta a su trabajo de auditoría, y para ello, deberá tener en cuenta este entorno en el diseño de los procedimientos necesarios para reducir el riesgo de auditoría a un nivel aceptable, dado que los métodos de obtención de evidencia, adecuada y suficiente, podrán verse afectados por los procesos informáticos.

Pero, además, la constante aparición de nuevas tecnologías aumenta la sofisticación del sistema informático de las empresas y la complejidad de sus aplicaciones específicas, incrementándose, por tanto, notablemente los riesgos inherentes y de control.

Somos conscientes de que aún nos queda camino por recorrer, pero, gracias a RASI, podremos hacerlo con muchas menos dificultades. Además, estamos seguros de que las incorporaciones de nuevos miembros impulsarán y dinamizarán la actividad de este joven Registro.

Dada la importancia que actualmente ocupan las Tecnologías de la Información y la Comunicación (TIC), hemos entendido que resulta fundamental poner el RASI a disposición de todo el colectivo unificado.

Lorenzo Lara
Vicepresidente del Consejo General de Economistas



Consejo General de Economistas

De acuerdo con la disposición transitoria segunda de la Ley 30/2011, de 4 de octubre, sobre la creación del Consejo General de Economistas, y previa publicación, el pasado 14 de marzo, de los Estatutos provisionales de dicho Consejo, mediante la Orden ECC/402/2013, de 12 de marzo, tuvo lugar, el 24 de mayo, la toma de posesión de los miembros del Pleno del Consejo General de Economistas, aprobando el nombramiento del resto de Órganos de Gobierno el Consejo.

Reunión de la Comisión Permanente del Consejo General de Economistas el día 5 de junio de 2013

RASI Nuevo Consejo Directivo

La Comisión Permanente del nuevo Consejo General de Economistas, en la sesión celebrada el pasado 5 de junio, aprobó la composición del nuevo Consejo Directivo del órgano especializado en Auditoría de Sistemas de la Información del Consejo, incluyendo representación de los Titulares Mercantiles.

economistas
Consejo General
RASI Auditores de Sistemas de la Información
Σ economistas y titulados mercantiles

De izda. a d dcha.: Lorenzo Lara, Vicepresidente del Consejo; Valentí Pich, Presidente del Consejo y Carlos Puig, Presidente de RASI.

La composición del Consejo Directivo actual de RASI es la siguiente:

PRESIDENTE

Carlos Puig de Travy

VOCALES

Carlos Alonso de Linaje

Abel Bonet Dolcet

José A. Canalejas Couceiro

Esteban García Pérez

Alejandro García Ruiz

Josep Puigvert Ibars

Miguel Ángel Sánchez Martin

ASESORES

Joaquim Altafaja Diví

Yazomary García García

Reglamento Europeo de Protección de Datos

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos

La propuesta de nuevo reglamento introduce cinco novedades de calado respecto al nuestro. La introducción del concepto "Accountability" (responsabilidad y rendición de cuentas) viene a decir que el responsable del tratamiento debe garantizar y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en el Reglamento. ¿Qué diferencias prácticas supone el concepto "Accountability" para los responsables y encargados de tratamiento en relación a la LOPD?

No existe una definición única y universalmente aceptada del concepto de "accountability". Para empezar, es un concepto que tiene difícil traducción al español. Quizás lo que más se aproxima es hablar de una responsabilidad activa y demostrable. Lo que se pretende es que quienes tratan datos asuman responsablemente esa función y adopten de manera proactiva una serie de medidas y mecanismos que permitan garantizar razonablemente que no se van a producir vulneraciones del derecho de los ciudadanos a la protección de sus datos personales. Y que estén en condiciones de "responder", de "rendir cuentas", de explicar cómo han aplicado esas medidas. En consecuencia, configura una aproximación diferente, orientada más a la prevención que a la reparación.

De hecho, en lo que concierne a la propuesta de Reglamento, es más innovador ese enfoque proactivo integral que las medidas concretas que se proponen. La protección de datos desde el diseño, la protección de datos por defecto o las evaluaciones de impacto sobre la protección de datos son conceptos a los que se da por primera vez carta de naturaleza legal en el entorno europeo. Pero no son algo nuevo o desconocido. En realidad, se trata de principios y métodos de actuación que ya tienen una trayectoria larga y que forman parte de lo que podría considerarse catálogo de buenas prácticas en las organizaciones que se preocupan del modo en que manejan los datos que tratan. En muchos casos, lo que a primera vista pueden parecer nuevas obligaciones o tareas no dejan de ser la consecuencia o la condición necesaria para un correcto tratamiento de datos personales. Una empresa que quiera iniciar un tratamiento de datos debiera, incluso con la vigente legislación en la mano, valorar qué características tiene ese tratamiento y qué impacto puede tener para la privacidad de los afectados, aunque sólo fuera, por ejemplo, para decidir qué medidas de seguridad tiene que aplicar.

Por eso, no creo que la práctica en un país como España, con una Ley de Protección de Datos que traspone muy fielmente la Directiva en todo lo relativo al papel de responsables y encargados, y con un régimen de protección de datos asentado, vaya a cambiar sustancialmente. Lo que sí ocurrirá en el nuevo escenario es que habrá una aplicación más sistemática y amplia de medidas y procedimientos que hasta ahora se han utilizado habitualmente como muestra de especial diligencia por parte de determinadas organizaciones.

El redactado del Art. 28 del nuevo reglamento, apartado 4-letra b), indica que Las obligaciones contempladas en los apartados 1 y 2 no serán aplicables a los responsables y los encargados del tratamiento, empresas u organizaciones que empleen a menos de doscientas cincuenta personas y que traten datos personales solo como actividad accesoria a sus actividades principales. ¿Es correcto pensar que las Agencias de Protección de Datos de los Estados miembros de la UE, tratan de simplificar las obligaciones de cumplimiento para las micro y pequeñas empresas, cuando utilizan datos personales para el tráfico mercantil de bienes o servicios pero que observan al dato como una necesidad para la identificación y no el dato como un fin?

El artículo 28 se refiere a la obligación de tener documentación sobre los tratamientos que lleve a cabo

Hay un consenso general en que el número de trabajadores de una empresa no puede ser el único factor determinante a la hora de decidir si tiene que aplicar o no ciertas medidas en materia de protección de datos (…)
Lo realmente definitivo es el tipo de datos que se tratan, el tipo de operaciones que se efectúan con ellos o el número de personas cuyos datos se están manejando.

una organización. Y es cierto que en él se contiene esa previsión para empresas de menos de 250 empleados. Las Agencias de Protección de Datos y otros actores implicados en el proceso de revisión de la Directiva nos preguntamos si es acertado el modo en que la propuesta de Reglamento aborda la cuestión de la modulación de las obligaciones, lo que se describe como escalabilidad.

Hay un consenso general en que el número de trabajadores de una empresa no puede ser el único factor determinante a la hora de decidir si tiene que aplicar o no ciertas medidas en materia de protección de datos. Básicamente porque no hay necesariamente una relación entre el número de empleados y los tratamientos que haga una empresa. Una empresa con trescientos empleados que fabrique tornillería es más que probable que no realice tratamientos de datos especialmente comprometidos y que requieran de medidas preventivas rigurosas. Pero una pequeña clínica con quince empleados entre médicos, enfermeros y administrativos puede estar manejando datos sanitarios sensibles de cientos o miles de personas, y eso sí exigiría cautelas adicionales. En definitiva, el tamaño de una empresa, se mida por los criterios que se mida, pero sobre todo si se hace usando el número de trabajadores, es a lo sumo un indicio de la posible existencia de tratamientos con un cierto nivel de riesgo. Lo realmente definitivo es el tipo de datos que se tratan, el tipo de operaciones que se efectúan con ellos o el número de personas cuyos datos se están manejando.

Como digo, a todos –y no sólo a las Agencias de Protección de Datos– nos preocupa el que las obligaciones que se establezcan para responsables y encargados sean las estrictamente necesarias en función de las exigencias que se derivan de los tratamientos en que participen. Las medidas que se prevean tienen que ser las justas para contribuir a lograr un nivel adecuado de protección atendiendo a las múltiples circunstancias en que pueden encontrarse responsables y encargados. Las obligaciones que se perciben como innecesarias o que no se entienden, sobre todo si suponen costes adicionales, se convierten en cargas burocráticas que se cumplen formulariamente.

Es por ello que se ha ido extendiendo una opinión en favor de sustituir los criterios que podríamos llamar cuantitativos por criterios de riesgo, de modo que cuanto mayor sea el riesgo de un tratamiento, más estrictas han de ser las medidas de protección.

Las Agencias compartimos esta aproximación, pero queremos evitar equívocos. No hay situaciones de riesgo cero. Todo tratamiento de datos conlleva un riesgo para el derecho del interesado. Puede haber situaciones de muy bajo riesgo, y situaciones de alto riesgo, pero el simple hecho de que unos pocos datos sean recogidos, almacenados y sometidos a algún tipo de operación supone en sí mismo que información personal de un ciudadano sale de su control y puede ser extraviada, robada, manipulada por terceros o utilizada de forma desleal por quien la recogió. Por ello, siempre hemos defendido que tampoco puede hablarse de ausencia total de obligaciones para tratamientos de bajo riesgo. Debe haber siempre un nivel de protección, aunque sin duda ajustado a las características del tratamiento.

La evaluación del impacto es otra de las novedades que nos trae el nuevo reglamento. El Art. 33 apartado 2, define los supuestos donde debe extremarse la evaluación del impacto y los siguientes apartados los procedimientos a seguir. ¿La Agencia Española tiene previsto marcar las pautas para la evaluación del impacto? ¿Está prevista la creación de un órgano dentro de la Agencia Española a la que los responsables y encargados de tratamiento puedan dirigirse para formular consultas que acoten el término, evaluación del impacto?

El Reglamento tiene ya un esquema básico de cuál ha de ser el contenido de estas evaluaciones de impacto de protección de datos en otro apartado de ese mismo artículo 34. Además, y como señalaba anteriormente, tampoco es que la evaluación de impacto de protección de datos sea una radical innovación del Reglamento. Lo que es algo nuevo es que el Reglamento establece un criterio para determinar cuándo hay que hacer necesariamente una evaluación de impacto, que es que haya un riesgo específico para los derechos o libertades de los interesados, enumerando un listado básico de supuestos. Hasta ahora no había un mandato legal de estas características, aunque sí hay normas sectoriales europeas que contemplan evaluaciones de impacto. Ello significa que no partimos de cero a la hora de diseñar los modelos de evaluación de impacto en este terreno y que en principio no sería imprescindible una acción en ese sentido.

Sin embargo, sí hay que tener en cuenta que el Reglamento es una norma que busca la máxima armonización no sólo en el contenido del marco legal europeo de protección de datos, sino en su aplicación. Por ello, es importante que las metodologías de evaluación sean también equiparables en toda la Unión.

El Reglamento prevé que la Comisión pueda adoptar actos delegados o de aplicación destinados a precisar los requisitos y procedimientos para llevar a cabo las operaciones de evaluación. Las Autoridades de Protección de Datos europeas coincidimos en que hay una necesidad de buscar una cierta estandarización en estos métodos, aunque no pensamos que esa armonización deba hacerse mediante instrumentos legales formalizados y vinculantes, como serían los actos delegados o de aplicación de la Comisión. Más bien entendemos que debiera ser el futuro Consejo Europeo de Protección de Datos el que marcara directrices, más flexibles y de un carácter más técnico, para la realización de las evaluaciones.

Por eso creo que, aunque es todavía pronto para anticipar si la Agencia Española va a redactar sus propias directrices, es más probable que ese ejercicio lo haga la Comisión, si el Reglamento prospera en su redacción actual, o todas las Autoridades de Supervisión europeas actuando de modo coordinado. Sin perjuicio de que si se considera necesario o útil pueda haber una versión adaptada a la realidad española de esas metodologías, siempre que las normas o directrices comunes den margen de actuación a nivel nacional.

En cuanto a la creación de un servicio específico en la Agencia Española, la respuesta es sin duda que sí. En realidad, no hará falta crear ese servicio, sino más bien dar continuidad o quizás formalizar más concretamente la actividad que ya desarrolla la Agencia. Actualmente recibimos con frecuencia peticiones de empresas que de un modo más o menos estructurado han hecho un análisis de riesgo o de impacto de tratamientos que quieren poner en marcha y quieren conocer la opinión de la Agencia sobre esos tratamientos. Unas veces se hace mediante la solicitud de un informe jurídico. En otras ocasiones por medio de reuniones en las que se analizan los tratamientos y las soluciones de protección de datos previstas por las empresas. Así pues, con independencia de la forma, la actividad ya se está desarrollando. Seguramente con la entrada en vigor del futuro Reglamento, y dependiendo del contenido final de estos artículos, haya que dotarla de una mayor formalidad, incluido un procedimiento adecuado, con fijación de plazos y aclarando las consecuencias de las decisiones de la Agencia y la posición de las compañías afectadas. Pero no supondrá un cambio sustancial en una línea de trabajo que ya existe en la Agencia.

Los conceptos "privacy by design" y "privacy by default" deberían haber sido bien recibidos por los grandes actores de Internet, pero se han oído voces que rumorean que han habido presiones para entorpecer la aprobación del nuevo reglamento. ¿Están realizando un ejercicio de transparencia los grandes operadores con sus usuarios/clientes más allá de la imposición legal? ¿En qué medida la presión que ejercen las Agencias de Protección de Datos de los Estados de la UE sobre los grandes operadores de Internet les obliga a ser más celosos con el respeto de los derechos de los ciudadanos?

El Reglamento va a influir, sin duda, en cómo desarrollarán esas empresas su actividad en el futuro. Pero no creo que sea sólo como consecuencia de la implantación de los principios de "privacy by design" o "by default". De hecho, incluso algunas de las propuestas que se han oído –o que se han conocido de forma más o menos pública– ni siquiera apuntan a modificar aspectos innovadores del Reglamento, sino que

pretenden más bien rebajar el nivel actual de protección introduciendo cambios en cuestiones que ya están presentes en la Directiva y que se han venido aplicando durante años.

El problema de fondo con la mayoría de empresas que operan en Internet es que tienen que conciliar de forma equilibrada un modelo de negocio basado en la recogida y utilización comercial de la información de los usuarios con la protección de los derechos de esos ciudadanos. Actualmente existe una cierta tendencia a recoger un gran volumen de datos y darles muchas utilidades para generar ingresos económicos, sin reparar en si esas prácticas son más o menos respetuosas con la privacidad de los usuarios y, con demasiada frecuencia, con políticas de privacidad poco transparentes, o redactadas en términos incomprensibles para el ciudadano medio, o que les ofrecen muy pocas posibilidades de controlar realmente el uso que se hace de sus datos.

Sin embargo, los ciudadanos están cada vez más preocupados por el uso que las empresas en Internet hacen de sus datos. Así nos lo dicen todas las encuestas y lo percibimos en el número creciente de reclamaciones en la Agencia. En este sentido, estoy seguro de que el futuro desarrollo de muchos negocios en Internet va a depender en gran medida de la confianza que sean capaces de generar entre sus potenciales clientes, y en este punto la protección de datos desempeñará un papel fundamental.

La figura del DPO (Data Privacy Officer) resulta doblemente interesante. De un lado supone incorporar una nueva figura que creerá más gasto a los obligados y de otro, nuevas oportunidades profesionales. ¿Cómo piensa encajar la figura del DPO la Agencia Española en nuestro país? ¿Está previsto pedir estar en posesión de alguna certificación profesional para el ejercicio o bien mediante la inscripción en un Registro de Delegados de Protección de Datos Ejercientes que dependa directamente de la Agencia Española?

Como con tantas otras obligaciones del Reglamento, hay que entenderla no como un requisito formal que hay que cumplir, sino como una pieza más en el esquema global de la organización para conseguir un mejor cumplimiento del Reglamento y para garantizar el respeto al derecho de los ciudadanos. Si una empresa realiza tratamientos de una determinada complejidad, o que implican determinados riesgos, necesita que alguien la asesore sobre cómo diseñar el tratamiento, cómo valorar sus riesgos, cómo implantarlo, qué medidas de seguridad adoptar, etc. El Reglamento lo hace obligatorio en ciertos casos, pero para esa empresa, aunque no existiera una obligación legal, habría una necesidad real de contar con ese asesoramiento.

El Reglamento ya prevé que no todas las empresas tendrán que dotarse de un DPO. De nuevo es importante que esta exigencia se reserve para organizaciones en las que verdaderamente suponga un valor añadido en términos de garantía de cumplimiento y no sea sólo un requisito formal.

Por otra parte, el Reglamento da mucha flexibilidad a las empresas que finalmente resulten obligadas a la hora de configurar su DPO según sus propias necesidades. Puede ser un empleado de la empresa o puede desarrollar sus funciones con un contrato de servicios, es decir, que puede ser un consultor externo. Puede desempeñar el puesto a tiempo completo o compaginarlo con otras obligaciones. Será la organización la que tenga que valorar qué tipo de DPO necesita. El Reglamento confiere un margen amplio, aunque sí establece una serie de requisitos como la independencia, o la vinculación con la dirección de la compañía, que deberán respetarse en todos los casos.

Creo que lo importante es valorar al DPO no como una carga, sino como una herramienta que contribuye al cumplimiento de las obligaciones legales. En último extremo las aportaciones del DPO pueden ayudar a prevenir incumplimientos y evitar sanciones económicas de las Agencias de Protección de Datos o reclamaciones de los interesados que acaben en indemnizaciones importantes.

Por otra parte, aún es pronto para decidir cómo se va a regular la que podríamos llamar profesión de DPO en España. También aquí el Reglamento contiene habilitaciones a la Comisión para adoptar actos delegados en que se especifiquen los criterios para las cualificaciones profesionales de los DPO. Habrá que esperar y ver cuáles son esos criterios. La experiencia actual de los países donde está implantada la figura del DPO indica que en algunos países sí se pide un grado universitario, y dentro de ellos algunos precisan que ese grado tiene que ser en Derecho, Informática o similares. Pero son ejemplos minoritarios. En términos generales la tendencia es a pedir que el DPO tenga una cualificación suficiente y adecuada para el desempeño de las tareas que se le van a encomendar.

Actualmente se habla de la aprobación del nuevo reglamento europeo para el 2015. ¿Cómo ven ustedes el calendario? ¿Para cuándo se espera su aprobación?

No es fácil prever cuándo puede aprobarse el Reglamento, porque hay factores muy diversos que influyen en los ritmos de una negociación que es en sí misma compleja. No puede olvidarse que participan el Parlamento Europeo, el Consejo y la Comisión Europea. Estamos además ante una norma de gran relevancia. Es la primera vez que un Reglamento europeo pretende regular la protección de un derecho fundamental de los ciudadanos. Al mismo tiempo, tiene un carácter horizontal, que proyecta sus efectos a todos los sectores de la actividad pública y privada. Y, finalmente, tiene especial incidencia en el ámbito de las nuevas tecnologías y los servicios de la sociedad de la información.

Ello supone que las discusiones resultan complejas, porque los resultados van a afectar muy significativamente a los derechos de los ciudadanos, pero también a la actividad de importantes sectores de la economía. Creo que es muy ilustrativo de la relevancia de esta norma, de los intereses en juego y de la envergadura del trabajo que se está llevando a cabo que en el Parlamento Europeo se hayan presentado más de 3.000 enmiendas al proyecto, una cifra que es muy superior a lo habitual incluso en normas que se han considerado como especialmente sensibles para sectores económicos.

Actualmente existen dudas crecientes sobre si se logrará completar la tramitación antes de que finalice la actual legislatura del Parlamento Europeo en mayo de 2014. Si no se logra, 2015 podría ser una posibilidad pero condicionado siempre a cómo impulsen el nuevo Parlamento y la nueva Comisión la tramitación de la iniciativa.

Creo que es muy ilustrativo de la relevancia de esta norma, de los intereses en juego y de la envergadura del trabajo que se está llevando a cabo que en el Parlamento Europeo se hayan presentado más de 3.000 enmiendas al proyectouna cifra que es muy superior a lo habitual incluso en normas que se han considerado como especialmente sensibles para sectores económicos.

Nuevo Reglamento Europeo de Protección de Datos

Joaquim Altafaja Diví, CISA, CISM, CGEIT
Asesor del Consejo Directivo de RASI-CGE

Desde su publicación como propuesta el pasado 25 de enero de 2012, mucho hemos oído hablar del nuevo Reglamento Europeo de Protección de Datos, intensificándose los últimos meses las informaciones y eventos relacionados con su supuesta aprobación que algunos señalaban para el pasado 29 de mayo. Y lo cierto es que el 6 de mayo de 2013, la Comisión del Parlamento Europeo de Libertades Civiles, Justicia y Asuntos de Interior, (LIBE) examinó los progresos de la propuesta de Reglamento General de Protección de Datos. El principal ponente de la Comisión LIBE, **Jan Philipp Albrecht,** señaló que, en vista del gran número de enmiendas presentadas, algunas fuentes hablan de cerca de 4.000, se necesita más tiempo para la deliberación. Lo cierto es que el 29 de mayo se debatía el reglamento en el seno del Parlamento Europeo posponiéndose su aprobación.

Por su parte, **Jan Philipp Albrecht** señaló que el objetivo es llevar a cabo la votación, antes de las vacaciones de verano, con el fin de continuar con las negociaciones en otoño. Mientras tanto, la Presidencia irlandesa ha confirmado que se centra en la propuesta de reglamento y que se están realizando extensas negociaciones. La reunión del Consejo Europeo del pasado 6 de junio de 2013, examinó las áreas en las que los Estados miembros de la UE pueden haber llegado a un consenso.

Cuestiones políticas al margen, nuestro interés se centra en los nuevos conceptos que introduce la hasta ahora propuesta de reglamento europeo en relación a la legislación española, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, plenamente vigentes a fecha de hoy.

En este sentido, la propuesta de reglamento introduce cinco **principales novedades:**

- Responsabilidad y Rendición de cuentas *(Accountability).*
- Evaluación de Impacto de protección de datos *(Análisis de riesgos o Privacy Impact Assessment).*
- Protección de datos desde el diseño *(Privacy by design).*
- Protección de datos por defecto *(Privacy by default).*
- La figura del delegado de protección de datos *(Data Privacy Officer).*

Responsabilidad y rendición de cuentas

La propuesta de reglamento, al introducir los conceptos Responsabilidad y Rendición de cuentas, viene a decir, que el responsable del tratamiento debe garantizar y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en el reglamento, para ello establece las **obligaciones del Responsable de Tratamiento** (Art. 22), en cuanto a **conservación de documentación** (Art. 28), donde se obliga a conservar la documentación de todas las operaciones de tratamiento efectuadas a excepción de aquellas empresas que tengan un número de empleados inferior a 250 y que traten datos personales sólo como actividad accesoria a sus actividades principales, la **seguridad del tratamiento** (Art. 30), que obliga al responsable y al encargado de tratamiento a implementar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, atendiendo a los riesgos del tratamiento y naturaleza de los datos, a evaluar los riesgos y adoptar las medidas adecuadas para mitigarlos, observando, las técnicas existentes y los costes asociados a su implementación, la **evaluación del impacto** relativa a la

protección de datos (Art. 33), que deberá realizarse cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados, por su naturaleza, alcance y/o fines, y en particular, cuando el tratamiento sirva para la creación de perfiles de los interesados, en el tratamiento de datos sensibles, datos genéticos o biométricos, en los casos de videovigilancia y en el tratamiento de datos de menores, la autorización y consulta previas a la autoridad de control (Art. 34), que se deberá obtener en el caso de que existan cláusulas contractuales en transferencias internacionales de datos, un elevado nivel de riesgos específicos motivado por la evaluación de impacto, por decisión de la autoridad de control, que entrañen riesgos específicos o las publicadas en una lista. El apartado 2 del Art. 33 detalla en particular qué operaciones entrañan riesgos. Además añade como obligación la figura del delegado de protección de datos (Art. 35), para aquellas empresas que cuenten con un número igual o superior a 250 empleados.

Integrar la privacidad en la lógica del negocio, posibilita la disminución de errores y es garantista con los derechos de los ciudadanos.

Evaluación de impacto de protección de datos

La evaluación de impacto de protección de datos, como contenido mínimo incluirá una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertados de los interesados, las medidas contempladas para hacer frente a dichos riesgos y garantías, las medidas de seguridad y mecanismos destinados a proteger los datos personales y la prueba de la conformidad con la legislación, una vez evaluado el impacto, si resulta probable que el tratamiento entrañe un elevado riesgo para los derechos y libertados de los interesados, se deberá consultar a la autoridad de control y mitigar los riesgos detectados. La autoridad de control también podrá determinar la obligatoriedad de que se le consulte previamente en aquellas operaciones que considere potencialmente peligrosas para la privacidad de las personas y publicará una lista detallada de tratamientos sometidos a control previo.

Protección de datos desde el diseño y por defecto

Estos dos nuevos conceptos se introducen en las obligaciones del responsable de tratamiento (Art. 22), en cuanto éste adoptará políticas e implementará medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el nuevo reglamento, adoptará políticas, (guía de privacidad, buenas prácticas, contratación, seguridad desde el diseño, seguridad por defecto, análisis de impacto, delegado de protección de datos, auditorías, ….), e implementará medidas, (cumplimiento normativo, derechos de los interesados, tratamiento sólo de los datos necesarios, recogida y conservación ajustadas con la finalidad, seguridad, análisis de riesgo, restricción de acceso, violación de datos y comunicación a la autoridad de control y al interesado, acuerdos con encargados u otros responsables, …).

En particular, el artículo 23, hace referencia a las técnicas existentes y los costes asociados a su implementación, debiendo el responsable implementar, en el momento de la determinación (diseño) de los medios de tratamiento como en el del tratamiento mismo, medidas y procedimientos técnicos y organizativos apropiados,…, el responsable implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos necesarios para cada fin específico, pudiendo la comisión europea especificar nuevos criterios y requisitos aplicables a los dos anteriores y definir normas técnicas. En resumen, integrar la privacidad en la lógica del negocio, posibilita la disminución de errores y es garantista con los derechos de los ciudadanos.

Delegado de protección de datos

Por último, la figura del delegado de protección de datos se contempla cuando, el tratamiento se dé por una autoridad u organismo público, en aquellas empresas con un número de empleados igual o mayor a 250 o la actividad principal del responsable consista en tratamientos que, en razón a su naturaleza, alcance y/o fines, requieran seguimiento periódico y sistemático de los interesados, pudiendo existir un único delegado para un grupo de empresas, autoridad u organismo público, teniendo en cuenta la estructura organizativa.

El perfil de este puesto deberá atender a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, así como, demostrar capacidad para ejecutar las tareas asignadas.

El estatuto del delegado de protección de datos contempla:

- La independencia respecto de la empresa y directivos.
- La segregación de funciones, a fin de evitar los conflictos de intereses.
- Un mandato mínimo de dos años, pudiendo optar a mandatos sucesivos.
- Ser un empleado o ejercer mediante contrato de servicio, debiendo el responsable comunicar el nombre y datos de contacto a la autoridad de control y al público.

Entre sus funciones, cabe destacar:

- Informar y asesorar al responsable de las obligaciones.
- Supervisar la implementación y la aplicación de las políticas, la asignación de responsabilidades, la formación del personal afecto y las auditorías.
- Supervisar la implementación y aplicación de los requisitos de protección de datos desde el diseño, por defecto y la seguridad de los datos.
- Proporcionar información a los interesados y a la autoridad de control y responder a sus solicitudes.
- Velar por la conservación de la documentación y supervisarla.
- Notificar y comunicar las violaciones de datos.
- Supervisar la realización de la evaluación de impacto de protección de datos.

Otros temas que se incluyen en la propuesta de Reglamento son: el alcance de ésta en lo que respecta al sector público, la portabilidad de datos y el derecho al olvido y el significado de los datos personales anónimos y seudónimos.

De momento, y sin más noticias del reglamento europeo, hemos de esperar, sin embargo, que las casi 4.000 enmiendas presentadas auguran un tedioso camino a la comisión, amén de conflictos de interés entre los 27 Estados que integran la UE y las empresas del sector de las comunicaciones e Internet y en especial aquellas del sector de las redes sociales y de la prestación de servicios a través de esta plataforma.

Peritaje Forense Informático

Pedro Sánchez
Perito Judicial Informático.
Miembro de Spanish Honeynet Project
Fundador de Conexión Inversa, empresa dedicada a peritajes y análisis forense informático
Director de Seguridad en SAYTEL
Responsable de capacitación en la Asociación Nacional de Ciberseguridad y Pericia Tecnológica.

Inseguridad 2.0

Estamos en un siglo en el que podemos decir que todo o gran parte de nuestro trabajo se basa en el funcionamiento de la informática y las comunicaciones de Internet. Conceptos como la nube, mensajería instantánea, aplicaciones SAS (Software As Service), datos, servidores, videoconferencias, todo se encuentra en formato digital.

Todas estas herramientas que nos ayudan en el trabajo diario constituyen un pilar fundamental a la hora de tener claro unas reglas de juego que permitan mantener los tres pilares de la seguridad informática como son la disponibilidad, integridad y confidencialidad, sin que ninguna de ellas pueda ser alterada.

La información de nuestra empresa y nuestras actividades, nuestros datos, nuestro dinero digital todo es confidencial: la información cada vez está más centralizada y tiene un alto valor para terceras personas que quieran disponer de ellas. Una fuga de datos puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta a su disponibilidad y la pone en riesgo. La información es poder.

Este mal uso ha provocado constantes problemas en la privacidad de las personas y han sugerido nuevos tipos de conceptos en la sociedad como **Sexting** que consiste en cómo algunos contenidos de fácil acceso, como la pornografía, influencian las relaciones entre niños y niñas creando, por un lado, un sentimiento de superioridad entre ellos, quienes llegan a exigir fotos de ellas desnudas y, por otro lado, generando unos patrones de belleza inalcanzables.

Acoso sexual por medio de dispositivos móviles, **fraude empresarial** en la que el personal descontento de una empresa se lleva toda la información de ésta a la competencia creando un problema de propiedad intelectual.

Todas estas cosas por desgracia están presentes en la vida diaria de la sociedad y eéstas se reflejan en los juzgados de España que, sin comprender estos nuevos delitos, hacen todavía más pesada la carga y resolución judicial, haciéndola interminable y, en muchos casos, quedando impune el defraudador o delincuente.

Perito Judicial Informático / Perito Forense Informático

El perito judicial informático es una figura amparada en los tribunales de justicia y reconocida por la magistratura, cuya función es la de auxiliar y asesorar al juez respecto a temas relacionados con la informática.

Este reconocimiento de experto o perito experto le designa como el encargado de analizar los diferentes elementos informáticos y buscar aquellos datos que puedan determinar el esclarecimiento del litigio al que ha sido asignado en un proceso legal, solucionando de esta manera los aspectos y conocimientos que el juez o los tribunales no están obligados a conocer por la cantidad de requisitos de especialización que requiere.

Todas estas herramientas que nos ayudan en el trabajo diario constituyen un pilar fundamental a la hora de tener claro unas reglas de juego que permitan mantener los tres pilares de la seguridad informática como son la disponibilidad, integridad y confidencialidad, sin que ninguna de ellas pueda ser alterada.

El análisis forense informático consiste en la obtención de pruebas y evidencias obtenidas en el análisis y explotación de datos que se encuentran en un soporte digital

Ser Perito

Para ser perito se debe disponer de una titulación oficial que lo acredite en la materia de la cual es especialista. También es válido su acreditación profesional para ejercer en los Juzgados y Tribunales españoles, de conformidad con lo establecido en los artículos 340 y 341 de la LEC y la instrucción 5/2001 de 19 de diciembre del Consejo General del Poder Judicial y el Protocolo de 9 de febrero de 2005, modificada recientemente por el Acuerdo del Pleno del Consejo General del Poder Judicial de 28 de octubre de 2010 sobre la remisión y validez de las listas de Peritos Judiciales remitidas a los Juzgados y Tribunales por las Asociaciones y Colegios Profesionales, publicado en el BOE nº 279 de 18 de noviembre de 2010, págs. 96464 y ss.

Cuando un Perito Informático es nombrado por un Juez, Magistrado o Administración, automáticamente se convierte en auxiliar de la Justicia y debe realizar la función pública de acuerdo con el cargo conferido; de igual manera que la policía judicial y se rigen por las leyes y reglamentos especiales (art. 470 a 480, LOPJ).

En el ámbito jurídico, el Perito Judicial Informático es un profesional nombrado por la autoridad del proceso, a fin de que mediante juicio científico-técnico, dictamine con veracidad e imparcialidad, opinando y emitiendo conclusiones sobre puntos concretos relacionados con hechos o circunstancias, sus causas o efectos, para cuya apreciación son indispensables conocimientos especializados.

La especialización

Todo perito tiene que ser especialista en alguna materia dentro del gran mundo de la informática, pero quiero destacar la **especialización en el análisis forense informático** que consiste en la obtención de pruebas y evidencias obtenidas en el análisis y explotación de datos que se encuentran en un soporte digital como por ejemplo, un disco duro, tarjeta de memoria, sistema operativo, aplicaciones, dispositivo móvil e, inclusive, en detalles como fotografías, bases de datos o correo electrónico.

Realización de un Peritaje Forense Informático

Un peritaje forense se compone de una serie de pasos que, de forma resumida, expongo a continuación.

IDENTIFICAR

Consiste en verificar el dispositivo, ordenador, material o aplicación que se va a analizar, esta verificación se realiza tanto visual como legal, incluyendo el proceso que verifica la integridad y manejo adecuado de la evidencia (Cadena de custodia). Pongamos. por ejemplo. un fraude cometido desde un ordenador al cual hay que analizar.

Para ello, los pasos necesarios para la identificación son:

- Apertura de acta donde se van a incluir todas las acciones que va a realizar el perito.
- Grabación con video-cámara del entorno donde se encuentra el ordenador donde se ha cometido el delito, esta deberá de llevar sobreimpresa la fecha y hora de grabación, grabando especialmente el entorno que pudiera ser más vulnerable como por ejemplo ventanas con acceso a la calle y poco protegidas.
- Fotografía a los elementos a analizar, como por ejemplo el ordenador, discos duros, pantallas de una aplicación.
- Etiquetado de los elementos a revisar e incluirlos en el acta.
- Clonación de los elementos a analizar y verificación de la integridad.
- Disposición de los presentes para la realización de una cadena de custodia que puede derivar en la custodia de los elementos en un juzgado (dependiendo del caso) o bien en un sitio seguro con registro de entradas y salidas como la caja fuerte de un banco.

PRESERVAR

Consiste en intentar realizar una copia del dispositivo a analizar, utilizando tecnología que permita poder mantener la integridad de la evidencia y la cadena de custodia. El proceso de imagen se realiza lo que se llama copia íntegra o copia "bit a bit", que consiste en realizar una copia idéntica, aún cuando ésta contuviera errores.

Ejemplo de clonado de un iphone

La copia íntegra se puede realizar con software especialmente dedicado a estos menesteres o bien con hardware específico, como clonadoras que son dispositivos que permiten la copia a muy alta velocidad garantizando y protegiendo la evidencia original.

El número de copias puede ser variable, ya que va desde una a tres o cuatro dependiendo del caso. Por ejemplo, en un delito empresarial como una fuga de datos se deberían realizar al menos tres copias, una para la defensa del acusado, otra para la empresa y la última para el perito el cual deberá de explotar la información contenida en la copia. Mientras el original se debería de poner a disposición del juzgado o en un sitio seguro a fin de mantener la cadena de custodia.

ANÁLISIS

También llamado Análisis Forense, es el proceso de explotación del medio duplicado o copia que consiste en técnicas de búsqueda por medio de herramientas automatizadas o manuales. Por ejemplo, búsqueda de ficheros concretos, datos de personas, tarjetas VISA, identificación de pendrives, correos electrónicos, etc.

En el análisis y en el previo clonado de discos se debe evitar:

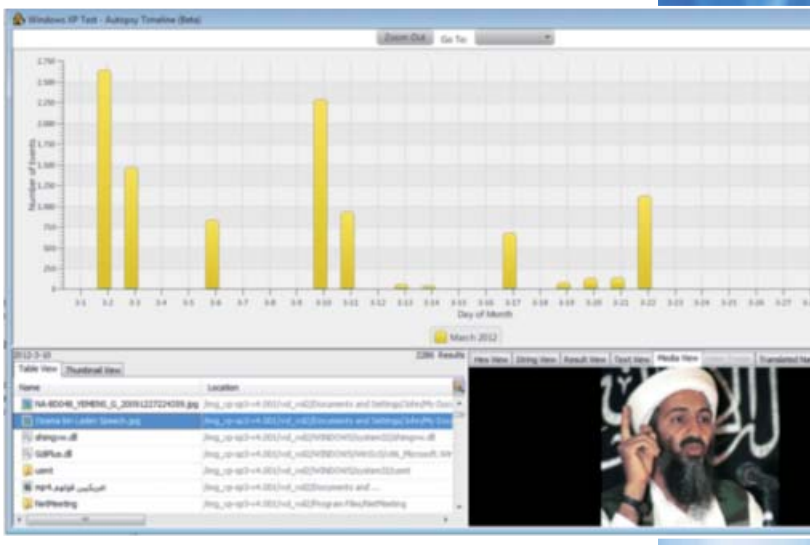
- Ejecutar cualquier tipo de aplicación que pueda cambiar las fechas de los archivos.
- Utilizar aplicaciones convencionales de clonación de imagen.
- Utilizar el disco duro sin bloquear la escritura.

Este proceso es el más complejo de todos y pone al límite la capacidad investigadora del perito a la hora del análisis. Tiene que disponer de los conocimientos necesarios para analizar, por ejemplo:

- Análisis de los encabezados de ficheros
- Comprobación de huellas de ficheros
- Verificación de malware
- Análisis de los procesos
- Búsqueda de información oculta o borrada
- Registro de Windows
- Cuentas de usuario
- Bitácoras del sistema
- Permisos de ficheros
- Perfiles de usuario
- Trazas de temporales
- Trazas de la memoria
- Tras de aplicaciones
- Perfil de navegación por internet
- Llamadas
- Agendas
- Mensajes instantáneos

Las evidencias encontradas se tienen que documentar y contrastar técnicamente e intentar crear una línea de tiempo, "Timeline", para que los abogados, fiscales y el juez puedan ver en todo momento las acciones en un periodo de tiempo.

En un principio, los gráficos muestran el número de eventos por año. La selección de un año muestra barras para cada mes del año. La selección de un mes mostrará entonces el número de eventos de cada día. La parte inferior de la pantalla le permite ver todos los archivos que tienen actividad y el contenido de cada archivo. Desde este punto de vista, se puede seguir utilizando la vista en miniatura para ver todas las imágenes en un día determinado y se pueden reproducir vídeos.



Ejemplo de una línea de tiempo

La evolución del peritaje informático está unida a las nuevas tecnologías y éstas requieren a su vez una especialización intensa y continua por parte del perito.

PRESENTACIÓN O INFORME

Consiste en recopilar toda la información que se obtuvo a partir del análisis inicial para realizar el informe y la presentación a los abogados. Este informe debe de evitar en la medida de lo posible tecnicismos y/o explicaciones complejas.

Actualmente disponemos de una norma UNE 197001:2011 que permite al colectivo de peritos realizar un informe basándonos en esta norma. Esta norma, en su contenido, indica cuales son los apartados que, al menos, deberían aparecer a un informe pericial para que éste tenga una estructura mínima de contenido.

CADENA DE CUSTODIA

Las personas que manejan una prueba o evidencia deben asegurar en el tiempo la integridad de ésta llevando un registro de accesos y protegerlo durante el tiempo necesario o requerido. También se debe asegurar la calidad de los datos y su accesibilidad siempre que se requiera judicialmente. Por lo tanto se garantiza que no ha sido alterado o modificado.

En una cadena de custodia se debe garantizar y dar respuestas a:

- Quién, cuándo y dónde se reunieron las pruebas recogidas.
- Quién examinó, cuándo y cómo se examinaron las evidencias.
- Quién tenía la posesión y el tiempo que estuvo con las evidencias.
- Cuándo y a partir de quién se transmitieron las evidencias.

Conclusiones

Hoy en día es muy difícil no encontrarse con algún caso donde no haya una evidencia electrónica o un sistema informático donde se produzca un delito.

Los delincuentes utilizan internet como medio de comunicación, venta y sistema de acoso sin pensar las consecuencias ni del rastro digital que pueden ir dejando.

Nuestra sociedad ha evolucionado sistemáticamente al uso cotidiano del ordenador y conexión a internet, así mismo los nuevos dispositivos como smartphones u otros teléfonos inteligentes y junto al almacenamiento virtual (cloud) en la nube, abren nuevos campos y están transformando la forma de comunicarse y el modo de obtener y de tratar las evidencias.

Los ciberdelitos y delitos en la red en su más amplia extensión y tipología son cada día más complejos, numerosos y peligrosos para los particulares, las empresas y las instituciones.

Por lo tanto, la evolución del peritaje informático está unida a las nuevas tecnologías y éstas requieren a su vez una especialización intensa y continua por parte del perito.

La función del perito ya no se limita al concepto de ayudante experto, ya que se da un paso más y el perito debe conocer el mundo digital que lo rodea, es impensable que no sepa de redes, vulnerabilidades, malware, análisis forense, etc.

El perito de hoy en día dispone de una alta cualificación con una buena formación técnica y formal que, con la ayuda de asociaciones o colegios, desarrollan y amplían la capacidad de estos profesionales experimentados que en un momento determinado puedan ayudar llegado el caso.

Pedro Sánchez ha trabajado en importantes empresas como consultor especializado en Computer Forensics, Honeynets, detección de intrusiones, redes trampa y pen-testing.
Ha implantado normas ISO 27001, CMMI (nivel 5), PCI-DSS y diversas metodologías de seguridad, especialmente en el sector bancario, durante más de diez años.

Ha impartido numerosas conferencias sobre seguridad informática de alto prestigio nacional e internacional.

También colabora sobre seguridad, peritaje y análisis forense informático con diversas organizaciones comerciales y con las Fuerzas de Seguridad del Estado, especialmente con el Grupo de Delitos Telemáticos de la Guardia Civil (GDT) y la Brigada de Investigación Tecnológica de la Policía Nacional (BIT). Ha trabajado como Information Security and Forensics Consultant para dos grandes compañías, como Bitdefender y Google Inc.

Ha participado en las jornadas JWID/CWID organizadas por el Ministerio de Defensa, donde obtuvo la certificación OTAN SECRET.

Responsabilidad penal de las personas jurídicas

Yazomary García García
Asesora del Consejo Directivo de RASI-CGE

La reforma del Código Penal en España como consecuencia de la Ley 5/2010, de 22 de junio de 2010 que entró en vigor el 23 de diciembre de 2010, tuvo como novedad que toda persona jurídica se enfrenta a dos riesgos penales y podrá responder penalmente por:

- Los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho y de derecho (consejeros).
- Los delitos cometidos por cuenta y provecho de la empresa por quienes, estando sometidos a la autoridad de las personas físicas que ejercen la dirección, hayan podido realizar los hechos por no haberse ejercido sobre ellos el debido control atendiendo a las circunstancias del caso (empleados).

Hasta el 23 de diciembre de 2010, la legislación española no reconocía la existencia de responsabilidad penal en el caso de las personas jurídicas; por lo tanto la inversión en Corporate Compliance, Internal Control y la lucha proactiva contra el fraude no eran una prioridad para la mayor parte de las Sociedades españolas (con excepción de las entidades financieras), sino por el contrario eran generalmente reactivas en relación con el fraude y las irregularidades.

El código penal contempla una lista de **delitos "corporativos"** que pueden afectar a las personas jurídicas, cuyas penas podrían establecerse en:

- Multa por cuotas o proporcionalidad –a establecer según el delito cometido– El impago de la multa puede dar lugar a la intervención judicial de la entidad hasta que se satisfaga.
- Disolución de la persona jurídica.
- Suspensión de sus actividades (no más de 5 años).
- Prohibición de realizar actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito (temporal o definitiva).
- Inhabilitación para obtener subvenciones públicas, para contratar con el sector público y para gozar de incentivos fiscales y de seguridad social.
- Intervención judicial para salvaguardar los derechos de los trabajadores y acreedores (no más de 5 años).

De igual forma existen ciertas **circunstancias atenuantes** del delito, tales como:

- La confesión antes del inicio de la investigación.
- El establecimiento de medidas de prevención.
- Reparación y colaboración en la investigación.

En este sentido **las empresas deben disponer de un Modelo de Prevención de Delitos,** el cual debe contemplar:

1. Análisis global del riesgo que supone cada delito para la empresa.
2. Recopilación de los controles y evidencias existentes, como parte de las medidas de prevención implementadas por la empresa, para mitigar el riesgo de cometer delitos penales.

3. Valoración de la consistencia de los controles *versus* los riesgos, tipificado en cada delito penal.
4. Reconsideración de la severidad del riesgo para cada delito.
5. Elaboración del Modelo de Prevención de delitos tipificado con impactos altos, medios y bajos.

Medidas de prevención de delitos

En función al análisis de riesgos, se deben desarrollar e implementar políticas y procesos que mitigan el riesgo de responsabilidad penal, tales como: código ético, política anti soborno y anti corrupción, política de prevención de blanqueo de capitales, procesos de gestión del riesgo, de cumplimiento y de Auditoría Interna (si aplica) y manual de políticas y procedimientos de seguridad y uso de los recursos tecnológicos.

Las empresas requieren formalizar su modelo de seguridad y establecer un marco de referencia para la gestión y control de los activos de información. Como parte de estas funciones, deben documentarse, aprobarse y comunicarse formalmente las políticas, estándares y lineamientos que se establezcan en la organización, de forma tal que éstas apoyen el cumplimiento de las metas estratégicas de la Gerencia.

A continuación, se presenta un breve resumen de los **principales tópicos que deben ser abordados en las políticas de seguridad de activos de información:**

- Control de acceso/seguridad lógica de datos: identificación, autenticación, autorización y registro.
- Control de cambios en las aplicaciones informáticas.
- Propietarios de la información –Data Clasification and Ownership– Cifrado.
- Seguridad Física.
- Monitorización - respuesta a incidentes.
- Uso de Internet y servicios relacionados.

Ahora bien, para evitar la imputación penal de la empresa por delitos cometidos por los empleados o, como mínimo, poder alegar circunstancias atenuantes, las empresas tendrán que justificar que disponen de mecanismos adecuados de control y prevención específicos de información, sensibilización del tema entre los empleados de las empresas y control de la conducta de sus empleados.

Desde RASI-CGE tenemos el compromiso de informar, asesorar y mantener actualizados a todos nuestros miembros. Por lo tanto, si necesitáis ampliar o aclarar cualquier información presentada en particular podéis contactar con nosotros a través de nuestra dirección de correo electrónico: rasi@economistas.org.

Tuenti apuesta por la privacidad y la seguridad como estrategia de negocio

Javier Tamayo
Abogado Senior del Equipo Jurídico y de Privacidad de Tuenti

Allá por enero de 2012, la Vicepresidenta de la Comisión Europea y responsable de la Agenda Digital, **Neelie Kroes,** ya apuntó una frase que refleja a la perfección cuál es el contexto general de Internet y las redes sociales en el que nos movemos en la actualidad: *"Los datos son el nuevo oro de la economía digital"*. Y es que a día de hoy, estamos ante una verdadera **economía de los datos personales** donde las empresas compiten en gran medida, por un lado, por conseguir el mayor número de información y datos de usuarios posible con el fin de poder obtener un rendimiento económico de los mismos y, por otro, por conseguir las mejores herramientas tecnológicas que atraigan el interés de los usuarios y, asimismo, les permitan realizar el tratamiento masivo de dicha información –lo que se conoce en el sector como sistemas o tecnologías de "Big data".

Sin embargo, si bien la información y los datos personales de los usuarios son, junto con la tecnología, piezas clave sobre las que se asienta cualquier negocio en Internet, en Tuenti estamos convencidos de que existe una tercera pieza o pilar básico, si cabe aún mucho más importante que los dos anteriores, que no es otra que **la garantía de la privacidad y la seguridad de los usuarios.** Estos dos elementos van a tener un papel primordial para garantizar el éxito de cualquier negocio online, a la par que se constituyen como los retos más importantes a los que nos enfrentamos diariamente todas las herramientas de comunicación social que operamos en Internet, un entorno cada vez más global y cada vez más centrado en el móvil.

Cada día los usuarios son mucho más exigentes, conscientes de que sus datos son la materia prima capital de la sociedad de la información y del conocimiento y, por ello, a cambio **exigen cada vez más que su información personal esté segura y su privacidad esté garantizada** en todo momento por los proveedores de estos servicios de Internet, con independencia del país donde éstos se encuentren ubicados. Prueba de ello es la enorme repercusión que está teniendo en la opinión pública y en los medios de comunicación la filtración de información sobre la presunta colaboración de las principales empresas americanas, tales como Facebook, Google, Microsoft o Apple en el programa de "alto secreto" dirigido al espionaje de ciudadanos extranjeros, incluidos los europeos, por parte del Gobierno de Estados Unidos en el marco del Proyecto PRISM de la Agencia de Seguridad Nacional (NSA).

A diferencia de lo que ocurre en Estados Unidos, donde con cierta frecuencia se da prioridad a otros derechos o bienes jurídicos frente a la privacidad, cuando estamos hablando de privacidad en Europa, ésta no se trata de un requisito accesorio u opcional, un simple lujo o un mero servicio de valor añadido para el usuario, sino que se constituye como un **verdadero derecho fundamental de las personas** que los proveedores de servicios de Internet como Tuenti tenemos la **obligación y la responsabilidad de proteger y garantizar.**

> Resulta esencial tanto el salvaguardar la privacidad y la seguridad de los ciudadanos en el mundo online como el contar con un marco de seguridad jurídica donde todas las compañías estén sujetas a las mismas reglas de juego en el desarrollo de su actividad al margen de dónde tengan establecido su domicilio social

En concreto, este derecho a la privacidad y a la seguridad de la información personal se encuentra reconocido por nuestro ordenamiento jurídico tanto por la legislación vigente en España –art. 18 de nuestra Constitución y Leyes Orgánicas 15/1999 y 1/1982, entre otras– como por diversas Directivas comunitarias a nivel europeo –Directivas 95/46/CE y 2002/58/CE. En

consecuencia, resulta esencial tanto el salvaguardar la privacidad y la seguridad de los ciudadanos en el mundo online como el contar con un **marco de seguridad jurídica donde todas las compañías estén sujetas a las mismas reglas de juego** en el desarrollo de su actividad al margen de dónde tengan establecido su domicilio social, sobre todo de cara a continuar potenciando el Internet social, la innovación y el desarrollo de nuevos productos y servicios digitales.

Esto se traduce en la práctica en que siempre deberían ser los propios usuarios los que tienen que poder decidir en cada momento, a través de **herramientas sencillas, ágiles y accesibles,** cómo y con quién quieren compartir la información que proporcionan cuando usan cualquier servicio en Internet. De hecho, toda la información presente en una red social debería ser propiedad del usuario y éste debería poder controlar su recogida, los tratamientos o usos que se van a realizar de los mismos (por ejemplo, si los datos se van a usar para fines publicitarios o comerciales), así como las posibles cesiones o comunicaciones posteriores de dicha información y/o datos del usuario a terceros (por ejemplo, si su información va a estar indexada y accesible para cualquier persona a través de buscadores de Internet).

Partiendo de esta particular visión, no compartida por gran parte de los proveedores de servicios de Internet y muy especialmente aquellos situados al otro lado del Atlántico, **Tuenti ha situado la privacidad y la seguridad siempre, desde su creación en el año 2006, en el centro de su estrategia de negocio y de crecimiento sostenido,** todo ello con el objetivo de ser la plataforma social de comunicación más simple, privada y segura de cuantas operan en Internet. Creemos que estos elementos son la base para poder obtener y mantener en el tiempo la confianza de nuestros usuarios, actuales y futuros.

Para nosotros no se trata sólo de cumplir con las exigencias de la normativa vigente existente en España y en Europa, bastante estricta ya de por sí si las comparamos con las legislaciones aplicables a las compañías con las que competimos en el entorno digital, sino que hemos decidido por voluntad propia ir un paso más allá, asumiendo el compromiso de incorporar estos elementos o pilares básicos en todas nuestras herramientas de comunicación social **desde el mismo momento en que empezamos a desarrollarlas** –es lo que se conoce como la aplicación de los principios de *"Privacy by design"* (Privacidad en el diseño) y de *"Privacy & security by default"* (Privacidad y seguridad por defecto).

Así, fruto del trabajo duro de estos últimos años con el enfoque comentado, Tuenti se ha posicionado con poco más de seis años de vida como **una de las compañías tecnológicas españolas más punteras,** muy centrada en la innovación y capaz de plantar cara de tú a tú a las empresas más grandes de Internet a nivel mundial, con más de 15 millones de usuarios registrados de los cuales alrededor de 10 millones son usuarios activos mensuales, con 6 millones de usuarios de sus aplicaciones móviles y un equipo formado por más de 250 profesionales de más de 20 nacionalidades, repartidos en 3 oficinas, 2 en Madrid y 1 en Barcelona.

Por aportar un dato que muestra nuestra constante evolución y transformación durante estos años y contrariamente a lo que se pueda pensar por la mayoría de la gente si atendemos a nuestros orígenes –compañía start-up fundada por cuatro jóvenes emprendedores– y al significativo éxito logrado por Tuenti entre la población más joven de nuestro país, hoy en día aproximadamente un **78% del total de usuarios registrados tiene más de 18 años y tan sólo un 22% sería menor de edad.**

El rápido crecimiento y expansión de Tuenti nos obligó a diseñar **un modelo legal propio que mantenemos en la actualidad, basado en la autorregulación** pero tomando como base todas las diversas recomendaciones recibidas de los organismos reguladores y de las autoridades competentes, entre los que ocupa un lugar destacado la Agencia Española de Protección de Datos, todo ello en pro de conseguir un nivel de cumplimiento de la normativa muy satisfactorio y de una forma adaptada a las condiciones técnicas de nuestra plataforma de comunicación.

Entre los principales **elementos diferenciales de Tuenti como multiplataforma social de comunicación web y móvil** que integra, entre otros, los servicios de red social, mensajería instantánea y, más recientemente, llamadas de voz sobre IP, podemos destacar los siguientes:

- El sometimiento de Tuenti a la legislación española, que hace que cumplamos con todas las exigencias en relación con la protección de datos personales, protección del menor, intimidad, honor y derecho a la propia imagen, entre otras. Asimismo, tenemos protocolos de actuación con numerosas autoridades nacionales y autonómicas.
- En Tuenti sólo se admiten perfiles reales con información real y por ello se ha partido de un modelo de acceso a la plataforma sólo por invitación de otro usuario o bien mediante la verificación de un número de teléfono móvil.
- Con carácter general no se permite la indexación de los datos de los usuarios en buscadores de Internet como Google con el fin de evitar que nuestros usuarios puedan ser localizados fuera de Tuenti.
- El acceso a Tuenti está prohibido a menores de 14 años, salvo que cuenten con consentimiento parental debidamente acreditado. De hecho, somos la primera red social a nivel mundial que ha implementado un sistema de verificación de identidad y de edad de usuarios mediante DNI electrónico.
- Aplicamos el máximo nivel de privacidad por defecto para todos los usuarios (denominado "Sólo amigos"), no sólo para aquellos usuarios de nuestra plataforma que sean menores entre 14 y 18 años.
- Permitimos a los usuarios hacer una distinción básica entre las categorías de amigos y contactos, de manera que cualquier usuario puede comunicarse por chat con aquellos otros usuarios de Tuenti que haya aceptado como contactos en su red pero manteniendo la información más privada disponible sólo para sus amigos.
- Disponemos de un Panel de privacidad extremadamente sencillo y fácil de configurar por cualquier usuario, con independencia de su edad.
- Tenemos implantados robustos sistemas de seguridad que garantizan la encriptación de las comunicaciones entre usuarios (por ejemplo, el protocolo SSL en las aplicaciones móviles).
- Contamos con sistemas muy sencillos de reporte de conductas ilícitas por parte de los usuarios que permiten, con tan sólo 3 clics, notificar a Tuenti cualquier perfil, fotografía y/o página sospechosa de ser ilícita y/o incumplir nuestras Condiciones de uso (por ejemplo, acoso entre menores –ciberbullyng–, acoso de un mayor de edad a un menor –grooming–, etc.). Se trata una vez más de un modelo de autorregulación donde son los propios usuarios los que a través de las herramientas y mecanismos que ponemos a su disposición, nos reportan dichas conductas o contenidos para que los retiremos y, en los casos más graves, los pongamos en conocimiento de las Autoridades.
- Tenemos a disposición de cualquier persona interesada, sin necesidad de estar siquiera registrado en Tuenti, un Centro de Ayuda y Seguridad (www.tuenti.com/privacidad), que hemos puesto en marcha con la colaboración de numerosas asociaciones e instituciones, con consejos y ayuda para usuarios, padres y educadores.

A modo de conclusión, para Tuenti la privacidad y la seguridad nunca han supuesto un problema en la práctica sino que ha sido en muchas ocasiones una solución útil para poder ofrecer lo que en la actualidad es la **plataforma más segura y privada,** lo que nos permite diferenciarnos de otras similares precisamente por esta especial protección de la privacidad y la seguridad.

Un ejemplo de cómo la privacidad nos ha ayudado a mejorar nuestro producto sería la distinción básica que ya hemos comentado entre amigos y contactos, puesta en marcha en septiembre de 2012 y que ha tenido una gran acogida en la medida que se trata de un servicio novedoso y una **alternativa real y gratuita, 100% española, a los servicios ya existentes de mensajería instantánea** como pueden ser la aplicación americana "WhatsApp" o la japonesa "Line", entre otros.

En los próximos años es muy probable que podamos encontrarnos ante empresas que ya no sólo compiten por tener la mejor tecnología, sino que competirán muy duramente por ofrecer a los usuarios herramientas que garanticen de un modo efectivo la **privacidad, transparencia y seguridad, incluso en dispositivos móviles** y allí es donde Tuenti continuará jugando un papel destacado gracias a su posicionamiento actual.

Javier Tamayo es abogado senior especializado en el ámbito de la Privacidad y el Derecho de las Nuevas Tecnologías y las Telecomunicaciones. Licenciado en Derecho por la Universidad Autónoma de Madrid. Master en Derecho de las Nuevas Tecnologías por la Fundación Universidad-Empresa y Master en Negocio y Derecho de las Telecomunicaciones, Internet y Audiovisual por el IEB.

SEEEEEEEEEEOOOOOOOOOO

Carlos Alonso de Linaje
Decano del Colegio de Economistas de Burgos
Vocal del Consejo Directivo de RASI-CGE
Presidente del Grupo de Trabajo de Marketing-CGE

Internet nos ha cambiado la vida de un modo u otro a todos nosotros. El conocimiento se ha democratizado residiendo en la voluntad del que lo genera, para su puesta a disposición de forma gratuita al resto de la humanidad. El cambio más influyente junto con la gratuidad es la accesibilidad a la información, desde cualquier lugar del mundo mediante un ordenador, una tablet o un teléfono (smartphone) podemos conectarnos con cualquier fuente de datos mundial en pocos segundos.

Con las técnicas SEO lo que pretendemos es mejorar la visibilidad de nuestros contenidos en los resultados orgánicos de los diferentes buscadores.

Estamos ante una nueva era de sobre-información en el sentido más estricto de la palabra. No solo se trata de la repetición hasta el hartazgo de la actualidad por los medios de comunicación; sino de la capacidad de la que disponemos todos nosotros de suministro de información a todos los niveles y de todas las materias que podamos imaginar. Ante esta situación, el reto es encontrar aquella información, aquel dato que necesitamos en un tiempo razonable.

SEO es el acróstico de Optimización de Motores de Búsqueda en inglés: **S**EARCH **E**NGINE **O**PTIMIZATION. El motor de búsqueda por excelencia en el mundo, pero de forma especial en Europa es GOOGLE por lo que fundamentalmente analizaré cómo funciona el posicionamiento SEO para este buscador o motor de búsqueda. En Junio de 2013, el 90,09% de los internautas mundiales utilizaba google llegando al 93,24% en Europa.

Con las técnicas SEO lo que pretendemos es mejorar la visibilidad de nuestros contenidos en los resultados orgánicos de los diferentes buscadores. Denominamos búsqueda orgánica a la que se realiza por palabras mediante un buscador. Para conseguirlo debemos conocer cuál es el proceso llevado a cabo por éstos para seleccionar las diferentes webs. El resultado que buscamos es estar en las primeras posiciones de la selección sugerida por el buscador por lo que en muchas ocasiones veremos cómo se refieren a estas herramientas como **Posicionamiento Web,** puesto que se persigue un buen posicionamiento, una buena posición.

La primera página de los resultados del buscador se lleva el 91,50% de los clicks de la búsqueda. Por lo tanto, podemos decir que si no consigues un lugar en esa primera página de google no existes o, si existes, la posibilidad de que seas encontrado o seleccionado por el internauta es muy baja. Podríamos analizar la trascendencia que tiene estar en uno de los tres primeros puestos del listado, pero perdería en gran medida importancia porque estos puestos suelen estar reservados al **Posicionamiento SEM** (**S**earch **E**ngine **M**arketing) que son los enlaces patrocinados, en definitiva, publicidad de pago. Es muy importante tener en cuenta que el uso de anuncios en Google (Google Adwords) no influye en la posición en la que un sitio aparece en las búsquedas orgánicas.

Los factores que influyen en el posicionamiento de nuestra página web, aunque deberíamos decir en los contenidos recogidos en nuestra página, puesto que el motor de búsqueda nos mostrará aquella parte de nuestra web que contenga las palabras que estén presentes en la búsqueda. La referencia al funcionamiento de estas herramientas la encontramos en el caso de Google en la página *Herramientas para*

La primera página de los resultados del buscador se lleva el 91,50% de los clicks de la búsqueda. Por lo tanto, podemos decir que si no consigues un lugar en esa primera página de google no existes o, si existes, la posibilidad de que seas encontrado o seleccionado por el internauta es muy baja.

Webmaster, para acceder a ella deberemos disponer de una cuenta personal en Google. En este sitio podrás descargarte en pdf una "Guía para principiantes para optimización para motores de búsqueda". En ella encontramos todos los conceptos necesarios para entender cómo funcionan los mecanismos de posicionamiento.

Podemos destacar dos tipos de factores: los primeros son aquéllos que están más cerca de la tecnología de programación y, los segundos, son los relacionados con los contenidos. A modo de aproximación al tema podemos destacar que los buscadores priman a aquellos que aportan valor a la red, por lo tanto será muy importante el contenido de nuestro sitio. El contenido ha de ser original y no redundante, si Google en su búsqueda encuentra contenidos iguales (copiados) nos penalizará en las búsquedas. No se debe tener la misma página con dos dominios distintos porque se entenderá como contenido repetido penalizándose en su posición. Son muy importantes las palabras de las que están compuestos los contenidos, debemos pensar que el motor de búsqueda funciona con palabra y por lo tanto cuantas más veces aparezcan las palabras buscadas en un texto entenderá que es más relevante su contenido. A su vez será muy importante que el contenido esté bien redactado, no debemos perder de vista el objetivo: que nos encuentre todo aquel que nos quiere buscar y al que potencialmente le interesamos. Debemos tener en cuenta nuestro ámbito competitivo –local, regional, nacional, internacional o mundial. No será lo mismo posicionar un sitio para aparecer en la primera página en Ávila que en Madrid o en Madrid que a nivel nacional, la competencia entre sitios hará que sea más difícil.

Como hemos venido explicando, el contenido es el rey pero existen otros factores, google en un principio se diferenció del resto de motores de búsqueda por priorizar la importancia de las páginas por un índice de relevancia denominado PAGERANK.

¿Que es el Pagerank?

Es el resultado numérico de un algoritmo creado por Google en 1999 para asignar la relevancia de las páginas web, indexadas por un motor de búsqueda. El nombre le viene dado por el apellido de su creador **Larry Page,** uno de los fundadores de Google. El valor de este indicador está en función de la notoriedad de las páginas que enlazan con un sitio, la notoriedad de las que enlazan desde este sitio. Así, si consigues enlaces a tu web desde páginas con mucha notoriedad como youtube, o slideshare, tendrás más posibilidades de obtener un mayor Pagerank. De igual modo, si desde tu página tienes enlaces a sitios de gran notoriedad mejoraras tu Pagerank. Su valor se encuentra entre cero y diez. En internet es fácil encontrar sitios que te faciliten el valor de tu Pagerank. En cuanto a los enlaces a tu página web, los puedes obtener en la página de *Herramientas de Webmaster* de Google.

El fin último del posicionamiento es conseguir tráfico a nuestro sitio. No debemos olvidar que la red y todas sus herramientas están al servicio del MARKETING. Son medios dentro de las herramientas de Comunicación o puede tener la consideración de Canal de Distribución dentro de la "P" de "Places", por lo que no debemos desvincular los resultados de la web de los objetivos de marketing, para no confundir los medios con el fin.

El fin último del posicionamiento es conseguir tráfico a nuestro sitio. No debemos olvidar que la red y todas sus herramientas están al servicio del MARKETING

SOBRE PREVENCIÓN DE BLANQUEO DE CAPITALES

El último párrafo del punto del punto 2 del art. 28 de la L 10/2010 dice:

"Los sujetos obligados no podrán encomendar la práctica del examen externo a aquellas personas físicas que les hayan prestado o presten cualquier otra clase de servicios retribuidos durante los tres años anteriores o posteriores a la emisión del informe".

1) ¿Significa esto que sí pueden encomendar la práctica del examen externo al que le preste otra clase de servicio retribuido en el mismo año del examen externo?

2) El punto 1 de mismo art. 28 dice: "...No obstante, en los dos años sucesivos a la emisión del informe podrá éste ser sustituido por un informe de seguimiento emitido por el experto externo, referido exclusivamente a la adecuación de las medidas adoptadas por el sujeto obligado para solventar las deficiencias identificadas. ¿Debe entenderse que la realización del informe de seguimiento no se considera "otra clase de servicio retribuido"?

3) ¿Está previsto que se emita alguna instrucción en relación con ese informe de seguimiento?

La LPBC y FT ha determinado la necesidad de independencia en la función y realización del informe anual de experto externo. Por este motivo está establecida la necesidad de que no hayan realizado servicios retribuidos ni tres años antes ni después del ejercicio de la emisión del informe. El mayor requisito de independencia es en el propio ejercicio de la emisión del informe.

Los informes de seguimiento son informes de revisión que cada experto deberá determinar la valoración del trabajo a realizar y los honorarios asociados. En relación a este informe no existen noticias de instrucciones al respecto. No obstante desde el CGE estamos realizando para el registro de expertos talleres y seminarios sobre realización de informes de experto externo de PBC y FT.

Soy asesor fiscal y tengo constancia de que uno de mis clientes lleva una contabilidad B ¿qué debo hacer? Si me acojo al secreto profesional ¿puedo seguir asesorando mi cliente como hasta ahora sin incurrir en un delito?

La Ley 10/2010, separándose de la evolución de la normativa anterior, en su artículo 22, no deja duda respecto de las obligaciones de los abogados en la prevención de blanqueo y de la compatibilidad de dichas obligaciones con el deber de secreto profesional. No ocurre lo mismo con el resto de los profesionales, entre los que están los asesores fiscales. En dicho artículo se establece que los abogados pueden establecer relaciones de negocio y ejecutar operaciones con los clientes, aunque no puedan aplicar las medidas de diligencia debida establecidas en la Ley, y no están sometidos a las obligaciones de proporcionar información y colaborar con el SEPBLAC, con respecto a la información que reciban de sus clientes u obtengan sobre los mismo al determinar la posición jurídica en favor de su cliente o en su misión de defenderle en procesos judiciales o en relación con ellos.

Se puede concluir, a la vista de varias diferencias entre los abogados y el resto de los profesionales, que no hay secreto profesional para los mismos –entre los que se encuentran asesores fiscales, contables y auditores– a partir de 2010. Hasta el 31 de abril de ese año les amparaba, al igual que a los abogados en el ejercicio de su profesión de defensa de su cliente, el secreto profesional.

De todo lo anterior, lo que tendrías que hacer es averiguar la procedencia del dinero en B y, a tenor de lo establecido en el artículo 19 de la citada Ley, abstenerte de ejecutar toda operación o pauta de comportamiento compleja, inusual o que presente indicios de simulación o fraude, que pueda estar relacionada con el blanqueo de capitales o la financiación del terrorismo, efectuando, en tal caso, una comunicación al SEPBLAC.

¿Qué se entiende por "medidas de diligencia debida"? En cuanto a su aplicación por terceros ¿puedo contratar a una consultora que se ocupe de la prevención de blanqueo de capitales de mi despacho de auditoría?

Por medidas de diligencia debida debemos entender el conjunto de actuaciones que deben desarrollar los sujetos obligados a fin de evitar las posibles operaciones de blanqueo de capitales, haciendo una diferenciación entre las medidas normales, las simplificadas y las reforzadas. Las medidas normales de diligencia debida son aquellas tendentes a la identificación del titular real o cliente, ya sea persona física o jurídica, recabar información para verificar su actividad y la procedencia de los fondos del cliente, realizar un seguimiento continuo de las actividades del cliente y clasificar al cliente según un análisis de riesgos.

Los sujetos obligados pueden recurrir a terceros sometidos a la Ley 10/2010, de prevención de blanqueo de capitales y financiación del terrorismo, para la aplicación de las medidas de diligencia debida, con excepción del seguimiento continuo de la relación de negocios con los clientes, manteniendo el sujeto obligado, tu despacho de auditoría en este caso, la plena responsabilidad respecto de la relación de negocios u operación, aún cuando el incumplimiento sea imputable al tercero, o consultora, sin perjuicio, en su caso, de la responsabilidad de este tercero.

Cuando se aceptó al cliente se comprobó que no estuviera incluido en las listas de personas de operativa restringida o susceptibles de estar vinculadas con la financiación del terrorismo. ¿debe realizarse dicha comprobación periódicamente aunque no diera positivo?

Sí, debe definirse un procedimiento de contraste periódico (anualmente, semestralmente,...) de toda la base de clientes contra las listas de personas de operativa restringida o susceptibles de estar vinculadas con la financiación del terrorismo para tener en cuenta posibles actualizaciones de las mismas.

SOBRE LEY ORGÁNICA DE PROTECCIÓN DE DATOS

En un momento determinado una empresa se plantea instalar cámaras de videovigilancia en sus instalaciones, el motivo es la avalancha de robos sufridos en los últimos meses. ¿Es suficiente la colocación de carteles informativos para cumplir la ley?

La respuesta es rotundamente no. Hay que tener en cuenta diversos aspectos y variables para cumplir con la norma, pero en todo caso la decisión de instalar cámaras de videovigilancia debe tomarse siempre y cuando no existan otras medidas menos intrusivas contra la intimidad de las personas que permitan garantizar la seguridad de las instalaciones.

Es muy importante que la instalación de las cámaras de videovigilancia y el posterior tratamiento de las imágenes cumplan, en todo caso, con lo previsto en la normativa laboral. Por ello es exigible proceder de forma concreta e individualizada a informar al respecto a cada uno de los trabajadores de la empresa, así como al Comité de Empresa en el caso que exista. Además, la videovigilancia debe cumplir con las exigencias de la normativa de protección de datos vigente, esto es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, complementada esta última con lo establecido en la Guía de Videovigilancia publicada por la misma Agencia Española de Protección de Datos en el año 2009.

La videovigilancia se debe limitar a los usos estrictamente necesarios captando imágenes en los espacios indispensables indicados para satisfacer las finalidades indicadas, respetándose el derecho a la intimidad del trabajador. En ningún caso se pueden instalar cámaras en espacios vetados para la utilización de este tipo de medidas como vestuarios, baños, taquillas o zonas de descanso, no registrándose tampoco las conversaciones privadas en el entorno laboral. En definitiva, la instalación de cámaras de videovigilancia que realice la empresa en ningún caso puede suponer la vulneración de derechos fundamentales del trabajador.

Asimismo, para dar cumplimiento a todas las exigencias establecidas legalmente y en la Instrucción anteriormente mencionada, es preceptiva la colocación de carteles informativos en lugares suficientemente visibles, tener a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999, así como el establecimiento de las medidas de seguridad atendiendo al tipo de datos tratados. De la misma manera, tanto el trabajador como cualquier persona que pueda ser videovigilada siempre tendrá la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición ante la empresa.

¿Cómo puedo asegurarme de que el proveedor de 'cloud' no conserva los datos personales si se extingue el contrato?

De hecho no puedes asegurarte de que el proveedor de cloud no vaya a conservar los datos una vez extinguido el contrato, a excepción que una auditoría independiente pueda certificarlo. Pero sí puedes asegúrate que el contrato de prestación de servicios con el proveedor de cloud, éste contrato debe firmarse antes de iniciar la relación mercantil, incluya una cláusula que dé cumplimiento a las previsiones del artículo 12 de la LOPD y relativo a tú pregunta concretamente el apartado 3 de dicho artículo.

RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

En relación a la responsabilidad penal de las personas jurídicas, en caso de producirse un delito por parte de un directivo que ha sido finalmente imputado y condenado, ¿tiene la empresa alguna responsabilidad?

La reforma del código penal a través de la L.O.5/2010 ha incorporado la responsabilidad penal de las empresas en aquellos delitos realizados, por su cuenta y en su beneficio, por los empleados si la empresa no ha implantado los controles para prevenir y evitar los mismos. Por este motivo, adicionalmente a la responsabilidad penal del empleado, se genera una responsabilidad penal complementaria para la empresa si ésta no ha cumplido los deberes de control.

RED SOCIAL CORPORATIVA

Hace dos años que desde Recursos Humanos llevamos impulsando el desarrollo de una red social interna como herramienta de comunicación. Sin embargo, pese a un comienzo muy ilusionante, la gente cada vez participa menos y la red está casi inactiva. ¿Podríais darnos algunas recomendaciones para su dinamización?

Es cierto que las redes sociales internas o corporativas son una potente herramienta de comunicación interna. Es común que sean utilizadas para generar espacios donde los empleados pueden comunicarse y colaborar entre si mejorando los niveles de eficiencia y productividad tal como ha quedado de manifiesto en algunos recientes estudios.

Sin embargo, hacer que estas plataformas funcionen no es sencillo. Una cultura empresarial poco colaborativa, el miedo a estar demasiado expuesto a los ojos del resto de la organización, la falta de tiempo o una errónea idea del objetivo de la red social que lleve a pensar que su uso supone una pérdida de tiempo, son algunos de los frenos más comunes con que se encuentran estos proyectos.

Para ayudarte a gestionar estas situaciones te damos algunos consejos que pueden serte de utilidad:

1. Define claramente los objetivos de la red social.
2. Elabora un plan de contenidos de acorde con los objetivos perseguidos.
3 Nombra un responsable de la red o Community Manager que ejecute el plan de contenidos y vele por el correcto funcionamiento de la red.
4. Identifica a las personas más proactivas e incorporarlas como aliados en las acciones de dinamización. Recompénsalas por ello.
5. Introduce técnica de gamificación que permitan vincular emocionalmente a los empleados con la red social de manera progresiva.
6. Incorpora un sistema de mediciones sencillo pero eficaz para medir la evolución de uso y reportar sus resultados.

CLOUD COMPUTING

Mis sistemas propietarios pueden estar en la nube sólo con pagar una IP fija, y tener los conocimientos necesarios para mantener un servidor en la red, con la suficiente confianza de que no me lo tumbarán los hackers ¿no es así?
Cloud computing es un paradigma que permite ofrecer servicios de computación a través de Internet.
Si externalizo mi gestión o mis sistemas, puede ser una decisión totalmente distinta.

Conectar tus sistemas propietarios a Internet no es estar en el cloud.

El cloud según la definición de NIST (National Institut of Standards and Technologies, 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf), es un "modelo para habilitar el acceso de red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio".

Este modelo de nube promueve la disponibilidad y está compuesto por:

- cinco características esenciales (Auto servicio bajo demanda, Acceso amplio desde la red, Conjunto de recursos, Rápida elasticidad y Servicio medido)
- tres modelos de servicio (Operadores de TI, Desarrolladores y Usuarios Finales)
- y cuatro modelos de despliegue (Privado, Público, Hibrido y Colaborativo)

Sólo y sólo si cumples con la definición anterior puedes considerar que estás trabajando en la nube.

La externalización de la gestión o de los sistemas no tiene porqué ir aparejada con el cloud, puede hacerse a través de Outsourcing o de Housing en plataformas que no tienen la consideración de cloud.

formación

Esta programación no está cerrada y se ampliará con más cursos que están en fase de preparación

Formación On Line

- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Expertos.
- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Socios y directivos.
- Curso on line de Protección de Datos Personales.
- Curso on line sobre Responsabilidad Penal de las Personas Jurídicas.
- Curso Oficial de Preparación al Examen CISA, Certified Information Systems Auditor (Disponible en modalidad presencial –Madrid y Barcelona– con importantes descuentos para miembros de RASI-CGE).

Formación Presencial

- Curso de Auditoría Informática: Fundamentos
- Aplicación e implicaciones de las recomendaciones del SEPBLAC
- Norma Técnica de Auditoría de Cuentas en Entornos Informatizados (BOICAC nº 54): Aplicabilidad de la norma utilizando el documento técnico y de referencia para la evaluación de los controles generales, preparado por ISACA Capítulo Barcelona.
- Norma Técnica de Auditoría de Cuentas en Entornos Informatizados (BOICAC Nº 54): Identificación y evaluación de los controles de aplicación en los sistemas de información que soportan los principales procesos del negocio significativos para la auditoría de cuentas.
- Políticas y Procedimientos de Seguridad de la Información: ISO 27001
- Continuidad del Negocio: ISO 22301
- Gestión del Riesgo: ISO 31000
- Gobierno y Gestión de las Tecnologías de la Información (COBIT 5)
- Control Interno y Gestión de Riesgos Corporativos (COSO II)
- Empleabilidad Economistas: Economía digital
- Adaptación de despachos a la economía digital
- Cómo gestionar mejor mi marca en las redes sociales
- Dinamización de mi empresa en las redes sociales

En colaboración con ISACA

- Preparación al examen CISA (Certified Information Systems Auditor)
- Preparación al examen CISM (Certified Information Security Manager)
- Preparación al examen CGEIT (Certified in the Governance of Enterprise IT)
- Preparación al examen CRISC (Certified in Risk and Information Systems Control)

Los Colegios interesados en realizar estos u otros cursos a nivel territorial, por favor, contactad con RASI a través del siguiente correo electrónico: rasi@economistas.org

Tercer Seminario Permanente de Protección de Datos Cátedra Google · CEU

El pasado 21 de mayo **Sara Argüello** y **Joaquim Altafaja** acudieron, en representación de RASI-CGE, al tercer Seminario permanente organizado por el CEU, en el marco de la Cátedra Google sobre Privacidad, Sociedad e Innovación, en el que –tras la ponencia sobre la percepción que de la protección de datos y su privacidad tienen los ciudadanos, impartida por **Alejandro Perales Albert,** Presidente de la Asociación de Usuarios de la Comunicación (AUC) y miembro del Consejo Consultivo de la Agencia Española de Protección de Datos, como vocal de los consumidores y usuarios– debatieron, junto a distintos expertos en Protección de Datos, Privacidad y Seguridad de la Información, distintos aspectos de interés en relación con el tema referido anteriormente.

Registro de Expertos en materia de Prevención de Blanqueo de Capitales

Nuestro registro va creciendo, agrupando ya a un gran número de profesionales que dedican parte o la totalidad de su actividad profesional a apoyar a otros despachos en el cumplimiento de sus obligaciones en materia de prevención de blanqueo de capitales y financiación del terrorismo. Desde RASI-CGE prestamos a estos profesionales distintos servicios de ayuda o estímulo en su quehacer diario, entre los que destaca el envío de boletines informativos, con novedades y noticias de interés en el ámbito de la prevención de blanqueo de capitales, así como un servicio de consultas.

Olimpiada de Cloud Computing

Del 8 al 12 de abril se celebró la Olimpiada de Cloud Computing en Madrid, una reunión plenaria del Comité Internacional de Normalización para la elaboración de normas técnicas para impulsar el desarrollo de las TIC en la nube. 80 expertos de 20 países –entre los que se encontraba **Alejandro García,** en representación de RASI-CGE– trabajan conjuntamente para defender los intereses de las empresas e instituciones de dichos países, de forma que se garantice unos niveles de calidad y estandarización óptimos dentro del sector de las Tecnologías de la Información.

Todos estos países son miembros del comité técnico internacional ISO/IEC JTC 1/SC 38, Servicios y plataformas para aplicaciones distribuidas, constituido en el seno de la Organización Internacional de Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC), con el fin de generar la estandarización de normas europeas e internacionales que afectan los sistemas y los equipos que permiten procesar la información por medios automáticos.

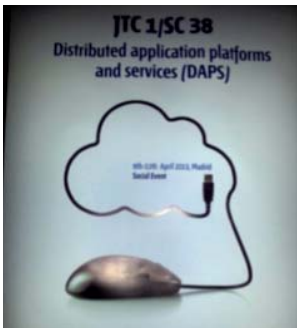
Actualmente, el Comité internacional de ISO e IEC trabaja en 5 proyectos de normas:

- ISO/IEC 17788 Tecnología de la información. Servicios y plataformas para aplicaciones distribuidas. Computación en la nube. Generalidades y vocabulario
- ISO/IEC 17789 Tecnología de la información. Computación en la nube. Arquitectura de referencia.
- ISO/IEC 18384-1 Especificación de servicios y plataformas para aplicaciones distribuidas de tecnología de la información. Arquitectura de referencia para arquitectura orientada al servicio. Parte 1: Terminología y conceptos para SOA.
- ISO/IEC 18384-2 Especificación de servicios y plataformas para aplicaciones distribuidas de tecnología de la información. Arquitectura de referencia para arquitectura orientada al servicio. Parte 2: Arquitectura de referencia para soluciones SOA.
- ISO/IEC 18384-3 Especificación de servicios y plataformas para aplicaciones distribuidas de tecnología de la información. Arquitectura de referencia para arquitectura orientada al servicio. Parte 3: Ontología para SOA.

Además, se trabaja en la elaboración de normas en el campo de la seguridad y la gestión de los servicios de cloud.

A pesar que las normas desarrolladas dentro de la ISO/IEC son voluntarias, ya que éstas no tienen la autoridad para imponer sus normas a ningún país, favorecen enormemente la prestación de servicios dentro del ámbito europeo y internacional. Por otra parte, están reconocidas globalmente por organizaciones tales como la Organización Mundial del Comercio o la Comisión Europea y los reguladores nacionales. Estas normas contribuirán al despliegue de los servicios TIC en la nube, permitiendo aumentar la calidad, seguridad y confianza de usuarios de todo el mundo en estas aplicaciones.

En estos momentos el Subcomité 38 está revisando el borrador de la norma UNE de Cloud enfocada a "Glosario de vocabulario y terminología". Se espera que esté publicada su aprobación en el BOE a finales de Septiembre del 2013 y posteriormente sea editada por AENOR, como norma UNE, antes de finalizar el presente año.



De igual modo, se está trabajando sobre el desarrollo de norma UNE enfocada a nivel de servicio. Dicho borrador debe ser presentado antes del 30 de Septiembre del 2013.

Jornada Formación RASI - Consejo General de Economistas

El pasado 31 de mayo se celebró una jornada con distintas sesiones sobre: estrategias de búsqueda y selección de contenido en internet, la importancia de las redes sociales para las empresas, tipologías y casos prácticos de prevención de blanqueo de capitales y el papel de los profesionales y la responsabilidad penal de las personas jurídicas.

José Ramón Castañares, Director de Estrategia de RRHH y Transformación de Telefónica, expuso la necesidad de alinear objetivos y estrategia desde la dirección para palpar los buenos resultados y las bondades que ofrecen las redes sociales, potenciando la agilidad, conexión global, digitalización y sociabilización. Concluye su presentación diciendo que "la red social es una decisión personal".

Mireia Ranera, Socia y Directora RRHH 2.0 Incipy, y **Fernando del Valle,** Director de RRHH del Grupo VIPS, recalcaron que "todo ha cambiado, estamos ante una revolución tecnológica y tenemos que adaptarnos" (…) "el social media es la conversación en curso del planeta".

Beatriz García, Consultora y dinamizadora de entornos de trabajo colaborativo en redes sociales, facilitó a los asistentes numerosas herramientas de búsqueda en internet e información sobre distintos gestores de contenidos.

Yazomary García, Asesora del Comité Directivo de RASI-CGE y responsable de la división de riesgo tecnológico de una firma de auditoría, señaló que "las compañías pueden establecer controles automáticos destinados a disuadir, prevenir, detectar y crear pruebas relacionadas con los delitos económicos, que puedan ser cometidos utilizando los recursos de tecnologías de información y comunicación corporativos, ya que existen fundamentos legales para ello".

Joaquim Altafaja, Asesor del Comité Directivo de RASI-CGE y Presidente de ISACA Barcelona, destacó que "las NIAs asientan un mayor trabajo sobre el control interno, pasando éste por las tecnologías de la información".

Saturnino Suances, del área penal y concursal de una firma de auditoría, hizo un repaso de los sujetos responsables, las penas y consecuencias de la responsabilidad penal e hizo un inventario de los requisitos del Plan Estratégico Penal que establece el anteproyecto de reforma del Código Penal.

A continuación, **Abel Bonet** hizo hincapié sobre la definición del posicionamiento y marco de actuación de la Alta Dirección en las áreas de riesgo.

VideoBlog del Consejo General de Economistas

El Consejo General de Economistas ha puesto en marcha una nueva iniciativa: un videoblog. **Joaquim Altafaja** ha participado, mediante la grabación de una *píldora* de un par de minutos sobre Cloud Computing, disponible en el blog, dando respuesta a las distintas consultas que le plantearon nuestros miembros.

Dados los buenos resultados de esta iniciativa buscaremos nuevos temas de interés para los miembros de RASI-CGE. Si queréis realizar alguna propuesta o sugerencia, estamos a vuestra disposición en rasi@economistas.org

Big Tent de Google

El 28 de junio, **Sara Argüello,** en representación de RASI-CGE, asistió al Big Tent de Google, foro de debate internacional que tiene por fin promover la reflexión en torno a internet, a las oportunidades que brinda para el desarrollo económico, cultural y social, así como los retos planteados en el entorno actual, bajo el título *Desarrollo económico y social para un nuevo paradigma.*

Inauguró la jornada **Bárbara Navarro,** Directora de Políticas Públicas y Asuntos Institucionales para el Sur de Europa de Google, dando paso a dos debates, una entrevista y una ponencia en las que se sacaron conclusiones muy interesantes sobre el papel de internet en el momento actual.

Emilio Ontiveros y **Francisco Ros** reflexionaron sobre si internet es un valor o un desafío. Ambos, al final, concluyeron que internet tiene parte de las dos.

Es un valor ya demostrado, dejando al margen prejuicios y guiándonos por una observación empírica, porque internet está transformando las economías, está permitiendo la democratización de las posibilidades de crecimiento y la difusión del conocimiento, esencia de los procesos de innovación. Por otro lado, es un desafío, asociado a cualquier revolución industrial, porque estamos ante la tercera..

Emilio Ontiveros, Ángel Expósito y Francisco Ros.

Julio Alonso y Vint Cerf

A continuación **Julio Alonso,** fundador y director de una empresa de blog, coordinó la sesión de **Vint Cerf,** vicepresidente y Chief Evangelist de Google, quien presentó las conclusiones siguientes: en primer lugar, "en España hay que aprovechar que en el mundo hay una gran población hispanoparlante pujante, por lo que se pueden aprovechar productos y servicios fabricados en España, no sólo debemos pensar a nivel local, si pueden dar servicio a mercado más grande, mayores oportunidades".

"Estamos ante un entorno propicio para promover nuevas oportunidades. Como en la teoría de la evolución de Darwin, hay dos opciones: adaptarse o morir. Eso se aplicará a las empresas, en las que se ha producido un cambio tecnológico o cambio en la demanda".

"La computación se convierte en parte de nuestro día a día, internet está omnipresente sin que nos demos cuenta, de momento somos conscientes de estar online, pero llegará un momento en que no se hará distinción online y offline".

En la siguiente sesión se reflexionó acerca de la educación, que está en el centro de modelo de sociedad que tenemos, aunque la tecnología está cambiando las cosas. Existe una nueva realidad aparte de la formación más tradicional, hay una clara demanda de formación a lo largo de toda la vida, pero tiene que ser capaz de resolver perfiles formativos que respondan a las nuevas profesiones, con instrumentos de formación online.

Maria Llopis, Javier Uceda y Cándido Méndez. Moderador: Carlos Salas.

Seminario Internacional
Los retos de la privacidad: innovación, derecho y seguridad

Los días 25 y 26 de junio, dentro del marco de la Cátedra Google sobre Privacidad, Sociedad e Innovación de la Universidad CEU San Pablo, se celebró un Seminario Internacional en el que, mediante 8 mesas redondas, se analizaron diversas cuestiones que se suscitan en torno a la privacidad y la innovación tecnológica en la sociedad actual y en el futuro. Distintas personalidades y profesionales debatieron sobre las respuestas de la industria frente a las exigencias de privacidad; el nuevo Reglamento europeo sobre el derecho a la protección de datos; la libertad de expresión y el derecho a la protección de datos personales; los desafíos que existen entre la privacidad e innovación; innovación, redes sociales y privacidad del menor y seguridad en internet; lucha contra la ciberdelincuencia y sistema de interceptación policial.

La conclusión principal extraída de las distintas sesiones de este seminario es la existencia de una gran preocupación por la seguridad jurídica de cara a usuarios y empresas, ya que cada prestador de servicios de internet tiene su propia política de privacidad y cada autoridad nacional aprueba su propia política de privacidad. El Reglamento, que proviene de una entidad supranacional, jugará un papel fundamental para acabar con esta inseguridad.

Además, la normativa española es escasa y obsoleta en esta materia. El reglamento 2007 no soluciona esta obsolescencia porque las circunstancias han cambiado, un ejemplo claro supone la figura del cloud computing, que cambia por completo el concepto de privacidad.

Las costumbres y la sociedad han cambiado; la cultura de protección de datos ha cambiado, … y las empresas tienen que ser sensibles a esta situación. Es necesario adaptar las normas a los nuevos entornos técnicos.

De izda. a dcha.: Juan Ignacio Sanz, Profesor de Tecnologías de la Información; José Luis Piñar, Catedrático de Derecho Administrativo y titular de la Cátedra; Ariane Mole, Socia de una empresa francesa y Nelson Remolina, de la Universidad de Colombia.

De izda. a dcha.: Francisco Fonseca, Jefe de la Representación de la CE en España; José Luis Piñar; Maria Ángels, Directora de la Autoridad Catalana de Protección de Datos; y Antonio Troncoso, Profesor de Derecho Constitucional de la Universidad de Cádiz y Ex Director de la Agencia de Protección de Datos de la Comunidad de Madrid.

RASI-CGE colabora con Fundetec en la elaboración del Informe ePyme

Fruto del Convenio de colaboración con FUNDETEC, RASI-CGE ha participado en la elaboración de la quinta edición del Informe ePyme *"Análisis Sectorial de la Implantación de las TIC en la Pyme española"*.

El día 5 de junio, RASI-CGE participó en el **I Congreso ePyme,** en el que se realizó un primer debate sobre las conclusiones del estudio y participamos en distintas mesas redondas sobre movilidad, cloud computing y comercio electrónico. La inauguración corrió a cargo de varios responsables de Red.es, la Oficina Española de Patentes y Marcas (OEPM), CEPYME y la Dirección General de Industria y de la PYME (DGIPYME).

Joaquim Altafaja, destacó en el debate principal del Congreso, algunos aspectos clave sobre cómo la tecnología incide en las pymes en el sector de economistas. Comentó que *"ha sido la Administración Pública quien ha impulsado la adopción de tecnologías, obligando a economistas y gestores a realizar los trámites con Hacienda por vía telemática."*

Continuó exponiendo *"la importancia de hacer un esfuerzo para luchar contra el inmovilismo ya que la sociedad está cambiando y nosotros hemos de evolucionar, la tecnología es complicada pero esto no puede ser una excusa, no es necesario que todos los profesionales lleguen a ser expertos en esta materia, pero al menos que llegue".*También comentó que *"RASI es el brazo armado de la innovación en el colectivo, cuyo fin último es mantener este liderazgo e impulsar el uso intensivo de las TIC, haciéndolas llegar al colectivo de economistas".*

La principal conclusión extraída de este Congreso es que a la pyme española le interesan las Tecnologías de la Información y la Comunicación (TIC), sobre todo aquellas que a un coste razonable le permiten obtener resultados inmediatos en la mejora de su negocio, y tiene claro que aprender a utilizar las nuevas herramientas digitales es imprescindible para conseguir ser competitivos en el mercado actual.

Últimas incorporaciones

Colegio de Economistas de Albacete:

Trigueros Romero, Emilio Francisco	Nº 270

Colegio de Economistas de Alicante:

Bernabeu Lledo, Pedro José	Nº 271
Miralles Verdú, Gabriel	Nº 285
Lledo Palomares, José Antonio	Nº 301

Colegio de Economistas de Almería:

Sierra Capel, Francisco Jesús	Nº 284
Mesa Batlles, Belén	Nº 314

Colegio de Economistas de Aragón:

Ramírez Espinosa, José	Nº 286
Fernández Lapetra, José Luis	Nº 306

Colegio de Economistas de Asturias:

Díez Noval, José Ignacio	Nº 297
Parrondo Rodríguez, Silvia	Nº 320

Colegio de Economistas de Burgos:

Payno de las Cuevas Díaz de la Espina, Alfonso	Nº 321

Colegio de Economistas de Cádiz:

Valdés Díaz, Faustino	Nº 272

Colegio de Economistas de Castellón:

Valiente Catalán, José Carlos	Nº 312
Ramírez Molina, José Manuel	Nº 317
Pineda San José, José Antonio	Nº 319
Latorre Relancio, Ana Beatriz	Nº 328

Colegio de Economistas de Cataluña:

Goma Piera, Salvador	Nº 274
Puigvert Ibars, Josep	Nº 289
Serracant Silvestre, Jordi	Nº 291
Bisquert Lafuente, Federico Joaquim	Nº 295
Ripoll Cortada, Santiago	Nº 305
Figueras Nadal, Ignacio	Nº 307
Coll Collet, Emili	Nº 322

Colegio de Economistas de Córdoba:

Montesinos Suárez, Rafael	Nº 329

Colegio de Economistas de Huelva:

Díaz Hernández, Mª de las Delicias	Nº 327

ÚLTIMAS INCORPORACIONES

Colegio de Economistas de Jaén:

Oya Casero, Alberto	Nº 299
Berrios Mesa, Sergio	Nº 304

Colegio de Economistas de La Coruña:

Pena Beiroa, José Antonio	Nº 292

Colegio de Economistas de La Rioja:

Martínez Torrecilla, Ángel María	Nº 300
Merino San Martín, José Antonio	Nº 318

Colegio de Economistas de León:

Bodelón Ovalle, Abel	Nº 280

Colegio de Economistas de Madrid:

Galindo Leal, Alberto	Nº 277
Pedraz González, Francisco José	Nº 282
Montava Llorens, José	Nº 287
Soltero Ramírez, Javier	Nº 296
Serrano Blanco, Francisco	Nº 309
Herrero Mallol, Ignacio	Nº 310
Rivas Clemot, Ricardo	Nº 313
Gutiérrez Narganes, Juan Carlos	Nº 315
García Corces, Juan Pablo	Nº 323

Colegio de Titulares Mercantiles de Madrid:

Fernández Martínez, Ernesto	Nº 278
Lara Lara, Lorenzo	Nº 283

Colegio de Economistas de Málaga:

Sánchez Aranda, José Luis	Nº 275
Galán Jiménez, Juan Ramón	Nº 281
Rueda García, Antonio	Nº 298

Colegio de Titulares Mercantiles de León:

Vallinas Antolín, Miguel Pedro	Nº 303
Llamazares Martínez, Ismael	Nº 324
Rodríguez Llanos, Manuel	Nº 326

Colegio de Economistas de Lugo:

Quindós Lindín, Cenen	Nº 288

Colegio de Economistas de Pontevedra:

Blanco Guerrero, Antonio	Nº 273
Prado Gallego, Jorge de	Nº 126

Colegio de Economistas de Sevilla:

Pérez Márquez, Francisco Manuel	Nº 276
Bausa Crespo, Susana	Nº 209
Rubio Rueda, Carlos	Nº 278
Gutiérrez Espá, Juan Carlos	Nº 293
Martínez Leal, José Manuel	Nº 308
Membrive Toledo, Francisco Javier	Nº 325

Colegio de Economistas de Valencia:

Torres Pérez, Antonio	Nº 279
Bravo Mateu, José Antonio	Nº 302
Peña Esteller, Carlos	Nº 311

Colegio de Economistas de Valladolid:

Alonso Álvarez, Javier	Nº 294
Hernández del Campo, Beatriz	Nº 316

REGISTRO DE EXPERTOS EN PBC Y FT

Colegio de Economistas de A Coruña:

Sánchez-Cendal Bermejo, Ángel

Colegio de Economistas de Albacete:

Fuster Matosas, Juan Antonio

Ruiz Jiménez, Ana Isabel

Colegio de Economistas de Alicante:

Peña Angulo, Miguel Ángel

Colegio de Economistas de Asturias:

Fernández Guinea, Juan Antonio

Fernández Rico, Valentín

Iglesias García, Ruperto

Colegio de Economistas de Cataluña:

Casals Altadill, Jaume

Coll i Collet, Emili

Fauria Reñe, María

Figueras Sans, Jordi

Goma Piera, Salvador

Herraiz Puchol, José Mariano

Llevat Palau, Jordi

Mestre Llop, Miquel

Montes Martínez, Carlos

Pallares Llorens, Merce

Prado Villarreal, Alberto

Colegio de Economistas de Ceuta:

Sánchez Aranda, José Luis

Colegio Economistas Extremadura:

Fernández Silva, Diego Mª

Colegio de Economistas de Illes Balears:

Lafuente Mir, Santiago

Colegio de Economistas de Madrid:

Carrillo Fernández, Emiliano

Godia Rada, Manuel María

Granda Coterillo, Ignacio Luis

Granero Yepes, Antonio

Núñez Astray, Adolfo

Soler de la Mano, Agustín María

Soltero Ramírez, Javier

Colegio de Economistas de Málaga:

Moreno Marín, José Antonio

Colegio de Economistas de Murcia:

Clemente Cayuela, Alberto

Colegio de Economistas de Navarra:

Ibarrola Navaz, José Luis

Colegio de Economistas de Pontevedra:

Prado Gallego, Jorge de

Colegio de Economistas de Sevilla:

Bausa Crespo, Susana

Rubio Rueda, Carlos

Colegio de Economistas de Valencia:

Lago Cordo, Federico Jaime

Moret Fort, Vicente

Roca Noguera, Martín

Colegio de Economistas de Valladolid:

Vidal Sevillano, Ana Belén

Colegio Vasco de Economistas:

Alaña Olabarri, Fermín Pablo

No están colegiados o no han identificado su Colegio de Economistas:

Borras Roma, Diana

Coma Batllori, Pere

Del Rio López, Iolanda

Lesan Solans, Lluis

Mauri Mur, Josep Mª

Palet Maso, Josep

Sueiras Calvo, Jordi

Villar Saltiberi, Sonia

RASI

¡inscríbete gratis durante 2013!

social media

compliance

e-commerce

cloud computing

protección de datos

prevención de blanqueo de capitales

abrimos el abanico de actuación de los economistas al mundo de los Sistemas de la Información

FORMACIÓN + INFORMACIÓN + CERTIFICACIONES

Para prestar soporte y ser un referente de los profesionales especializados en la auditoría y evaluación de los sistemas de información. Por la propia evolución de la tecnología en el entorno de los negocios, nos encontramos con la necesidad creciente de desarrollar profesionales en este área y fomentar el apoyo a las pymes.

economistas
Consejo General
RASI Auditores de Sistemas de la Información
Σ economistas y titulados mercantiles

solicitud de inscripción
www.rasi.economistas.org