economistas
Consejo General
RASI · economistas auditores de sistemas de la información

Junio 2012

actualidad RASI

Revista del Registro de Economistas Auditores de Sistemas de la Información

Contenido

Nuevo Comité Consultivo del RASI-CGCEE

El nuevo Comité Consultivo del Registro de Auditores de Sistemas de Información, RASI-CGCEE, está compuesto por: **Valentín Pich Rosell,** Presidente; **Carlos Puig de Travy,** Vicepresidente 1º (…)

Página 12

Tribunas de opinión

Sistemas de Información Informatizados, un desafío a la seguridad

Alonso Hernández García

Son de todos bien conocidas las ventajas aportadas por la informática a los sistemas de información. Las operaciones viables (…)

Página 5

Continuidad de Negocio: respaldo internacional

Alejandro García Ruiz

La Continuidad de Negocio, ese activo, esa capacidad de prevenir cualquier tipo de incidencia que nos impida suministrar nuestro producto (…)

Página 6

Incidentes de seguridad de la información: cómo monitorizarlos y gestionarlos

Yazomary García García

En la actualidad, los incidentes de seguridad son inevitables y cada vez más tienen una mayor repercusión en la imagen corporativa (…)

Página 8

Nuevo espacio para difundir la actualidad empresarial y profesional en el ámbito de los Sistemas de Información

Valentí Pich Rosell
Carlos Puig de Travy

Página 2

Nuevo espacio para difundir la actualidad empresarial y profesional en el ámbito de los Sistemas de Información

Es muy satisfactorio para mí dirigiros estas líneas en el primer número de nuestra revista, que con mucha ilusión y trabajo acabamos de sacar a la luz. Se trata de una revista práctica, cuyo principal objetivo es la promoción y creación de un espacio para la difusión de distintos aspectos de la actualidad empresarial y profesional en el ámbito de los sistemas de información.

Este proyecto cuenta con una gran variedad de contenidos, sobre los que reconocidos profesionales y expertos en las materias relacionadas con las Tecnologías de la Información y la Comunicación, TIC, y los Sistemas de la Información, SI, trabajan activamente, aportando sus opiniones e ideas y ayudando a impulsar la adopción de las nuevas tecnologías y fomentando la auditoría de los Sistemas de la Información, fundamentalmente entre los economistas y la sociedad en general.

El Registro de Auditores de Sistemas de Información, RASI-CGCEE, como órgano especializado del Consejo General de Colegios de Economistas, tiene como principal fin prestigiar la imagen pública del economista auditor de sistemas de información en la Sociedad, fomentando y elevando la cualificación profesional de sus miembros mediante la formación profesional y la información en las materias que le son propias, precisamente en este sentido ha venido trabajando RASI, desde su creación hace ya diez años.

Me gustaría destacar y agradecer muy especialmente el trabajo y la dedicación que le está poniendo **Carlos Puig,** como vicepresidente 1º del RASI-CGCEE que, además, compatibiliza con su cargo de Presidente del REA-CGCEE. **Carlos Puig** está siendo el verdadero motor e impulsor de este registro en esta nueva etapa.

No quiero olvidarme de mencionar a **Alonso Hernández,** que ha decidido seguir con nosotros como vicepresidente 2º. Su experiencia, su conocimiento de la materia y el haber estado ligado a RASI-CGCEE desde su creación, nos va a permitir contar con un bagaje profesional insustituible.

Esperamos que la lectura de la Revista sea de vuestro agrado y confío en que la prolongación de su publicación constituya, con el tiempo, un referente útil en la actividad de los Economistas en relación con los Sistemas de la Información, cuya evolución ha sido vertiginosa en los últimos años y cuyas perspectivas de desarrollo no pueden dejar indiferente a nadie.

Valentí Pich Rosell. Presidente CGCEE. Presidente RASI-CGCEE

Hace apenas unos meses que el nuevo Comité Consultivo de RASI-CGCEE tomaba posesión de sus cargos, pero en tan breve plazo podemos constatar ya su buen hacer y el acierto de las nuevas iniciativas, y desde aquí quiero, como Vicepresidente 1º, hacer llegar a todas y cada una de las personas involucradas en este registro mi agradecimiento y mi apoyo.

Es una realidad incuestionable la presencia de las Tecnologías de la Información en la actividad diaria de los economistas y es precisamente la permanente actualización de los conocimientos en este área una de nuestras principales motivaciones.

Tener la mejor información disponible sobre la materia es también una necesidad imperiosa y, en este sentido, nace esta revista que contiene varias secciones fijas. Así, en cada número publicaremos una serie de artículos de expertos, noticias de RASI-CGCEE, con los acontecimientos y realizaciones del periodo, normas publicadas en el periodo que puedan afectarnos, entrevistas con personajes relevantes en el mundo de las TIC y SI; y una sección en la que publicaremos las altas recibidas.

Espero que esta revista sea considerada como un valioso instrumento de información tanto para los economistas, como también para aquellos interesados en los Sistemas de la Información.

Los miembros del Comité Consultivo de RASI-CGCEE nos ponemos a vuestra disposición para cualquier sugerencia que queráis hacernos llegar con el fin de mejorar su utilidad.

Carlos Puig de Travy. Presidente REA-CGCEE
Vicepresidente 1º RASI-CGCEE

editorial

Los economistas asesores fiscales y los Sistemas de Información

Jesús Sanmartín Mariñas
Presidente del REAF-CGCEE

Como en todas las actividades, somos muchos los profesionales que, por haber alcanzado una determinada edad, si tenemos la suerte de conservar algo de esa maravillosa facultad que es la memoria, podemos darnos cuenta de como ha cambiado la forma de trabajar en los despachos dedicados a la asesoría fiscal durante los últimos quince o veinte años.

No hace tanto que traqueteaban los dedos sobre las máquinas de escribir eléctricas –y no eléctricas–, que los compendios de doctrina y jurisprudencia se enseñoreaban de las estanterías o que se dedicaba un encomiable esfuerzo a actualizar las publicaciones de hojas intercambiables. Los ordenadores, las computadoras que decían algunos, quedaban para las grandes empresas, eran enormes, tanto que tenían su propia habitación, y refrigerada, haciéndose las copias en cintas que parecían rollos de película. En mi caso, desde luego, no siento ninguna añoranza por esta época, salvo por que "en cualquier tiempo pasado éramos más jóvenes".

Después descubrimos la utilidad de un adelanto espectacular: el fax. A través de este aparato, conectado al teléfono –¡qué bonito esperar a que dejase de hablar el que tenía que recibirlo!– nos cruzábamos documentación sin necesidad de ir a buscar un buzón de Correos y esperar dos o tres días. Además, podíamos mancharnos las manos al leerlo y, ¡sorpresa!, cuando recurríamos a un fax antiguo recordábamos nuestros juegos de espías en la infancia: se había esfumado la información como si estuviera escrita con tinta invisible.

Después se fueron implantando los PC´s y tuvimos acceso a los programas de tratamiento de texto y a las hojas de cálculo. Se desarrollaron programas contables y fiscales que revolucionaron nuestro trabajo, de tal forma que ahora no podemos imaginar la llevanza de una contabilidad sin la utilización de software. La Agencia tributaria comprendió con rapidez el camino y puso a nuestra disposición el programa de ayuda a la declaración de la renta, el PADRE. ¡Qué hermosas tardes las de junio oyendo cómo se rellenaban las declaraciones de Renta en papel continuo con el repiqueteo de las impresoras de agujas! Hermoso si no fuera porque se descuadraban y se enganchaban incitando a la maldición y a la blasfemia.

El siguiente hito en esta revolución incesante creo que fue la generalización del correo electrónico; todavía hoy maravilla este tráfico de archivos a través del e-mail. Llegó también la presentación telemática de declaraciones, el borrador de declaración, los datos fiscales que la Agencia tributaria nos deja descargar, el certificado electrónico, los SMS, etc.

Los programas fiscales y contables ya ni siquiera tenemos que almacenarlos en nuestro ordenador o en CD´s, podemos usarlos en la web del proveedor; nuestros datos y los de los clientes también se pueden guardar en servidores en cualquier lugar del mundo; las facturas pueden ser electrónicas; se puede subcontratar el tratamiento o la conservación de ficheros, incluso la emisión de facturas; y hasta las notificaciones se hacen obligatoriamente de manera electrónica para las sociedades con todas las ventajas e inconvenientes que ello conlleva.

Por supuesto, estas novedades también han cambiado la forma de acceder a la información y la cantidad de información disponible. Si antes conocer la doctrina y la última jurisprudencia, o simplemente la última redacción vigente de una norma, era un ejercicio que ponía a prueba la memoria y la organización de un despacho de asesoría fiscal, Internet ha revolucionado este aspecto. Es frecuente que sin acudir, por supuesto, a los libros, pero tampoco a una base de datos comercializada, se pueda acceder "gratis total" a la última redacción de un texto normativo en Internet o a comentarios fiscales en las redes sociales. Así, las bases de datos y las publicaciones tributarias, para sobrevivir, han tenido que incorporar más valor añadido. No se trata, como antes, de disponer de mucha información, ahora se trata de que, por tener tanta información, estamos más interesados en seleccionar la más relevante y de interpretarla con criterio.

Paralelamente, una pretendida seguridad en diversos campos, casi siempre auspiciada por la UE, ha propiciado el desarrollo de normas que afectan tangencialmente a nuestra actividad y a las de nuestros clientes. Son normas que siempre nos han preocupado, pero las que, por pereza y falta de tiempo, hemos tardado en interiorizar. No obstante, van calando en nosotros como la lluvia fina que no deja de caer y a ellas no nos queda más remedio que irnos adaptando: me refiero, por ejemplo, a las normas sobre protección de datos de carácter personal o sobre la prevención de blanqueo de capitales.

Estas normas que, en principio, nada tienen que ver con las TIC´s, sin embargo se ven afectadas de pleno por ellas, ya que todos nuestros procesos, nuestros datos o las posibilidades de detección de operaciones de riesgo se llevan a cabo a través de sistemas de la información.

RASI-CGCEE, el órgano de los Auditores de Sistemas de Información, registro que pilota una nueva actividad de los economistas de carácter transversal y emergente en este nuevo escenario de prestación de servicios profesionales que nos ha tocado vivir.

No es que nuestro trabajo haya cambiado, no, sigue siendo el mismo en cuanto que un asesor fiscal sigue intentando comprender las operaciones que realiza su cliente, analizar la incidencia tributaria que pueden tener, aconseja sobre la planificación que minimice el coste fiscal y, en su caso, elabora las autoliquidaciones que procedan y atiende las incidencias que se presenten con posterioridad. Sin embargo, sí ha cambiado radicalmente la forma de prestar ese servicio. Las visitas presenciales son muchas menos, el conocimiento de la norma, doctrina y jurisprudencia correspondiente se da por supuesto y el profesional aporta intangibles diferentes como son su capacidad para relacionar unos impuestos con otros, la imaginación para buscar soluciones o su disposición para transmitir los puntos de vista del contribuyente a la Administración o para moverse por los procedimientos tributarios.

En este nuevo mundo, las TIC´s constituyen las herramientas básicas de trabajo que, por un lado, nos facilitan la prestación eficaz de servicios de calidad, y por otro están detrás de la información que manejamos. Si hoy día tenemos que adoptar medidas de protección de los datos que se utilizan en el despacho, como que dichos datos se almacenan electrónicamente y no en papel, tendremos que tener protegidos nuestros sistemas. Y si debemos adoptar unas determinadas medidas en relación con la prevención del blanqueo de capitales, en tanto en cuanto toda la información que incide en este campo nos llega y se almacena de manera informática, estaremos obligados a controlar este flujo electrónico.

Por ello, tanto en los despachos como en las empresas de nuestros clientes, será inevitable que adoptemos medidas de seguridad para que nadie pueda acceder a nuestros datos si no se lo hemos autorizado, igual que antes teníamos que custodiar nuestros archivadores o, de la misma manera que antes adoptábamos medidas para salvar la información de los clientes si se producía un incendio o una inundación, ahora tendremos que prevenir un borrado de nuestros archivos por un virus informático.

Es en este campo donde se mueven nuestros compañeros del RASI-CGCEE, el órgano de los Auditores de Sistemas de Información, registro que pilota una nueva actividad de los economistas de carácter transversal y emergente en este nuevo escenario de prestación de servicios profesionales que nos ha tocado vivir.

Sistemas de Información Informatizados, un desafío a la seguridad

Alonso Hernández García
Vicepresidente 2º de RASI-CGCEE

Son de todos bien conocidas las ventajas aportadas por la informática a los sistemas de información. Las operaciones viables de ejecutarse son ampliamente superiores a las de cualquier sistema de información tradicional.

La electrónica con su representación digital permite cálculos, comparaciones, deducciones, análisis, etc. automáticamente, de imposible realización de esta forma en un sistema tradicional.

Pero a tanta ventaja no le podía faltar su compensación problemática. La forma de registrar los datos y la estructura del ordenador permiten accesos desde el exterior sin limitación alguna lo que constituye la vulnerabilidad del sistema.

Estas vulnerabilidades pueden materializarse de diversas formas, bien actuando sobre la integridad de la información almacenada o impidiendo su disponibilidad y confidencialidad.

La época feliz de la caja fuerte que cerrándola bastaba para proteger plenamente los libros y documentos constitutivos del sistema de información a la necesidad de analizar todas las vulnerabilidades que ofrezca un sistema informatizado, evaluando el riesgo que se presenta y estableciendo los controles necesarios para superarlos.

Es de destacar que esta función de evaluar riesgos y establecer controles es una necesidad de las entidades para salvaguardar su activo y una obligación establecida por las NORMAS en vigor, como el Boicac nº 4 que establece que el auditor ha de proceder a analizar estas funciones y si no está preparado para ello, nombrar a un profesional que lo realice. Esta norma está igualmente establecida internacionalmente.

Específicamente la Agencia Española de Protección de Datos Personales abunda en esta ordenanza clasificando la información de datos personales en tres niveles de importancia, estableciendo controles para las mismas, auditables bianualmente y con sanciones de hasta 600.000 euros.

RASI, es un órgano especializado, de carácter técnico, del Consejo General de Colegios de Economistas de España, de los previstos del Capítulo VIII de sus Estatutos, aprobados por Real-Decreto 1/1998, de 9 de enero, que se rige por lo dispuesto en el presente Reglamento, por las normas que dicte el Pleno del Consejo General y la Comisión Permanente, y subsidiariamente, en lo no previsto en el mismo, por el Estatuto del Consejo General.

El RASI-CGCEE, tiene la finalidad, entre otras, de mejorar la oferta de servicios prestados por los economistas que, voluntariamente inscritos, desarrollan, o quieran desarrollar, sus funciones en el ámbito de la auditoría informática, o la asesoría para el desarrollo e implantación de un sistema de controles certificable.

Para ello, se vienen impartiendo diversos cursos destacando el de obtención del diploma CISA de reconocimiento mundial, así como conferencias y charlas sobre legislación vigente a objeto de colaborar con la formación de sus integrantes.

Continuidad de Negocio: respaldo internacional

Alejandro García Ruiz
Miembro del Comité Consultivo de RASI-CGCEE

La **Continuidad de Negocio,** ese activo, esa capacidad de prevenir cualquier tipo de incidencia que nos impida suministrar nuestro producto o servicio en condiciones óptimas, va a tener un breve un respaldo a nivel internacional.

Ante el interés que suscitó en su momento la normativa BS 25999, enfocada a la Continuidad de Negocio, tema del que, estamos tratando, la comunidad internacional y en concreto ISO, dará su conformidad y dicha normativa, actualmente inglesa, pasará a denominarse cómo normativa internacional (ISO). La fecha estimada de publicación de dicha normativa será Junio/Julio 2012, y pasará a denominarse cómo ISO 22301.

La perspectiva de la norma, es interesante. El crecimiento en certificaciones de empresas contra esta norma será gradual pero no impactante

Si bien, por la experiencia anterior existente de pasos de normas nacionales a normas internacionales (BS 5750 dio lugar a ISO 9001, BS 7750 a la ISO 14001, BS 7799 a la ISO 27001,….) los cambios no son excesivamente drásticos, manteniendo prácticamente su troncal (pero cambiando su estructura) y aceptando varias matizaciones.

El primer punto que llama la atención es la denominación de la norma, pasando de "Sistemas de Continuidad de Negocio" a "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio". Lo que se pretende es hacer popular la normativa, que puede llegar y ser aplicable a cualquier tipo de organización, independientemente, de su tamaño o actividad. La idea es acercarla a la popularidad de la ISO 9001, actualmente la norma de certificación de Sistemas más conocida y aceptada a nivel mundial con más de un millón de certificaciones existentes en todo el mundo. Ahora bien, cabe destacar e informar que la complejidad de la implantación de la norma ISO 22301 es muchísimo mayor que una implantación de un Sistema de Calidad (contra ISO 9001), por lo que el mercado potencial de implantación y certificación se limita enormemente, si bien es cierto, que la utilidad y parabienes de la implantación de la ISO 22301, para una compañía, son innumerables (capacidad de respuesta, sistema de organización, análisis de datos,…).

Cómo comentábamos antes, el troncal de la norma BS 25999 se mantiene en la ISO 22301 (Política de Continuidad, Evaluación de Riesgos, Análisis del impacto en el negocio, Planes de Continuidad, Pruebas, Comprobaciones,…además de los requerimientos de todo tipo de norma de gestión, P-D-C-A, Plan-Do, Check, Act, que son tales como la Revisión del Sistema por la Dirección, definición de objetivos, Auditorías Internas, No Conformidades, Acciones Correctivas, Análisis de las necesidades formativas en materia de Continuidad de los empleados, etc,…). Pero se incluyen diferencias y matizaciones significativas en la nueva norma (el concepto de "Estrategia de Continuidad" la ISO 22301 lo llama "Opciones de Continuidad", el Análisis del Impacto en el Negocio es más detallado y requiere de mayor información y datos, al igual que los procedimientos de

planes de respuesta y recuperación, las Acciones Correctivas pasan a denominarse "Medidas para atender incidentes e inquietudes" y la documentación se denomina "información documentada"…)

Sí que se puede decir que la ISO 22301, es una norma totalmente enfocada a la mejora de las organizaciones a nivel de gestión, ya que se ha construido sobre las base de otras normas internacionales ya revisadas y mejorada con las particularidades específicas de su actividad, por lo que, podemos afirmar, que esta norma ayudará, sin lugar a dudas, a las empresas en su gestión.

En materia de planificación, cabe destacar que la ISO 22301 es muchísimo más rigurosa en la planificación y preparación de los recursos, identificando este requisito de manera mucho más detallada, ya que los requisitos identificados en este punto de la norma son más amplios y contundentes.

Si bien, todos estos comentarios y reflexiones, los hemos realizado sobre el borrador de la norma (de Febrero del 2011); por la experiencia que se tiene con anteriores normas internacionales, desde la emisión del borrador a la publicación de la norma definitiva, prácticamente, el contenido será en un 95% idéntico al existente en el borrador, por lo que no nos encontraremos grandes sorpresas a la hora de la presentación de la ISO 22301.

Seguramente, una pregunta típica que se están realizando es…¿qué ocurrirá con los certificados de BS 25999 que han sido emitidos a compañías en los anteriores años?. Muy sencillo, el procedimiento de certificación, indica que en la siguiente auditoria anual a realizar en la sociedad, el enfoque ha de ser de auditoría de recertificación (y no de certificación ni de seguimiento), realizando la Entidad de Certificación la auditoria contra la nueva norma ISO 22301. Si todo fuese conforme, se pasaría a emitir un nuevo certificado, contra ISO 23301, y con una vigencia trienal.

Este tipo de norma, es necesaria de implantar en grandes organizaciones, corporaciones, administraciones públicas, y organizaciones que por su naturaleza de negocio, necesiten suministrar su actividad sin interrupción

La perspectiva de la norma, es interesante. El crecimiento en certificaciones de empresas contra esta norma será gradual pero no impactante, ya que, cómo comentábamos antes, es una norma ambiciosa, y compleja de implantar, no siendo accesible, en un primer plano, a todas las organizaciones, además de encontrarnos en un escenario económico, en el que no habrá ayudas gubernamentales que ayuden a la implantación y posterior certificación de esta norma (cómo ha ocurrido históricamente en España con normas cómo la ISO 9001, ISO 14001 o recientemente con la normativa ISO 27001).

Aún así, este tipo de norma, es necesaria de implantar en grandes organizaciones, corporaciones, administraciones públicas, y organizaciones que por su naturaleza de negocio, necesiten suministrar su actividad sin interrupción, por lo que a corto plazo las siglas ISO 22301 comenzarán a ser enormemente populares.

Incidentes de seguridad de la información: cómo monitorizarlos y gestionarlos

Yazomary García García
Miembro del Consejo Consultivo del RASI-CGCEE

En la actualidad, los incidentes de seguridad son inevitables y cada vez más tienen una mayor repercusión en la imagen corporativa y probablemente en los estados financieros. Adicionalmente, si las organizaciones no disponen de un registro de las incidencias que afecten a la seguridad de los datos de carácter personal, estarían incumpliendo con el **Artículo 90 del Reglamento de la Ley de Protección de Datos personales,** el cual lleva por título: "Registro de Incidencias", y su texto dice "que todo fichero automatizado deberá contar con un registro de incidencias en el que se hará constar cualquier anomalía que afecte o pudiera afectar la seguridad de los datos de carácter personal, por lo tanto deberá existir un procedimiento de notificación y gestión de las incidencias……".

Un incidente de seguridad puede ser definido como un evento cualquiera que pueda comprometer la seguridad de la información de una compañía. Cada vez más, el crecimiento tecnológico dificulta a las organizaciones la detección de vulnerabilidades y ataques que puedan impactar de manera negativa. En este sentido, las organizaciones deben estar preparadas para detectar y dar respuesta a incidentes de seguridad de la información, tales como: accesos no autorizados, infección de virus, fallos de hardware, barrido de puertos (Scan), ingeniería social, etc. Por tal motivo, las organizaciones deben emprender actitudes y acciones proactivas, para asegurar que sus entornos informatizados estén lo suficientemente preparados y adecuados para identificar eventos, mitigar su impacto en el menor tiempo posible y reducir así el costo de la investigación forense.

Un incidente de seguridad puede ser definido como un evento cualquiera que pueda comprometer la seguridad de la información de una compañía.

Una adecuada definición e implantación de un **"Proceso de Respuesta a Incidentes",** permite a las compañías gestionar de manera correcta y eficiente los eventos de seguridad, cuando éstos ocurren, a través de la ejecución sistemática de cada una de las siguientes actividades o etapas:

- Identificación del incidente.
- Clasificación del incidente.
- Notificación del incidente.
- Respuesta al incidente.
- Recuperación del incidente.
- Evaluación y reflexión sobre el incidente.

Identificación del incidente

Determinar principalmente si el incidente es un evento de riesgo o una falsa alarma. En caso afirmativo se debe identificar el tipo específico de evento, ya que contribuye a hacer seguimiento y entender el riesgo al que se encuentra sometida la organización. Algunos tipos comunes de incidentes incluyen: ataques a website, ataques de denegación de servicio, sniffing, acceso no autorizado, etc.

Clasificación del incidente

Se clasifica y se categoriza el incidente en función al grado de severidad y daño que pueda causar en la organización, por lo tanto se hace imprescindible desarrollar una escala de calificación, como:

- **Nivel de Severidad 1: Crisis**. Es el más severo. Una situación bajo esta categoría indica que existe un alto peligro. Por ejemplo: un acceso no autorizado o pérdida de la información almacenada en un servidor crítico.
- **Nivel de Severidad 2: Incidente serio.** Se requiere atención inmediata para prevenir que el incidente escale a un nivel de crisis. Por ejemplo: información de cuentas de usuario ha sido expuesta y puede ser utilizada para realizar un acceso no autorizado.
- **Nivel de Severidad 3: Incidente.** Nivel de urgencia es bajo. Por ejemplo: un IDS (sistema de detección de intrusos) ha identificado que se ha realizado un Scan de la red interna de la organización, por lo tanto el incidente no causa ningún daño pero si advierte que alguien está intentando identificar sistemas o encontrar vulnerabilidades que pueda utilizar.
- **Nivel de Severidad 4: Evento.** Debe ser resuelto, pero el grado de urgencia es menor. Por ejemplo: una cuenta de usuario ha sido bloqueada después de múltiples intentos fallidos de acceso, lo que podría representar que una persona no autorizada está intentando adivinar las contraseñas de los perfiles y ganar de este modo el acceso al sistema.

Un "Proceso de respuesta a incidentes" deber ser consistente con los objetivos de la organización, con el grado de importancia y niveles de riesgos que representan las operaciones y con los recursos que están disponibles

Notificación del incidente

El incidente se debe notificar a las personas apropiadas en función a la clasificación que se le haya dado al incidente, con el fin de que se realicen las acciones correspondientes.

Respuesta al incidente

El diseño de modelos de respuestas, en función al nivel del incidente, se puede realizar en paralelo con las etapas de clasificación y notificación. Para ello se debe realizar una recolección y evaluación de todos los datos relevantes sobre el incidente, una investigación para determinar la causa y el alcance que ha tenido el incidente (lo que permite a su vez, revelar vulnerabilidades técnicas que han permitido el evento) y por último la organización debe disponer de un equipo de soporte técnico que brinde apoyo al equipo de investigación y pueda proveer acceso a los recursos.

Una adecuada definición e implantación de un "Proceso de Respuesta a Incidentes", permite a las compañías gestionar de manera correcta y eficiente los eventos de seguridad

Recuperación del incidente

Devolver los procesos de la organización a un estado seguro y operacional, de la manera más eficiente posible. Permite realizar un análisis de los daños ocurridos, de la información que se ha perdido y del estado del entorno informatizado posteriormente al incidente. Por ejemplo: en caso de perfiles de usuarios compartidos y contraseñas capturadas, que no fueron utilizadas, un cambio simple de contraseñas podría ser toda la recuperación adecuada.

Evaluación y reflexión sobre el incidente

Se discuten las lecciones aprendidas y las mejoras que pueden ser implementadas para resolver de la mejor forma posible, un evento similar en el futuro. Es recomendable que se realice dentro de las dos semanas siguientes a la resolución del incidente.

Un "Proceso de respuesta a incidentes" deber ser consistente con los objetivos de la organización, con el grado de importancia y niveles de riesgos que representan las operaciones y con los recursos que están disponibles. De igual forma, se debe asegurar durante el diseño del proceso la interrelación de éste con otros procesos de la organización, tales como: acuerdos de niveles de servicio (SLA), planes de continuidad del negocio, evaluaciones independientes de seguridad, entre otras.

SOBRE PREVENCIÓN DE BLANQUEO DE CAPITALES

En relación a las implicaciones y obligaciones a considerar en materia de Prevención del Blanqueo de Capitales y Financiación del Terrorismo (PBC y FT) por parte de los **Auditores, Asesores Fiscales, Contables Externos y determinadas actividades de los Asesores de ámbito jurídico / económico** y atendiendo al elevado número de consultas y solicitud de información que se han efectuado queremos clarificar los aspectos básicos a considerar en las anteriores actividades:

AFECTACIÓN DIRECTA: Todas las actividades anteriores son sujetos obligados, por el ejercicio de dicha actividad a la normativa de PBC y FT. Todo ello con independencia del número de clientes, empleados y las actividades de los clientes.

OBLIGACIONES FUNDAMENTALES: Como sujetos obligados a dicha normativa deberemos asegurarnos de los siguientes aspectos fundamentales:

- **Inscripción formal en el SEPBLAC:** Inscripción en el registro de sujetos obligados, con identificación de la persona representante en materia de PBC y FT.
- **Comunicación al SEPBLAC:** de cualquier hecho o presunción de que existe indicio o certeza de estar relacionado con el blanqueo de capitales.
- **Procedimientos y Documentación de cumplimiento PBC y FT:** Todos los sujetos obligados deben aplicar determinados procedimientos (y aprobarlos por escrito) e identificar a TODOS sus clientes. Dichos procedimientos y la documentación, en la que se formalice el cumplimiento de sus obligaciones en este campo, debe de estar adecuadamente acreditada y custodiada (mínimo 10 años).
- **Aprobar un manual de prevención en blanqueo de capitales.**
- **Formación:** Todos los empleados y específicamente las de mayor responsabilidad (Socios y Directivos) deben de realizar y acreditar la realización de formación en PBC y FT.
- **Examen Anual Externo:** Todos los sujetos obligados (con excepción de los empresarios o profesionales que ejercen a titulo individual) deben de realizar un examen anual por parte de un experto externo independiente. A tal efecto se ha creado un registro de control por parte del SEPBLAC. (En los dos años siguientes se puede sustituir por informes de seguimiento).
- **Implicaciones y Oportunidad Profesional en Clientes:** Los Auditores deben de evaluar en los clientes afectados en PBC y FT el adecuado cumplimiento de los aspectos fundamentales de la norma. A nivel general los clientes necesitan soporte profesional en esta área por lo que nuestro colectivo está en la mejor disposición de asesorar en esta materia.

PROGRAMA SOPORTE CGCEE

Tal como os hemos informado desde el CGCEE hemos abierto el canal de soporte en LPBC y FT para atender las dudas que tengáis en esta materia y específicamente hemos creado los **Programas de Formación** para Socios/Directivos y un programa avanzado para la función de experto en LPBC y FT, creando un registro a tal efecto.

Estos programas de formación se han creado para cumplir con los requisitos de obligado cumplimiento que la LPBC y FT requiere a las actividades sujetas y adicionalmente incluyen guías de evaluación y referencia para poder detectar las situaciones y necesidades para un adecuado cumplimiento de la LPBC y FT tanto a nivel directo como de los clientes sujetos a dicha normativa.

Tal como os hemos informado en los comunicados anteriores los programas cumplen con los requisitos de formación continua del ICAC, y para todos aquellos que todavía no habéis efectuado ni acreditado la formación obligatoria en LPBC y FT quedamos a vuestra disposición para aportaros mayor detalle de los mismos.

Esperamos que esta nota os sirva de ayuda y aclaración en los aspectos críticos de la norma y quedamos a vuestra disposición para seguir atendiendo cualquier duda en relación a los requisitos y plazos para el 2012 que debemos considerar en nuestras actividades profesionales.

SOBRE LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Como asesor en materia laboral tengo acceso a ciertos datos de carácter personal de los trabajadores de mis clientes (empresas), ¿debo pedir el consentimiento a cada uno de ellos para tratar esos datos?

La respuesta es no. Usted, como asesor laboral, tiene la consideración de encargado de tratamiento, es decir, es un tercero (persona física o jurídica) que por razón de un servicio determinado debe tener acceso a datos de carácter personal, en este caso de trabajadores, a cuenta del responsable del tratamiento. En virtud del artículo 12 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, no se considera una comunicación de datos y por tanto no se requiere consentimiento del interesado (trabajador), "únicamente" la necesidad de proceder a la firma de un contrato entre las dos partes que regule el tratamiento de los datos. Entre otros aspectos, este contrato deberá establecer que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas, así como las medidas de seguridad a aplicar.

Soy un auditor de cuentas y para la gestión de mi actividad necesito tener acceso a cierta documentación que podría contener datos de carácter personal. ¿Hay algún problema en ello?

No hay ningún problema. Efectivamente cuando un auditor de cuentas accede a datos personales de las empresas en la que presta servicios se produce una cesión de datos, por ello hay que atender a lo dispuesto en el artículo 11 de la Ley Orgánica de Protección de Datos de Carácter Personal. Este artículo establece que se requiere consentimiento del interesado para proceder a esta cesión de datos, a no ser que concurra una serie de excepciones que también se detallan, y entre ellas se encuentra el caso que la cesión esté autorizada en una ley. En este sentido la Ley de Auditoría de Cuentas establece que el auditor debe tener acceso a aquella documentación que requiera para la emisión del informe correspondiente, no obstante en base al principio de calidad de los datos el acceso debe limitarse a los datos que resulten estrictamente necesarios para el servicio prestado. No obstante, esta misma norma también exige que el auditor de cuentas mantenga el secreto de cuanta información conozca en el ejercicio de su actividad. Dicho esto, también corresponde al auditor de cuenta tomar las medidas de seguridad oportunas para el tratamiento de los datos personales a los que tiene acceso, por ejemplo en relación a la custodia de la documentación.

He leído que al ser asesor fiscal y disponer de ciertos datos de carácter personal de mis clientes (personas físicas), debo inscribir un fichero ante un organismo oficial. ¿Es así?

La respuesta es sí. El asesor fiscal dispone en este caso de datos de carácter personal de sus clientes, personas físicas, para la prestación de un servicio, pasando a tener la consideración de responsable del fichero o tratamiento. En este sentido debe proceder a inscribir un fichero al efecto ante la Agencia Española de Protección de Datos cuyo nombre debe decidir él mismo, por ejemplo fichero de clientes. Un fichero es un conjunto organizado de datos de carácter personal cualquiera que sea su forma o modalidad, que responde a un tratamiento de datos entorno a una finalidad determinada. De todas maneras hay que tener en cuenta que inscribir el fichero es sólo el primer paso para garantizar un correcto cumplimiento en materia de protección de datos, debe cumplir también con el derecho de información previsto en el artículo 5 de la Ley Orgánica de Protección de Datos indicando la finalidad del tratamiento de los datos que obtenga, así como establecer las medidas de seguridad exigibles que se determinan en el Título VIII del Real Decreto 1720/2007 por el que se aprueba el Reglamento de la mencionada Ley Orgánica.

Nuevo Comité Consultivo RASI, 5 de marzo 2012

El nuevo Comité Consultivo del Registro de Auditores de Sistemas de Información, RASI-CGCEE, está compuesto por: **Valentín Pich Rosell,** Presidente; **Carlos Puig de Travy,** Vicepresidente 1º; **Alonso Hernández García,** Vicepresidente 2º; **Joaquím Altafaja Diví, Abel Bonet Dolcet, Yazomary García García, Alejandro García Ruíz, Ramón Miñones Crespo** y **Eloy Peña Ramos**

RASI-CGCEE orienta su actividad a la formación, información y defensa de la auditoría de sistemas de la información en el colectivo de los Economistas y a la sociedad en general.

Convenio ISACA Barcelona, Valencia y Madrid

El Consejo General de Colegios de Economistas de España, CGCEE, ha firmado recientemente un convenio de colaboración con ISACA, en sus tres capítulos en España, Barcelona, Madrid y Valencia, con el propósito de sumar esfuerzos y complementar el desarrollo de las actividades para potenciar los objetivos de ambas partes.

Agencia Española de Protección de Datos

El pasado10 de mayo, se ha reunido una representación del Comité Consultivo de RASI-CGCEE con el Director de la AEPD. El Presidente, **Valentí Pich,** y los Vicepresidentes 1º y 2º de RASI-CGCEE, **Carlos Puig** y **Alonso Hernández** respectivamente, han mantenido un encuentro institucional con el Director de la Agencia Española de Protección de Datos (AEPD), **José Luis Rodríguez Álvarez,** en el marco del convenio de colaboración firmado entre ambas instituciones en 2008. Este convenio tiene como objetivo contribuir a la consolidación y desarrollo de la protección de datos y las materias relacionadas dentro del colectivo de los economistas en su actuación profesional y en los Colegios de Economistas.

Se asume como compromiso de ambas instituciones contribuir a la consolidación y el desarrollo de la protección de datos y materias relacionadas dentro del colectivo de los economistas en su actuación profesional y en los Colegios de Economistas.

SEPBLAC

El pasado 24 de mayo se celebró una reunión institucional entre SEPBLAC y CGCEE, a la que asistieron el Director y dos responsables del área de inspección del Servicio Ejecutivo de la Comisión de Prevención y Blanqueo de Capitales e Infracciones Monetarias, **Manuel Caro, Iván Aritio** y **Sebastián Denia,** respectivamente, junto con el Presidente de este Consejo General y de RASI, **Valentí Pich,** y el Vicepresidente 1º de RASI y Presidente del REA, **Carlos Puig.** En dicha reunión se han fijado objetivos comunes para ambas Instituciones y se han establecido unas líneas de colaboración con las que perseguimos ofrecer una más completa prestación de servicios para nuestros miembros.

Esta reunión ha hecho Experiencia y conocimiento del personal especializado del SEPBLAC para colaborar en el diseño y ejecución de cursos así como otras acciones divulgativas y formativas en esta materia.

Joaquím Altafaja, elegido Presidente de ISACA Barcelona

Joaquim Altafaja Diví ha sido elegido Presidente del Capítulo de ISACA Barcelona, asociación sin ánimo de lucro, con socios en Catalunya, Baleares y Andorra. El hasta ahora Director de socios del capítulo catalano-balear releva a Albert Lladó Palau quien deja la Presidencia después de 4 años para incorporarse como Past President y Vicepresidente. Altafaja es miembro del Comité Consultivo del RASI-CGCEE y Coordinador del equipo redactor de la Guía Orientativa para la aplicación de la Norma Técnica de Auditoría de Cuentas en entornos informatizados liderada por ISACA Barcelona y que cuenta con la colaboración técnica de las dos corporaciones españolas de auditoría financiera. Dispone de una dilatada trayectoria profesional en los ámbitos de sistemas, seguridad y auditoría, protección y privacidad de datos de carácter personal y cumplimiento normativo en la prevención del blanqueo de capitales. Profesional independiente colabora habitualmente con Pich Asociados y Abante Auditores.

Próximos Eventos

2º Congreso Anual de ISACA Barcelona bajo el lema "Valor y gestión garantizada a los profesionales de las Tecnologías de la Información"

3 de Julio

El objeto de este acto es propiciar un foro anual de encuentro entre los profesionales de la Auditoría, la Seguridad y la Gobernanza de las Tecnologías de la Información.

En esta 2ª edición se presentará una Guía Orientativa que proporcione Material de Referencia y Ayuda a la Norma Técnica de Auditoría de Cuentas en Entornos Informatizados. Este documento, que ha sido elaborado por voluntarios de nuestra asociación conjuntamente con técnicos del Registro de Economistas Auditores-CGCEE y del Colegio de Censores Jurados de Cuentas de Catalunya, pretende dotar a los auditores financieros de herramientas que permitan evaluar el grado de complejidad de un entorno informatizado en un trabajo de auditoría, en el que las aplicaciones informáticas estén implicadas en la elaboración de información financiera, ayudando a identificar riesgos y sirviendo de modelo a los principales objetivos de control interno.

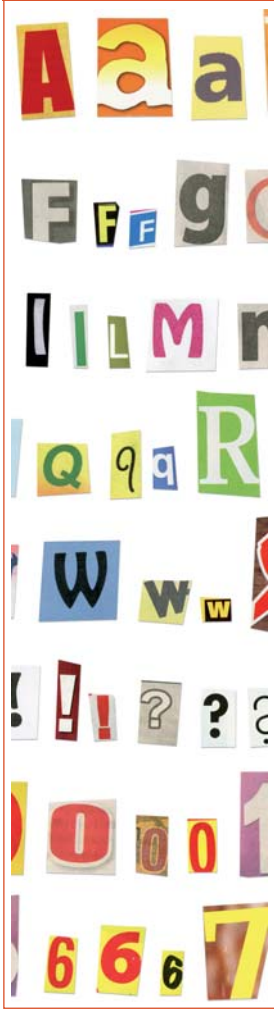
Cursos disponibles

- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Expertos.
- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Dirigido a socios y directivos.
- Curso on line de Protección de Datos Personales.
- Sesión formativa sobre Prevención de Blanqueo de Capitales y Financiación del Terrorismo en el Sector de Automoción. 30 de mayo de 2012.

Próximos Cursos

- Seminario de Prevención de Blanqueo de Capitales y Financiación del Terrorismo en el Sector Fundacional.
- Seminario de Prevención de Blanqueo de Capitales y Financiación del Terrorismo: Implicaciones en materia de responsabilidad penal.

El potencial informativo de las revistas del Consejo General



economistas
Consejo General

amplio abanico de revistas técnicas y profesionales al servicio del mundo académico, empresarial, responsables de la administración y economistas


"economistas"
Información general


"3conomi4"
Macroeconomía y universidad


"newsREA"
Auditoría


"REAF revista"
Fiscal


"REFOR revista"
Forense


"boletín ECIF"
Contabilidad

"actualidad RASI"
Sistemas de Información


"EAFInforma"
Asesoramiento Financiero

últimas incorporaciones a RASI-CGCEE

Colegio de A Coruña:

Canalejas Couceiro, José Ángel	Nº 211
López de Paz, Luis	Nº 189
González Castro, José María	Nº 166

Colegio de Alicante:

Manresa Guillén, Antonio	Nº 200
García Bernabé, Ezequiel	Nº 192
Martínez García, María Teresa	Nº 187
Burlo Caravaca, Juan Francisco	Nº 182

Colegio de Almería:

Santana Peramo, Óscar	Nº 165

Colegio de Aragón:

Nieto Avellaneda, Javier Francisco	Nº 214
Gracia Herreiz, Francisco José	Nº 205

Colegio de Asturias:

Antuña Vigil, José Carlos	Nº 193
García Cosmea, Roberto	Nº 175

Colegio de Cádiz:

Brotons Llobregat, Baltasar	Nº 184

Colegio de Cataluña:

Ávila Morera, Carles	Nº 216
Álvarez Pérez, Emilio	Nº 213
De Anta Puig, Carlos	Nº 194
Ginesta Albert, Carles	Nº 167
Puig de Travy, Carlos	Nº 156
Pich i Rosell, Valentí	Nº 155
Bonet Dolcet, Abel	Nº 152

Colegio de Córdoba:

Obrero Castilla, Vicente	Nº 163

Colegio de Extremadura:

Uviedo Silva, Amanda	Nº 171

Colegio Islas Baleares:

Ramírez Vázquez, Francisco	Nº 179

Colegio de Madrid:

Rabadán Rituerdo, Eduardo	Nº 215
Calleja Bermejo, José Miguel	Nº 212
Delgado Coque, Martín	Nº 210
Guardón Curto, Enrique	Nº 209
García Pérez, Juan Carlos	Nº 195
Olmeda León, Juan Luís	Nº 186
Baena Jiménez, Roberto	Nº 183
Jiménez Sánchez-Seco, Alberto	Nº 181
Oliveros Sastre, Jacobo	Nº 174
Gafforio Maldonado, Antonio	Nº 172
González Alemany, Gerardo	Nº 168
Martínez Fernández, Fernando	Nº 160
Granados Dávila, José Antonio	Nº 158

Colegio de Málaga:

Oliva Tortello, Victoria	Nº 199
Talavera Gabaldón, Abel	Nº 198
Gil Navarro, Isabel María	Nº 190
Llull Cejudo, Sergio	Nº 178

Colegio de Murcia:

Madrid Nicolás, Ramón	Nº 204
Martínez Cano, Francisco	Nº 201
García Moya, Antonio	Nº 196
Mompeán Franco, Antonio	Nº 180

Colegio de Navarra:

Aldaz Pastor, Enrique	Nº 203

Colegio de Sevilla:

Berraquero Calero, Alberto	Nº 208
Corredera Córdoba, Francisco	Nº 159

Colegio de Pontevedra:

Miguez Docampo, Luis Alberto	Nº 170
Martín Saracho, Alejandro	Nº 169

Colegio de Tenerife:

Hergog Niebla, Enrique	Nº 202

Últimas incorporaciones a RASI-CGCEE

Colegio de Valencia:

Gutiérrez Morales, María de los Reyes	Nº 191
Caudeli García, David	Nº 188
Alfonso Escorihuela, Fernando	Nº 185
Molero Prieto, Rafael	Nº 173
Forner Pérez, Mario	Nº 157

Colegio de Valladolid:

Lomas Frechilla, Francisco Javier	Nº 197
Villegas Díez, Óscar Julio	Nº 176

Colegio Vasco:

Gómez Angulo, José Luis	Nº 177
Comas Valls, Raquel	Nº 164
Cazenave Zarandona, Amadeo	Nº 161

Asociados:

Martínez Quiles, Federico	Nº 207
De Hermeneguildo Salinas, Rafael	Nº 206
Martín Molina, Pedro Bautista	Nº 162
García García, Yazomary José	Nº 154
Altafaja Divi, Joaquím	Nº 153

RASI-CGCEE

Órgano especializado del Consejo General de Economistas en Auditoría de Sistemas de Información. Registro pionero en la conexión entre tecnología y empresa.

Funciones RASI

- **Soporte profesional** → Comité consultivo multidisciplinas con perspectiva global. Enfocado a las necesidades reales del profesional.
- **Formación especializada** →
  - Implicaciones IT
  - Cumplimiento Normativo
- **Reconocimiento Profesional** →
  - Diploma Miembro
  - Certificaciones
    - Especialización
    - Experto
- **Información actualizada** →
  - Notas de aviso
  - Notas informativas
  - News RASI
- **Recomendaciones y guías de actuación profesional** → Marco de referencia y soporte en auditoría y en servicios especiales

economistas
Consejo General
RASI · economistas auditores de sistemas de información

Diploma de acreditación como miembro de RASI-CGCEE

D. _____

con número de miembro de RASI _____ está interesado en recibir el Diploma.


El Presidente del Consejo General de Colegios de Economistas de España
acredita que
D. Nombre Apellido Apellido
es miembro del Registro de Auditores de Sistemas de Información
del Consejo General de Colegios de Economistas de España
Madrid, a 14 de Junio de 2010
El Presidente
El interesado
economistas

Y para ello autoriza el cargo de 30 euros *(gastos de envío incluidos)* en su cuenta.

En _____

a _____ de _____ de _____

Tamaño del Diploma: A-3

Enviar email a: rasi@economistas.org

Cómo formar parte de RASI-CGCEE

¿Qué es necesario para ser miembro de RASI-CGCEE?

a) Estar colegiado

b) Estar dispuesto a cumplir las normas deontológicas

¿Qué es necesario para ser asociado de RASI-CGCEE?

a) No poder estar colegiado en un Colegio de Economistas, por no estar en posesión de la titulación requerida

b) Estar dispuesto a cumplir las normas deontológicas

Cuotas de Inscripción

· Miembros de los Órganos del Consejo General: 25 euros anuales

· Resto de colegiados: 65 euros anuales

· Asociados: 100 euros anuales

Para inscribirse habrá de cumplimentar el formulario que aparece en el siguiente enlace: http://www.rasi.economistas.org/index.php/miembros.html

solicitud de inscripción