

Conferencia Latinoamericana de Seguridad de la Información y Administración del Riesgo

del 1º. al 2 de Marzo de 2010
Hotel Cosmos 100
Bogotá, Colombia



- Aprenda más sobre la gestión de la seguridad de información
- Comprenda más sobre los aspectos prácticos de la seguridad de información
- Obtenga hasta 21 horas de educación continua

www.isaca.org/isrm

Sí conocimiento es poder, que tan poderoso es usted?

ISACA® tiene el gusto de anunciar la cuarta conferencia anual Latinoamericana de Seguridad de Información, diseñada para satisfacer una variedad de sesiones que atañen a la comunidad responsable de seguridad de la tecnología de información. El evento presentará dos pistas simultáneas de temas relacionados con el aspecto gerencial y aspectos prácticos de la seguridad de información. Esta combinación de sesiones de alto nivel y de detalle en el material, permitirá a los asistentes asociar la experiencia de la conferencia a intereses específicos y a sus necesidades profesionales. Profesionales interesados en estos temas, así como quienes cuentan con la certificación Certified Information Security Manager® (CISM®), encontrarán valor en este evento.

La conferencia se enfocará en los elementos clave que abarcan las prácticas efectivas de la gestión de seguridad de información.

El participante aprenderá más sobre:
Nuevas tecnologías
Nuevos riesgos
Marcos legales y gubernamentales
Soluciones de seguridad
Seguridad Gestionada



Tendencias de Seguridad de la Información y su Impacto en los Esquemas de Gobierno, Riesgo y Control

Ramiro Merchán Patarroyo, CISA, GIAC-GSEC
Digiware
Bogotá, Colombia

El crecimiento del comercio electrónico transformó los conceptos de los límites físicos y lógicos de las organizaciones. La revolución del comercio electrónico ha impulsado dos (2) grandes cambios: Nuevas formas de integración electrónica con los socios de negocios, indistintamente del lugar geográfico donde ellos se localicen.

El incremento en el uso de redes públicas (internet)

De un lado, el uso de las tecnologías de redes para la integración de socios de negocios sin duda alguna brinda muchos beneficios: rápido acceso a la información, mejoramiento de las comunicaciones, reducción de costos, incremento de la colaboración, mejoramiento del servicio al cliente e impredecibles posibilidades de conducir el comercio electrónico; pero por otro lado, ha generado preocupación en las organizaciones la temática relacionada con la seguridad: Hackers, ingeniería social, empleados deshonestos, fallas de hardware y software, errores humanos, desastres naturales, etc.

En Latinoamérica se muestra una tendencia en la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como la protección de datos de clientes, lo cual denota que la función de seguridad de la información se concentra en los temas tecnológicos, sin embargo comienza a sentirse un marcado interés por el aseguramiento de los flujos de información en la organización, que nos dice que la administración de riesgos de tecnología comienza a enfocarse más hacia el negocio y sus impactos, aunque impulsado aún por el cumplimiento de regulaciones y normas internacionales.

Lo anterior genera un reto mayúsculo para las áreas de seguridad de la información en las organizaciones de hoy día pues su misión es la implementación y mantenimiento de programas estratégicos de seguridad que se integren con la estrategia del riesgo que consideran a toda la organización y, sobre todo al negocio.

El objetivo de esta sesión es presentar una panorámica general de las tendencias en seguridad de la información en los diferentes sectores económicos y cómo estos cambios impactan los procesos de gobierno, riesgos y control e inducir a las diferentes temáticas que se tratarán en el evento ISRM 2010.

Ramiro Merchán Patarroyo es ingeniero de Sistemas de la Universidad Distrital Francisco José de Caldas, especializado en Desarrollo de Software de Redes de la Universidad de los Andes. Ha obtenido las siguientes certificaciones profesionales: CISA de la ISACA; GIAC-GSEC del Sans Institute y CBCP del DRIL.

Cuenta con más de quince años (15) de experiencia profesional en las áreas de Seguridad y Auditoría Informática. Durante los últimos 5 años se ha desempeñado como consultor en proyectos de administración de riesgos, sistemas de gestión de seguridad de la información y planes de continuidad del negocio en importantes empresas del sector público y privado en diferentes países de la región.

Ha sido conferencista invitado en los eventos LATINCACS de San José (Costa Rica 2000), Acapulco (México 2001), CIASI – Madrid (España 2001), Sao Paulo (Brasil 2003), Bogotá (Colombia 2006) y San José (Costa Rica 2009).

En la actualidad se desempeña como Gerente de Servicios Profesionales de Digiware de Colombia S.A., empresa especializada en seguridad de la información.

Pista 1—Gestión de la Seguridad de la Información (Information Security Management)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
111	<p>Organizando el Departamento de Seguridad—Experiencias Prácticas</p> <p>I</p>	<p>Julio César Ardita, CISM <i>CYBSEC</i> Argentina</p>	<ul style="list-style-type: none"> • Experiencias concretas sobre la conformación del departamento de seguridad en diferentes organizaciones de distintos tamaños y áreas de negocio de América Latina, las problemáticas detectadas y las soluciones aplicadas para lograr una exitosa implementación del departamento. Se describirán cuales son las tendencias sobre la ubicación y conformación del departamento de seguridad • Los grados de madurez de las organizaciones y la adopción del departamento de seguridad • Modelos actuales y tendencias sobre el departamento de seguridad • Las tendencias sobre la ubicación y conformación del departamento de seguridad en los próximos años <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable
121	<p>La Norma ISO 20000 y su Relación con la ISO 27000</p> <p>I</p>	<p>Evelyn Antón, CISA, CISM, CGEIT <i>UTE (Usinas y Trasmisiones del Estado)</i> Uruguay</p>	<ul style="list-style-type: none"> • Cómo las normas ISO han irrumpido con fuerza en los entornos relacionados con los sistemas de información. • El estado actual de las ISO 20000, la ITIL cuyo objetivo es regular la prestación de servicios de TI y por otro la ISO 27001 junto con el resto de las normas de la familia 27000 tratan de optimizar la gestión de la seguridad de la información. • Cómo la adopción de ambas normas supone unos beneficios claros para cualquier organización, pero la adopción de estas metodologías supone cierta inversión y el éxito de su implantación, no tiene a priori resultados claros. Las dificultades que representa el implantar dos sistemas de gestión. • Las coincidencias, diferencias y cómo resulta la implantación conjunta de ambos estándares. • Procesos y Servicios de TI • Sistema de Gestión de Seguridad de Información (SGSI) • Sistema de Gestión de Tecnología de Información (SGTI) • Procesos de SI • Beneficios de usar las normas ISO <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente. • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • El participante deberá contar con experiencia o conocimientos sobre las normas ISO20000 and ISO27000.

Pista 1—Gestión de la Seguridad de la Información (Information Security Management) (continuación)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
131	<p>Políticas y Cumplimiento de la Seguridad de Información</p> <p>I</p>	<p>Areán Hernando Velasco Melo <i>Velasco, Calle & D'Alleman Abogados</i> Colombia</p>	<ul style="list-style-type: none"> • La importancia y efectos que tiene el cumplimiento de las normas jurídicas en la estructuración, formulación, gestión y aplicación de las Políticas de Seguridad de la Información en una organización, sea ésta, pública o privada. • Fundamentos en la experiencia adquirida como consultor en elaboración de políticas e instrumentos normativos, así como auditor en temas de cumplimiento vinculados a la seguridad de la información. • Cómo explicar y demostrar la íntima relación que existe entre el cumplimiento y las políticas de seguridad de la información de una organización; con base en ello, los riesgos a tener en cuenta al momento de elaborar, gestionar y aplicar las políticas de seguridad de la información a los destinatarios de las mismas, para efectos de que éstas adquieran eficacia. • Algunos hallazgos y riesgos en Políticas de Seguridad de la Información • Derecho, Ley y Políticas de Seguridad de la Información • El cumplimiento en las Políticas de Seguridad de la Información • Eficacia de las Políticas de Seguridad de la Información <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Los asistentes preferiblemente deberán tener responsabilidad respecto de los ciclos de vida PHVA (Planear, hacer, verificar, actuar), de las políticas de seguridad de la información, así como respecto de su aplicación y verificación de su eficacia jurídica.
211	<p>Herramientas de ISACA (ITGI) para Gestionar la Seguridad de la Información</p> <p>I</p>	<p>Carlos Villamizar, CISA, CGEIT <i>Digiware, S.A.</i> Colombia</p> <p>Fernando Ferrer Olivares, CISM <i>FERROL Internacional Group, Universidad Católica de Colombia, Banco de la República de Colombia</i> Colombia</p>	<ul style="list-style-type: none"> • Relevancia del Gobierno de Seguridad de la Información en las organizaciones. • Publicaciones de ISACA (ITGI) que contribuyen a gestionar la seguridad de la información en las organizaciones, resaltando sus principales características y alcance, y planteando a los participantes como se pueden integrar dentro del modelo de seguridad de la información en una empresa • <i>CobiT Security Baseline, 2nd Edition</i> • <i>Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1</i> • <i>Information Security Governance Guidance for Information Security Managers</i> • <i>ISACA® Model Curriculum for Information Security Management</i> • <i>Defining Information Security Management Position Requirements—Guidance for Executives and Managers</i> • <i>Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit</i> • <i>An Introduction to the Business Model for Information Security</i> • COBIT, VAL IT y RISK IT. • Integración de las publicaciones dentro del modelo de seguridad de la información. • La adopción de marcos o modelos, el cumplimiento de regulaciones y la implementación de controles que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información y cómo éstos se han convertido en un requerimiento de negocio fundamental. <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable

Pista 1—Gestión de la Seguridad de la Información (Information Security Management) (continuación)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
221	<p>Riesgos Asociados a las Comunicaciones Unificadas</p> <p>I</p>	<p>Aureo Monteiro Tavares da Silva, CISM, CGEIT Brasil</p>	<ul style="list-style-type: none"> Las tecnologías para comunicaciones unificadas, sus ventajas para los negocios y los riesgos de seguridad asociados. ¿Qué son las Comunicaciones Unificadas? Beneficios para las empresas Ejemplos de soluciones disponibles para la sobrecarga de llamados e informaciones Las mejoras en la eficacia y colaboración a través de una comunicación más inteligente, integrada y con mucho más funcionalidades que de las tecnologías separadas El cambio cultural Estrategias de implantación e integración Riesgos inherentes a las comunicaciones unificadas que implican cumplir con todos los requerimientos de gestión, seguridad y disponibilidad, para que la empresa obtenga todos los beneficios de la colaboración en tiempo real <p>Prerrequisitos:</p> <ul style="list-style-type: none"> El participante deberá contar con conocimientos básicos de las distintas tecnologías para comunicaciones en el ambiente de las empresas. Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI Experiencia gerencial sería deseable
231	<p>Caso Práctico de Análisis de Riesgos y su Integración con el Modelo de Gestión de Tecnología</p> <p>I</p>	<p>Efraín Baldenebro, CISA, CGEIT <i>Bolsa Mexicana de Valores S.A.B. de C.V.</i> México</p>	<ul style="list-style-type: none"> Establecimiento de un modelo de Gestión de Tecnología dentro de una empresa. Técnicas utilizadas para implementar, medir y mejorar un modelo de Gestión de Tecnología. Principios de la administración de riesgos. Como relacionar los resultados de un análisis de riesgos dentro de la implementación de un proceso de Gestión de Tecnología. La importancia de un equipo interdisciplinario. Los principios básicos a considerar para implementar un modelo de Gestión de Tecnología asociado a apoyar en la identificación y medición del Riesgo Operativo Tecnológico. <p>Prerrequisitos:</p> <ul style="list-style-type: none"> Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI Experiencia gerencial sería deseable
241	<p>Tercerización de la Seguridad desde la Perspectiva del Negocio (Mesa Redonda)</p> <p>I</p>	<p>Héctor R. Ortiz G. Banco de Occidente Honduras</p> <p>Carlos Mauricio Fiallos <i>Banco de Occidente</i> Honduras</p>	<ul style="list-style-type: none"> Determinar las necesidades reales de las empresas, respecto a la tercerización de seguridad Establecer puntos de control adicionales, para determinar si las tercerizaciones de seguridad son adecuadas para las Organizaciones Soporte legal de la región, para tercerizar Determinación de riesgos de la tercerización de la seguridad Experiencias de tercerización de seguridad <p>Prerrequisitos:</p> <ul style="list-style-type: none"> Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI Experiencia gerencial sería deseable

Pista 2—Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
112	Cumplimiento del Estándar PCI I	Héctor R. Ortiz G. <i>Banco de Occidente</i> Honduras	<ul style="list-style-type: none"> • Fraude de tarjetas de crédito • Ámbitos de aplicación del Estándar PCI • Contenido y aplicación de acuerdo a la función dentro del ciclo de las tarjetas de crédito • Fechas a considerar para el cumplimiento • AIS Program <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable
122	Técnicas para Explotar Vulnerabilidades del Lado del Cliente (Client Side Explotation) I	Ezequiel Sallis <i>Root-Secure</i> Argentina	<ul style="list-style-type: none"> • Las técnicas actuales que los atacantes emplean para ganar acceso a la red interna, explotando debilidades del lado del cliente. • Las técnicas de ofuscación de malware • Las técnicas de inyección de proceso en memoria • Algunas contramedidas disponibles para la correcta mitigación de riesgos • Una demostración práctica de la etapa de compromiso de un sistema actual desde el exterior al interior • Una demostración práctica de las técnicas de evasión actual de software anti-malware • Una demostración actual del impacto de las acciones de los usuarios desprevenidos • Evolución de una tendencia predecible • Ingeniería Social 2.0 + Client Side Exploit • Demostracion Client Side Exploit via MS Excel • Demostracion Client Side Exploit via PDF • Demostracion Client Side Exploit “The Phishing Way” <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Conocimietos de conceptos generales de seguridad de la información • Conocimietos generales de la Suite de Protocolos TCP/IP • Conocimientos generales respecto de Metodologías de Análisis de Seguridad • Conocimientos Generales sobre técnicas de explotación de vulnerabilidades. • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable

Pista 2—Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues) (continuación)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
132	<p>Ciberseguridad y Cibercrimen: Estado Actual y Tendencias</p> <p>I</p>	<p>Ulises Castillo Hernández, CISA, CISM <i>SCITUM</i> México</p>	<ul style="list-style-type: none"> • Las distintas formas de ciber-delitos. • La manera en que el crimen organizado, grupos terroristas y países hostiles están ejecutando ataques hoy en día. • Posibles escenarios de amenazas y ataques para un futuro cercano. • Los programas de ciber-seguridad que gobiernos y empresas están organizando. • Formas concretas de armar e implementar un programa de ciber-seguridad en su organización. • Ideas para apoyar estas iniciativas a nivel gubernamental. <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • El participante debe estar familiarizado con la terminología y problemática general de la seguridad informática.. • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable
212	<p>Armando un CSIRT Interno para Manejo de Incidentes de Seguridad</p> <p>I</p>	<p>Julio César Ardita, CISM <i>CYBSEC</i> Argentina</p>	<ul style="list-style-type: none"> • El proceso de manejo de incidentes de seguridad dentro de la Organización • La interacción con otras áreas y con el sector público y privado • El armado de un equipo de respuesta ante incidentes de seguridad dentro de la Organización • Se comentarán como es el proceso de manejo de incidentes de seguridad dentro de una Organización y cual es el grado de madurez de la Organización en la adopción de un CSIRT interno en base a experiencias concretas en empresas de America Latina • Se describirá como es el proceso para formar un CSIRT interno, cuales son las funciones reales que debe cumplir y cuales son los procedimientos estándares a nivel mundial a utilizar basados en el FIRST • Se expondrán los diferentes tipos de CSIRT que se pueden utilizar (públicos, privados, internos, etc.). • Se comentarán como es el proceso de manejo de incidentes de seguridad dentro de una Organización y cual es el grado de madurez de la Organización en la adopción de un CSIRT interno. • Se detallará el mapa de interacción con otras áreas de la propia organización y con el sector público y privado. • Se describirá como es el proceso para formar un CSIRT interno, cuales son las funciones que debe cumplir y cuales son los procedimientos estándares a nivel mundial a utilizar <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable

Pista 2—Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues) (continuación)

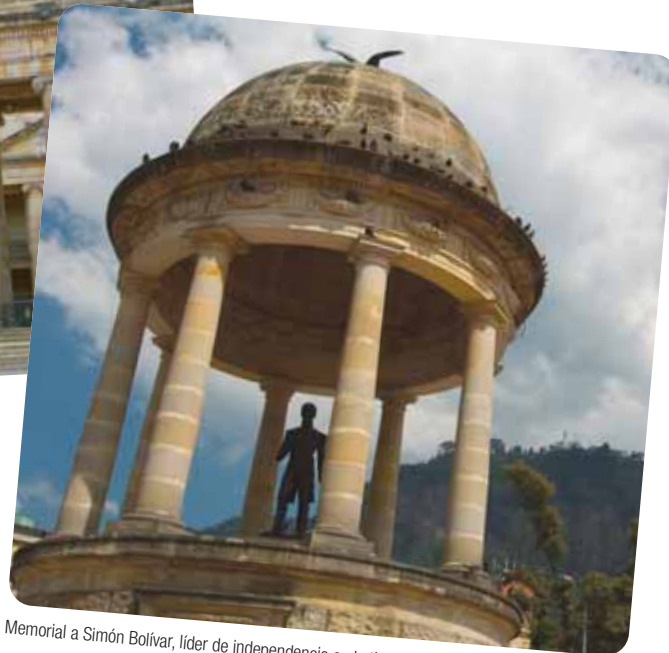
SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
222	<p>Implementación del Sistema de Gestión de Continuidad del Negocio Basado en BS25999</p> <p>I</p>	<p>Mario Ureña Cuate, CISA, CISM, CGEIT <i>Secure Information Technologies</i> México</p>	<ul style="list-style-type: none"> • Retos actuales de la Gestión de Continuidad del Negocio y como la implementación del Sistema de Gestión de Continuidad del Negocio (SGCN) ayuda a enfrentarlos. • Elementos que conforman el SGCN. • Dos elementos claves: Análisis de Riesgos y BIA. • Factores críticos de éxito para la implementación. • Diferencias e integración entre BS25999-1 y BS25999-2. • Integración del SGCN con otros Sistemas de Gestión. • Camino a la certificación. <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable
232	<p>Integración del Análisis Forense en la Respuesta a Incidentes</p> <p>I</p>	<p>Aureo Monteiro Tavares da Silva, CISM, CGEIT Brasil</p>	<ul style="list-style-type: none"> • Definición de incidentes • Amenazas a los sistemas informáticos y el número de delitos relacionados con los sistemas informáticos • Leyes y reglamentaciones • Políticas y procedimientos para la respuesta a incidentes de seguridad • Respuesta a incidentes • CIRT/CSIRT • Preparación y recolección de datos • Técnicas de análisis forense • Técnicas forenses para recolección, preservación y análisis de evidencias digitales en caso de sospecha de delitos informáticos. • Limitaciones en el ambiente de TI • Herramientas • Capacitación del Staff • Demostración práctica <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Conocimientos básicos de respuesta a incidentes, herramientas y procedimientos de análisis forense en sistemas operativos (Mac OS X, UNIX, Linux y Windows) • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable

Pista 2—Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues) (continuación)

SESIÓN #	TÍTULO DE LA SESIÓN	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
242	<p>Cómo Mejorar la Seguridad en su Empresa, Basado en CobiT</p> <p>I</p>	<p>Evelyn Antón, CISA, CISM, CGEIT <i>Usinas y Trasmisiones del Estado (UTE)</i> Uruguay</p> <p>Gerardo Alcarraz, CISA <i>Banco de la República Oriental del Uruguay</i> Uruguay</p>	<ul style="list-style-type: none"> • Cómo tener una visión de los riesgos basados en CobiT • Los Controles clave que provee <i>CobiT Security Baseline</i>, exploración y selección de los mismos. • La implementación de planes de acción. • La seguridad de la información como un aspecto clave en el Gobierno de las Tecnologías de la Información, siendo un tema de vital importancia que todos los usuarios finales, usuarios de mediana y pequeña empresa así como para los ejecutivos y la alta gerencia de las organizaciones deben conocer y comprender. • La guía o “kit” de seguridad llamado <i>CobiT Security Baseline</i>, desarrollada para proveer un conjunto de controles, sugerencias y herramientas prácticas para ayudar a proteger a los usuarios de computadores y a las empresas, de los múltiples riesgos que existen en la actualidad y tratar de lograr un correcto balance entre la gente los procesos y la tecnología. <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Al menos tres años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente • Familiaridad con la terminología, enfoques, metodologías y técnicas para evaluar y asegurar el ambiente de TI • Experiencia gerencial sería deseable



Congreso Nacional en Bogotá, Colombia.



Memorial a Simón Bolívar, líder de independencia en Latinoamérica.

Talleres

SESIÓN #	TÍTULO DEL TALLER	CONFERENCISTA	EL PARTICIPANTE APRENDERÁ MÁS SOBRE:
WS1	<p>Ejecución del Análisis y Evaluación de Riesgos</p> <p>I</p>	<p>Mario Ureña Cuate, CISA, CISM, CGEIT Secure Information Technologies México</p> <p>Carlos Villamizar, CISA, CGEIT Digiware Colombia</p>	<ul style="list-style-type: none"> • La implementación de una estrategia de seguridad de la información, sin importar el estándar, guía, práctica y/o norma que utilizemos como base, siempre requiere que en alguna de sus etapas más tempranas conozcamos cuáles son los riesgos a los que se encuentra expuesta la información de nuestra organización. Esta tarea se logra mediante la ejecución de un análisis de riesgos y amenazas y preferentemente mediante la implementación de procesos de administración/gestión de riesgos. • Por otra parte, para lograr la conformidad con el estándar ISO 27001 y sobre todo, para efectos de certificación, se requiere ejecutar el análisis de riesgos y amenazas utilizando guías como el BS7799-3, ISO27005 y el recién publicado BS31100. • En este taller presentaremos los principios de la administración de riesgos y conoceremos las etapas que comprende la ejecución del análisis de riesgos y amenazas, apoyándonos de ejemplos prácticos y guías para su ejecución • Metodologías y mejores prácticas: ISO 27005; ISO 2700; ISO 31000; BS31100; COBIT; BSI Guide To BS7799 Risk Assessment; ISACA Risk IT; <i>CobIT Security Baseline</i>; MAGERIT; CRAMM; OCTAVE. • Estrategias de acción: Presentación de conceptos relacionados con la administración de riesgos y ejecución de casos prácticos. <p>El participante aprenderá más sobre:</p> <ul style="list-style-type: none"> • Principios de la administración de riesgos. • Etapas que conforman un análisis de riesgos y amenazas. • Técnicas utilizadas y resultados esperados de la ejecución del Análisis de Riesgos y Amenazas. • Estándares y mejores prácticas relacionados con la administración de riesgos de TI. • Como ejecutar en la práctica un análisis de riesgos y amenazas de TI. . <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • El participante debe contar con al menos 3 años de experiencia en seguridad de TI y/o experiencia de gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para asegurar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.
WS2	<p>Cómputo Forense: La Reacción</p> <p>I</p>	<p>Andrés Velázquez México</p>	<p>El taller estará enfocado en cuáles son las mejores prácticas para que los asistentes puedan realizar una contención del incidente o el inicio de una investigación, manteniendo cadena de custodia y realizando una imagen forense del medio con herramientas gratuitas. Este taller será práctico, con equipo de cómputo instalado en la sala del evento.</p> <p>El participante aprenderá más sobre:</p> <ul style="list-style-type: none"> • Qué es el cómputo forense • Los pasos del cómputo forense • Qué es una cadena de custodia • Qué es una imagen forense • Generación de imágenes forenses • Uso de Protectores contra escritura (Hardware y Software) . <p>Prerrequisitos:</p> <ul style="list-style-type: none"> • Conocimientos básicos de Sistemas de Archivos y Redes • Conocimientos básicos de MS-DOS • Asistir con una Memoria de USB que hayan estado usando anteriormente de no más de 2 GB

PISTAS DE LA CONFERENCIA	Lunes 1º de Marzo, 2010				Martes 2 de Marzo, 2010				Talleres después de la conferencia
	8.30 – 10.00	10.30 – 12.00	13.30 – 15.00	15.30 – 17.00	8.30 – 10.00	10.30 – 12.00	13.30 – 15.00	15.30 – 17.00	Miércoles 3 de Marzo, 2010
Pista # 1 Gestión de la Seguridad de la Información (Information Security Management)	<i>Sesión Inaugural—Presentación Inaugural—Tendencias de Seguridad de la Información y su Impacto en los Esquemas de Gobierno, Riesgo y Control—Ramiro Merchán Patarroyo, CISA</i>								
	111 Organizando el Departamento de Seguridad—Experiencias Prácticas I <i>Julio César Ardita, CISM (Argentina)</i>	121 La Norma ISO 20000 y su Relación con la ISO 27000 I <i>Evelyn Antón, CISA, CISM, CGEIT (Uruguay)</i>	131 Políticas y Cumplimiento de la Seguridad de Información I <i>Areán Hernando Velasco Melo (Colombia)</i>	211 Herramientas de ISACA (ITGI) para Gestionar la Seguridad de la Información I <i>Carlos Villamizar, CISA, CGEIT y Fernando Ferrer Olivares, CISM (Colombia)</i>	221 Riesgos Asociados a las Comunicaciones Unificadas I <i>Aureo Monteiro Tavares da Silva, CISM, CGEIT (Brasil)</i>	231 Caso Práctico de Análisis de Riesgos y su Integración con el Modelo de Gestión de Tecnología I <i>Efraín Baldenebro, CGEIT, CISA (México)</i>	241 Tercerización de la Seguridad desde la Perspectiva del Negocio (Mesa Redonda) I <i>Héctor R. Ortiz G. y Carlos Mauricio Fiallos (Honduras),</i>	WS1 Ejecución del Análisis y Evaluación de Riesgos <i>Mario Ureña Cuate, CISA, CISM, CGEIT (México) y Carlos Villamizar, CISA, CGEIT (Colombia)</i>	
Pista # 2 Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues)	112 Cumplimiento del Estándar PCI I <i>Héctor R. Ortiz G. (Honduras)</i>	122 Técnicas para Explotar Vulnerabilidades del Lado del Cliente (Client Side Explotation) I <i>Ezequiel Sallis (Argentina)</i>	132 Ciberseguridad y Cibercrimen: Estado Actual y Tendencias I <i>Ulises Castillo Hernández, CISA, CISM (México)</i>	212 Armando un CSIRT Interno para Manejo de Incidentes de Seguridad I <i>Julio César Ardita, CISM (Argentina)</i>	222 Implementación del Sistema de Gestión de Continuidad del Negocio Basado en BS25999 I <i>Mario Ureña Cuate, CISA, CISM, CGEIT (México)</i>	232 Integración del Análisis Forense en la Respuesta a Incidentes I <i>Aureo Monteiro Tavares da Silva, CISM, CGEIT (Brasil)</i>	242 Cómo Mejorar la Seguridad en su Empresa, Basado en COBIT I <i>Evelyn Antón, CISA, CISM, CGEIT y Gerardo Alcarraz, CISA (Uruguay)</i>		

Enfoque Educativo: **B** Básico **I** Intermedio **A** Avanzado

Inscríbese en línea ahora! www.isaca.org/isrm

Información General

Beneficios del Programa

La cuota de registro para la Conferencia de Seguridad de la Información y Administración de Riesgo incluye:

- Asistencia a las conferencias de su elección
- Un juego completo en formato electrónico que incluye todas las conferencias que hayan sido recibidas hasta la fecha de producción
- La oportunidad de obtener hasta 21 horas de educación profesional continua (CPEs)

Lugar y Alojamiento

Hotel Cosmos 100

Calle 100 No. 21A-41

Bogotá, Colombia

Tel: +57.1.621.7771

Fax: +57.1.257.1035

Web: www.cosmos100.com

Precio de habitación: US \$180 Sencilla/Doble

Fecha límite para las reservaciones de hotel:

9 de febrero de 2010

Precios (en dólares americanos)

La Conferencia

Inscríbese hasta el 13 de enero de 2010 y reciba la tarifa de descuento por inscripción temprana!

Asociado de ISACA hasta el 13 de enero	\$650
Asociado de ISACA	\$700
No Asociado de ISACA hasta el 13 de enero	\$850
No Asociado de ISACA	\$900

Talleres

Asociado de ISACA	\$400
No asociado	\$500

Impuesto sobre el ingreso/Impuesto sobre el valor agregado

(VAT)/Impuesto Municipal de Industria y Comercio: Las cuotas de inscripción indicadas arriba, no incluyen los impuestos que aplican. La cuota completa de inscripción deberá ser recibida por ISACA para considerar el pago completo de la inscripción del participante. Los impuestos asociados con su inscripción son la responsabilidad de quien realice el pago y deberán ser remitidos a las autoridades de impuestos correspondientes en Colombia.

Nota: ISACA es una Asociación sin ánimo de lucro.

Recepción

Lunes, 1º de Marzo 2010 17.00-19.00

Política de Cancelación

Todas las cancelaciones deben ser recibidas antes y hasta el de **3 de febrero 2010** ya sea vía telefónica, fax o por correo electrónico, para recibir un reembolso de las cuotas de registro de la conferencia menos un cargo por cancelación de \$100 USD y de las cuotas de registro a los talleres menos un cargo de cancelación de \$50 USD y, si es aplicable, menos la cantidad aplicada a la cuota de la membresía como resultado de haber seleccionado la opción señalada como: "Deseo aplicar la diferencia entre las cuotas de miembro y no miembro para una membresía en ISACA".

No se podrán reembolsar las cuotas pagadas después del **3 de febrero 2010**.

La sustitución de un asistente registrado se puede dar en cualquier momento incluso hasta el momento de la conferencia misma. La sustitución de un no miembro de ISACA por un miembro resultará en una cuota adicional por ser no miembro.

Nota: La inscripción no será válida hasta que se reciba el pago completo de la cuota de la inscripción. Para garantizar la inscripción, las cuotas de la conferencia o de los talleres deben ser recibidas en las fechas límites publicadas. Una transferencia electrónica de pago o un cheque enviado por correo a ISACA, puede tomar 10 o más días hábiles en ser recibida, por lo anterior, por favor considere estos tiempos respecto a las fechas límite. Si por cualquier razón, ISACA debe cancelar un curso o el evento, su responsabilidad está limitada solamente al monto de las cuotas de inscripción pagadas. ISACA no es responsable por otros gastos incurridos, incluyendo gastos de viaje y hospedaje. Los materiales de la conferencia no se garantizan a aquellos participantes que se inscriban en el mismo evento o que no hayan enviado su pago con anticipación del inicio del evento.

Para más información acerca de nuestras políticas administrativas, tales como quejas y/o reembolsos, favor de contactar al departamento de conferencias de ISACA.

Teléfono: +1.847.660.5585

Fax: +1.847.253.1443

Correo electrónico: conference@isaca.org

Créditos Para Educación Profesional Continua (Cpe)

Para mantener las certificaciones Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) y Certified in the Governance of Enterprise IT® (CGEIT®), los profesionales certificados requieren obtener 120 horas de créditos de CPE en un período de 3 años de acuerdo con la política de educación profesional continua de ISACA. Los participantes podrán obtener hasta 21 créditos CPE; 14 por asistir a la conferencia y 7 adicionales por asistir a uno de los talleres opcionales o posteriores a la conferencia.

Vestimenta

Vestimenta casual de negocios es apropiada para la conferencia.

Requerimientos Especiales

Si usted tiene requerimientos de dieta especiales o requerirá asistencia durante el evento, por favor notifique al departamento de conferencias y complete la sección relacionada a esto en el formulario de inscripción. De esta manera ISACA le servirá de la mejor forma posible.

Para preguntas acerca de este proceso, contacte el departamento de conferencias por correo electrónico conference@isaca.org o por teléfono al +1.847.660.5585.

El proceso de obtención de Visa es responsabilidad total del participante. Por favor contacte a las oficinas de gobierno del país sede para mayor detalle. Una vez que se ha recibido el pago de inscripción, una carta de invitación podrá ser emitida por ISACA de acuerdo con su solicitud.

Información General

Política Verde De Isaca

En un esfuerzo por la conservación del papel, las conferencias de ISACA ahora son verdes. Una vez que se procese el registro, los participantes a la conferencia de ISACA recibirán un CD conteniendo el material más actualizado de las presentaciones de la conferencia. Esto les permitirá a los participantes ver las presentaciones en sus laptops y hacer notas durante la conferencia. Los participantes recibirán acceso en línea a todas las presentaciones de la conferencia disponibles, dos semanas antes de la conferencia, permitiéndoles ver las sesiones en las que están interesados o imprimirlas para traerlas a la conferencia. Por favor considere que: no habrá facilidades de impresión en el sitio de la conferencia. Si tiene cualquier pregunta, por favor contacte al departamento de conferencias por correo electrónico conference@isaca.org o por teléfono al +1.847.660.5585.

Límite De Responsabilidad

La información en este folleto está correcta en el momento que ha sido impreso. ISACA se reserva el derecho de alterar o eliminar algunos aspectos del programa en el caso de circunstancias no previstas. El material ha sido preparado para el desarrollo profesional de los miembros de ISACA y otros profesionales en la comunidad de seguridad y gestión de la seguridad de los sistemas de información. Tanto los expositores como ISACA no pueden garantizar que el uso del material presentado será adecuado para liberar de responsabilidades legales o profesionales de los miembros en la conducción de sus prácticas profesionales. Todos los materiales utilizados en la preparación y entrega de las presentaciones a nombre de ISACA son materiales originales creados por los expositores, o son materiales sobre los cuales los expositores tienen todos los derechos y la autoridad para usarlos y/o reproducirlos en conexión con su presentación y otorgan los derechos a ISACA como se especifica en el acuerdo establecido con los expositores. Sujeto a los derechos otorgados en el acuerdo establecido con los expositores, todos los derechos de autor aplicables, secretos industriales y otros derechos de propiedad intelectual en los materiales son y permanecen en el lado de los expositores.

Por favor tome en consideración: Queda prohibido grabar de manera no autorizada las presentaciones y/o los talleres en cualquier formato.

Aerolínea

Avianca Airlines ha sido designada como la aerolínea oficial para la Conferencia de Seguridad de la Información y Administración del Riesgo 2010. Se ha acordado con Avianca un descuento en el precio del boleto de todos los asistentes a la conferencia.

Contacte con su oficina de reservas de Avianca local y haga referencia de ISACA y el código: GN087.

Permiso para ser Fotografiado

Al asistir a este evento, el participante otorga permiso para ser fotografiado durante el evento. Las fotografías resultantes podrían ser utilizadas por ISACA para promociones futuras de eventos educacionales en el web site de ISACA y/o en materiales promocionales impresos, y al asistir a este evento, el participante consiente en cualquiera de estos usos. El participante comprende que cualquier uso de estas fotografías no implica remuneración alguna. El participante sede el derecho a inspeccionar o aprobar el uso antes mencionado de las fotografías en este momento o en el futuro.

Sea Miembro De Isaca

Los no miembros de ISACA pueden empezar a aprovechar los beneficios de la membresía de ISACA desde hoy mismo. La diferencia entre las cuotas de la conferencia para miembros y no miembros ISACA pueden ser aplicadas a la membresía de ISACA permitiéndole ser un miembro a nivel internacional y a nivel de capítulo sin costo adicional. Si usted desea aprovechar esta oportunidad, seleccione esta opción en la forma de registro.

Para más información acerca de la membresía de ISACA, visite el sitio www.isaca.org/membership o contacte al departamento de membresías en membership@isaca.org

Nota: Esta oferta expira 30 días después de terminado el evento. Los no miembros de ISACA pagan la cuota de la conferencia de no miembros al momento de registro.



Vista del centro de Bogotá, Santuario de Nuestra Señora del Carmen.



Plaza de toros en Bogotá.

Formulario de Inscripción a la Conferencia y al Taller

del 1º. al 2 de Marzo de 2010 • Bogotá, Colombia

Inscríbese en línea! www.isaca.org/isrm

1. Complete la siguiente información con letra mayúscula. (Por favor utilice máquina de escribir o letra de molde)

Nombre (Sr., Sra., Srita.)

(Nombre) _____ (Segundo nombre) _____ (Apellidos) _____

Título/Cargo _____ Teléfono de la empresa _____

Empresa _____ Fax de la empresa _____

Nombre de identificación (nombre en el gafete/escarapela) _____ Dirección de e-mail _____

(Indique si es:) Domicilio empresarial ó Domicilio residencial Cambio de domicilio.

Dirección (Calle o avenida y número) _____

Ciudad _____

Estado/Provincia _____ Código postal _____ País _____

NO incluir mi dirección completa en la lista facilitada a delegados, ponentes y expositores.

¿Miembro de ISACA? Sí Número de miembro _____ No

SEA MIEMBRO DE ISACA

¿Aún no es socio? Si se asocia a ISACA, podrá solicitar el descuento de la cuota. Esto podría permitirle que se convierta potencialmente en un asociado tanto a nivel internacional como de un capítulo local sin ningún cargo adicional y disfrutando de todos los beneficios de la membresía. Sólo tiene que marcar el cuadro del formulario de inscripción para aceptar nuestra oferta.

Deseo aplicar la diferencia de la cuota de la conferencia entre el costo de asociado y el de no asociado hacia la membresía de ISACA. Estoy de acuerdo con el descargo de responsabilidad de membresía señalada en este folleto.

2. Marque con un círculo las sesiones a las que desee asistir (No más de una sesión por período de tiempo).

Pista	TALLERES							
	Lunes 1º de Marzo, 2010			Martes 2 de Marzo, 2010				Miércoles 3 de Marzo, 2010
	10.30-12.00	13.30-15.00	15.30-17.00	8.30-10.00	10.30-12.00	13.30-15.00	15.30-17.00	9.00-17.00
Gestión de la Seguridad de la Información (Information Security Management)	111	121	131	211	221	231	241	WS1
Aspectos Prácticos de la Seguridad de la Información (Information Security Practical Issues)	112	122	132	212	222	232	242	WS2

Formulario de Inscripción a la Conferencia y al Taller

del 1º. al 2 de Marzo de 2010 • Bogotá, Colombia

Inscríbese en línea! www.isaca.org/isrm

Nombre _____

3. Cuotas de inscripción (Marque con un círculo sus elecciones)

(todas las cuotas están indicadas en dólares americanos)

Inscríbese hasta el 13 de enero de 2010 y reciba la tarifa de descuento por inscripción temprana!

Inscripción a la conferencia

Asociado de ISACA hasta el 13 de enero	US \$650
Asociado de ISACA	US \$700
No Asociado hasta el 13 de enero	US \$850
No asociado	US \$900

Inscripción a talleres (dólares americanos)

	Asociado	No-Asociado
WS1 Ejecución del Análisis y Evaluación de Riesgos	US \$400	US \$500
WS2 Cómputo Forense: La Reacción	US \$400	US \$500
TOTAL (Sume todos los importes que apliquen.)	US \$ _____	

Impuesto sobre el ingreso/Impuesto sobre el valor agregado (VAT)/Impuesto Municipal de Industria y Comercio: Las cuotas de inscripción indicadas arriba, no incluyen los impuestos que aplican. La cuota completa de inscripción deberá ser recibida por ISACA para considerar el pago completo de la inscripción del participante. Los impuestos asociados con su inscripción son la responsabilidad de quien realice el pago y deberán ser remitidos a las autoridades de impuestos correspondientes en Colombia.

IMPUESTOS: Las cuotas de inscripción que aquí se indican no incluyen impuestos. Si se han de deducir impuestos, habrá un incremento en la tarifa, equivalente al porcentaje del impuesto retenido. ISACA debe recibir la cantidad total de cuotas de inscripción indicada, antes de considerar que su inscripción ha sido pagada por completo.

Nota: ISACA es una Asociación sin ánimo de lucro.

Descuento de inscripción a la conferencia: Se aplicará un descuento de inscripción de US \$50 por persona cuando tres o más empleados de la misma organización se inscriban al mismo tiempo a la conferencia. Este descuento no es acumulable a otros descuentos de inscripción ofrecidos a miembros de ISACA.

4. Favor de indicar su forma de pago

Se adjunta cheque pagadero en dólares americanos, expedido en un banco americano y pagadero a: ISACA.

Transferencia Electrónica/Giro telegráfico

Fecha de transferencia de dólares americanos y número de referencia _____
(Favor de indicar en la descripción de la transferencia electrónica:
1. Nombre de quien asiste a la conferencia y 2. Concepto: Seguridad Conferencia)

Cargar a mi tarjeta Internacional:

Visa MasterCard American Express Diners Club
(AVISO: Todos los pagos con tarjeta de crédito se procesarán en dólares americanos.)

Número de la tarjeta: _____

Fecha de Vencimiento: _____

Nombre del titular de la tarjeta de crédito (tal como aparece en la tarjeta)

Firma del Titular de la tarjeta

Dirección completa para elaborar factura (si difiere de la página anterior)

5. Métodos de inscripción

A.  **INSCRIPCIÓN ELECTRÓNICA** en el web site de ISACA:
www.isaca.org/isrm.

B.  Enviar por **FAX** el formulario de inscripción completo a +1.847.253.1443.

C.  **ENVIAR POR CORREO EL FORMULARIO DE INSCRIPCIÓN COMPLETO**
A: ISACA, 1055 Paysphere Circle, Chicago, Illinois 60674 USA.

D.  **TRANSFERENCIAS ELECTRÓNICAS/GIROS BANCARIOS:**
Enviar pagos electrónicos en dólares americanos a:
Bank of America, 135 S. LaSalle St., Chicago, Illinois 60603
ABA nº 0260-0959-3, cuenta de ISACA nº 22-7157-8, código SWIFT BOFAUS3N
Número de identificación tributaria de ISACA (Tax ID Number): 23-7067291
[Incluir el nombre del asistente y Seguridad Conferencia en la descripción o notificación de la transferencia.]

Aviso: Todo aquel que se inscriba en forma electrónica y cuya inscripción no quede pagada antes del comienzo del evento no se le garantizará la entrega de los materiales de la conferencia.

6. Política de cancelación

Todas las cancelaciones deben ser recibidas antes ó hasta en **3 de febrero 2010** ya sea vía telefónica, fax o por correo electrónico, para recibir un reembolso de las cuotas de registro de la conferencia menos un cargo por cancelación de \$100 USD, y de las cuotas de registro a los talleres menos un cargo de cancelación de \$50 USD y, si es aplicable, menos la cantidad aplicada a la cuota de la membresía como resultado de haber seleccionado la opción señalada como: "Deseo aplicar la diferencia entre las cuotas de miembro y no miembro para una membresía en ISACA".

No se podrán reembolsar las cuotas pagadas después del **3 de febrero 2010**.

La sustitución de un asistente registrado se puede dar en cualquier momento incluso hasta el momento de la conferencia misma. La sustitución de un no miembro de ISACA por un miembro resultará en una cuota adicional por ser no miembro.

Nota: La inscripción no será válida hasta que se reciba el pago completo de la cuota de la inscripción. Para garantizar la inscripción, las cuotas de la conferencia o de los talleres deben ser recibidas en las fechas límites publicadas. Una transferencia electrónica de pago o un cheque enviado por correo a ISACA, puede tomar 10 o más días hábiles en ser recibida, por lo anterior, por favor considere estos tiempos respecto a las fechas límite. Si por cualquier razón, ISACA debe cancelar un curso o el evento, su responsabilidad está limitada solamente al monto de las cuotas de inscripción pagadas. ISACA no es responsable por otros gastos incurridos, incluyendo gastos de viaje y hospedaje. Los materiales de la conferencia no se garantizan a aquellos participantes que se inscriban en el mismo evento o que no hayan enviado su pago con anticipación del inicio del evento.

Para más información acerca de nuestras políticas administrativas, tales como quejas y/o reembolsos, favor de contactar al departamento de conferencias de ISACA.

Teléfono: +1.847.660.5585

Fax: +1.847.253.1443

Correo electrónico: conference@isaca.org

7. Arreglos Especiales

Requisitos de dieta especiales _____

Solicitaré asistencia. Favor de contactarme para gestionar los arreglos pertinentes.

¿Tiene alguna pregunta?

Póngase en contacto con el departamento de conferencias de ISACA en la oficina internacional en Rolling Meadows:

Teléfono: +1.847.660.5585

Fax: +1.847.253.1443

Correo electrónico: conference@isaca.org

Por favor comparte este brochure con

- ___ Director/gerente de Auditoría
- ___ Auditor de Sistemas de Información
- ___ Director/gerente de Seguridad de Sistemas de Información
- ___ Auditor/Contador Externo
- ___ Director General de Auditoría
- ___ Director de Complimiento



**Conferencia Latinoamericana de
Seguridad de la Información y
Administración del Riesgo**

del 1º. al 2 de Marzo de 2010
Hotel Cosmos 100
Bogotá, Colombia



Inscríbese en línea ahora!

www.isaca.org/isrm

**Miembros del Comité
de Trabajo para ISRM Bogotá**

Julio César Ardita, CISM
Presidente del Comité
CYBSEC
Argentina

Evelyn Susana Antón, CISA, CISM, CGEIT
UTE (Usinas y Transmisiones del Estado)
Uruguay

Carlos Villamizar, CISA, CGEIT
Digiware, S.A.
Colombia

Mario Ureña Cuate, CISA, CISM, CGEIT
Secure Information Technologies
México

Héctor R. Ortiz G.
Banco del Occidente
Honduras

Elia Fernández Torres, CISA,
ISACA
Estados Unidos