

Madrid News

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



Jornadas Técnicas 2010

Otro año más volvemos a la rutina y tomar el pulso al día a día tras nuestras vacaciones.

Me llena de satisfacción comunicaros que coincidiendo con la llegada del otoño, tendrán lugar las Jornadas Técnicas 2010 organizadas por ISACA Madrid (ASIA). Las hemos bautizado como **“Contribución y Riesgos de TI: equilibrio inteligente como estrategia para afrontar el futuro”**.

Las jornadas que tendrán lugar los próximos días 27 y 28 de Septiembre en el Hotel Husa Princesa, abordaran toda la temática que cubre la asociación internacional, focalizando en los temas más relevantes del momento actual, tales como el Cloud Computing, el co-sourcing de auditoría, la actuación de control relativa a las normativas de la CMNV, el Esquema Nacional de Seguridad, el Gobierno de IT, la certificación de calidad en el Software y las últimas tendencias de la auditoría en TI.

Creemos que es un foro excelente para que nuestros profesionales se formen y mantengan actualizados en este rol que nos toca jugar, nos brinda la posibilidad del acercamiento a los mejores profesionales del sector sumará valor y además permitirá que nos conozcamos más y que todos participemos más.

Contenido

Este número	1
Firma invitada	2
Noticias de la Asociación	6

Asimismo, durante este segundo semestre continuaremos ofreciendo nuestras charlas gratuitas a los asociados cumplimentando así las actividades de formación y actualización. Aprovecho también, para recordarles que tenemos habilitadas dos páginas (una en Facebook y otra en LinkedIn) para que canalicen por ahí, vuestras propuestas y compartan aspectos profesionales con el resto de la comunidad de ISACA Madrid.

Espero veros en las jornadas, un fuerte abrazo,

Alejandro Rembado Mendizábal
 Presidente

Firma Invitada

Miguel García Menéndez

Dos años de ISO 38500: ¿es éste el camino?

¡El tiempo vuela! Sin duda, una afirmación carente de toda originalidad; pero no por ello, menos cierta.

Así lo demuestran los acontecimientos. Hace poco se conmemoraba el primer aniversario de la constitución de la *Comisión para el estudio y el desarrollo del Buen Gobierno Corporativo de las TIC, dentro de las organizaciones*, del Capítulo de Madrid de ISACA. Ahora toca recordar la aparición de la norma *ISO/IEC 38500:2008, Corporate Governance of Information Technology*, de cuya publicación se han cumplido, este verano, dos años.

La aparición, en aquellos momentos, de una norma de alcance internacional, como la citada, constituyó, cuando menos, un hito “ilusionante”; y ello, por dos motivos:

- en primer lugar, el respaldo de ISO no debía, sino suponer la, ampliamente esperada, puesta de largo de una disciplina que había venido cocinándose, durante una década, en los fogones de otras reputadas y respetadas instituciones como el IT Governance Institute, de ISACA, o la Escuela de Dirección Sloan, del MIT; y,
- por otro lado, la norma, de manera relativamente escueta, pero clara, apuntaba hacia la esencia del concepto de ‘buen gobierno corporativo’, hundiendo su raíz en el “Informe Cadbury”; e identificando, con esa misma nitidez, a los individuos que deberían recoger el mensaje enviado,

a dúo, por ISO e IEC: los consejeros y miembros de la alta dirección de las organizaciones.

Lo que dice la norma

Por supuesto que dice, y mucho. Hay que saber leerla. No debe confundir el hecho de que lo diga en pocas páginas. Quienes realmente deberían leerla –no parece que lo estén haciendo– a buen seguro que sabrían interpretar con claridad lo que les dice y sacarle el debido partido. (Ello, básicamente, debido al carácter trivial y de sentido común de los mensajes que encierra).

La propia norma comienza avisando de su intencionalidad, que no es otra que la de “asesorar” a quienes tienen responsabilidades sobre el correcto funcionamiento de las organizaciones, en relación al papel que les toca jugar respecto de las TI –sustento, en gran medida de la actividad de aquellas–. Y finaliza definiendo y detallando media docena de principios generales para el Buen Gobierno Corporativo de las TIC: responsabilidad, estrategia, inversión, conformidad, rendimiento y comportamiento.

Si Ud. echa de menos un mayor nivel de detalle –procesos, procedimientos, instrucciones técnicas concretas,...– para poner esos seis principios en marcha, disculpe la franqueza, pero, claramente, no se encontrará Ud. entre los destinatarios naturales de la norma; o, lo que es, aún, peor, Ud. no se habrá enterado de nada.

Sobre la supuesta “implantación”

Al hilo del anterior comentario, y en el marco general de banalización de la norma, se oye hablar, no pocas veces, de “implantarla”; e, incluso –los más osados– de desplegar un sistema de gestión, en torno a ella, como si de una norma de calidad, al uso, se tratase.

Lo que debe hacer Ud. con la norma ISO 38500, o más concretamente, con sus seis principios generales, es adoptarlos; esto es, hacerlos suyos e incorporarlos a la cultura y al día a día de la organización. Como dicen los amigos y colegas Manolo Palao y Ricardo Bría (1), una norma como ésta ha de ser sometida a un proceso de *ad@ptación* (léase, “*adaptación*”), una combinación de *adopción* y *adaptación* a las particularidades micropolíticas de la organización.

Naturalmente, ya vendrá después la necesaria puesta en marcha de una serie de mecanismos [de Buen Gobierno] que faciliten tal “*adaptación*”.

Optar por un enfoque diferente, no supondrá, sino un alejamiento de la intencionalidad original de la norma y una delimitación del mensaje de Gobierno Corporativo de TI al perímetro del Departamento de Calidad, como se está observando en más de una organización.

Moraleja

Si Ud. quiere llevar el mensaje de Gobierno Corporativo de TI a sus verdaderos destinatarios, hableles de principios como los citados en este artículo (a lo mejor, tiene suerte y están dispuestos a adherirse a ellos). Si, por el contrario, se conforma con seguir discutiendo con sus iguales en los foros profesionales dispuestos a tal fin, siga ejercitando su memoria e incorporando como parte de su lenguaje la extensa codificación empleada por los cuerpos normativos del panorama internacional.

Los destinatarios

El análisis de la segunda expectativa creada hace dos años con la publicación de la norma ISO/IEC 38500:2008 obliga a reconocer, igualmente, que la comunidad que mejor acogida le ha dado es la conformada por los profesionales de los SSII y las TIC, a los que, como es evidente, no iba estrictamente dirigida.

El vals del Elefante

Fue precisamente ese hecho, esa realidad, la que empujó al australiano Mark Toomey –co-autor de las normas *AS 8015-2005*, *ISO/IEC 38500:2008* y, más recientemente, *AS/NZS 8016(Int):2010*- a escribir su libro *“Waltzing with the Elephant”* (2), un intento de transmitir el verdadero significado de la norma ISO 38500, a sus oportunos destinatarios.

La obra, de lectura absolutamente recomendable, nació –según ha declarado el propio Toomey– con el objetivo de poner las cosas en su sitio, de ejercer un cierto acto de rebeldía frente a una evidente y aplastante realidad: eran los profesionales informáticos los que, de forma mayoritaria, acudían a los foros de debate abiertos durante la elaboración de la norma (subcomités y grupos de trabajo de *Australian Standards*, de ISO,...).

Los foros de normalización

ISO ha sabido resolver el problema –sólo parcialmente– mediante la creación, a finales de 2008, de un grupo de trabajo específico (WG6), e independiente del resto de subcomités y grupos de trabajo sobre Tecnologías de la Información, que componen

el Comité Técnico Conjunto 1 (JTC1), paraguas de todos ellos. El WG6 está dedicado, en exclusiva, al estudio y desarrollo de normativa en torno a la disciplina del Gobierno Corporativo de TI. Ahora sólo falta que ISO sea capaz de atraer al mismo a otros profesionales, procedentes del ámbito de la dirección empresarial.

En España, AENOR, aún no ha dado ese paso. El desarrollo normativo del Buen Gobierno Corporativo en materia de TIC está todavía excesivamente ligado (cercano) al de otras disciplinas no menos importantes en materia de TI, como son las relativas a la Gestión de los Servicios Informáticos; pero cuya forzada “proximidad” no hace sino dificultar la correcta difusión del espíritu de la norma ISO/IEC 38500:2008.

Moraleja

Parafraseando a G. Vaughn Jhonson (3) –*“la Informática es demasiado importante como para dejarla en manos de los informáticos”*–, cabe sugerir que ISO, AENOR y los demás organismos normalizadores deberían echarnos –disculpen esta gotita de protagonismo– de estos grupos de trabajo, a todos los informáticos, procediendo a su refundación y habilitando la entrada en ellos, únicamente, a individuos procedentes de los órganos de gobierno de las corporaciones privadas y entidades de la Administración.

En suma, ¿cuál habrá de ser el camino?

Aún reconociendo la trascendencia de hitos como la publicación de la norma ISO 38500, tal vez, la manera más adecuada de llegar a los miembros de los Consejos de Administración y a los responsables de dirigir las organizaciones, no haya de venir por ahí, y sí por la vía de otros esfuerzos reguladores/normativos como podría ser una revisión y mayor desarrollo de los Códigos de Buen Gobierno Corporativo. El Código e Informe “King III”, en Sudáfrica, constituyen un claro ejemplo de ello.

En este mismo sentido, y dada la proximidad de los auditores a esos órganos de gobierno, por vía de los Comités de Auditoría, ¿no cabría pensar en la oportunidad que aquellos tienen en sus manos, para hacer llegar a los consejeros-administradores ese mismo mensaje de la necesidad de asumir las debidas responsabilidades sobre el gobierno de las TI?

Finalmente y de otro modo, habría que preguntarse, también, ¿qué le está faltando a la Gobernanza de TI para alcanzar los niveles de identificación y aceptación que, a nivel directivo, están teniendo otras disciplinas como la Sostenibilidad y la Responsabilidad Social Corporativa? (Por cierto, ámbitos para los que también existe, dentro del mundo ISO, un particular desarrollo normativo).

(1) Palao García-Suelto, Manolo y Bría Menéndez, Ricardo. *“Implantación de Buen Gobierno de los SI y las TIC adaptando COBIT, ITIL y Val IT: Una caricatura respetuosa”*. Novática, nº 191, págs. 39 y ss. Enero-febrero de 2008. URL:: <http://www.ati.es/novatica/2008/191/Nv191-Presentacion.pdf>.

(2) Toomey, Mark. *“Waltzing with the Elephant”*. Infonomics Pty. Ltd. August 2009. URL:: <http://www.infonomics.com.au>

(3) Vaughn Jhonson, G. *“Information Systems. A Strategic Approach”*. Mountain Top Publishing. Nebraska, 1990.

Miguel García Menéndez, CGEIT, CISM, CISA, desarrolla su actividad profesional en el área de *Gestión del Riesgo Corporativo de TI de Atos Consulting. Socio de ISACA y del Capítulo de Madrid de esta misma Asociación, desde su fundación en 2002; hoy es miembro de su Junta Directiva y coordinador de la Comisión para el estudio y el desarrollo del Buen Gobierno Corporativo de las TIC, dentro de las organizaciones. Está, igualmente, vinculado a otras asociaciones profesionales y foros del sector.*

Puede ser localizado en
miguel.gmenendez@atosorigin.com

ISACA® Publica en Español el Marco de Riesgos de TI para Ayudar a las Organizaciones a Obtener Beneficios y a Mitigar los Riesgos

Para dotar a las Organizaciones de todo el mundo de una visión de los riesgos asociados a las iniciativas de TI, ISACA ha desarrollado la edición en Español del Marco de Riesgos de TI: Partiendo como base del COBIT, ISACA reconocida mundialmente por su desarrollo del Marco de Buen Gobierno TI COBIT, proporciona el “eslabón perdido” entre la convencional gestión de riesgos empresariales y la gestión de riesgos de TI y el control.

“Las Organizaciones pueden lograr beneficios al aceptar sus riesgos, sin embargo cuando sus riesgos son mitigados son inducidas para lograr mayores beneficios de forma sostenible” dijo el Dr. Manuel Ballester, CISA, CISM, CGEIT, que dirigió el proyecto de traducción. “Disponible para Descargar Gratuitamente en www.isaca.org/riskit, el Marco de Riesgos TI está concebido para ayudar a las Organizaciones para obtener mayores beneficios de sus oportunidades, mediante la gestión eficaz de sus riesgos, en vez de eliminarlos completamente.”

Marco de Riesgos de TI reduce costes, esfuerzo y tiempo proporcionando una metodología clara enfocada en los riesgos de los negocios basada en TI como la finalización tardía de proyectos, cumplimiento normativo y legal, desalineamiento, arquitectura obsoleta de TI, problemas en la entrega de servicios,” dijo Urs Fischer, CISA, CPA (Suiza), CIA, uno de los desarrolladores del Marco de Riesgos TI. “Marco de Riesgos TI provee una guía para los ejecutivos y gestores a centrarse en las preguntas clave, tomar mejores decisiones ajustadas a sus riesgos y dirigir sus organizaciones a gestionar los riesgos de forma eficiente”

Marco de Riesgos de TI ofrece una visión única y completa de los riesgos de los negocios basada en TI, que pueden costar a las organizaciones millones al año por la pérdida de ingresos y oportunidades.

“Riesgo y Valor son dos caras de la misma moneda. El Riesgo es inherente a todas las Organizaciones, debemos lograr un equilibrio que evite la destrucción del valor y asegurarnos que las oportunidades de creación de valor no se pierdan,” dijo Brian Barnier, CGEIT, uno de los desarrolladores del Marco de Riesgos TI. “Marco de Riesgos TI ayuda a todos los niveles de la organización a gestionar los riesgos para obtener mayores beneficios y ayuda a detectar anticipadamente las señales de alerta.”

Marco de Riesgos TI complementa y extiende COBIT y Val IT, además siendo muy eficaz como marco independiente. Siendo un aspecto clave para todas las organizaciones que utilicen TI, desde empresas unipersonales hasta consorcios multinacionales, pueden obtener beneficios y ventajas de Marco de Riesgos TI. También puede ser adoptado por cualquier tipo de empresa en cualquier ubicación geográfica.



Secretaría Técnica
ISACA Madrid
Tel: 91 636 29 60
eventos@isacamadrid.es



JORNADAS TÉCNICAS 2010

CONTRIBUCIÓN Y RIESGOS DE TI

EQUILIBRIO INTELIGENTE COMO ESTRATEGIA
PARA AFRONTAR EL FUTURO

- Gestión Inteligente del riesgo de TI
- La auditoría de servicios del outsourcing
- Análisis de los nuevos riesgos de seguridad
- Aseguramiento de la calidad en la industria del desarrollo software

27 y 28
de Septiembre
Hotel Husa Princesa

www.isacamadrid.es

Únete al líder

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

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

*ISACA® Madrid, no
comparte necesariamente las
opiniones vertidas, siendo
estas expresadas por los
autores a título personal*

Consulta la web para ver el contenido de los cursos



Sistemas de información fiables y valiosos

Madrid Chapter