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

Mayo 2014

RASI actualidad

REVISTA RASI · Asesores de Gobierno y Sistemas de la Información

Contenido

Presentación 2
Carlos Puig de Travy, Presidente RASI-CGE
Entrevista 4
Comisiones 12
Tribunas de opinión 15
Consultas 32
Formación 34
Noticias 36

NOTICIAS

El director del SEPBLAC visita la sede del CGE

El director del SEPBLAC, Juan Manuel Vega, tras estampar su firma en el Libro de Honor del Consejo, junto a Valentín Pich y Sara Argüello.

Página 37

Consejo Editorial

EDITA:
RASI-CGE

COORDINADORA:
Sara Argüello

COMITÉ DE REDACCIÓN:
Carlos Puig, Carlos Alonso de Linaje, Esteban García, José A. Canalejas, 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 4

Agenda Digital Europea

Francisco García Morán

La Agenda Digital para Europa es una de las siete iniciativas emblemáticas de la estrategia Europa 2020, y su propósito es definir la función capacitadora esencial que (...)

Tribunas de opinión

Obligaciones que impone la Ley de Prevención del Blanqueo de Capitales

Gregorio Labatut

Es conocido que el art. 2.1 letra m) de la Ley 10/2010 de prevención de blanqueo de capitales y financiación del (…) **Página 15**

La figura del economista-auditor en el desarrollo del Plan de Prevención Penal de las empresas

Yazomary García

Con la reforma del Código Penal en el año 2010 se introdujo un nuevo artículo, el 31 bis, y desde entonces toda Persona (…) **Página 22**

¿Qué haría falta modificar para que la inseguridad afectara a la contabilidad?

Antonio Ramos

El objetivo de este artículo es continuar explorando la propuesta que hicimos en el artículo titulado "El efecto contable que (…) **Página 24**

El whistleblower (denunciante) y los canales de denuncia

Pablo Paladini

La figura del whistleblower (denunciante) se torna clave dentro del esquema de control interno de una compañía, ya que (…) **Página 26**

Cómo usar las redes sociales para alcanzar los objetivos de negocio

Josep Puigvert y Andrés González

Las tecnologías 2.0 están cambiando la forma de comunicar de las empresas. Las inversiones de las marcas se están (…) **Página 28**

Ampliando nuestro campo de actuación

Carlos Puig de Travy
Presidente del RASI
y socio de Crowe Horwath

El desarrollo de las actividades del Registro se proyecta a través en tres líneas de actuación, a saber: Economía Digital, Gestión Tecnológica y Cumplimiento Normativo.

En la nueva etapa que el Registro emprendió fruto de la remodelación de su Consejo Directivo se puso como principal objetivo delimitar el alcance de las actuaciones que se deberían llevar a cabo al objeto de dar un servicio adecuado a sus miembros y en consonancia con la realidad del mercado que contempla desarrollos importantes en el campo de las tecnologías de la información.

El desarrollo de las actividades del Registro se proyecta a través en tres líneas de actuación, a saber Economía Digital, Gestión Tecnológica y Cumplimiento Normativo. Para cada una de estas líneas de actuación se establece una Comisión que será la encargada de llevar a cabo su plan de actuación y así delimitar el camino a seguir.

Dentro del área de Economía Digital se trabajarán, entre otras, las siguientes disciplinas, a saber, la estrategia digital, marketing digital, social media y *e-commerce*. El área de Gestión Tecnológica trabajará los temas de sistemas de gestión de calidad, auditoría y consultoría en TI, seguridad informática y *cloud computing*. Por último la Comisión de Cumplimiento Normativo se ocupará de los temas relacionados con protección de datos, prevención de blanqueo de capitales y responsabilidad penal de empresas, en general, todo lo relacionado con el cumplimiento legal y el derecho de las TIC.

Creemos que esta reorganización de las actividades del Registro permite orientar mejor nuestras líneas de trabajo y sobre todo con la creación de grupos específicos para cada una de las disciplinas que promoverán en mayor medida las actividades del Registro. Como veis estamos dando un papel más proactivo, tanto en temas de economía digital como en gestión tecnológica, disciplinas que hoy en día deben ser punteras en el ejercicio profesional de nuestras actividades debido a la enorme implicación que tienen en la economía actual.

Haciendo repaso de la historia, las tecnologías de la información podemos decir que hemos ido pasando por distintas etapas, una primera que se

estableció con el uso de las computadoras para pasar posteriormente al uso de las computadoras personales, todos recordamos la enorme revolución que trajo en nuestro trabajo los "pc's". A partir de aquí y fruto del desarrollo de internet se pasa del concepto de una computadora a la utilización de la red como ampliación de las capacidades de la computadora. Esta etapa inicia una era de nuevas formas de comunicación y nos lleva al fenómeno de la globalización, que no solo ha arraigado en el tema personal, sino también en el mundo de los negocios en donde empezó a hablarse de empresas virtuales, tiendas virtuales, etc como complementos y/o sustitutos de la realidad económica anterior. Por ello, los economistas no podemos trabajar obviando estos desarrollos que impactan fuertemente en la actividad económica y debemos tomarlos como aliados tanto para utilizarlos en nuestro propio trabajo como para ser un componente más dentro del rango de los servicios que ofrecemos al mercado.

A través de este número de nuestra revista que presentamos en el Foro del Economista queremos hacer partícipes a todos los economistas y titulares mercantiles de nuestro proyecto y emplazaros a que viváis con nosotros todos estos desarrollos que en el campo de las tecnologías de la información se vienen dando día a día, y que sin duda se darán en el futuro y presumiblemente con un mucho mayor impacto sobre el mundo en general y sobre el entorno económico en particular.

Creemos que esta reorganización de las actividades del Registro permite orientar mejor nuestras líneas de trabajo y sobre todo con la creación de grupos específicos para cada una de las disciplinas que promoverán en mayor medida las actividades del Registro.

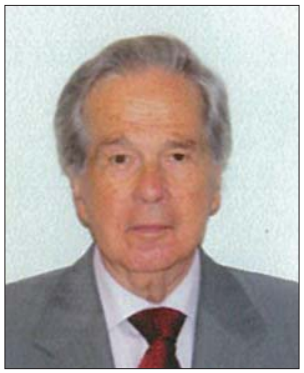
In memóriam

Alonso Hernández García

El 20 de febrero falleció nuestro querido compañero Alonso Hernández García, anterior presidente del Registro de Asesores de Gobierno y Sistemas de la Información (RASI).

Desde 1987, este Consejo General ha trabajado, primero a través de la Organización de Auditoria Informática, OAI, y después desde RASI, en la implantación y mejora de la Auditoria Informática en España. Para ello, este Consejo tuvo la fortuna de contar con Alonso Hernández, un pionero que supo reconocer la necesaria vinculación entre la economía y las tecnologías de la información, y la importancia de estas últimas en el ámbito empresarial, en la sociedad en general y en el desarrollo económico.

La favorable evolución del registro y las actividades que ha venido desarrollando hasta la fecha no hubieran sido posibles sin la dedicación que Alonso Hernández ha aportado a este Consejo.



Descansa en paz, compañero.

Agenda Digital Europea

Francisco García Morán
EC's Chief IT Advisor
Comisión Europea

La Agenda Digital para Europa es una de las siete iniciativas emblemáticas de la estrategia Europa 2020, y su propósito es definir la función capacitadora esencial que deberá desempeñar el uso de las tecnologías de la información y la comunicación (TIC) si Europa quiere hacer realidad sus ambiciones para 2020.

En esta entrevista se responden diversas cuestiones de interés sobre el funcionamiento y objetivos de la Agenda Digital.

A grandes rasgos, ¿qué es la Agenda Digital Europea? ¿cuál es el escenario que plantea la Agenda Digital en el marco de la iniciativa Europa 2020?

La finalidad genérica de la Agenda Digital es obtener todos aquellos beneficios económicos y sociales sostenibles que pueden derivarse de un mercado único digital basado en un internet rápido y ultrarrápido y en unas aplicaciones interoperables.

La crisis ha destruido años de progreso económico y social y dejado al descubierto los puntos débiles estructurales de la economía de la Unión Europea (UE). El objetivo principal de la UE debe ser hoy volver a la senda del crecimiento y el pleno empleo. Para conseguir un futuro sostenible, hay que ver más allá del corto plazo. Enfrentados a una situación de envejecimiento demográfico y competencia mundial, disponemos de tres opciones: trabajar más, trabajar durante más tiempo o trabajar con más inteligencia. Lo más probable es que tengamos que hacer las tres cosas, pero la última es la única que garantizará un incremento del nivel de vida de los europeos. A tal efecto, la Agenda Digital propone medidas que ha sido preciso adoptar de manera sistemática para poner a la UE la senda hacia un crecimiento inteligente, sostenible e incluyente. Sus propuestas establecerán el marco para las transformaciones a largo plazo que traerán consigo una sociedad y una economía crecientemente digitales.

En Septiembre del 2009, el presidente de la Comisión Europea (CE) José Manuel Durao Barroso, buscando el apoyo del Parlamento Europeo (PE) para su nombramiento para un segundo mandato como presidente de la CE, presentó a los recién elegidos diputados europeos visión sobre los objetivos a alcanzar por la UE en los próximos años que constituiría el marco de los trabajos de la institución durante su mandato. Sobre esta base, la Comisión Europea puso en marcha en marzo de 2010 la estrategia Europa 2020, con el objetivo de salir de la crisis y preparar a la economía de la UE para los retos de la próxima década. Europa 2020 expone una estrategia para conseguir unos niveles elevados de empleo, una economía de baja emisión de carbono, productividad y cohesión social, que debe aplicarse a través de medidas concretas a nivel nacional y de la UE. Esta batalla por el crecimiento y el empleo exige una toma de conciencia en las altas esferas políticas y la movilización en toda Europa de la totalidad de los agentes.

La Agenda Digital para Europa es una de las siete iniciativas emblemáticas de la estrategia Europa 2020, y su propósito es definir la función capacitadora esencial que deberá desempeñar el uso de las tecnologías de la información y la comunicación (TIC) si Europa quiere hacer realidad sus ambiciones para 2020.

La Agenda Digital no es una iniciativa que se hay gestado en un día; se ha basado en amplias consultas, y

en particular en las aportaciones del Informe sobre Competitividad Digital 2009 (COM 2009)390, en la consulta pública efectuada por la Comisión en 2009 sobre las futuras prioridades en TIC, en las Conclusiones del Consejo TTE de diciembre de 2009, la consulta y la estrategia Europa 2020, y en la ICT *Industry Partnership Contribution to the Spanish Presidency Digital Europe Strategy*, en el informe por propia iniciativa del Parlamento Europeo sobre 2015.eu y de la Declaración acordada en la reunión ministerial informal celebrada en Granada en abril de 2010. Todos estos documentos están disponibles en: http://ec.europa.eu/information society/eeurope/i2010/index en.htm.

El objetivo de esta Agenda es trazar un rumbo que permita maximizar el potencial económico y social de las TIC, y en particular de internet, como soporte esencial de la actividad económica y social: para hacer negocios, trabajar, jugar, comunicarse y expresarse en libertad. Si se consigue llevarla a buen fin, la Agenda fomentará la innovación, el crecimiento económico y la mejora de la vida cotidiana tanto para los ciudadanos como para las empresas. De esta manera, el despliegue generalizado y la utilización más eficaz de las tecnologías digitales permitirán a la UE afrontar los retos esenciales que tiene planteados y proporcionará a los europeos una mejor calidad de vida manifestada, por ejemplo, en una mejor atención sanitaria, unas soluciones de transporte más seguras y eficientes, un medio ambiente más limpio, nuevas oportunidades en materia de medios de comunicación y un acceso más fácil a los servicios públicos y a los contenidos culturales.

El objetivo de la Agenda Digital es trazar un rumbo que permita maximizar el potencial económico y social de las TIC, y en particular de internet, como soporte esencial de la actividad económica y social.

¿Cuáles son las principales prioridades y acciones previstas en la Agenda Digital?

El sector de las TIC es directamente responsable del 5 % del PIB europeo, con un valor de mercado de 660 000 millones de euros al año, pero contribuye mucho más al crecimiento de la productividad general (un 20 % directamente del sector de las TIC y un 30 % de las inversiones en TIC). Esto se debe al elevado grado de dinamismo e innovación inherente al sector y a su capacidad para transformar el modo de funcionamiento de otros sectores. Al mismo tiempo, ha ido aumentando la repercusión social de las TIC: por ejemplo, el hecho de que existan más de 250 millones de personas que usan Internet a diario en Europa y de que la práctica totalidad de los europeos disponga de teléfono móvil ha transformado el estilo de vida.

Pero, aun cuando el poder de transformación asociado a las TIC sea evidente, no es menos cierto que para explotarlo hay que hacer frente a retos importantes. Los muchos ciudadanos europeos que están adoptando un modo de vida digital, basado en una tecnología que se declara «mundial» y sin fronteras, no pueden aceptar que un mercado único concebido antes de internet siga tan incompleto en el entorno en línea. El disfrute de las tecnologías digitales en tanto que ciudadano, consumidor o trabajador se ve ensombrecido por preocupaciones relativas a la privacidad y la seguridad, por insuficiencias en el acceso a Internet o en la "usabilidad" y por la ausencia de la capacitación pertinente o de una accesibilidad para todos. Los europeos se sienten frustrados cuando las TIC no cumplen su promesa de mejora de los servicios públicos. Les inquieta que, tras haber acelerado internet la competencia por la inversión, el empleo y la influencia económica a nivel mundial, Europa no se esté equipando adecuadamente para prosperar en este sector en crecimiento de la economía del conocimiento.

Sobre la base de una consulta con las partes interesadas y de los elementos contenidos tanto en la Declaración de Granada como en la Resolución del Parlamento Europeo, la Comisión ha confeccionado la lista de los siete obstáculos más importantes

- *Fragmentación de los mercados digitales*
- *Falta de interoperabilidad*
- *Incremento de la ciberdelincuencia y riesgo de escasa confianza en las redes*

- *Ausencia de suficiente inversión en infraestructuras de telecomunicación*
- *Insuficiencia de los esfuerzos de investigación e innovación*
- *Carencias en la alfabetización y la capacitación digitales*
- *Pérdida de oportunidades para afrontar los retos sociales*

La Agenda Digital para Europa estructura sus acciones clave en torno a la necesidad de abordar sistemáticamente estos siete aspectos problemáticos, que como iniciativa horizontal abarca las tres dimensiones de crecimiento establecidas en Europa 2020. Estos aspectos se explicitan con más detalle en las secciones que figuran a continuación, demostrando la urgente necesidad de que las acciones definidas como conjunto de agendas positivas impulsen el rendimiento social y económico de Europa. La comisión permanecerá atenta a la aparición de obstáculos adicionales y reaccionará en consecuencia.

La Agenda Digital para Europa estructura sus acciones clave en torno a la necesidad de abordar sistemáticamente estos siete aspectos problemáticos, que como iniciativa horizontal abarca las tres dimensiones de crecimiento establecidas en Europa 2020.

La Agenda Digital exigirá un nivel sostenido de compromiso tanto a nivel de la UE como de los Estados miembros (incluido el nivel regional). No podrá tener éxito sin una importante contribución de las demás partes interesadas, incluidos los jóvenes «nativos digitales», que tanto tienen que enseñarnos. Esta Agenda constituye una instantánea de los problemas y oportunidades actuales y previsibles, y evolucionará a la luz de la experiencia y de las rápidas transformaciones de la tecnología y la sociedad.

Por lo tanto, los campos de actuación de la agenda Digital son los siguientes:

1. Un mercado único digital dinámico: Ya es hora de que un nuevo mercado único permita acceder a las ventajas de la era digital

2. Interoperabilidad y normas: Para construir una verdadera sociedad digital, es necesaria una interoperabilidad efectiva entre los productos y servicios de las TIC

3. Confianza y seguridad: Los europeos no adoptarán una tecnología en la que no confíen; la era digital no es ni el «Gran hermano» ni el «salvaje oeste cibernético».

4. Acceso rápido y ultrarrápido a Internet: Necesitamos una internet muy rápida para que la economía crezca vigorosamente y genere puestos de trabajo y prosperidad, así como para garantizar que los ciudadanos puedan acceder a los contenidos y servicios que desean.

5. Investigación e innovación: Europa debe invertir más en I+D y garantizar que nuestras mejores ideas lleguen al mercado.

6. Fomentar la alfabetización, la capacitación y la inclusión digitales: La era digital debe significar autonomía y emancipación; los antecedentes o la capacitación no deben constituirse en barreras para acceder a este potencial.

7. Beneficios que hacen posibles las TIC para la sociedad de la UE: Un uso inteligente de la tecnología y la explotación de la información nos ayudará a afrontar los retos que tiene planteados la sociedad, tales como el cambio climático y el envejecimiento de la población.

En la comunicación sobre la Agenda Digital de Mayo del 2010 se identificaron un total de 101 acciones a realizar por las isntituciones europeas y los estados mimebros. A finales del 2012 se añadieron algunas más relativas al empleo, una estrategia industrila europea para la fabricación de circutos electrónicos, la puesta en marcha de Connecting Europe Facility, Lanzamiento de una coalición para una mejora de las habilidades digitales y la creación de empleo en el sector TIC en el que se calcula que en el 2016 faltarán unos 700.000 profesionales, etc.

¿En qué medida la Agenda Digital paliará la creciente, y preocupante, expansión del "cibercrimen"? ¿cuáles son las necesidades identificadas, las políticas aplicadas y la estrategia de ciberseguridad para la Europa?

En Febrero del 2010, la Comisión Europea publicó una comunicación titulada *"Estrategia de Ciberseguridad de la UE: Un ciberespacio abierto, protegido y seguro"* dirigida al Consejo Europeo, el Parlamento Europeo y el Comité Económico y Social.

En esta comunicación se reconoce que durante las dos últimas décadas, Internet y más generalmente el ciberespacio ha tenido un tremendo impacto en todos los sectores de la sociedad. Nuestra vida cotidiana, los derechos fundamentales, las interacciones sociales y económicas dependen hoy día de que las TIC funcionen a la perfección. No cabe la menor duda que un ciberespacio abierto y libre ha promovido la inclusión política y social en todo el mundo ; se han roto las barreras entre los países, las comunidades y los ciudadanos, lo que permite la interacción y el intercambio de información e ideas de todo el mundo ; se ha proporcionado un foro para la libertad de expresión y el ejercicio de los derechos fundamentales y las personas empoderadas en su búsqueda de la democracia y sociedades más justas –como pasó, por ejemplo, durante la primavera árabe .

Para que el ciberespacio se mantenga abierto y libre, las mismas normas, principios y valores que la UE acepta en el mundo físico o real, deben aplicarse también online. Los derechos fundamentales, la democracia y el estado de derecho necesitan ser protegidos en el ciberespacio. Nuestra libertad y la prosperidad dependen cada vez más de un Internet robusto e innovador, que continuará prosperando mientras siga la contribución tanto del sector público o la sociedad civil como del sector privado a la innovación de manera a impulsar su crecimiento. Pero la libertad en línea requiere también seguridad. Internet y el ciberespacio deben ser protegidos de incidentes, actividades maliciosas y mal uso y los gobiernos tienen como tarea de gran envergadura el garantizar que el ciberespacio se mantenga libre y seguro. En este Los gobiernos tienen pues varias tareas: salvaguardar el acceso y la apertura, hacer respetar y proteger los derechos fundamentales en línea y mantener la fiabilidad y la interoperabilidad de Internet.

Al mismo tiempo, no hay que olvidar que el sector privado posee y opera partes muy significativas del ciberespacio, por lo que cualquier iniciativa que pretenda tener éxito en esta área, tiene que reconocer su liderazgo y responsabilidades.

En Febrero del 2010, la Comisión Europea publicó una comunicación titulada *"Estrategia de Ciberseguridad de la UE: Un ciberespacio abierto, protegido y seguro"* dirigida al Consejo Europeo, el Parlamento Europeo y el Comité Económico y Social.

La ciberseguridad no tiene fronteras y es por ello que la UE debe garantizar un entorno en línea que proporcione la mayor libertad y seguridad posible para beneficio de todos. Aunque la responsabilidad sobre la seguridad es predominantemente de los estados miembros, para hacer frente a los desafíos de seguridad en el ciberespacio, cuya naturaleza es cada vez más transnacional, la CE propone una estrategia que comprende un conjunto de acciones específicas con el objetivo de contribuir a mejorar el rendimiento global de la seguridad de Internet y del ciberespacio en la UE. Las acciones propuestas son tanto a corto como a largo plazo, e incluyen una variedad de instrumentos de política implicando diferentes tipos de actores, ya sean las instituciones de la UE, los estados miembros o la industria.

La visión de la UE que se presenta en la estrategia antes mencionada, se articula en cinco prioridades estratégicas para hacer frente a los retos indicados anteriormente:

- Asegurar una capacidad de recuperación en caso de ciberataques.

- Reducir drásticamente el cibercrimen.
- Desarrollar la política de ciberdefensa y las capacidades necesarias para asegurar una verdadera Política Común de Defensa y Seguridad adecuada (CSDP)
- Desarrollar los recursos industriales y tecnológicos necesarios para que la UE sea líder en el campo de la ciberseguridad.
- Establecer una política internacional coherente internacional coherente de la Unión Europea en lo que se refiere al ciberespacio, promoviendo al mismo tiempo los valores fundamentales de la UE.

¿Existe una estrategia de Gobierno Electrónico en la UE? Si este es el caso, ¿cuáles son los elementos básicos de dicha estrategia?

En Diciembre del 2010 la Comisión Europea hizo una comunicación al Consejo, el Parlamento Europeo y el Comité Económico social en la que se presentaba un *"Plan de Acción Europeo sobre Administración Electrónica 2011-2015: Aprovechamiento de las TIC para promover una administración pública inteligente, sostenible e innovadora"*.

La Agenda Digital para Europa sitúa la administración electrónica dentro de un conjunto completo de medidas encaminadas a explotar los beneficios asociados a las tecnologías de la información y la comunicación (TIC) en toda Europa. En un momento en que los recursos públicos se ven severamente limitados, las TIC pueden ayudar al sector público a crear formas innovadoras de prestar sus servicios a los ciudadanos, al tiempo que potencian la eficiencia y contienen los costes.

La disponibilidad de tecnologías innovadoras, tales como las redes sociales, ha hecho que los ciudadanos sean más exigentes en cuanto a lo que esperan cuando acceden a todo tipo de servicios en línea. Sin embargo, son contados los servicios transfronterizos de administración electrónica y, cuando se ofrecen, la mayor parte de los ciudadanos de la UE se muestran reacios a utilizarlos. Es absolutamente necesario avanzar hacia un modelo más abierto de diseño, producción y prestación de servicios en línea, aprovechando las posibilidades que ofrece la colaboración entre ciudadanos, empresarios y sociedad civil. La combinación de tecnologías nuevas, especificaciones abiertas, arquitecturas innovadoras y la disponibilidad de información del sector público pueden aportar más valor a los ciudadanos que disponen de menos recursos.

La Agenda Digital para Europa sitúa la administración electrónica dentro de un conjunto completo de medidas encaminadas a explotar los beneficios asociados a las tecnologías de la información y la comunicación (TIC) en toda Europa.

Por consiguiente, la Comisión propone un segundo Plan de Acción, el primero data del año 2006 (COM 2006/173 de 25.4.2006) sobre la administración electrónica cuyo objetivo es hacer realidad la ambiciosa visión contenida en la Declaración formulada con motivo de la 5ª Conferencia Ministerial sobre Administración Electrónica (la Declaración de Malmö), que contó también con el apoyo de la industria y de un grupo de representantes de los ciudadanos.

Con arreglo a esta ambiciosa visión, se aspira a que, para 2015, los *«gobiernos europeos sean reconocidos por ser abiertos, flexibles y cooperativos en sus relaciones con los ciudadanos y con las empresas. A que utilicen la administración electrónica para aumentar su eficiencia y eficacia y para mejorar constantemente los servicios públicos de manera a que atiendan las distintas necesidades de los usuarios y maximicen su valor público para, de esa manera, apoyar la transición de Europa a una economía líder basada en el conocimiento.»*

La Declaración de Malmö establece cuatro prioridades políticas para todas las administraciones públicas europeas a lo largo de los próximos cinco años:

- Los ciudadanos y las empresas han de ser empoderados por servicios de administración electrónica diseñados en base a las necesidades de los usuarios y

desarrollados en colaboración con terceros, así como por un acceso creciente a la información pública, la mayor transparencia y métodos más efectivos para la implicación de los participantes interesados en el proceso político.

- La movilidad en el mercado único ha de ser reforzada por servicios integrados de administración electrónica para la creación y la gestión de empresas, para el estudio, el trabajo, la residencia y la jubilación en cualquier país de la Unión Europea.
- La eficiencia y la eficacia ha de hacerse posible gracias a una esfuerzo constante para utilizar la administración electrónica y reducir así las cargas administrativas, mejorando así los procesos organizativos y promocionando una economía sostenible baja en emisiones de carbono.
- La implementación de las prioridades políticas ha de realizarse mediante los habilitadores clave apropiados y las precondiciones legales y técnicas.

Las administraciones tienen que prestar unos servicios públicos mejores utilizando menos recursos. Cada una de las prioridades políticas mencionadas apunta hacia ese objetivo, así como a aportar formas nuevas y mejores de entrar en contacto con los ciudadanos. La aparición de tecnologías innovadoras tales como las «arquitecturas orientadas al servicio» (SOA) o las «nubes» de servicios, junto con unas especificaciones más abiertas que facilitan la puesta en común, la reutilización y la interoperabilidad refuerzan la capacidad de las TIC para desempeñar un papel clave en esta búsqueda de la eficiencia en el sector público.

Las administraciones tienen que prestar unos servicios públicos mejores utilizando menos recursos. Cada una de las prioridades políticas mencionadas apunta hacia ese objetivo, así como a aportar formas nuevas y mejores de entrar en contacto con los ciudadanos.

Inscrito en el esfuerzo de toda la Comisión por promover una economía inteligente, sostenible e integradora para la Unión Europea, según se bosqueja en la estrategia Europa 2020, el presente Plan de acción contribuye al logro de dos objetivos clave de la Agenda Digital para Europa, a saber:

- A más tardar en 2015, deberían estar disponibles en línea determinados servicios públicos transfronterizos esenciales, permitiendo que los empresarios creen y exploten un negocio en cualquier lugar de Europa, con independencia de su localización original, y que los ciudadanos estudien, trabajen, residan y se jubilen en cualquier lugar de la Unión Europea.
- A más tardar en 2015, el 50 % de los ciudadanos de la UE habrán utilizado los servicios de administración electrónica.

Toda vez que los servicios de administración electrónica son también de gran importancia para las empresas, el presente Plan de acción se propone asimismo que, para 2015, el 80 % de las empresas hayan usado la administración electrónica.

Se proponen a continuación varias acciones relacionadas con las cuatro prioridades políticas enunciadas:

- Capacitación del usuario: Se trata de incrementar la capacidad de ciudadanos, empresas y otras organizaciones para comportarse proactivamente en la sociedad a través del uso de nuevas herramientas tecnológicas.
- Mercado interior: La mayor parte de los servicios en línea no funcionan más allá de las fronteras o solo son accesibles mediante procedimientos engorrosos. A fin de favorecer el mercado interior, los gobiernos deberían elaborar unos servicios «sin discontinuidades» para que los empresarios puedan crear y gestionar empresas, y resulte posible estudiar, trabajar, residir, recibir atención sanitaria y jubilarse en cualquier país de la Unión Europea.
- Eficiencia y eficacia de los gobiernos y las administraciones: Las acciones correspondientes a esta prioridad se centrarán en el uso de las TIC para hacer posibles cambios organizativos que permitan prestar unos servicios públicos mejores, menos invasivos, más

sostenibles y más rápidos, reduciendo la carga administrativa, mejorando los procesos organizativos y promoviendo una economía sostenible de bajas emisiones de carbono.

• Condiciones previas para el desarrollo de la administración electrónica: Es necesario instaurar diversas condiciones previas, técnicas y jurídicas, para que puedan ejecutarse las acciones que potenciarán los servicios de administración electrónica en Europa. Entre ellas figura la promoción de la interoperabilidad a través de las fronteras, que permitirá, entre otras cosas, compartir información, implantar ventanillas únicas y utilizar en toda Europa los sistemas (nacionales) de identidad electrónica y de pago. La interoperabilidad resulta más fácil si se dispone de unas especificaciones abiertas y se desarrollan habilitadores clave tales como la gestión de la identidad electrónica y el estímulo a la innovación en materia de administración electrónica.

¿Cuál es la estrategia de la Agenda Digital en el desarrollo del Cloud Computing?

En Septiembre del 2012 la Comisión Europea publicó una comunicación dirigida al Consejo, al Parlamento Europeo y al Comité Económico y Social titulada *"Agenda Digital: Una nueva estrategia para impulsar la productividad de las empresas y los gobiernos europeos a través de la computación en nube"*.

Esta estrategia describe las acciones necesarias para alcanzar el objetivo de crear 2,5 millones de nuevos empleos en Europa, y un producir un aumento anual de 160 mil millones de euros al PIB de la UE (en torno al 1 %), en 2020.

Las acciones clave de la estrategia son:

• Encontrar la forma de navegar en la jungla de normas técnicas existentes con objeto de asegurarse de que los usuarios de la computación en la nube puedan asegurarse la interoperabilidad, la portabilidad de datos y la reversibilidad. Es necesario identificar lo antes posible (2014) el conjunto mínimo de normas necesarias para alcanzar el objetivo antes mencionado.

• Apoyo al desarrollo de sistemas de certificación de confianza y seguridad a escala comunitaria para los proveedores de servicios de computación en la nube.

• Desarrollo de modelos de condiciones "seguras y justas" para los contratos de computación en la nube, incluyendo Acuerdos de Nivel de Servicio

• Un Partenariado Europeo para la Computación en la Nube en Europa, del que formen parte los Estados miembros y la industria con el fin de aprovechar el poder de compra del sector público (20 % del gasto total de TIC en la UE) para ayudar al desarrollo del mercado de la computación en la nube en la UE, de forma que se puedan aumentar las posibilidades de que los proveedores de computación en la nube europeos puedan crecer y alcanzar un tamaño que les permita ser competitivos y al mismo tiempo proporcionar una reducción de costes en la provisión de servicios de administración electrónica.

Esta estrategia describe las acciones necesarias para alcanzar el objetivo de crear 2,5 millones de nuevos empleos en Europa, y un producir un aumento anual de 160 mil millones de euros al PIB de la UE (en torno al 1 %), en 2020.

Predicar con el ejemplo: ¿La Comisión Europea tiene una estrategia interna de Gobierno Electrónico?

En efecto, la Comisión Europea quiere predicar con el ejemplo y su iniciativa interna de administración electrónica se llama la eCommission. La primera versión de esta iniciativa data del año 2001 y ha sido actualizada regularmente a lo largo de estos años. Una de la acciones importantes de la Agenda Digital Europea era precisamente la actualización de la eCommission y su alineamiento con los principio de la citada Agenda. En cumplimiento de este objetivo, la Comisión Europea aprobó el 1 de Agosto de 2012 la comunicación titulada *"eCommission 2012-2015: Delivering User Centric Digital Services"*.

Todas las administraciones públicas de la UE tienen como objetivos prioritarios "hacer más con menos" y lograr alcanzar un mejor alineamiento entre las TIC y las prioridades del "negocio" y todo ello con el fin de lograr ahorros y aumentar la eficiencia en la prestación de los servicios públicos.

Esto alentó a la Comisión a poner en marcha en Octubre del 2010 un proceso importante para racionalizar las TIC tanto en materia de infraestructuras como de sistemas de información para conseguir los antes mencionados ahorros y aumentar la calidad de los servicios. Al mismo tiempo y para garantizar el alineamiento entre la estrategia TIC y las estrategias del "negocio" mencionada más arriba, se puso en marcha un nuevo marco de Gobernanza de las TIC con participación tanto de los servicios horizontales como de los servicios a cargo de la definición y soporte de las políticas europeas. Dichas estructuras se encargan de establecer prioridades anuales y aprobar los planes de trabajo, lo que permitirá a la Comisión presentar, de manera eficiente y eficaz, moderna, flexible y centrada en el usuario los servicios digitales necesarios para el soporte de las políticas de la UE y así servir mejor a los ciudadanos, empresas y administraciones de la UE.

La iniciativa eComisión 2012-2015, es una progresión lógica de la eComisión 2006-2010 y totalmente alineada con los principios y prioridades de la Agenda Digital Europea y del Plan Europeo de eGovernment del que se ha hablado antes.

En efecto, los objetivos de la eCommission 2012-2015 son los siguientes:

- Reforzar la eficacia y la eficiencia y garantizar la continuidad de los servicios informáticos de la Comisión;
- Reducir los costes de desarrollo y de producción e incrementar su valor público a través de la innovación dentro del Marco Financiero Plurianual 2014-2020;
- Contribuir a la reducción de las cargas administrativas tanto para la Comisión como para los estados miembros mediante los correspondientes procesos de simplificación administrativa;
- Contribuir a mejorar la transparencia de la Comisión; y
- Eliminar las barreras digitales entre las administraciones públicas europeas.

Presentación de la Comisión de Economía Digital

La Comisión de Economía Digital es un grupo de reflexión e investigación del Registro de Asesores de Gobierno y Sistemas de la Información (RASI-CGE) que estudia la unión entre tecnología y economía, cómo interactúan y su aportación en la transformación en la forma de hacer negocios con respecto a cómo se venía haciendo tradicionalmente.

El objetivo de esta Comisión es facilitar a nuestros profesionales la adopción efectiva de las mejores prácticas en su actividad económica, buscando impulsar su modelo de negocio gracias a las herramientas que ha proporcionado la evolución de la tecnología y el entorno de la sociedad de la información. Las actividades que desarrolla la Comisión responden a los objetivos de proveer la formación y capacitación de los economistas y titulares mercantiles en las áreas de especialización de: estrategia digital, marketing digital, social media y e-commerce. Esta Comisión identifica la potencialidad de las técnicas de marketing digital en el sector de los servicios profesionales, proporcionando al profesional los conocimientos necesarios para la adopción de planes efectivos.

La Comisión está compuesta por un equipo de profesionales especializados en la digitalización de los despachos profesionales, cuyo interés común es compartir conocimientos y experiencias, así como colaborar con otros colegiados que busquen el propio desarrollo profesional y que deseen introducirse o profundizar en la estrategia a desarrollar.

La Comisión de Economía Digital elabora un plan de formación anual, proporciona cursos y seminarios on-line y presenciales, participa en jornadas y foros organizados por los colegios o el CGE, elabora documentos y guías de trabajo de utilidad para los economistas y titulares mercantiles, redacta documentos informativos y propone al Consejo Directivo del RASI las futuras líneas de orientación respecto a la estrategia digital.

Para la divulgación de contenidos y documentos, la Comisión utiliza los medios que RASI pone a disposición de los colegiados y asociados entre los que destacan la página web, las notas de aviso, las notas de prensa, InfoRasi y la revista trimestral del RASI.

Componen esta Comisión los siguientes miembros del Consejo Directivo de RASI-CGE:

Esteban García Pérez, Esteban Romero Frías, Carlos Alonso de Linaje García, Francisco José Vázquez Núñez, Victoria Cánovas Sánchez y Alfonso López Viñegla

Esteban García

Esteban Romero

Carlos Alonso de Linaje

Francisco José Vázquez

Victoria Cánovas

Alfonso López

Presentación de la Comisión de Gestión Tecnológica

La Comisión de Gestión Tecnológica está encuadrada dentro de la estructura organizativa del Registro de Asesores de Gobierno y Sistemas de la Información (RASI) y tiene como principal función la coordinación y el desarrollo de aquellas actividades que realiza el Registro en las áreas de evaluación de riesgos tecnológicos, auditoría y consultoría de los sistemas de información, seguridad y gobierno de las TIC, cloud computing y sistemas de gestión (ISO) orientados a las TIC.

Las actividades que desarrolla la Comisión responden a los objetivos de proveer la formación y capacitación de los economistas y titulares mercantiles en las TIC, relacionarse transversalmente con los Registros del CGE en aquellos aspectos relativos a las tecnologías de la información que les sean de interés, la elaboración de documentos técnicos en las áreas de competencia y por último, servir de vínculo de enlace y divulgación entre el colectivo de profesionales y la sociedad.

La Comisión está compuesta por un equipo de profesionales especializados en Tecnologías de la Información cuyo interés común es compartir conocimientos y experiencias, así como colaborar con otros colegiados que deseen introducirse o profundizar en la promoción y el uso de las TIC en la Pyme y que buscan el propio desarrollo profesional en torno a los Sistemas de Información.

La Comisión de Gestión Tecnológica elabora un plan de formación anual, participa en jornadas y foros organizados por los colegios o el CGE, elabora documentos y guías de trabajo de utilidad para los economistas y titulares mercantiles, redacta documentos informativos y propone al Consejo Directivo del RASI las futuras líneas de orientación respecto a las novedades que surgen del universo TIC.

Para la divulgación de contenidos y documentos, la Comisión utiliza los medios que RASI pone a disposición de los colegiados y asociados entre los que destacan la página web, las notas de aviso, las notas de prensa, InfoRasi y la revista trimestral del RASI.

Componen esta Comisión los siguientes miembros del Consejo Directivo de RASI-CGE:

Alejandro García Ruíz
Joaquim Altafaja Diví
Yazomary García García
César Martínez Barselo
Josep Puigvert Ibars

Alejandro García

Joaquim Altafaja

Yazomary García

César Martínez

Josep Puigvert

Presentación de la Comisión de Cumplimiento Normativo

Miguel Ángel Sánchez

Joaquim Altafaja

Yazomary García

Abel Bonet

Eduardo Rivera

La Comisión de Cumplimiento Normativo se encuadra dentro de la estructura organizativa del Registro de Asesores de Gobierno y Sistemas de la Información (RASI), tiene como principal función la coordinación y el desarrollo de aquellas actividades que realiza el Registro en las áreas de cumplimiento normativo, gestión de riesgos tecnológicos, protección de datos, prevención del blanqueo de capitales y financiación del terrorismo, plan de prevención penal y de forma amplia las áreas de conocimiento propias del llamado derecho digital.

Las actividades que desarrolla la Comisión responden a los objetivos de proveer la formación y capacitación de los economistas y titulares mercantiles en estas materias que relacionan las tecnologías de la Información y la Comunicación con el derecho digital, relacionarse transversalmente con los Registros del CGE en aquellos aspectos relativos al campo del derecho digital y al cumplimiento normativo que implique la actuación profesional del economista y titulado mercantil de forma individual o en un despacho profesional y la elaboración de documentos divulgativos del marco legislativo enfocados a las específicas necesidades de los colegiados.

La Comisión está compuesta por un equipo de profesionales especializados en derecho de las nuevas tecnologías cuyo interés común es compartir conocimientos y experiencias, así como colaborar con otros colegiados que busquen el propio desarrollo profesional y que deseen introducirse o profundizar en el derecho digital.

La Comisión de Cumplimiento Normativo elabora un plan de formación anual, proporciona cursos y seminarios *on-line* y presenciales, participa en jornadas y foros organizados por los colegios o el CGE, elabora documentos y guías de trabajo de utilidad para los economistas y titulares mercantiles, redacta documentos informativos y propone al Consejo Directivo del RASI las futuras líneas de orientación respecto a las novedades legislativas.

Para la divulgación de contenidos y documentos, la Comisión utiliza los medios que RASI pone a disposición de los colegiados y asociados entre los que destacan la página *web*, las notas de aviso, las notas de prensa, InfoRasi y la revista trimestral del RASI.

Componen esta Comisión los siguientes miembros del Consejo Directivo de RASI-CGE:

Miguel Ángel Sánchez Martín, Joaquim Altafaja Diví, Yazomary García García, Abel Bonet Dolcet y Eduardo Rivera Dianez

Obligaciones que impone la Ley de Prevención del Blanqueo de Capitales

Gregorio Labatut Serer
Profesor Titular de la Universidad de Valencia.
Presidente de Honor del Instituto de Expertos en Prevención de Blanqueo de capitales. INBLAC.
http://gregorio-labatut.blogspot.com.es/

Gregorio Labatut Serer aborda el tema de las Obligaciones que impone la Ley de Prevención del Blanqueo de Capitales a los auditores de cuentas, asesores fiscales y contables externos.
Analiza también el Régimen de umbrales del Reglamento.
Finalmente, tras la publicación del Reglamento de PBCyFT, Gregorio Labatut nos enumera la conclusiones extraídas tras asistir, junto a otros conferenciantes, a una jornada sobre compliance en Prevención de Blanqueo de Capitales en Valencia.

Es conocido que el art. 2.1 letra m) de la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo (FT), incluye como sujetos obligados a los "auditores de cuentas, contables externos o asesores fiscales".

En la Disposición Final Quinta de la Ley se habilitaba al Gobierno para que en el plazo de un año a contar desde la entrada en vigor de dicha Ley (30 de abril de 2010) aprobara las disposiciones reglamentarias para su ejecución y desarrollo. En la actualidad, casi cuatro años desde su aprobación, el desarrollo reglamentario sigue pendiente, pero mientras tanto, se aplicará el reglamento de la legislación anterior. Esto significa, que sigue vigente el Real Decreto 925/1995 y R.D. 54/2005 por el que se desarrolla el reglamento de la antigua ley 19/1993, y mantendrá su vigencia hasta que no entre en vigor el nuevo Reglamento según Ley 10/2010. (Disposición transitoria primera de la Ley 10/2010).

No obstante, actualmente existe un proyecto de reglamento que apareció en Septiembre de 2013, y que en los momentos de escribir este artículo todavía no ha visto la luz, pero que se espera se apruebe próximamente.

La Ley y el Proyecto de Reglamento impone una serie de obligaciones, que los asesores fiscales, contables y auditores deben conocer, porque el desconocimiento de la Ley no exime de su cumplimiento *"Ignorantia legis neminem excusat"*.

Todo ello es necesario porque la propia ley contempla un régimen sancionador que también es obligatorio conocer ya que el delito está tipificado con sanción administrativa por la propia Ley, pero también es un delito de blanqueo de capitales se recoge en el art. 301 del Código Penal.

Las obligaciones que la Ley impone pivotan sobre dos obligaciones fundamentales, que son el concepto de "diligencia debida" y la obligación de comunicación al Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de capitales (SEPBLAC) de las operaciones

sospechosas. Estas dos obligaciones se llevarán a cabo con más o menos intensidad en función del riesgo que tienen los sujetos obligados de que sus clientes puedan realizar operaciones de blanqueo de capitales.

Estas dos obligaciones que se establecen en los capítulos II y III de la Ley 10/2010, es para todos los sujetos obligados, sin posibilidad de excepción de ninguno de ellos, ni por razón de tamaño, ni por ningún otro motivo.

La Directiva 2005/60/CE del Parlamento Europeo y del Consejo 26, introdujo el enfoque basado en el riesgo, lo que supone que cada sujeto obligado debe conocer el riesgo de blanqueo que soporta sus clientes y desarrollar métodos para mitigarlo y manejarlo.

Para poder cumplir de forma correcta con estas dos obligaciones fundamentales, se contemplan otras obligaciones, pero teniendo en cuenta que las mismas tienen como finalidad poder cumplir con estas dos obligaciones básicas de diligencia debida con los clientes y deber de comunicación de operaciones sospechosas al SEPBLAC.

El concepto de "diligencia debida" impone a los sujetos obligados la responsabilidad de tomar las medidas oportunas para poder detectar y denunciar los indicios de delito de blanqueo de capitales que cometan sus clientes. Esto significa que ante el conocimiento de un delito, "no se puede mirar hacia otro lado", porque también es delito de blanqueo de capitales el encubrimiento o la ocultación de tales hechos.

En definitiva, se considera delito de blanqueo de capitales, el que adquiera, posea, utilice, convierta, o transmita bienes… Esto es quien adquiera o venda o convierta el dinero procedente de actos ilícitos (incluido el delito contra la Hacienda Pública), pero también se castiga la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes.

Por lo tanto, los auditores, asesores fiscales y contables deben tomar las medidas de diligencia debida con sus clientes para que no puedan ser acusados de encubrimiento. Todo ello en función del riesgo que cada despacho asume con el tipo de cliente que tiene. Con el fin de ayudar a detectar posibles operaciones de riesgo, el SEPBLAC ha publicado una serie de Catálogos ejemplificativos de operaciones de riesgo, los denominados COR, para algunos de los sujetos obligados[1].

Es fundamental, como medida de diligencia debida la identificación formal del titular real de la operación mediante documento justificativo, normalmente DNI, y de otras medidas contempladas en la Ley, pero obsérvese que se trata de identificar al titular real, con lo que habrá que tener mucho cuidado con los testaferros, para llegar al titular real. También es necesario tener un conocimiento de las operaciones del cliente y hacer un seguimiento de las mismas.

La Directiva 2005/60/CE del Parlamento Europeo y del Consejo 26, introdujo el enfoque basado en el riesgo, lo que supone que cada sujeto obligado debe conocer el riesgo de blanqueo que soporta sus clientes y desarrollar métodos para mitigarlo y manejarlo.

En este mismo sentido se pronunció recientemente el SEPBLAC que hizo público un documento sobre Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo (FT)[2].

Lo más importante del documento, es que la Ley 10/2010 de prevención del blanqueo de capitales y FT. no se aplicará por igual a todos clientes del sujeto obligado, sino que se realizará en función del riesgo

[1] En concreto para los asesores fiscales, contables y auditores de cuentas, existe el documento denominado: Catálogo ejemplificativo de operaciones de riesgo de blanqueo de capitales para profesionales.

[2] Puede verse en su página web: http://www.sepblac.es/espanol/home_esp.htm

que tengan sus clientes de cometer delitos de blanqueo de capitales y FT.

La propia Ley 10/2010 en su art.7 se indica claramente, que *"Los sujetos obligados deberán estar en condiciones de demostrar a las autoridades competentes que las medidas adoptadas tienen el alcance adecuado en vista del riesgo de blanqueo de capitales o de financiación del terrorismo mediante un previo análisis de riesgo que en todo caso deberá constar por escrito"*.

Por ese motivo, el SEPBLAC en su documento, indica que el riesgo o grado de exposición de los distintos sujetos obligados ante los intentos de blanqueo o FT de sus clientes, es muy diferente en función del tipo de actividad, cliente, zona geográfica, nacionalidad del cliente, procedencia de los fondos, etc.

Las estructuras, los procedimientos de control interno, herramientas y recursos a emplear en la prevención por parte de los distintos sujetos obligados deberán adaptarse a este distinto riesgo. Por ejemplo no soporta el mismo riesgo un banco que un asesor fiscal o un abogado. Tampoco es el mismo el riesgo que corre un asesor fiscal que tiene clientes con negocios en el extranjero y con mucho movimiento de dinero procedente de paraísos fiscales, que otro asesor fiscal cuyos clientes sean tradicionales y con poca posibilidad de realizar ningún delito de blanqueo.

Por ello, para detectar este riesgo, es necesaria la elaboración por parte de los sujetos obligados, con carácter previo, un informe de autoevaluación ante el riesgo de blanqueo de capitales ajustado al tipo de negocio el sujeto obligado.

Con respecto a la obligación de comunicación, el art. 18 de la Ley impone claramente la obligación de comunicar de inmediato y sin dilación cualquier conducta sospechosa de los clientes del despecho respecto de los delitos de blanqueo de capitales y financiación del terrorismo.

La conclusión de ese informe será determinar el grado de riesgo a que está expuesto el sujeto obligado, con arreglo al cual habrá que establecer las medidas adecuadas para abordarlo.

Según el documento del SEPBLAC, se trata de un documento eminentemente práctico y que hay que adaptar al tipo de negocio del sujeto obligado. Por lo que, en palabras del SEPBLAC debe ser una radiografía previa del negocio del sujeto obligado desde la óptica de la prevención de blanqueo de capitales.

Entre otras obligaciones, el concepto de diligencia debida, impone la obligación de establecer en el seno del despacho un órgano de Control Interno de supervisión y comunicación (salvo en algunas excepciones, que posteriormente comentaremos según el proyecto de reglamento) y establecer también una especie de protocolo interno o manual de procedimientos donde se explique una manera formal de actuación con respecto a los clientes del despacho. Todas estas obligaciones que establece la ley, y que el reglamento puede relajar según el tamaño del sujeto obligado, son instrumentos para la consecución de las obligaciones principales, que son los de diligencia debida y la obligación de comunicación.

El objetivo que se pretende es establecer una serie de procedimientos y medidas a tomar con respecto a los clientes, que garantice la susodicha diligencia debida y la obligación de comunicación.

Con respecto a la obligación de comunicación, el art. 18 de la Ley impone claramente la obligación de comunicar de inmediato y sin dilación cualquier conducta sospechosa de los clientes del despecho respecto de los delitos de blanqueo de capitales y financiación del terrorismo.

A este respecto, los sujetos obligados comunicarán, por iniciativa propia al SEPBLAC cualquier hecho u operación, incluso la mera tentativa, respecto al que, tras un examen especial de la operación o de la situación, exista indicio o certeza de que está relacionado con el blanqueo de capitales.

En particular, se comunicarán las operaciones que muestren una falta de correspondencia ostensible con la naturaleza, volumen de actividad o antecedentes operativos de los clientes, siempre que en el examen especial previsto, no se aprecie justificación económica, profesional o de negocio para la realización de las operaciones.

El art. 22 del Proyecto de Reglamento indica que los procedimientos de control interno determinarán, en función del riesgo, alertas adecuadas por tipología, intervinientes y cuantía de las operaciones. Las alertas generadas serán revisadas a efectos de determinar si procede el examen especial de la operación, de conformidad con lo establecido en este artículo.

En resumen, es obligatorio, y sin posibilidad de excepción:

1. Gestión del riesgo o exposición del sujeto obligado. Aplicable a todos los sujetos obligados, sin posibilidad de excepción.
2. Diligencia debida con respecto a la identificación del titular real. Requiere conocimiento de las operaciones y de las actividades de los clientes, origen de los fondos que deben quedar reflejadas por escrito. Aplicable a todos los sujetos obligados, sin posibilidad de excepción.
3. Conservación de documentos durante 10 años. Aplicable a todos los sujetos obligados, sin posibilidad de excepción.
4. Comunicación de sospechas al SEPBLAC, incluso por indicios. Análisis específico y comunicación al SEPBLAC de cualquier operación sospechosa de estar particularmente vinculada al blanqueo de capitales, tras un examen especial de la misma. Modelo F-19 aplicable a todos los sujetos obligados, sin posibilidad de excepción.
5. Cumplimentación de la información requerida por el SEPBLAC en cualquier momento. Aplicable a todos los sujetos obligados, sin posibilidad de excepción.
6. Abstención de ejecución de operaciones sospechosas. Aplicable a todos los sujetos obligados, sin posibilidad de excepción.
7. Confidencialidad. Deber de confidencialidad (no comunicar nada al cliente sobre las comunicaciones realizadas de sus posibles actividades ilícitas). Aplicable a todos los sujetos obligados, sin posibilidad de excepción.

Para poder cumplir de una forma eficiente con estas obligaciones fundamentales, la Ley contempla otras medidas complementarias, como son:

1. Medidas de control interno. Comprenden:
a. Nombramiento del representante ante el SEPBLAC y comunicación a este organismo.
b. La constitución en el seno del despacho del llamado órgano de Control Interno de supervisión y comunicación (en función del riesgo) y
c. La confección del manual de procedimientos de protocolo interno de actuación.
Algunas de estas obligaciones pueden ser relajadas reglamentariamente en función del tamaño del sujeto obligado, como veremos posteriormente.
2. Formación de su personal del despacho en cuanto al conocimiento de la Ley. La Ley no prevé en ningún momento su relajación.
3. Se impone por parte de la Ley (art.29) la obligación de someterse a un examen anual por experto externo, con el fin de evaluar los procedimientos de control interno establecidos. Esta obligación puede ser relajada reglamentariamente.

El art. 22 del Proyecto de Reglamento indica que los procedimientos de control interno determinarán, en función del riesgo, alertas adecuadas por tipología, intervinientes y cuantía de las operaciones. Las alertas generadas serán revisadas a efectos de determinar si procede el examen especial de la operación, de conformidad con lo establecido en este artículo.

Todas estas son las obligaciones, que impone la Ley a los sujetos obligados, y que el proyecto de reglamento desarrolla, existe obligación de dejar constancia escrita de todo ello, por lo tanto hay que preparar los ficheros correspondientes que habrá que conservar durante un periodo de 10 años.

En cuanto a la constitución de un órgano de control interno de prevención de blanqueo de capitales, los sujetos obligados establecerán un órgano adecuado de

Control Interno y comunicación en materia de prevención del blanqueo de capitales.

Este órgano de control interno será responsable de la aplicación de las políticas y procedimientos descritos en cuanto a la prevención del blanqueo de capitales. Dicho órgano de control interno, debe constar, en su caso, con representación de las distintas áreas de negocio del sujeto obligado (ejemplo: contabilidad, asesoría, auditoría, etc.).

Se reunirá, levantando acta expresa de los acuerdos adoptados, con la periodicidad que se determine en el manual de procedimiento de control interno.

En cuanto a esta obligación de constituir el órgano de control interno, se puede llevar a cabo de dos formas:

1. Mediante un órgano centralizado de prevención de las profesiones colegiadas.
2. Mediante un órgano de control interno en el seno de cada uno de los despachos.

La constitución de un órgano centralizado de prevención de las profesiones colegidas, debe realizarse a través de un colegio profesional, de tal modo que mediante Orden del Ministro de Economía y Hacienda podrá acordarse la constitución de órganos centralizados de prevención de las profesiones colegiadas sujetas a la presente Ley. De momento solamente se ha aprobado dichos órganos internos de profesiones colegiadas para los notarios y los registradores de la propiedad. Lo han solicitado también los abogados. Cualquier colectivo colegiado lo puede solicitar y posteriormente se regulará, pero tiene que solicitarlo un Colegio Profesional.

Estos órganos centralizados de prevención tendrán por función la intensificación y canalización de la colaboración de las profesiones colegiadas con las autoridades judiciales, policiales y administrativas responsables de la prevención y represión del blanqueo de capitales y de la financiación del terrorismo, sin perjuicio de la responsabilidad directa de los profesionales incorporados como sujetos obligados. Se nombrará un representante del órgano centralizado de prevención, que tendrá la condición de representante de los profesionales incorporados a efectos de la designación de un representante ante el SEPBLAC.

Los profesionales incorporados deberán facilitar al órgano centralizado de prevención toda la información que éste les requiera para el ejercicio de sus funciones.

Las comunicaciones al SEPBLAC se realizarán directamente por el sujeto obligado o a través del órgano centralizado.

Los profesionales incorporados deberán facilitar al órgano centralizado de prevención toda la información que éste les requiera para el ejercicio de sus funciones.

En definitiva, se trata de que el Colegio profesional asuma la función de organizar para todo el colectivo la constitución de un órgano de control interno único para todos, con el fin de canalizar a través de él las relaciones con el SEPBLAC.

Finalmente comentar que el proyecto de reglamento suaviza alguna de estas obligaciones para algunos sujetos obligados de menor tamaño. Es lo que se ha venido a denominar el Régimen de Umbrales, de tal manera que para aquellos sujetos obligados que con inclusión de los propietarios, ocupen menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 2 millones de euros, pues para estos sujetos obligados, no es obligatorio:

1. Comunicación del nombramiento del representante ante el SEPBLAC. Cuidado con esto porque no exceptúa la obligación de nombramiento, sino de comunicación al órgano correspondiente.
2. Confección del manual de procedimiento de prevención de blanqueo de capitales.
3. Examen externo por profesional independiente.
4. Formación de los empleados. Hay que matizar que no se obliga a la formación de los empleados pero si del titular de la explotación o del responsable del despacho.

Del mismo modo, no se obliga a la constitución de un órgano de control interno a aquellos sujetos obligados que con inclusión de los propietarios, ocupen menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 10 millones de euros.

Esto es lo que indica el proyecto de reglamento, no sabemos cómo quedará la versión definitiva del mismo. Pero en cualquier caso sobre estas excepciones hay cuestiones que queremos recalcar, como por ejemplo que se deben dar las dos circunstancias simultáneamente: Se ocupe a menos de un número determinado de personas y que el volumen de negocios o balance general no supere ciertas cantidades.

No se obliga a la constitución de un órgano de control interno a aquellos sujetos obligados que con inclusión de los propietarios, ocupen menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 10 millones de euros

También ante esto, hay que decir que no se explica que se entiende por:

- Personas ocupadas. ¿son trabajadores fijos, temporales?, ¿Cómo se hace el computo?
- Balance general, ¿a qué se refiere con esto?, ¿al activo, al patrimonio neto?

Todo esto son dudas importantes que el reglamento definitivo tendrá que aclarar.

Finalmente, comentar que la Ley 10/2010 en su art. 10.3 indica que *"Asimismo, reglamentariamente podrá autorizarse la no aplicación de todas o algunas de las medidas de diligencia debida en relación con aquellas operaciones que no excedan un umbral cuantitativo, bien singular, bien acumulado por periodos temporales, que, con carácter general, no superará los 1.000 euros"*.

En la misma línea, el art. 4.1 del Proyecto de Reglamento indica que es obligatoria tal identificación con documentos fehacientes, y con carácter previo al establecimiento de relaciones de negocio o a la ejecución de operaciones ocasionales por importe igual o superior a 1.000 euros, con excepción de las operaciones de envío de dinero y gestión de transferencias, donde no será aplicable umbral alguno para la identificación.

Un saludo cordial para todos los amables lectores.

Tras la publicación del Reglamento de PBCyFT, Gregorio Labatut asiste, junto a otros conferenciantes, a una jornada sobre compliance en Prevención de Blanqueo de Capitales en Valencia, en la que se extrajeron las siguientes conclusiones:

1. El polémico artículo 31.1 sobre la excepción de los corredores de comercio y los sujetos obligados comprendidos en el artículo 2.1 i) a u), ambos inclusive, que, con inclusión de los agentes, ocupen a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 2 millones de euros, quedan exceptuados de las obligaciones referidas en este artículo y en los artículos 32, 33, 35, 38 y 39, se concluyó, lo siguiente:

a. La referencia a los corredores de comercio debe ser un error, posiblemente se refiere a los corredores de seguros.

b. Existen dos obligaciones fundamentales, y que el Reglamento no puede eximir de ellas a nadie. Estas dos obligaciones fundamentales son: Diligencia debida con respecto a los clientes y obligación de comunicación de las operaciones sospechosas al SEPBLAC.

Para poder cumplir estas dos obligaciones con ciertas garantías existen unas obligaciones formales que ayudan a conseguir las dos obligaciones expuestas. En este sentido, la exención contemplada en el art. 31.1 del reglamento, con respecto a los contenidos de los artículos 32 (análisis de riesgos), 33 (manual de prevención, 35 (Órganos de control interno), 38 (examen externo) y 39 (formación), lo será en el contenido que dichos artículos del reglamento exceden sobre las obligaciones que establece la Ley. Esto es, el reglamento no puede exceptuar de obligaciones establecidas en la Ley y cuya exención no esté prevista en la misma de forma reglamentaria. Por lo tanto, estas obligaciones pueden ser relajadas, pero nunca exceptuadas de forma total. Por ejemplo:

- Análisis de riesgos. A estos sujetos más pequeños no se les exige todo lo expuesto en el art. 32, pero sí que deben realizar un análisis de riesgos de sus clientes de una forma más sencilla y adaptados a su tamaño y necesidades, tal y como expone el documento de Recomendaciones del SEPBLAC.

- La obligación del manual, es una obligación formal pero que el reglamento relaja para estos sujetos obligados más pequeños, pero que sin duda, para poder llevar a cabo las dos obligaciones establecidas antes, algún manual de protocolo debe existir, aunque no sea tan amplio como las exigencias que se dan a los sujetos obligados normales en el reglamento.

- Órgano de control interno. La Ley no exime a nadie, solamente para los sujetos obligados que no sean sociedades esta responsabilidad recaerá sobre el titular de la actividad, entonces, para estos sujetos más pequeños contemplados en el art. 31.1 del reglamento por lo menos se les debe de exigir lo mismo que para las personas físicas. Evidentemente esta función debe recaer sobre el administrador de la sociedad.

- Representante ante el Sepblac, entendemos que es necesario, ya que la Ley lo exige. Lo establecido en el art. 31.1 debe entenderse de que esta obligación debe recaer en el administrador, y que no se comunicarán al SEPBLAC.

- Formación. Los más pequeños serán preceptito que reciba la formación anual el representante o administrador de la sociedad, mientras que no se exige la formación anual para el resto de empleados, pero evidentemente alguna formación debe tener, aunque no sea de forma anual.

2. No se puede eximir a los sujetos obligados de las consecuencias de las sanciones administrativas o penales que puedan derivarse de sus actuaciones.

3. Posible uso de la Ley de prevención de blanqueo de capitales para combatir el fraude fiscal.

4. El delito contra la Hacienda Pública como delito subyacente del delito de blanqueo de capitales. Problemática y jurisprudencia. Casos en los que el delito fiscal es delito subyacente del delito de blanqueo y casos en los que no.

5. Nuevos paradigmas de la lucha contra el blanqueo de capitales. Surgimiento y evolución del concepto de delito.

6. Utilización del compliance en prevención de blanqueo como mecanismo propio de protección de la empresa ante los riesgos del delito de blanqueo y reducción de riesgos de situaciones no deseadas.

La figura del economista-auditor en el desarrollo del Plan de Prevención Penal de las empresas

Yazomary García
Miembro del Consejo Consultivo del RASI-CGCEE

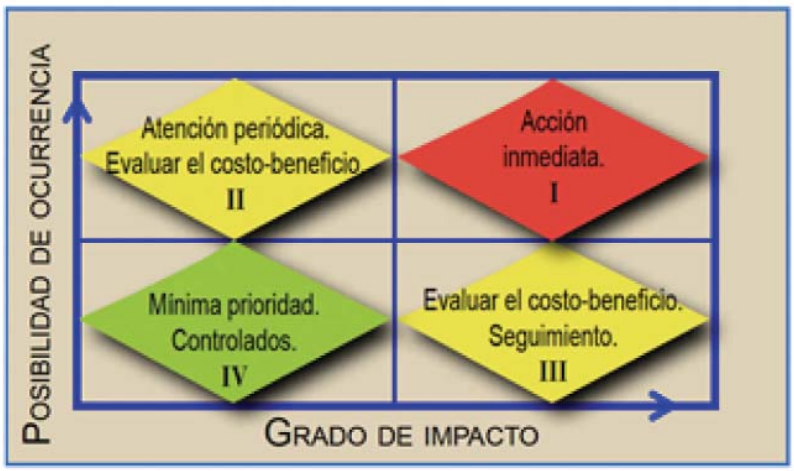
Con la reforma del Código Penal en el año 2010 se introdujo un nuevo artículo, el 31 bis, y desde entonces toda **Persona Jurídica** se enfrenta a dos nuevos riesgos penales por:

- 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 atendidas las concretas circunstancias del caso.

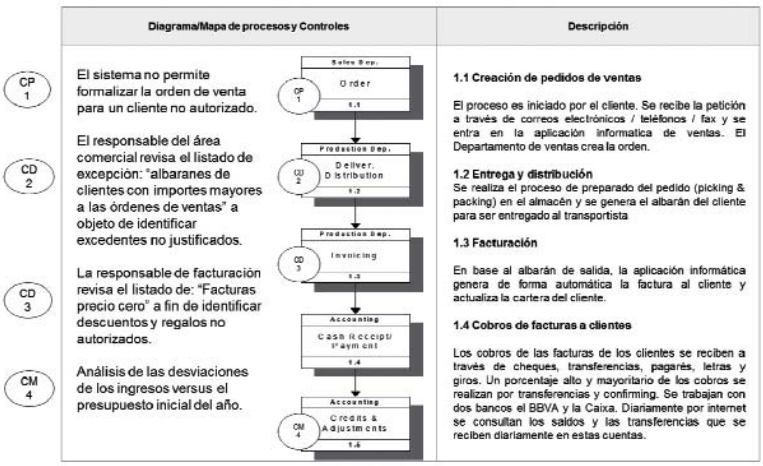
Asimismo, se encuentra en trámite un Proyecto de Ley de Reforma del Código Penal (nº 121/000065) cuya aprobación por las Cortes Generales y entrada en vigor está prevista para finales del año 2014.

Dicho Proyecto de Ley establece, como **deber y exigencia**, la obligación de aplicar un Plan de Prevención Penal para las empresas. A su vez, amplía la responsabilidad de las personas jurídicas y prevé sanciones para los directivos de las entidades en las que se cometan delitos por falta de adopción de medidas de prevención.

El Proyecto de Ley expresamente establece como eximente de responsabilidad penal en la empresa el haberse adoptado y ejecutado un modelo de gestión y control eficaz para la prevención del delito, incluyendo medidas de vigilancia, control y supervisión por órgano autónomo.



Ejemplo de mapa de riesgos de delito penal



Ejemplo de Diagrama/Mapa de procesos y controles

En este sentido, en la elaboración del Plan de Prevención Penal se presentan diversas oportunidades de actuación para los economistas-auditores, por ser profesionales con amplios conocimientos sobre los procesos del negocio y riesgos en los diferentes sectores e industria.

En la aplicación de la metodología de trabajo para el desarrollo del Plan, nos encontramos que gran parte del mismo se centra en:

- el entendimiento del negocio, a través de la revisión de información financiera, organigramas funcionales y jerárquicos, manuales internos de la compañía, entre otros.
- la evaluación de procesos, donde se realiza un análisis de las actividades y áreas de negocio de la entidad, empresas vinculadas y filiales (en su caso) a fin de identificar los eventos, personal clave, interdependencia de procesos y los controles en cada una de las actividades susceptibles de generar riesgos con transcendencia penal. Para ello se utilizan herramientas de diagramación de procesos/controles (flowcharts).
- el análisis e identificación de riesgos y oportunidades a lo largo de todos los procesos que previamente han sido determinados como relevantes en la identificación de riesgos de delitos penales. Para ello, se representa de forma gráfica el nivel de exposición (bajo, mediano o alto) de la compañía frente a los riesgos identificados.

Es destacable pues que los tres aspectos indicados sobre los que se centra el Plan son ampliamente conocidos por los economistas-auditores que podemos aportar nuestra experiencia adquirida en auditorías en aspectos tales como conocimiento del negocio y, principalmente, en la identificación de riesgos.

Ahora bien, me gustaría destacar que para la elaboración del plan de prevención penal debe existir una estrecha colaboración entre los economistas-auditores y abogados penalistas, consultores de riesgos/procesos/negocio, consultores en tecnologías de la información y otros profesionales especialistas que permitan conformar un equipo multidisciplinar con todas las competencias necesarias para el desarrollo de un Plan de Prevención Penal.

Para ampliar o aclarar la información presentada en particular pueden contactar con nosotros a través de nuestra dirección de correo electrónico: rasi@economistas.org

¿Qué haría falta modificar para que la inseguridad afectara a la contabilidad?

Antonio Ramos
Presidente de ISACA Madrid y Socio Director de n+1 Intelligence & Research

El meollo de la cuestión está en cómo interpretar el deterioro de valor de los activos.

¿Se puede pensar que una vulnerabilidad estaría entre los hechos y circunstancias que podrían causar un deterioro de valor?

El objetivo de este artículo es continuar explorando la propuesta que hicimos en el artículo titulado *"El efecto contable que debería tener la inseguridad informática"* publicado en el pasado número de esta misma revista.

Como recordará el lector, la propuesta que se presentaba era que **la inseguridad tuviera reflejo contable como un menor valor de los activos** con el objetivo de que las decisiones de las organizaciones en materia de ciberseguridad consideraran los potenciales efectos de no invertir en seguridad (que como vimos, en muchas ocasiones son externalidades) y tomaran mejores decisiones sobre las necesidades de protección de sus sistemas de información.

Pero, ¿cómo se podría lograr esa afectación? ¿Qué leyes habría que cambiar? ¿Es realmente factible o es una quimera?

Para intentar responder estas preguntas (que cómo es lógico le han surgido a cualquier que haya considerado la propuesta como útil), vamos a comenzar analizando la Resolución de 18 de septiembre de 2013, del Instituto de Contabilidad y Auditoría de Cuentas, por la que se dictan normas de registro y valoración e información a incluir en la memoria de las cuentas anuales sobre el deterioro del valor de los activos.

En cuanto al objeto, la *"Resolución desarrolla los criterios sobre deterioro de valor del inmovilizado material, inmovilizado intangible […]"* por lo que entendemos que cubriría lo requerido por la mencionada propuesta.

El meollo de la cuestión está en cómo interpretar **el deterioro del valor de los activos**. Según la resolución, *"el deterioro es la pérdida estimada en el valor del activo que representa la dificultad de recuperar, a través de su uso, su venta u otra forma de disposición, la totalidad de su valor contable"*. Por lo tanto, interpretando que las vulnerabilidades significaran que no se podría recuperar a través de su uso su valor contable, lo cual no es tan ilógico, sino que es justo lo que argumentábamos en nuestro anterior artículo, estaría justificado defender cierto deterioro de su valor.

Sin embargo, el límite siempre es su valor contable, como así se establece el mismo artículo: *"Un activo se ha deteriorado cuando su valor contable es superior a su importe recuperable"*. Y decimos que es una limitación,

porque nuestra propuesta era que se dotara una provisión por el valor del negocio que soportaba el activo con vulnerabilidades, que siempre sería superior al valor contable de dicho activo.

Aunque, podríamos encontrar acogida a nuestra propuesta en la norma tercera en la que la resolución indica que *"el término activo […] deberá entenderse extensivo al de unidad generadora de efectivo"*. Con esta redacción, ¿no podría interpretarse que el proceso de negocio que es el que genera el efectivo (con el soporte del activo con vulnerabilidad) sería el que tendría que recoger el deterioro de valoración? De hecho, la propia resolución llega a decir que *"Cuando no pudieran identificarse unidades generadoras de efectivo a un nivel inferior, desde la perspectiva de cuentas anuales, la empresa en su conjunto se calificará como una unidad generadora de efectivo"*.

Si no se atendiera a esta interpretación, sí que haría falta encontrar una norma que habilitara a reconocer un pasivo en el caso en el que el importe estimado de la pérdida fuera mayor que el importe en libros del activo (apartado 3. Reconocimiento y valoración de las pérdidas por deterioro del valor de un activo)

En cualquier caso, esta *"circunstancia obliga a reconocer una pérdida por deterioro en la cuenta de pérdidas y ganancias y la correspondiente corrección valorativa"* que es justo el argumento para nuestra propuesta: Causar un efecto en la contabilidad de la organización con vulnerabilidades en sus activos.

Otro aspecto interesante es la cuantificación de la pérdida. Según nuestra propuesta, el importe de la corrección debería ser proporcional a la gravedad de la vulnerabilidad del activo, es decir, *"las estimaciones se realizarán con imparcialidad y objetividad"*, por tanto, de nuevo vemos que la propuesta encuentra respaldo en el texto de la resolución que estamos analizando.

También en esta norma se recogen los hechos y circunstancias que deberán ser considerados al evaluar si existe indicio de que el valor de un activo se ha deteriorado. En este punto, la pregunta es obvia, ¿se puede pensar que una vulnerabilidad estaría entre los hechos y circunstancias que podrían causar un deterioro de valor? A mi juicio, existen dos puntos en los que se podría encajar este concepto (aunque la relación de indicios propuesta no es exhaustiva y cualquier otro también podría ser utilizado):

- *"g) Existen **dudas razonables de que el rendimiento técnico** y económico del activo se pueda mantener en el futuro […]*
- *i) Cese **o reducción significativa de la demanda** o necesidad de los servicios prestados con el activo."*

Otro aspecto no menos relevante para que la figura del auditor tenga el protagonismo necesario en esta materia es la información que es necesario incluir en la memoria. En este sentido, la resolución exige que, entre otras cosas, la *"empresa revelará […] el importe de las pérdidas por deterioro del valor reconocidas en el resultado del ejercicio"*, así como, *"los principales eventos y circunstancias que han llevado al reconocimiento de estas pérdidas por deterioro del valor"*, es decir, habría que informar sobre el tipo y gravedad de vulnerabilidades que han conducido al deterioro del valor del activo.

Por tanto, una vez analizada la Resolución , habría que dar respuesta a la pregunta que nos planteábamos al inicio, ¿qué habría que modificar para que la inseguridad afectara a la contabilidad? Claramente, **no parece ser necesario modificar la resolución ni incluir ningún tipo de disposición** nueva para encontrar el marco para hacer que las vulnerabilidades afecten a la valoración contable de los activos; quizás podría ser interesante una guía para aclarar cómo la gravedad de las vulnerabilidades reduce dicho valor de manera proporcional a su gravedad o en qué casos se puede utilizar la unidad generadora de efectivo como sujeto de la reducción de valor.

Por tanto, ¿a qué esperamos para hacer que la inseguridad afecte al valor contable de las empresas?

El *whistleblower* (denunciante) y los canales de denuncia

Pablo Paladini
CIA, QAR - Gerente de Operaciones de Resguarda

La importancia de la actividad del *whistleblower* (Denunciante) dentro del proceso activo del fraude, instrumentada en base a una línea de reporte de irregularidades interna o externa, se encuentra íntimamente relacionada con las estructuras de control interno de las empresas y sus debilidades.

La figura del *whistleblower* (denunciante) se torna clave dentro del esquema de control interno de una compañía, ya que su existencia desencadena la detección de las irregularidades dentro de grandes corporaciones, tal como sucedió en casos como ENRON, WorldCom, MCI, entre otras, y asimismo en entidades de gobierno (por ejemplo el IRS de Estados Unidos mantiene una oficina especial de *"Whistleblower (Denunciante) activity"* que realiza un reporte anual al congreso a través de la sección 7623 de la Ley nominada originalmente como *"Tax Relief and Health Care Act of 2006"*[1] y hasta en empresas de pequeña y mediana envergadura.

Se destaca que en Estados Unidos existe todo un marco legal regulatorio tendente a las personas que actúan como *whistleblower* (denunciante) debido al importante rol que juegan dentro de las grandes empresas. Estadísticas proporcionadas por la ACFE *(Association of Certified Fraud Examiners)* en sus reportes anuales[2,3] de 2008 y 2006 (se emiten en forma bianual) revelan que el principal método para la detección de fraudes dentro de las empresas es la realización de denuncias por participantes pasivos, sobre otras formas de control tales como auditoría interna o controles internos.

La importancia de la actividad del *whistleblower* (denunciante) dentro del proceso activo del fraude, instrumentada en base a una línea de reporte de irregularidades interna o externa, se encuentra íntimamente relacionada con las estructuras de control interno de las empresas y sus debilidades.

Una de las principales debilidades de un sistema de control interno, de acuerdo al Marco Integral de Control Interno (Reporte COSO), es la elusión de los controles por parte de los directores y gerentes ejecutivos debido a que su posición dentro de la organización les permite mantener una gran cantidad de recursos económicos y personal a su disposición.

¿Cómo diseñar controles efectivos para mitigar artilugios de contabilidad creativa para exagerar resultados o esconder pérdidas, cuando los mismos son llevados a cabo por la alta gerencia y personal clave del área de otras áreas?

[1] Para un mayor desarrollo de las etapas resumidas remitirse al documento original mencionado.

[2] Report to the Nation 2006 (fuente ACFE)

[3] Report to the Nation 2008 (fuente ACFE)

Bajo estas circunstancias resulta muy complejo para las organizaciones establecer y parametrizar controles internos efectivos que actúen de manera oportuna sobre esas debilidades, por lo que resulta indispensable incorporar un ambiente de control que contemple la existencia de canales de comunicación ágiles y efectivos que den lugar a que el personal que observe desviaciones respecto de las políticas de la empresa o bien reciba presiones para ocasionarlas, pueda reportar tales actividades en forma anónima, como se encuentra descripto en la etapa 11 del modelo presentado.

Tal importancia se le ha dado a los canales independientes de reporte de irregularidades, que su implementación es de carácter obligatorio para empresas que coticen en bolsa bajo la órbita de la SEC y se encuentran alcanzadas por Sarvanes Oxley Act.

Conclusiones

Los delitos de cuello blanco son acciones de carácter complejas que involucran la participación de varias personas dentro de la organización de niveles altos y medios, que normalmente actúan mediante un patrón de 12 etapas de acuerdo a la investigación.

Su complejidad radica en las estructuras internas que se configuran para su realización y en los objetivos que se persiguen.

Dentro de las acciones que resultan para ejercer un control efectivo para estas situaciones, es indispensable establecer canales de comunicación efectivos dentro de la organización, conjuntamente con una adecuada estructura de control interno que fomente un apropiado clima ético y de confianza, en donde las acciones que se desvían a los objetivos de la empresa y a las buenas prácticas de los negocios, sean sancionadas y, por otra parte, sean premiadas a los empleados que colaboran con este esquema.

En caso de requerir información adicional sobre el tema u otros temas relacionados, podéis poneros en contacto con nosotros a través de la siguiente dirección de correo electrónico: rasi@economistas.org

Cómo usar las redes sociales para alcanzar los objetivos de negocio

Josep Puigvert Ibars
Miembro del Consejo Directivo de RASI-CGE.
CEO en Clavertask.

Andrés González García
Ingeniero Telecomunicaciones.
Postgrado en Marketing Online y estrategia digital
EAE Business School.

Lanzarse a abrir perfiles en las redes sociales sin tener claro qué vas a hacer en ellas es como mínimo arriesgado y podría ser más perjudicial que beneficioso. Las redes sociales deben contribuir a conseguir los objetivos de la compañía y el desarrollo de actividad en las mismas debe estar al servicio de la estrategia del negocio.

Las tecnologías 2.0 están cambiando la forma de comunicar de las empresas. Las inversiones de las marcas se están desplazando de los clásicos departamentos de prensa y relaciones públicas a áreas de gestión de medios sociales y comunicación *online*. Los directivos se están dando cuenta del cambio de comportamiento social de los consumidores y se están animando a formarse en el mundo de la comunicación digital y las redes sociales, seguramente no para tener una participación activa, sino para saber cómo desarrollar las ventajas competitivas que ofrecen. Se estima que en el último año más del 70% de las empresas españolas han decidido ampliar sus departamentos de comunicación con perfiles relacionados con las redes sociales y el marketing digital. Estas cifras van en línea con lo que sucede en el resto de Europa y ponen de manifiesto el cambio gradual del modelo de comunicación tradicional, basado en notas de prensa en la página web, a uno de gestión de medios sociales y comunicación digital.

Las redes sociales, los *blogs*, las *newsletters*, los motores de búsqueda, en definitiva lo digital, ponen al alcance no sólo de las grandes empresas sino de PYMES, *startups* o emprendedores herramientas que les permiten llegar directamente al nicho de mercado para ofrecerle nuevos servicios de valor añadido que atraen y fidelizan clientes. Las herramientas son las mismas para todos; la estrategia es lo que te diferenciará de la competencia. Las redes sociales no pueden ser un objetivo en sí mismo sino que deben contribuir a conseguir los objetivo de la compañía.

Vale, ¿entonces abrimos un Facebook y un Twitter?

Un momento, sin prisas. Lanzarse a abrir perfiles en las redes sociales sin tener claro qué vas a hacer en ellas es como mínimo arriesgado y podría ser más perjudicial que beneficioso. Un perfil en Facebook (o cualquier otra red) sin actividad o con sólo mensajes institucionales no aporta valor a alguien que te sigue. Nuestro público no está en los medios sociales para ver comunicados, sino para encontrar algo que le sea útil, que le resulte interesante o que le haga esbozar una sonrisa.

Si queremos sacarles todo el jugo a los medios sociales, antes de lanzarnos a abrir perfiles es recomendable saber qué está pasando en esos entornos y, posteriormente, plantear la estrategia de comunicación. Lo primero es monitorizar dónde están los potenciales clientes, en qué redes, de qué hablan, qué tipo de contenidos reclaman (información sobre productos, solución de dudas, recomendaciones, tutoriales…), en qué formatos, quiénes son los usuarios más influyentes (importantes para comunicarnos con ellos), qué hace la competencia… Para

tener una foto completa, hay que analizar también cómo se comunica nuestro público objetivo con el resto canales de comunicación: ¿hacen comentarios en *blogs* de mi sector? ¿Comparten el contenido de *webs* de prestigio? Las redes sociales forman parte de un ecosistema digital. Un análisis parcial nos llevará a resultados no óptimos.

Las herramientas de monitorización de redes disponibles en el mercado nos ayudan a hacer el análisis. La monitorización no sólo nos servirá en esta etapa de análisis y definición, sino que más adelante volveremos a hacerla para verificar si estamos consiguiendo los objetivos que nos proponemos, analizaremos los resultados y tomaremos decisiones.

El resultado de la monitorización será un mapa de redes sociales, actores, frecuencia de las conversaciones, contenidos reclamados, presencia de la competencia...

Muy bien, ya sé en qué redes tengo que estar. Abro ya los perfiles, ¿no?

Como ya hemos apuntado, la estrategia en redes sociales se debe integrar en la estrategia general de comunicación digital (*blog* corporativo, página *web*, *newsletters*, publicidad…). ¿Qué queremos conseguir globalmente? Los objetivos deben estar alineados con los de la compañía. No hay que estar en las redes porque está de moda, sino porque queremos conseguir un beneficio empresarial, como estos:

- Aumentar las ventas.
- Aumentar la notoriedad de la marca.
- Convertirse en un referente en el sector.
- Ampliar la cuota de mercado.
- Fidelizar clientes.
- Mejorar el servicio postventa.

Una *startup* querrá dar visibilidad a la marca. Si la empresa ya está consolidada, quizás desee ganar posiciones respecto a la competencia. Estos objetivos generales de negocio se deben desarrollar para llegar a los **objetivos más concretos y medibles** en cada uno de los entornos digitales en los que trabajemos (página *web*, *blog*, medios sociales…). Es probable que las piezas por separado no consigan los objetivos, pero la unión de todos los esfuerzos sí debe hacerlo. En el caso de las redes sociales podríamos plantearnos:

- Aumentar un 20% los accesos a la *web* de usuarios interesados en los productos (tráfico de calidad para aumentar los pedidos *online*).
- Lograr que un 10% más de clientes potenciales envíen el formulario de contacto de la *web* (para que un comercial se ponga en contacto con ellos y aumentar la cuota de mercado).
- Aumentar un 20% las menciones positivas de mi marca (para aumentar la notoriedad de la marca).
- Eliminar los comentarios negativos sobre mi empresa (para preservar la imagen de marca).
- Aumentar las descargas de los tutoriales un 15% (para ayudar a convertirse en un referente en el sector).
- Conseguir un 10% más de subscriptores a la *newsletter* (para fidelizar clientes).
- Llegar a 20.000 seguidores en Twitter (¿para… qué?).

Los objetivos deben ser realistas, ambiciosos y alcanzables con los recursos de los que disponemos. Pero sobre todo deben ser medibles. En la Red todo se puede medir, es una gran diferencia respecto al marketing tradicional. A los objetivos de la lista anterior les falta algo: en cuánto tiempo queremos conseguirlos y las métricas que necesitamos para saber si se están cumpliendo.

De los 7 objetivos y métricas anteriores, hay una que se considera una *vanity metric*. Las *vanity metrics* son medidas que nos hacen engordar como pavos reales cuando las mostramos, pero que sirven de poco para conseguir los objetivos globales del plan. Tener 20.000 seguidores en Twitter sirve para sacar pecho delante del jefe, pero para poco más. Esta métrica, ¿nos ayuda a tomar decisiones? ¿Qué calidad tienen esos seguidores? ¿Están interesados en mi producto o los he atraído con concursos a los que todo el mundo se apunta? ¿Son usuarios activos? ¿Los seguidores han entrado en mi *web*, se han apuntado a la *newsletter* o han hecho alguna compra? Frente a las *vanity metrics* tenemos las *actionable metrics*, que sí sirven para tomar decisiones:

¿Qué porcentaje de visitas de las redes sociales acaban comprando un producto?¿Cuántas entran en la *web*, ven sólo una página y se marchan? **Las métricas nos deben indicar qué estamos aportando para cumplir con los objetivos de negocio**.

¿Qué contenidos difundo? ¿Con qué frecuencia? ¿Tengo que adaptar el mensaje en función de la red?

A estas preguntas debe responder el Plan de Comunicación y Contenidos, que de nuevo debe estar alineado con la estrategia digital global. Si queremos aumentar un 10% las ventas *online*, una estrategia sólo en medios sociales puede no ser suficiente. Las redes sociales pueden llevar tráfico a la *web* de compras y debemos preocuparnos de que las visitas realmente tengan interés en el producto (tráfico de calidad), pero cuando las visitas aterricen en la *web* deben encontrarse con un portal que cumpla con las expectativas de lo comunicado o en caso contrario el usuario se sentirá decepcionado y abandonará la página.

El Plan de Comunicación y Contenidos definirá:

- **¿Qué contenidos comunicar?**. En el análisis inicial se habrá podido ver qué piden los usuarios en cada red. Ese es el contenido que tenemos que proporcionarle: de valor, que le interese a él y a los suyos para que lo comparta, que persuada para entrar en la *web*. Si una empresa se dedica a hacer auditorías de sistemas de información y el objetivo es aumentar la notoriedad de la marca, ¿por qué no crear artículos en un *blog* sobre las *Best Practices* en distintos entornos tecnológicos, videos sobre cómo solucionar problemas comúnmente detectados o imágenes de infraestructuras que cumplen con los estándares de seguridad? Los artículos o vídeos convenientemente "troceados" pueden servir al canal de las redes sociales para su difusión. Este tipo de contenidos, además de ser de interés, aumentan la credibilidad y la reputación de la empresa. Hay que encontrar el hilo a la madeja y empezar a tirar. Todos los sectores tienen contenidos de valor que comunicar. También es interesante aprovechar los contenidos de calidad creados por otros que sean útiles para tus seguidores. No se trata de plagiar, sino de poner a disposición y difundir aquello que interesa a tu público objetivo. Es lo que se conoce como "curación de contenidos" (o *content curation*).

- **¿Dónde y cuándo publicar?**. En el estudio inicial se habrán detectado las particularidades de cada red (tipo de mensajes, tipos de usuarios, tipos de contenidos…). Esta información nos servirá para hacer una programación de la frecuencia y contenidos en cada una. ¿Publicar 5 tuits diarios es mucho o poco? Depende de tus objetivos y de los resultados que obtengas. Pueden ser muchos si sólo mandas mensajes institucionales que ahuyentan a tus seguidores. Pero pueden ser los adecuados si la gente los retuitea y consigues tráfico para tu *web* que acaba comprando. Plantea una estrategia, mide resultados y corrige para la siguiente vez.

El Plan de Comunicación y Contenidos dará como resultado un mapa de contenidos, canales y frecuencias de publicación que sirva como base suficiente para desarrollar la actividad de comunicación social. No será una estructura rígida, sino que formará los fundamentos que moldearemos a medida que veamos los resultados de nuestra actuación.

¿Cómo sé si alcanzo los objetivos?

Pongamos por ejemplo que uno de los objetivos del área digital es aumentar un 15% el número de descargas del portfolio. El objetivo del departamento de medios sociales es enviar tráfico de calidad a la *web* (es decir, usuarios que están interesados en los servicios de la empresa) y también promover las descargas directas en las redes sociales. Ahora toca medir para sacar conclusiones y tomar decisiones.

Tenemos a nuestra disposición multitud de herramientas que nos permiten hacer las mediciones. Pero lo importante no son las herramientas, sino qué medimos. Se pueden medir tantos parámetros que es fácil caer en la *parálisis por análisis*. Por eso es importante tener claro qué métricas nos ayudan a saber si las campañas cumplen sus objetivos y tomar decisiones para mejorarlas. Tiene sentido que el objetivo *"aumentar un 15% las descargas de un documento"* conste de varias métricas asociadas. ¿Cuántas descargas han venido de cada red social? Los usuarios que descargaron el *portfolio*, ¿se han puesto en contacto con nosotros posteriormente para solicitar más información? Con la primera métrica podemos decidir si una red social es más adecuada para enviar ciertos mensajes, o si es necesario mejorar el contenido, frecuencia o estilo de éstos. La segunda métrica nos ayudará a entender si el *portfolio* se entiende correctamente y si cumple con su objetivo de convencer (se puede enviar una versión del *portfolio* a un grupo de usuarios y otro a otro grupo para ver cuál tiene más éxito, es lo que se llama un *testing A/B*).

Si el objetivo era aumentar un 20% las menciones positivas, las métricas deberían desvelarnos en qué redes, quién los hace (seguidores influyentes, personas cercanas a la empresa, usuarios que participan en un concurso…) y a cuánto público han llegado. Las respuestas nos llevarán a optimizar y redirigir los esfuerzos de comunicación allá donde veamos que son más efectivos.

Medir los resultados y optimizar la estrategia es tan importante como comunicar correctamente. No es extraño tener una dedicación de un 50% del tiempo a preparar las campañas de comunicación y el otro 50% a medir y proponer mejoras para las siguientes. En un ámbito de cambios rápidos y constantes como es el de los medios sociales, debemos aprender a adaptarnos a lo que los usuarios consideran de valor. *"El primer paso para crear tu plan es definir tus metas"*, dice Lee Oden, director de TopRank Online Marketing. *"Después, entiende las metas de tus clientes, y luego aprende cómo tu estrategia en social media conectará ambos"*.

Ahora sí, cuando ya sabemos dónde tener actividad social, cuando ya has alineado los objetivos con los de la compañía, cuando sabes qué contenidos, cuándo los vas a comunicar y qué parámetros medir, podemos empezar a abrir cuentas en redes sociales.

Conclusiones

Las redes sociales, lo digital, no pueden ser un objetivo en sí mismo sino que deben contribuir a conseguir los objetivo de la compañía y por lo tanto el desarrollo de actividad en las mismas debe estar al servicio de la estrategia del negocio. Las redes sociales son una pieza en el puzzle de la comunicación digital y sirven como herramienta potente para relacionarnos con el público objetivo y para aumentar nuestra ventaja competitiva. El proceso cíclico de construcción descrito más arriba (estudio, definición de objetivos, estrategia, táctica, acciones, métricas y optimización) es aplicable a otros entornos de comunicación digital.

La actividad que desarrollemos debe estar dotada de los recursos adecuados. La gestión de lo digital se puede hacer internamente en la compañía –una persona o un departamento– o se puede pedir el acompañamiento profesional de un partner con experiencia en el sector.

La gestión profesional de los medios sociales de la empresa no es una opción, sino una obligación para aquellas que entienden lo digital como un segmento que se integra en el desarrollo global del negocio. No tener un plan estudiado y acorde con los objetivos globales facilita el derroche de recursos además poner en peligro la imagen de marca.

PREVENCIÓN DE BLANQUEO DE CAPITALES

Quería saber si la exención que prevé el Reglamento de Prevención de Blanqueo de Capitales para aquellos sujetos obligados que no superen unos determinados niveles de actividad es de aplicación para el ejercicio 2013, en concreto la revisión de un experto independiente.

El Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo, según su disposición final tercera, entra en vigor el mismo día de su publicación en el Boletín Oficial de Estado (6 de mayo de 2014), salvo para el umbral de identificación de operaciones ocasionales del artículo 4.1, que entrará en vigor el 6 de noviembre de 2014.

Así, hasta este momento, atendiendo a lo establecido en la Ley citada con anterioridad, todos los sujetos obligados (Art 2 de la misma), con excepción de los empresarios que ejercían a título individual, debían de realizar un examen anual por parte de un experto externo independiente (Art 28 de la citada Ley). A tal efecto, el experto externo debía de realizar y emitir el informe a la mayor brevedad posible, sin que en ningún caso pudiera exceder de dos meses desde la fecha de referencia del informe (Art 5 O.EHA 2444/2007).

En este sentido, para los sujetos obligados cuyo periodo de revisión a considerar coincidiera con el año natural (es lo más normal, en caso contrario habría que adaptar las diferencias) la fecha límite de referencia para la emisión del informe de experto externo del año 2013 finalizó el 28 de febrero de 2014, por lo que dicha exención no es de aplicación para el pasado ejercicio.

CONSULTAS SOBRE REDES SOCIALES

¿Con que frecuencia debo publicar algo en las Redes Sociales de mi empresa?

La frecuencia de publicaciones está estrechamente relacionada con el aumento de tráfico. Lo ideal es conjugar cantidad y calidad de publicaciones. Cada red social tendrá su frecuencia específica de publicaciones dependiendo de la estrategia definida en plan de social media. Es aquí cuando recordamos que lo importante es la definición de objetivos de manera previa a salir en redes sociales, estar por estar conllevará a una infrautilización y desaprovechamiento de recursos.

Cualquier acción que pongamos en marcha como parte de nuestra estrategia *online*, debe tener un objetivo claro, y para diseñarlo tendremos que acudir a un plan de *marketing online*, fijando qué vamos a hacer y qué soportes necesitamos poner en marcha para potenciar nuestro negocio, ya sea aumentando ventas, manteniendo un servicio de atención al cliente, potenciando nuestra marca, fidelizando clientes y atrayendo nuevos…

Para definir correctamente un objetivo existe una "regla" que nos ayudará a recordar cómo deber ser estas normas, SMART:

S: específicos *(Specific)*; M: medibles *(Measurable)*;
A: alcanzables *(Achievable)*; R: realistas *(Realistic)*
y T: definidos en el tiempo *(Time based).*

PROTECCIÓN DE DATOS PERSONALES

En el caso de que una persona quiera ejercer el "derecho al olvido" en lo relativo a la protección de los datos personales, tengo entendido que la Agencia de Protección de Datos se ha pronunciado a favor de que los buscadores de internet tengan que eliminar los datos de la persona o, al menos, ocultarlos para que no aparezcan en sus resultados de búsquedas ¿esto es así?

Mediante resolución de 30 de julio de 2010, la AEPD estimó una reclamación frente a un buscador de internet en un determinado litigio, considerando que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimó que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso, cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal.

Esta decisión de la AEPD fue recurrida ante la Audiencia Nacional por los gestores de búsqueda afectados. El mencionado tribunal expuso en el auto de remisión que estos recursos plantean la cuestión de cuáles son las obligaciones que tienen los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y sea puesta a disposición de los internautas de forma indefinida. Consideraba que la respuesta a esta cuestión dependía del modo en que deba interpretarse la Directiva 95/46 en el marco de estas tecnologías, que han surgido después de su publicación. En estas circunstancias, la Audiencia Nacional decidió suspender el procedimiento y plantear al Tribunal de Justicia de la Unión Europea, que recientemente se ha pronunciado al respecto con una sentencia de 13 de mayo de 2014, en el asunto C-131/12, respaldando la tesis de la Agencia Española en relación con los buscadores y el derecho al olvido en internet.

OBLIGACIONES DE CORREDURÍAS DE SEGUROS

Les planteamos las siguientes consultas sobre unas dudas que tenemos sobre el Real Decreto 340/2014, de 05 de Mayo, por el que se aprueba el Reglamento de la Ley 10/2010 de 28 de Abril. En concreto con las obligaciones de las corredurías de seguros con menos de 10 empleados y cuyo volumen anual es de menos de 2 millones de euros.
La primera duda es saber si deben realizar la comunicación semestral de experto correspondiente al primer semestre del 2014 y como ya ha empezado el año no sabemos si aparte de realizar la del primer semestre deben realizar también la del segundo.
En el caso de que no estén obligados a realizar dicha declaración si dichas corredurías deben realizar alguna comunicación al Banco de España.
Por último los gerentes /directivos deben realizar formación y acreditarla pero nos gustaría saber cómo debemos comunicarla y saber si es obligatoria para los gerentes de las corredurías que hemos descrito antes (menos de 10 empleados etc).

Los corredores de seguros (sujetos obligados según el Art. 2.1.b de la Ley 10/2010, de PBCyFT) no están incluidos en la exención a la que hace referencia, del Art. 31.1 Reglamento, que establece lo siguiente: "Los sujetos obligados aprobarán por escrito y aplicarán políticas y procedimientos adecuados de prevención del blanqueo de capitales y de la financiación del terrorismo. Los corredores de comercio y los sujetos obligados comprendidos en el artículo 2.1 i) a u), ambos inclusive, que, con inclusión de los agentes, ocupen a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 2 millones de euros, quedan exceptuados de las obligaciones referidas en este artículo y en los artículos 32, 33, 35, 38 (examen de experto externo) y 39. Estas excepciones no serán aplicables a los sujetos obligados integrados en un grupo empresarial que supere dichas cifras". Por lo tanto, los expertos externos, durante el mes siguiente al semestre de referencia, comunicarán al SEPBLAC las revisiones de experto externo realizadas a dichas entidades (durante el mes de julio, que responde al primer semestre de 2014 y en enero, que corresponde al segundo).

Asimismo, los corredores de seguros mantienen la obligación de comunicar al SEPBLAC cualquier indicio de Blanqueo, en el momento en que se tuviese conocimiento.

Independientemente de lo anterior, quedan exceptuados de la obligación de comunicación sistemática los corredores de seguros a los que se refiere el artículo 2.1 b) de la Ley 10/2010, de 28 de abril, las empresas de asesoramiento financiero y los sujetos obligados mencionados en los párrafos k) a y), ambos inclusive, del artículo 2.1 de la misma ley (Art.27.3 Reglamento).

Con respecto a la formación, los corredores no están exentos de realizar un plan anual de formación, debiendo recibir formación externa a tal efecto, y conservando los correspondientes certificados o justificantes de su efectiva realización, como prueba frente a un posible requerimiento de dicha información en el marco de una inspección.

OBLIGACIONES SECTOR AUTOMOCIÓN

Me gustaría que me aclararan la obligación en el sector de automoción de aplicar la ley 10/2010. En cuanto a las obligaciones por operaciones superiores a ¿qué cuantía en efectivo? ¿Pueden, hoy, solicitarme datos del año 2007? ¿Es necesario que se me notifique expresamente, por el órgano en cuestión que requiere los datos? La notificación por correo electrónico ¿es válida?

El SEPBLAC se ha pronunciado respecto a este asunto en el siguiente sentido: "un concesionario de automóviles u otros medios de transporte puede ser sujeto obligado respecto a la compraventa del bien o respecto a su financiación, en el caso de que intermedie en la misma.

En cuanto a la compraventa de vehículos, será sujeto obligado cuando realice cobros o pagos en efectivo, u otros medios de pago previstos en el artículo 34.2, por importe superior a 15.000 euros*, ya sea en una o en varias operaciones en las que parezca existir algún tipo de relación. El artículo 38 de la Ley 10/2010 determina las obligaciones –no todas– que tienen estos sujetos obligados.

** En relación con este artículo hay que tener presente que el día 19 de noviembre de 2012 entró en vigor la limitación a los pagos en efectivo prevista en el artículo 7 de la Ley 7/2012.*

En el caso de que un concesionario intermedie en la financiación de la compraventa del automóvil que vende no es sujeto obligado, pero sí lo sería si intermedia en la concesión de préstamos o créditos para financiar operaciones distintas a las anteriores."

En cuanto a la solicitud de datos que comenta, con el fin de que pueda verificarse con posterioridad un adecuado cumplimiento del sistema de prevención de este tipo de delitos así como un seguimiento del camino seguido por el dinero o por los bienes y derechos objeto del mismo, se establece una obligación de conservación de todos los datos relativos a la identidad, titularidad real, actividad económica, operaciones, etc. por un periodo de diez años. Por lo que sí sería posible que le solicitasen la citada documentación fechada en 2007.

Por último, las inspecciones u otras actuaciones del Servicio Ejecutivo, SEPBLAC, se realizan siempre siguiendo un cauce estrictamente formal, en el que la realización de la visita de inspección se anuncia por escrito con carácter previo y con antelación suficiente.

Curso online de PBC y FT "Prevención del blanqueo de capitales y financiación del terrorismo para expertos"

Contiene las principales novedades establecidas en el Reglamento

Objetivo: A pesar de lo reciente de su regulación, todas las obligaciones que implica el cumplimiento normativo en materia de prevención del blanqueo de capitales, en especial la realización del examen de experto externo, del artículo 28 de la citada Ley, han experimentado un rápido desarrollo. Pretendemos dar a conocer a quienes deseen actuar como expertos externos los principales aspectos a analizar, así como las pruebas de cumplimiento mediante las que se ha de hacer dicho análisis, a la hora de evaluar la suficiencia, idoneidad, eficacia y racionalidad, tanto teórica como práctica, de los procedimientos internos de las empresas para la prevención del blanqueo de capitales, y su implantación, ayudándole a emitir su informe en el que pondrá de manifiesto los resultados obtenidos, las posibles irregularidades o deficiencias encontradas, que deberán ser resultas por el sujeto obligado, las recomendaciones que se crean convenientes, y, en definitiva, aportando calidad al trabajo del experto.

El presente curso se ha adaptado y actualizado respecto al presentado en períodos anteriores, lo que supone un importante avance, al incluir todas aquellas experiencias que se han ido adquiriendo por las personas que han intervenido en su preparación, actualización y contiene recomendaciones realizadas tanto por el SEPBLAC como por otros organismos involucrados, tanto del ámbito nacional como internacional, y por último responde a las sugerencias que nos han hecho llegar alumnos de anteriores acciones formativas.

El curso, de carácter eminentemente práctico, aborda la forma, estructura y contenido del examen de experto externo.

Horas computables: 30 Horas (10 horas en contabilidad y auditoría y 20 horas en otras materias).

Curso online de PBC y FT "Prevención del blanqueo de capitales y financiación del terrorismo para socios y directivos"

Contiene las principales novedades establecidas en el Reglamento

Objetivo: Mediante el presente curso se alcanzará un alto grado de conocimiento y especialización en materia de Prevención de Blanqueo de Capitales, permitiendo a la persona que deba asumir la responsabilidad y control de las medidas a implantar derivada de la normativa de prevención de blanqueo de capitales dar respuesta a problemas jurídicos o administrativos relacionados con esta materia.

Este curso se dirige a los sujetos Obligados por la Ley 10/2010, así como sus empleados y colaboradores, a empresas o profesionales que quieran adaptarse a la normativa de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo así como a profesionales que quieran completar su formación, o que tengan como clientes a sujetos obligados.

Horas computables: 15 Horas (10 horas en contabilidad y auditoría y 5 horas en otras materias).

Curso online de PBC y FT

"Procedimientos de Auditoría en entidades sujetos obligados de la Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo"

Contiene las principales novedades establecidas en el Reglamento

Objetivo

El objetivo del presente curso es determinar la responsabilidad del auditor a la hora de enfrentarse a encargos d entidades que son sujetos obligados de la LPBCyFT, estableciendo cuáles son los procedimientos a realizar (de acuerdo a lo establecido en las Normas Internacionales de Auditoría), la obtención de la evidencia y el efecto de las conclusiones obtenidas en el informe de auditoría.

Horas computables

10 Horas, en Contabilidad y auditoría

Cursos de Formación Presencial

- Ayuda y Referencias a las Nuevas Técnicas en la Auditoría de Cuentas en entornos informatizados. 3 horas
- Enfoque práctico a la Auditoría de Cuentas en entornos informatizados. 6 horas
- Enfoque al riesgo en la Auditoría de Cuentas, NIAs, PBCm LOPD, etc. 4 horas
- Entorno de control interno:
  Controles generales. 4 horas
  Controles de aplicación. 4 horas
- Responsabilidad penal: delitos económicos. 3 horas
- Novedades legislativas en materia de PBC. 4 horas
- Novedades legislativas en materia de LOPD. 4 horas
- Curso de Auditor Jefe en ISO 9001: 2008. 4,5 días
- Curso de Auditor Jefe en ISO 14001: 2004. 4,5 días
- Curso Auditor Jefe / OHSAS 18001: 2007. 4,5 días
- Curso de Auditor Jefe en ISO 27001: 2005. 4,5 días

Los Colegios interesados en realizar estos u otros cursos en sus sedes, por favor, contactar con RASI-CGE, a través del siguiente correo electrónico: rasi@economistas.org

Se está cerrando la programación de otros cursos, tanto presenciales como online, de los que os mantendremos oportunamente informados.

Cloud Computing, su interés económico y lo que puede aportar a la Auditoría

Alejandro García Pérez y **Tomás Sánchez** fueron los ponentes de este seminario celebrado el 27 de febrero en la sede del Consejo. Durante el mismo se expuso, desde un punto de vista eminentemente práctico y de aplicación inmediata, los conocimientos y habilidades que capacitan a los profesionales para la planificación, implementación, realización, gestión, control y mejora del "Cloud computing" en las organizaciones en las que trabajan.

Curso sobre "Novedades en materia de prevención de blanqueo de capitales y financiación del terrorismo"

El 11 de marzo tuvo lugar un curso donde se abordaron las novedades en materia de prevención de banqueo de capitales y financiación del terrorismo. En el transcurso del mismo, **Abel Bonet**, **Luis Ramallo** y **Jorge Pérez** analizaron el alcance de las recomendaciones del SEPBLAC y las actualizaciones y reformas normativas en materia de PBCyFT, junto con las implicaciones en la operativa de entidades sujetas a la norma.

Auditoría de Cuentas en Entornos Informatizados, en A Coruña

Un momento de la Jornada sobre Normas Técnicas de Auditoría de Cuentas en Entornos Informatizados.

Joaquim Altafaja durante su intervención.

El 12 de mayo, **Joaquim Altafaja**, visitó el Colegio de Economistas de A Coruña, como ponente de la Jornada sobre "Normas Técnicas de Auditoría de Cuentas en Entornos Informatizados". Durante la misma, con un contenido muy completo, se estudiaron a fondo los puntos clave de una auditoría dentro de medios informatizados, teniendo en cuenta la complejidad de estos a la hora de tratar los datos y la naturaleza del trabajo del auditor, asegurándose de la consecución de sus objetivos.

El director del SEPBLAC visita la sede del Consejo General de Economistas

El director del SEPBLAC, **Juan Manuel Vega**, se reunió el 22 de abril con el presidente y la secretaria general del Consejo General de Economistas, **Valentín Pich** y **Sara Argüello**.

Entre los temas que se trataron, el director hizo especial hincapié en la necesidad de cambiar la "cultura del miedo a la sanción" por un enfoque proactivo y positivo, centrado en la gestión de los riesgos y la responsabilidad social. Desde el Servicio Ejecutivo, en su función de supervisar e inspeccionar el cumplimiento por los sujetos obligados de las obligaciones que establece la Ley 10/2010, de 28 de abril, se está desplegando una intensa actividad supervisora en función del riesgo, tomando en consideración el volumen de actividad de los sujetos obligados, así como las características de sus clientes y de sus operaciones.

En este sentido, serán las entidades de mayor dimensión y cuyo perfil de negocio presente riesgos superiores aquellos que serán objeto de un mayor esfuerzo supervisor, respondiendo a criterios de eficiencia y uso adecuado de los recursos públicos. Esto no obsta a que todos los sujetos obligados han de estar concienciados, formados, en congruencia con el grado de responsabilidad de los receptores y el nivel de riesgo de las actividades que desarrollen, y han de ser capaces de detectar posibles clientes u operaciones sospechosas, para evitar verse inmersos en responsabilidad tras la posible detección de conductas irregulares, o falta de diligencia debida, por cualquier organismo competente.

Asimismo, el director comentó que las comunicaciones de operaciones sospechosas que se han recibido por parte de nuestro colectivo se mantienen en niveles muy bajos en relación con las presentadas por otros sectores aunque, por otro lado, el número de auditores, contables y asesores fiscales, sujetos obligados, registrados en el SEPBLAC ha aumentado en los últimos años, superando los 5000 registros en 2012 (más de 1200 nuevas altas desde 2010).

El director del SEPBLAC, Juan Manuel Vega, tras estampar su firma en el Libro de Honor del Consejo, junto a Valentín Pich y Sara Argüello.

El director del SEPBLAC, **Juan Manuel Vega**, señaló que el Reglamento de la Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo, facilitará el cumplimiento de la normativa por los sujetos obligados e incrementará la eficacia de la lucha contra el blanqueo de capitales y la financiación del terrorismo.

El presidente del Consejo General de Economistas, **Valentín Pich**, comentó la oportunidad de su aprobación dado el grado de sensibilización de la sociedad con esta clase de delitos.

Durante la reunión, también se analizó la colaboración mantenida hasta el momento entre ambas Instituciones, fijando nuevas actuaciones conjuntas con objeto de concienciar al colectivo y, por ende, al conjunto de la sociedad, de la necesidad de prevenir esta clase de delitos y proporcionar las herramientas necesarias a nuestros profesionales para estudiar y trabajar la prevención de blanqueo de capitales con un enfoque pluridisciplinar, en sintonía con la actuación del resto de países desarrollados, desde una perspectiva práctica y de eficiencia.

Reunión del Consejo Directivo

El pasado 26 de marzo tuvo lugar la última reunión del Consejo Directivo. En ella se concretó la nueva programación de actividades, en formación e información. También se informó sobre el estado de desarrollo de la nueva página *web*, que forma parte de la nueva estrategia digital del Consejo General, más usable y con un enfoque práctico que otorga mayor protagonismo a los Colegios. Por último, se coordinó la organización de las ponencias de RASI-CGE en el Foro de Anual de Economistas 2014, que se celebró los días 29 y 30 de mayo en CaixaForum Madrid.

Seminario sobre prevención de blanqueo de capitales

Asistentes durante la celebración del Seminario.

Un momento de la intervención de Gregorio Labatut.

El pasado 19 de mayo, **Gregorio Labatut** impartió el exitoso seminario "El compliance sobre prevención de blanqueo de capitales y FT para el economista. El régimen especial de umbrales." Labatut repasó las obligaciones de estos sujetos obligados haciendo especial hincapié en el recién aprobado reglamento de la nueva Ley de PBC.

Presentación del Informe ePyme 2013

El pasado 27 de mayo tuvo lugar la presentación del Informe ePyme 2013. Por sexta edición consecutiva, FUNDETEC, en colaboración con el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, ha elaborado el Informe ePyme 2013, un año más en colaboración con RASI-CGE, donde se analiza el grado de implantación y el impacto de las TIC en los procesos de negocio de diez sectores de actividad.

Los objetivos que se persiguen con el Informe ePYME son:

- Mostrar el grado de implantación de las TIC en los diferentes sectores.

ePyme 13

D. Víctor Calvo-Sotelo, secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, se complace en invitarle a la presentación del

Informe ePyme 2013.
Análisis sectorial de implantación de las TIC en la pyme española

que tendrá lugar el martes 27 de mayo a las 11:00 horas, en el salón de actos de la SETSI (C/ Capitán Haya, 41. Madrid).

En su VI edición, este informe, elaborado por Fundetec y RedLes a través del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), analiza el grado de desarrollo tecnológico de las microempresas, pymes y grandes empresas de diez sectores de la Economía española

(Industria; Construcción; Venta y reparación de vehículos; Comercio mayorista; Comercio minorista; Hoteles, campings y agencias de viaje; Transporte y almacenamiento; Informática, telecomunicaciones y servicios audiovisuales; Actividades inmobiliarias, administrativas y servicios auxiliares; y Actividades profesionales, científicas y técnicas)

y ofrece consejos y recomendaciones para mejorar su situación respecto a las TIC.

En la presentación intervendrán D. César Miralles, director general de RedLes; y D. Alfonso Arbaiza, director general de Fundetec.

Se ruega confirmación

red.es ontsi fundetec Colabora: economistas

Presentación del Informe ePyme 2013.

- Analizar el impacto de las TIC en los procesos de negocio específicos de cada sector.
- Analizar las tecnologías y aplicaciones que mayor impacto han producido en cada sector.
- Identificación de barreras y dificultades para la incorporación de las TIC a los procesos de negocio de cada sector.

Foro Anual de Economistas 2014

El Foro anual tuvo lugar los días 29 y 30 de mayo en las instalaciones madrileñas de CaixaForum.

El esperado Foro Anual de Economistas 2014, supone para nuestro colectivo en general, y para nuestro registro en particular, todo un acontecimiento, ya que tenemos una importante participación en el mismo.

El primer día del Foro, 29 de mayo, tuvo lugar una importante ponencia de la dirección de la Agencia Española de Protección de Datos, en la que nos pusimos al día sobre el nuevo reglamento europeo, la ley de cookies, las novedades en lo que a jurisprudencia se refiere sobre el derecho al olvido, la concienciación del colectivo frente a este derecho y demás aspectos de actualidad en materia de protección de datos personales.

Asimismo, el día 30 de mayo impartió una ponencia el director del SEPBLAC, **Juan Manuel Vega**. Junto al mismo estuvo **Gregorio Labatut**, colaborador habitual del Consejo General. Durante esta sesión se trataron los principales aspectos e implicaciones de la normativa sobre los despachos profesionales, una ponencia muy esperada, por parte de los miembros del registro de EPBC.

En ese mismo día tuvimos la oportunidad de asistir a un taller de marketing referente a las soluciones de marketing móvil para los despachos profesionales, tema actual y que compete al campo que interesa a los miembros de nuestro registro. Estuvo a cargo de **Jesús Redondo Velasco**, director de Microsoft Windows Phone.

El Foro de este año fue considerado un gran éxito y contó con una nutrida participación en el mismo.

Próximamente...

RASI-CGE realizará unas jornadas en los Colegios de Economistas de Murcia y Alicante durante el mes de junio. En unos días comunicaremos las fechas y las sesiones previstas para cada una de estas jornadas.

cumplimiento normativo (PBCyFT, protección de datos ...)

RASI

cloud computing

e-commerce

estrategia digital

social media

influyendo en la Sociedad de la Información

RASI

- Auditoría
- Asesoría Fiscal
- Economía Forense
- Expertos Contables
- Asesoría Financiera
- Docencia e Investigación
- Asesoramiento Laboral

→ Formación
→ Información
→ Investigación
→ Colaboración
→ Apoyo

→ sobre TIC → a todo el Colectivo Profesional

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

solicitud de inscripción
www.rasi.economistas.es