

Madrid News

ISACA MADRID, Paseo de la Castellana nº 91 3ª-I. Madrid 28046
<http://www.isacamadrid.es> administración@isacamadrid.es 91.636.29.60



Este número

Julio San José Sánchez
Vocal Relaciones con Asociados

Llega tras el paréntesis laboral del verano y ahora nos toca volver a la rutina y tomar el pulso al día a día.

Este segundo número de Madrid News llega con el afán de superar la buena acogida que vosotros, los profesionales de la asociación le habéis dado.

Habéis recogido muy bien *'el guante'* de la participación y podemos decir con orgullo que hemos recibido bastantes colaboraciones para este segundo número, todas ellas de un excelente nivel tanto profesional como intelectual, desde aquí os continuaremos animando para que sigáis enviándonos vuestras colaboraciones y sugerencias para este boletín, que es el vuestro,

Seguimos creyendo firmemente en esta forma de comunicación con los asociados y por ello trabajaremos para hacerla cada día un poquito mejor, por aquello de predicar con el ejemplo en la mejora continua.

Contenido

Este número	1
Firma invitada	2
Noticias de la Asociación	6
Formación	8
La asociación en cifras	9

Reiteramos el compromiso ofrecido en el primer número y te invitamos a que nos envíes tu opinión, comentarios o si lo deseas, artículos o temas que creas interesante publicar.

Un cordial Saludo,

Firma Invitada

Isabel M. Gómez González

MEDICION CONTINUA DE RIESGOS

YO YA NO CALCULO RIESGOS MANUALMENTE, ¿Y TÚ?

Una de las principales funciones de un área de seguridad, es ser capaz de identificar de manera clara y precisa cual es el nivel de riesgo de su negocio.

El abanico de posibilidades para calcularlo es muy amplio. Se mezclan conceptos variados como impactos, probabilidades, requisitos de seguridad y múltiples posibilidades que pretenden ser encuadradas en fórmulas matemáticas diversas, intentando dar objetividad a un proceso que en la mayoría de las Entidades y Organizaciones a veces resulta "adivinatorio".

Recoger en un proceso metodológico, objetivo, fiable, medible y replicable algo que por naturaleza parece indefinible es complicado. Especialmente, cuando hasta el momento no existía ningún actuario de seguridad en el mercado sobre el que apoyarse.

El ciclo de vida de gestión de riesgo no sólo conlleva un análisis y una identificación de los riesgos intrínsecos, efectivos y residuales sino una toma de decisión. Una vez identificado el nivel de riesgo de cada Entidad y Organización debe decidirse qué hacer o qué no hacer a partir de una metodología adecuada a sus necesidades.

Todo este proceso está enmarcado en la ardua tarea de cumplimentar hojas de cálculo interminables, la recopilación de millones de vulnerabilidades, agrupadas según diversos criterios en grupos de amenazas que no se sabe muy bien cómo valorar, interminables entrevistas

y búsquedas de datos, todo ello sazonado con una sensación de "persona que cruza el desierto" mientras se realiza.

Se acabó. ¡Revolución! Llega la medición continua del riesgo. El uso de metodologías y herramientas que sean capaces de proporcionar datos objetivos, que permitan comunicarnos con la alta dirección a través de datos que les permitan tomar decisiones sobre la tecnología, con su forma habitual de gestionar. Herramientas que sean sencillas, intuitivas, que reduzcan en más de un 70% la carga de trabajo y, sobre todo, que ayuden y aporten valor a los procesos de negocio.

El arte de parametrizar el mecanismo de una bola de cristal.

Desde tiempos inmemoriales, las bolas de cristal han sido empleadas para dar credibilidad y espectacularidad a todo tipo de ritos adivinatorios. En muchas ocasiones, especialmente cuando un responsable de seguridad se enfrenta a su primer análisis de riesgos, se siente un poco adivino y por desgracia la mágica esfera no suele decirle nada. Si a esto añadimos las múltiples metodologías existentes en el mercado, tan válidas unas como otras, soportadas a su vez por organismos internacionales, códigos de buenas prácticas y normativas, parece imposible no suponer que la primera elección marcará la trayectoria de gestión del riesgo.

Por tanto, el primer paso para dar soporte al ciclo de vida de la Gestión del Riesgo es intentar abstraerse del día a día, mirar hacia los procesos de negocio de nuestra Organización, incluyendo las normativas de obligado cumplimiento, y buscar un buen traductor "factor económico - factor tecnológico" (No se debe olvidar nunca que la tecnología da soporte a negocio y que la primera sin la segunda no tiene razón de existir).

Elección de una metodología de análisis y gestión del riesgo: ¿tecnología o negocio?, ¿cualitativo o cuantitativo?

Una de las grandes elecciones a la hora de gestionar el riesgo es seleccionar una metodología capaz de ofrecernos valores objetivos adecuados a los activos, a los requisitos de seguridad, a las amenazas, a las salvaguardas, a los procesos de negocio y sobre todo a nuestra alta dirección.

No obstante, algo que frecuentemente se pasa por alto, es que la metodología no sólo tiene que ser buena si no que tiene que estar soportada en una herramienta de fácil gestión, muy sencilla, muy visual y que ofrezca valores que permitan, por ejemplo, tomar decisiones importantes en medio de una contingencia.

Es aquí donde la vieja tesis sobre el cálculo de valores se hace más patente: valores “en cifra” o valores “en letra”. Mi opinión es tajante a este respecto; si se quiere medir algo de forma objetiva hay que utilizar cifras. ¿Eso significa que alguien que mida sus riesgos dentro de una escala de alto, medio y bajo lo está haciendo mal? En absoluto. Sin embargo, el paso del tiempo desde mi primer análisis de riesgos me ha enseñado una cosa: Cuando alguien me pregunta cuál es mi nivel de riesgo, no es lo mismo decir que el riesgo es alto a decir, por ejemplo, que nuestra organización se esta jugando un 0,03% por millón de euros si no se arregla un agujero de seguridad.

Las cifras son palpables, comparables y sobre todo dan una idea más cercana de la situación siempre que hayan sido obtenidas de una forma adecuada. No es lo mismo, decir que alguien es “alto” a decir que alguien mide 1,85cm. Es evidente que el segundo valor da una imagen más nítida de la realidad.

Pero claro, los cálculos y las cifras deben estar soportados por herramientas o se volverán inmanejables. Es en este punto cuando me viene a la cabeza una reflexión que me dijo una vez uno de los directores y que representa de forma clara a que se debe aspirar “esto que me presentas me gusta. No entiendo al detalle cómo funciona la herramienta, pero si que veo con claridad los resultados en el cuadro de mandos. Si me dices que es una “caja negra” y que tu metes por un lado una de las vulnerabilidades que afectan a nuestras aplicaciones y es capaz de darme el impacto en euros sobre mi negocio si la saco a producción sin arreglar, me vale”.

“Me vale”, que palabras más grandes. Palabras que todos nosotros deberíamos oír más a menudo. Pocas veces recuerdo que “nuestros mayores” nos den el visto bueno de una forma tan clara. Sin embargo, cuando las utilizan, dejamos por un momento de ser el sector “paranoico que no habla su idioma sin algo objetivo que aportar salvo nuestro gran conocimiento” por “me ayuda a tomar decisiones para mover este trasatlántico”

Y ahora que sé cuál es mi riesgo, ¿qué hago con él?

La gestión del riesgo significa la creación de una serie de acciones a corto, medio y largo plazo. Eso lo sabemos todos. Pero, ¿qué acciones? ¿Quién o qué me las dice? ¿Son válidas en mi plan de tecnología anual? ¿Cómo casan con la evolución de mis procesos de negocio? Demasiadas preguntas a contestar, pero sobre todo hay una de ellas que ha acechado, al menos en una ocasión, a cualquier responsable que haya hecho un análisis de riesgos ¿Y ahora qué?

Se necesita ir más allá con la gestión del riesgo; que sea capaz de aportar soluciones de forma sencilla mediante el desarrollo de planes de acción obtenidos de forma semi-automatizada. Es imposible automatizar por completo el proceso, pero sí liberarnos de la mayor parte de carga manual que conlleva.

Me temo que aquí no hay recetas completas. Es necesario aprender a convivir con el riesgo y poder adelantarse a las situaciones que puedan afectar a las funciones que dan soporte a los procesos de negocio.

Existen herramientas en el mercado que nos ayudan a tomar este tipo de decisiones. Sólo hay que aplicar la adecuada a nuestras necesidades.

Herramientas de gestión: Qué pedir.

El proceso de análisis y gestión del riesgo, cuyo planteamiento en principio es robusto, se vuelve lento e ineficaz cuando no permite contestar a preguntas tan necesarias y a la vez tan complicadas como las siguientes:

- 1. ¿Cuál es el nivel de riesgo que va a sufrir una organización al poner en producción una nueva aplicación que da soporte a una función de negocio vital para la Organización?*
- 2. ¿Cómo aumenta mi nivel de riesgo en el momento que cae una de mis aplicaciones, tal y como reflejan las alarmas de los sistemas de monitorización?*
- 3. ¿El nivel de riesgo de mi organización es adecuado con respecto al sector de mercado en el que está ubicada mi organización?*
- 4. ¿Cómo se recalcula el riesgo cuando es descubierta una nueva amenaza?*

La forma más sencilla de contestarlas es desarrollando o adquiriendo una herramienta capaz de facilitar y realizar de forma repetitiva (automatizada) algunas de las tareas, especialmente aquellas que manualmente son más costosas.

CONCLUSION

Estas, y otras muchas pinceladas que no son objeto de este artículo, reflejan que ha comenzado una nueva era en la Gestión del Riesgo. Una época clara y nítida que deja atrás la palabra “riesgo”, tan manida en otros años, por un nuevo vocablo con el que se identifica la gestión del riesgo: Brújula. Las Brújulas continuas que ya se utilizan a día de hoy darán mucho que hablar por su trascendencia e importancia dentro de otros procesos y el propio entramado de nuestras Organizaciones. Especialmente durante los años venideros, en los que el horizonte dibuja un panorama restrictivo donde saber quien o qué supone un riesgo real va a ser una de las informaciones más preciadas para una compañía.

La medición y gestión continúa de los riesgos no es una utopía: es una realidad. Así que, ¿a qué espera para poner en marcha ya la Seguridad 2.0? Quizás, sea una buena idea comenzar a gestionar riesgos objetivamente de forma continua y convertirse en “Brújula”.

CONCLUSION (cont)

Yo, ya no gestiono riesgos de forma subjetiva, manual, costosa, complicada o no entendible por la alta dirección. Sigo los principios aquí descritos muy brevemente, y gestiono riesgos de forma continua obteniendo hechos y resultados que en mí día a día constituyen un pilar sólido para la consulta y la toma de decisiones. Ahora le toca decidir a usted.

Isabel M.Gómez González CGEIT, CISM, CISA, con más de una década de experiencia en el mundo de la Seguridad de la Información, desarrolla su actividad profesional en el grupo Caja Madrid. Master en Dirección de la Seguridad de la Información y protección del patrimonio por el IADE, cuenta con las certificaciones CGEIT, CISA y CISM por el ISACA.

Esta en posesión del título de Auditora Jefe de Sistemas de la Información. Como miembro del SC27 participa en la redacción de varias normas, entre ellas es coeditora de la futura norma de evidencias electrónicas. Posee una larga trayectoria en el sector de las TIC, ámbito en el que ha dirigido y participado en múltiples proyectos, especialmente en el sector de Banca, Telecomunicaciones e Industria, centrados en el desarrollo de planes estratégicos de seguridad, inteligencia en la gestión del riesgo y creación de cuadros de mando

Puede ser localizada en

isabelmaria.gomez@gmail.com

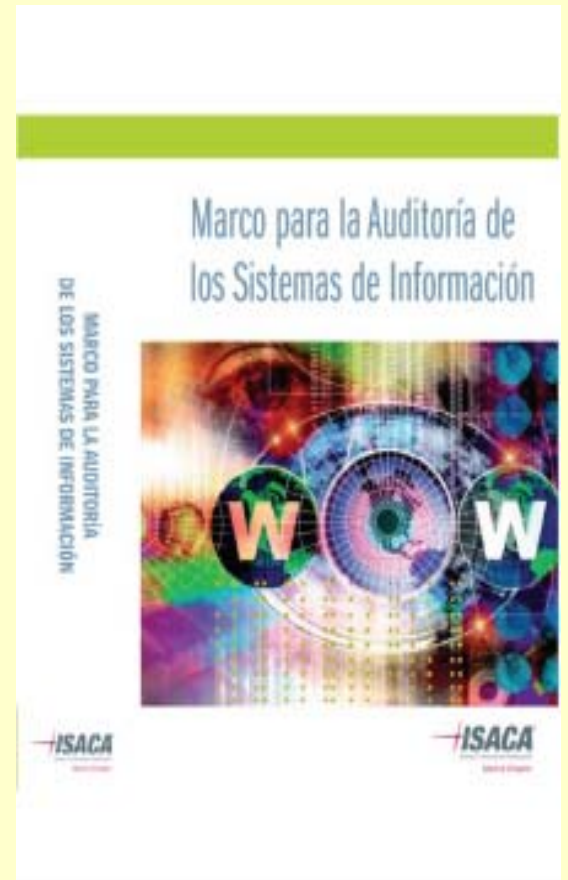
Noticias de la Asociación

El pasado día 30 de septiembre tuvimos la ocasión de volver a reunirnos en el *Hotel Holliday In* de Madrid para celebrar la presentación de nuestro libro titulado **MARCO PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**

Este libro continua con la línea tradicional de publicar materiales que guiarán a los Auditores de Sistemas en la realización de sus trabajos de Auditoría. Así, comenzado por el propio Código de Ética Profesional (de obligado cumplimiento para todos los auditores certificados CISA ®), se ha desarrollado todo un cuerpo normativo que incluye Estándares, Guías y Herramientas y Técnicas. Estos más de cincuenta documentos, en su versión original proporcionan:

- **A los auditores**, los niveles mínimos de calidad que debe reunir su trabajo para cumplir con su responsabilidad profesional.
- **A la Dirección y terceros** de cualquier tipo interesados en la función de auditoría, bases para la generación de expectativas adecuadas.
- **A todos ellos**, información adicional sobre cómo cumplir y cómo interpretar las propias normas de aplicación.

En definitiva, un conjunto de materiales que merece la pena reunir en una obra de referencia que pueda ser utilizada como fuente de consulta para todos aquellos que tengan alguna relación con la auditoría de sistemas de información.

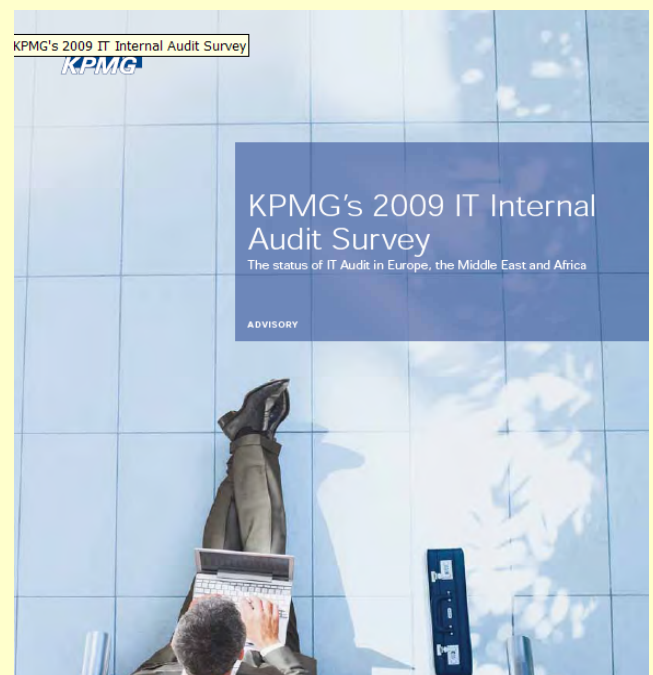


Presentación del IT Survey in Europe, ME and Africa

Durante el mes de Abril, **ISACA Madrid** participó de la presentación del Primer Estudio sobre la actividad de Auditoría en Tecnología de la Información en Europa, Oriente Medio y Africa.

Este Estudio fue desarrollado por la consultora **KPMG** y contó con la colaboración de nuestro capítulo y la del **Instituto de Auditores Internos de España**.

Entre otros aspectos el estudio muestra que la **Auditoría Interna de TI es un componente fundamental en la actividad moderna del Control Interno**. Asimismo, el informe pone de manifiesto, entre otros aspectos, que la actividad de auditoría en TI debe incrementarse en las organizaciones a fin de garantizar, desde un marco de independencia y transparencia, el control interno de las organizaciones.



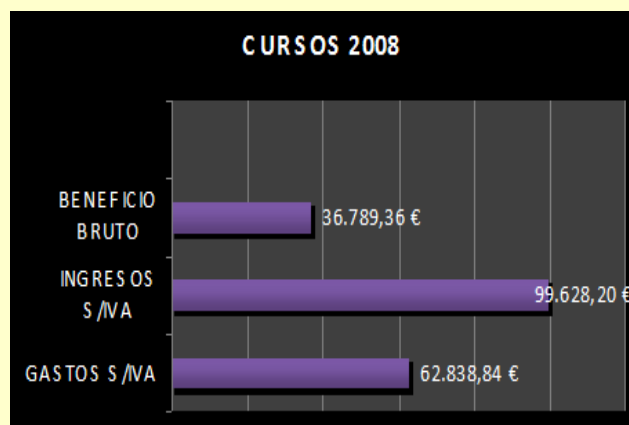
Formación ISACA Madrid

Elena Maestre – Vocal de Formación

En la Asociación de auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones, nos dedicamos a fomentar y promover la Auditoría, Gobierno Corporativo y Seguridad Informática en beneficio de nuestros miembros, de los responsables y usuarios de SI/TIC y de la sociedad en general.

A lo largo del próximo trimestre se celebraran los siguientes cursos:

- Auditando la firma digital, 8 de Octubre
- Auditoria del Outsourcing en los SI, 5 de Octubre
- Plan de Contuidad de Negocio, 26 y 27 de Octubre
- Estandares de Auditoria, Seguridad, Control y buen gobierno de las TI, 23 y 24 de Noviembre



Consulta la web para ver el contenido de los cursos

Amplio catalogo con cursos básicos y avanzados

“La formación es el valor fundamental en la ecuación de la seguridad”.



Cifras ISACA Madrid

Buenas noticias, ya **somos** mas de un **millar** de **asociados**, a Septiembre de 2009

ISACA, Capítulo de Madrid (183)
Pº Castellana, 91 - 3º Izda. 28046
Madrid

Teléfono
91.636.29.60

Fax
91.634.42.44

Correo electrónico
administracion@isacamadrid.es

Isaca Madrid, no comparte necesariamente las opiniones vertidas, siendo estas expresadas por los autores a titulo personal

Únete
al
líder