

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



CRISC® de ISACA®

Alejandro Rembado Mendizábal

Como seguramente todos ya sabréis, se ha anunciado recientemente una nueva certificación relativa al Control de los Riesgos en TI, denominada "Certificado en Riesgo y Control de los Sistemas de Información" (CRISC®, *Certified in Risk and Information Systems Control*).

Este nuevo certificado apunta a dar soporte a los profesionales de TI (auditoria, riesgos, cumplimiento, etc.) en la ardua tarea de identificar y gestionar los riesgos mediante la elaboración, puesta en marcha y mantenimiento de marcos de control sobre los Sistemas de Información.

Al igual que ocurre con los otros certificados de ISACA® (CISA, CISM, CGEIT) para obtener el CRISC® se requerirá una combinación de experiencia y conocimientos, principalmente vinculados a temas tales como: identificación de riesgos, diseño y aplicación de controles, y supervisión y mantenimiento de éstos, sobre TI. Los candidatos deberán aprobar un examen específico y comprometerse con un código de ética y un programa de formación continua.

Se ha habilitado un periodo de '*grandfathering*' (veteranía), en el que aquellos profesionales que acrediten una dilatada experiencia, podrán solicitar la certificación sin necesidad de realizar el examen correspondiente.

Contenido

Este número	1
Firma invitada	2
Noticias de la Asociación	4
Otras noticias del trimestre	5

En materia de formación y certificación, todo suma, nada resta; por lo cual, disponer de una certificación como ésta, supone un reforzado aval para el profesional que la ostenta.

Y por último, pero no menos importante, quiero reiterar el compromiso ofrecido en el primer número de Madrid News, invitándote a que nos envíes tu opinión, comentarios o, si lo deseas, artículos o temas que creas interesante publicar.

Un cordial Saludo.

Firma Invitada

Ana Belén Galán López

RiskIT® en la vida real

Actualmente, en la mayoría de las organizaciones es necesario contar con un marco de riesgos de TI que permita gestionar los riesgos más allá de un alcance puramente técnico y aislado, que utilice un lenguaje de alto nivel y que se englobe dentro del marco de riesgos global de la empresa.

Con este enfoque, la alta dirección puede entender mejor la importancia de los riesgos permitiéndoles tomar decisiones más eficaces sobre qué riesgos están dispuestos a aceptar y qué riesgos deben ser gestionados sin perder beneficios y valor para el negocio.

RiskIT® como marco para la gestión de riesgos, nos sirve de referencia para llevar a la práctica este modelo ya que a diferencia de otras metodologías de riesgos orientadas más a la seguridad TI como la ISO 27005 o enfocadas a entornos generales como la ISO 31000, nos permite estar más alineados con los objetivos de negocio. Con este modelo acercaremos los riesgos de TI al negocio y no tendremos una visión sesgada de los riesgos cubriendo el *gap* existente entre lo específico y lo general.

Dentro del universo de riesgos, un primer paso para construir el mapa de riesgos de TI es realizar una evaluación a alto nivel que nos permita tener una visión global de los riesgos TI a los que la organización se enfrenta y así poder definir el alcance de la gestión de riesgos, el apetito y la tolerancia.

Para hacer los riesgos TI más tangibles, podemos englobarlos en escenarios de riesgo y construir una relación entre estos escenarios y nuestros procesos de TI.

Los escenarios de riesgo relacionarán los eventos que pueden causar un impacto a nuestro negocio, su magnitud, su frecuencia, sus componentes y estarán conectados con nuestros activos, recursos y procesos.

Al ser una declaración de riesgos de alto nivel, estos escenarios los podremos relacionar con otras categorías de riesgo de negocio existentes en la organización y con sus impactos sobre el negocio (legal, económico, imagen, estrategia, ventaja competitiva, etc.)

Para cada escenario de riesgo, indicaremos:

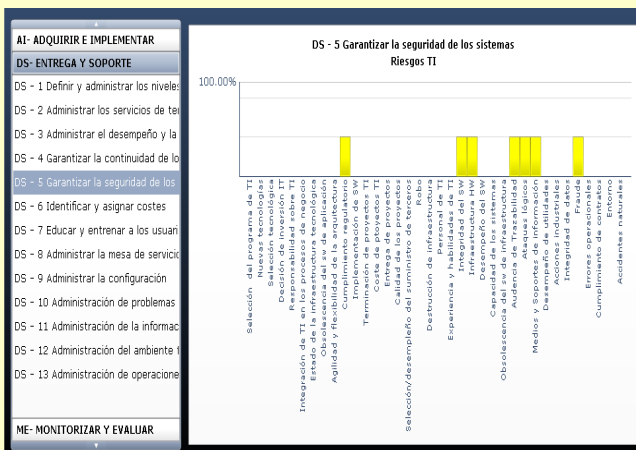
- Actores internos y externos que originen las amenazas: personal, proveedores, reguladores, etc.
- Tipos de Amenazas: intencionadas, accidentales, fallos, etc.
- Eventos: Divulgación de información sensible, interrupciones, diseño ineficaz, etc.
- Activos y Recursos de valor para el negocio que puedan ser afectados por los Eventos y causar un impacto al negocio: La información, la infraestructura de TI, la arquitectura del software, el proceso de gestión de cambios, etc.
- Factor tiempo: duración del evento, momento en el que puede ocurrir, tiempo que transcurre entre el evento y la consecuencia, etc.
- Impactos del evento que tengan repercusión sobre el negocio
- Frecuencia : Ocurrencia del evento en un periodo de tiempo determinado

RiskIT® proporciona además la correspondencia entre los escenarios de riesgo y los procesos de **CobiIT®** y **VallIT®** por lo que podremos determinar los controles que son de aplicación en nuestro entorno, sus características (automáticos, preventivos, trazables, etc.) y su estado actual, facilitándonos la evaluación de los riesgos y la construcción de un plan de acción como estrategia de respuesta.

Así, basaremos nuestras decisiones en factores como son el coste de la respuesta, su eficacia y su eficiencia.

La creación de medidas de resultados y desempeño nos facilitarán la confección de cuadros de mando sobre la gestión de los riesgos y el entorno de control.

Al desarrollar nuestro plan de acción, las actividades de control como son el establecimiento de políticas, procedimientos y buenas prácticas tendrán un efecto sobre la frecuencia y el impacto de los escenarios de riesgo, de tal forma que podemos mantener los riesgos dentro de unos niveles aceptables recogiendo las evidencias necesarias sobre las acciones realizadas para su posterior análisis.



Además de tener esta relación, será necesario contar con un marco de gobierno para responder a preguntas como ¿quién es el responsable del riesgo? ¿Quién debe rendir cuentas sobre el riesgo? ¿A quién debo informar?, etc. Con el mapa de riesgos creado y apoyándonos en RiskIT®, los flujos de comunicación y los roles sobre los riesgos estarán establecidos pudiendo identificar quién es responsable de asegurar que las actividades se realicen adecuadamente y quién, como propietario de los recursos, tiene la autoridad para la ejecución de las actividades y aceptar sus resultados.

Conclusión

El mapa de riesgos creado será flexible y adaptable a los factores particulares del entorno de nuestra organización y nos permitirá trabajar en común hablando de riesgos de TI en términos de negocio.

Una vez establecido este entorno de control y gestión de riesgos, el grado de cumplimiento de los controles y los modelos de madurez, nos guiarán tanto en la evaluación de nuestra situación actual y los riesgos que esta situación conlleva, como en la priorización y focalización de los esfuerzos en los procesos que necesitan más atención para mantener unos niveles tolerables de riesgo.

Ana Belén Galán López

Ingeniera Técnica en Informática por la Universidad Politécnica de Madrid, Ana Belén es, además, CISA y CISM, por ISACA, y Lead Auditor ISO 27001.

Actualmente trabaja en el Área de Riesgos Tecnológicos y Seguridad en una entidad financiera española, habiendo desplegado recientemente una implementación Risk IT.

Comenzó su trayectoria profesional en Red.es y trabajó como consultora de seguridad en Telefónica Soluciones y T-Systems, desarrollando e implantando Sistemas de Gestión de Seguridad de la Información, así como Planes de Continuidad de Negocio.

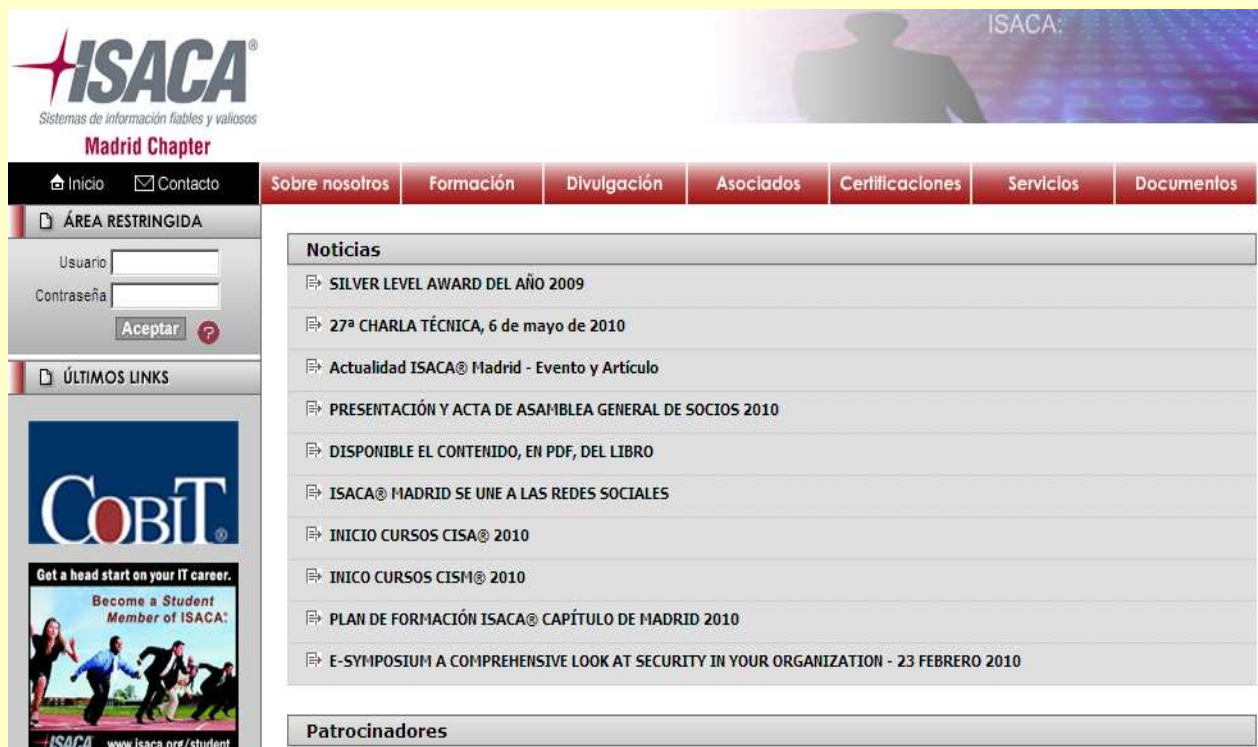
Puede ser localizada en anabgalan@gmail.com

Noticias de la Asociación

El 28 de abril de 2010, el Capítulo ISACA® Madrid (183) recibió de parte del Sr. Summer Cole, Coordinador de Servicios para Miembros de ISACA® Internacional, un comunicado en el que se informaban del reconocimiento al diseño, los contenidos y la administración de la sede web del Capítulo, lo que le ha valido para obtener el *Silver Level Award* del año 2009.

Era un objetivo estratégico marcado el pasado año y el esfuerzo ha dado sus frutos.

Este premio no viene sino a corroborar, el excelente trabajo realizado por todas aquellas personas de la Asociación que se ocupan de dar 'vida' a la web. Desde aquí les damos nuestras más sinceras gracias.



The screenshot shows the ISACA Madrid Chapter website. The header features the ISACA logo with the tagline 'Sistemas de Información fiables y valiosos' and 'Madrid Chapter'. A navigation menu includes links for Inicio, Contacto, Sobre nosotros, Formación, Divulgación, Asociados, Certificaciones, Servicios, and Documentos. On the left, there is a login section for 'ÁREA RESTRINGIDA' with fields for 'Usuario' and 'Contraseña', and an 'Aceptar' button. Below the login section is a 'ÚLTIMOS LINKS' section featuring a COBIT advertisement with the text 'Get a head start on your IT career. Become a Student Member of ISACA!' and the URL 'www.isaca.org/student'. The main content area is titled 'Noticias' and lists several news items:

- SILVER LEVEL AWARD DEL AÑO 2009
- 27ª CHARLA TÉCNICA, 6 de mayo de 2010
- Actualidad ISACA® Madrid - Evento y Artículo
- PRESENTACIÓN Y ACTA DE ASAMBLEA GENERAL DE SOCIOS 2010
- DISPONIBLE EL CONTENIDO, EN PDF, DEL LIBRO
- ISACA® MADRID SE UNE A LAS REDES SOCIALES
- INICIO CURSOS CISA® 2010
- INICIO CURSOS CISM® 2010
- PLAN DE FORMACIÓN ISACA® CAPÍTULO DE MADRID 2010
- E-SYMPOSIUM A COMPREHENSIVE LOOK AT SECURITY IN YOUR ORGANIZATION - 23 FEBRERO 2010

At the bottom of the news section is a 'Patrocinadores' section.

Otras noticias del trimestre

Desayuno–debate en torno a la Auditoría Interna de los SSII

El pasado 28 de enero de 2010, ISACA® Madrid fue invitada a participar como patrocinador en el Desayuno especial de Red Seguridad bajo el título “*El auge de la Auditoría Interna como potenciadora del negocio*”.



Acto organizado por la Editorial Borrmarkt, a través de sus publicaciones ‘Seguritecnia’ y ‘RedSeguridad’.

Los asociados de ISACA®, Capítulo de Madrid, estuvieron representados, por D. Alejandro Rembado Mendizábal, Presidente, y por D. Fernando Hervada, Vicepresidente, de ISACA® Madrid.

En el transcurso de la presentación se hizo un pequeño repaso de la historia de ISACA®.

Se destacaron, de manera particular, los esfuerzos realizados por la Asociación en materia de Seguridad de la Información, de los que ha sido testigo la presente década y, de forma muy relevante, el último año. Si una cuestión es cierta en Tecnologías de la Información es que el riesgo existe y su análisis y control es prioritario, sobre todo si hablamos de grandes organizaciones.

Al auditor compete supervisar que se toman las salvaguardas correctas, de acuerdo a las buenas prácticas y los estándares promovidos por asociaciones como ISACA®, que avalan la independencia de la profesión.

XXVII Charla Técnica

La tarde del 6 de mayo ISACA® Madrid convocaba a sus asociados a una nueva Charla Técnica.

El contenido de la misma giró en torno a la presentación del primer “Cuaderno de ISACA®Madrid”, una **guía de autoevaluación** del grado de adopción de los mecanismos de Gobierno Corporativo de TI.

La nueva *Guía* constituye el primero de los trabajos desarrollados en el seno de la **Comisión para el estudio y el desarrollo del Buen Gobierno Corporativo de las TIC, dentro de las organizaciones.**



ISACA® invitada en Red Seguridad

La revista Red Seguridad publicó en su pasado número de marzo un artículo de D. Miguel García Menéndez, Miembro de la Junta Directiva de ISACA®.

EL artículo titulado *De la auditoría como dimensión del Gobierno de TI a la "metáfora de la balanza"* realiza un breve repaso por las dimensiones del Gobierno Corporativo de TI e introduce el principio de "equilibrio del valor" como vía para dar respuesta a una serie de interrogantes surgidos en torno a la figura del auditor y la estrategia seguida por ISACA® en los últimos años.

Partiendo de las múltiples interpretaciones que se han dado, y aún se dan, de la disciplina del Gobierno Corporativo de TI, el autor revisa algunas de las principales fuentes de referencia en la materia –la norma *ISO/IEC 38500:2008, Corporate governance of Information Technology*, o el propio IT Governance Institute de ISACA, entre otras–, y, a partir de ellas, destaca sus no pocas similitudes, las cuales permiten comenzar a dibujar los dominios (dimensiones) por los que se extiende la Gobernanza de TI.

Una de tales dimensiones es aquella vinculada a las actividades de evaluación y medición del rendimiento de las propias TI, en la que la figura del **Auditor de Sistemas de Información** adopta un especial protagonismo.



Las jornadas técnicas de ASIA se celebrarán el 28 y 29 de Septiembre

Bajo el lema: *"Contribución y Riesgos de TI: equilibrio inteligente como estrategia para afrontar el futuro"* la asociación ASIA, ISACA® Capítulo de Madrid abordará sus segundas Jornadas Técnicas.

Si en 2008 el hilo conductor fueron las nuevas tendencias en auditoría y seguridad de los Sistemas de Información, en esta ocasión se pretende ofrecer a los asistentes una visión constructiva del valor que aporta al buen gobierno de las TI el uso apropiado de la seguridad, la gestión de riesgos y la auditoría.

Entre otros, se tratarán temas tan interesantes como la gestión inteligente del riesgo de TI, la auditoría de servicios de outsourcing, el análisis de los nuevos riesgos de seguridad y el Cloud Computing.

Las jornadas se llevarán a cabo los días 28 y 29 de septiembre y están orientadas tanto a Socios como al resto de profesionales.

Contarán con la participación de las firmas de consultoría Deloitte, KPMG, Ernst & Young, PricewaterhouseCoopers y BDO como patrocinadores.

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

