

Conferencia Latinoamericana de Auditoría, Control y Seguridad (Latin America CACSSM)

Del 17 al 20 de Agosto de 2008

Santiago Marriott Hotel

Santiago de Chile



**La conferencia de IT governance, control, seguridad y
aseguramiento en tecnología de información líder en el mundo**

Las pistas de la conferencia son:

- Gobierno y Control de TI (IT Governance and Control)
- Auditoría de Sistemas de Información (IT Assurance)
- Gestión de Seguridad de Sistemas de Información (IT Security Management)

Obtenga hasta **40** horas de
educación profesional continua (CPE)

www.isaca.org/latincacs

Haga planes en su agenda para asistir a la 13ª Conferencia Anual Latinoamericana de Auditoría, Control y Seguridad (Latin America CACSSM), que se celebrará en la ciudad de Santiago de Chile.

Latin America CACS goza de gran prestigio en toda Latinoamérica por proporcionar una cobertura detallada de los aspectos técnicos y administrativos actuales relacionados con gobierno, control, seguridad y aseguramiento de tecnología de la información.

Expertos en la industria y conferencistas de clase mundial reúnen gran experiencia y conocimiento en las mejores prácticas, seguridad de sistemas, procesos y herramientas de auditoría, así como en otros temas que afectan no sólo a los profesionales de un área geográfica determinada, sino a todos los profesionales de TI en todo el mundo. Ésta es una oportunidad extraordinaria para hacer contactos en el mundo de los negocios y descubrir las distintas formas de resolver problemas similares. Además, puede obtener hasta 40 horas de educación profesional continua (CPE).

PRESENTACIÓN INAUGURAL



Santiago Moral Rubio, CISA, CISM
Director de Seguridad Lógica
Grupo BBVA
España

El nuevo papel del CISO

La presentación describe los cambios existentes en la relación entre Seguridad de la Información y el Fraude Electrónico (o Delincuencia Tecnológica) y cómo estos cambios están afectando a la responsabilidad del CISO. Para ayudar a gestionar este proceso de transformación entre Seguridad y Fraude, se presenta una aproximación a un modelo de gestión de la Seguridad de la Información basado en la Teoría de Juegos.

Santiago Moral Rubio es Ingeniero Técnico en Informática por la Universidad Politécnica de Madrid. Cuenta con las certificaciones CISA y CISM de ISACA. Comenzó a mediados de los 80 a trabajar sobre entornos UNIX, Oracle e Informix fundando su propia compañía "Open Systems Administration Group". En 1996 pasó a trabajar en Atos Origin, donde desarrolló la Unidad de Negocio de Seguridad de la Información. En el año 2000 comenzó a trabajar en el banco Uno-e (del Grupo BBVA) como Director de Seguridad de la Información. En 2001 pasó al BBVA como responsable del departamento de Seguridad Lógica del que es su actual Director, con responsabilidad global dentro del Grupo BBVA.

BIENVENIDA

Bienvenida del Capítulo Santiago de Chile

La mesa directiva del Capítulo Santiago de Chile de ISACA y todos sus miembros que lo conforman nos enorgullecemos de extenderles nuestra más atenta invitación a la décimo tercera conferencia Latin America CACS 2008 que se llevará a cabo en la ciudad de Santiago de Chile en el mes de Agosto.

Cuenta nuestra leyenda que cuando Dios terminó de crear el mundo le sobraron desiertos, montañas, islas, lagos, etc., y estos los desparramó formando este largo país que es Chile, país de grandes contrastes, de desiertos y hielos, de cordillera y mar, un país pujante que quiere destacarse en el concierto latinoamericano y lo que es más importante, entregar el cariño de su gente y su hospitalidad, haciendo realidad lo que dice la canción "y veras como quieren en Chile al amigo cuando es extranjero".

Estamos seguros que disfrutarán de su estadía en nuestro país, especialmente en la ciudad de Santiago, que es una ciudad moderna y cosmopolita, llena de lugares interesantes e historia, gozarán de nuestros mostos y de nuestra nieve, admirarán nuestros paisajes, del extenso Pacífico y apreciarán qué tan fácil es estar en el mar como en la nieve.

Los invitamos a que desde ya reserven estas fechas para disfrutar de esta gran experiencia que conlleva el Latin America CACS 2008.

Alfonso Mateluna, CISA
Presidente
ISACA Santiago de Chile Chapter

Patrocinadores:

ISACA® quiere reconocer a los patrocinadores de la Conferencia Latin America CACS 2008 (vigentes a la fecha de impresión):

Patrocinadores de Oro

Deloitte.

KPMG

Patrocinadores de Bronce

ACL

CASEWARE
IDEA INC.

ERNST & YOUNG
Quality In Everything We Do

Pistas de la Conferencia

Pista 1—Gobierno y Control de TI (IT Governance and Control)

111

Caso práctico de implantación de Gobierno de TI en la banca ▲

Francisco Seixas Neto, CISA

CPMBraxis

Brasil

El participante aprenderá más sobre:

- Los desafíos impuestos a proyectos de implantación de Gobierno de TIs:
 - Aspectos políticos y de poder
 - Aspectos técnicos
- Un caso real de implantación y el tratamiento de los dominios de riesgos, calidad, gestión de recursos, alineamiento estratégico, gestión del desarrollo organizacional y gestión financiera de TI
- La manera como han sido tratados los temas acerca de las metodologías y mejores prácticas utilizadas, definición de Modelo Objetivo y estrategia de implantación, problemas enfrentados y las estrategias de resolución utilizadas
- Las principales lecciones aprendidas, las buenas y malas experiencias de forma que puedan ser utilizadas por los asistentes en sus propios proyectos

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

121

Val IT—El valor integrado en el negocio—pronóstico, medición y sustentación: Panel de discusión ▲

Jose Luis Diniz, Moderador

Quint Wellington Redwood

Brasil

Fernando Ferrer Olivares, CISM

Banco de la República

Estébanos International Group

Colombia

El participante aprenderá más sobre:

- El framework Val IT™ que consiste en un conjunto de guías, principios y varios procesos que se definen más allá de un conjunto de prácticas de dirección
- La responsabilidad de los directores, el chief executive officer y todos los ejecutivos en asegurar a los accionistas y las partes interesadas el mejor retorno de las inversiones
- La apropiada consideración y la aplicación de las prácticas más adecuadas contenidas dentro del framework *Control Objectives for IT and related Technology* (CobIT®)
- Cómo maximizar las decisiones en inversiones de TI y evaluaciones donde el potencial para la creación de valor significativo es grande, pero los costos y los riesgos y la visibilidad de una potencial destrucción de valor son altos

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.



131

Gestión automatizada de riesgos de IT compliance ▲

Nathaly Rey

AnyHelp International

España

José Luis Sánchez, CISA, CISM

AnyHelp International

España

El participante aprenderá más sobre:

- Cómo el cumplimiento normativo está afectando a toda la organización
- Qué papel juega IT Compliance dentro de los riesgos informáticos
- Cuál es la trascendencia de los riesgos normativos
- Una forma de gestionar los riesgos de IT Compliance

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

211

Automatizando e integrando el GRC—Gobierno, Riesgo y Cumplimiento ▲

Alberto Bastos

Módulo SA

Brasil

El participante aprenderá más sobre:

- El concepto de GRC—gobierno, riesgo y conformidad
- Cómo integrar y establecer un lenguaje común basado en los principales estándares incluyendo la *ISO Guide 73—Risk Management Guideline*, *ISO 27001—Information Security Series*, *CobIT*, *COSO* y *NIST*
- Un nuevo anteproyecto de gerencia de riesgo: *ISO 31000* y cómo aplicar e integrar estos frameworks para el cumplimiento con leyes y regulaciones incluyendo *US Sarbanes-Oxley Act*, *Basilea II*, *FISMA*, *ISO/IEC 27005—Information Security Risk Management* y *BS 25999—Business Continuity Management*
- Ejemplos de aplicaciones prácticas y estudios de caso de cómo implementar una Gestión de Riesgos Automatizada
- El proceso manual: sus problemas y desafíos

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

221

Modelo para la implementación de procesos de TI bajo CobiT 4.1 ▲

Olga Botero Peláez

*Bancolombia
Colombia*

El participante aprenderá más sobre:

- Cómo implementar el framework CobiT® 4.1 en una empresa, abordando temas como los retos del área de tecnología
- Las claves para lograr una implementación exitosa de un marco de referencia como CobiT
- Cuáles son las mejores estrategias de mejora basada en mejores prácticas
- Cómo analizar los antecedentes a considerar en una implementación de los procesos de TI bajo CobiT, qué se debe considerar cuando hacemos una intervención en la cultura y las prácticas que estamos por adoptar
- La evaluación de un modelo real de implementación de los procesos de TI bajo CobiT, la estrategia de divulgación y puesta en marcha y los resultados obtenidos

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

231

Alineación de procesos operacionales a CobiT para el Gobierno de TI en una empresa postal ▲

Dr. João Souza Neto

*Correios—Brazil Post
Brasil*

El participante aprenderá más sobre:

- Conceptos de gobierno de TI
- Conceptualización de la empresa postal brasileña (ECT)
- Experiencia de ECT con CobiT y gobierno de TI
- Situación actual de trabajo utilizando CobiT incluyendo: autoevaluación de madurez, alineación de procesos operacionales a CobiT, e identificación de procesos prioritarios

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión. El participante debe contar con conocimientos básicos de CobiT.

311

El Estado digital, un desafío para el Gobierno de TI ▲

Jorge Mérida Muñoz

*Contraloría General de la República
Chile*

El participante aprenderá más sobre:

- Las repercusiones a las cuales se enfrentan las diferentes entidades, sean públicas o privadas, frente a la modernización de los Estados y/o Países, los cuales procurando el uso efectivo y eficiente de TI en todas sus relaciones operacionales y de gestión
- Cómo enfrentar el control y qué se debe considerar cuando un Estado se está volcando a la Internet, a los sistemas y servicios electrónicos
- Cómo evaluar los aspectos clave frente a estos desafíos, los riesgos y las obligaciones tecnológicas asociadas y los efectos de seguridad y control asociados con la Rendición de Cuenta de Gestión Institucional a través de medios electrónicos

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

321

Estrategia de control interno en la implementación de un ERP y GRP—Soluciones Exitosas: Panel de discusión ▲

Pedro Hernández, Moderador

*Deloitte
Chile*

José Antonio Lagos Melo, CISA

*Deloitte
Chile*

El participante aprenderá más sobre:

- Aspectos de riesgos y controles a considerar en la implementación del ERP
- Los lineamientos de seguridad en consideración de acuerdo con las mejores prácticas, las metodologías de control interno en una implementación de ERP y las áreas de riesgo
- Experiencias de seguridad y control en implementaciones de ERP y el rol del auditor interno y de los equipos de cumplimiento en la implementación del ERP
- El éxito final de una buena arquitectura de control interno en un ERP tales como la relación profesional y contractual del contratante y el usuario
- Consideraciones de seguridad y control en la planeación y la coordinación del proyecto ERP
- La resistencia al cambio, la nueva operación modular, el control considerando la integración del sistema, todo ello basado en lograr cadenas de valor y procesos certificados bajo estándares de calidad como el ISO 9000

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

331

Implementación de un sistema de gestión de servicios de TI basado en ISO 20000, CobiT e ISO 27001 ▲

Juan Carlos Martínez Ventura, CISA

*SCITUM
México*

El participante aprenderá más sobre:

- Por qué ISO 20000 se está convirtiendo en un estándar indispensable para administrar de manera eficaz y eficiente los servicios que proporcionan las áreas de TI y las empresas que tienen como proceso principal la provisión de servicios de TI
- La necesidad de conocer la estructura y procesos necesarios para implementar de manera adecuada un sistema de gestión de servicios de TI alineado a las cláusulas que requiere el ISO 20000
- La aplicación del modelo PDCA (plan, do, check, act) a los procesos de soporte y entrega de servicios de TI
- Cómo considerar a CobiT y a la ISO 27001 para complementar la visión que la ISO 20000 establece, para así conformar un todo que apunte la estrategia y el cumplimiento de los objetivos organizacionales de cara a los nuevos retos que la era de la información presenta

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Evaluación de outsourcing y Gobierno de TI en el sector público: experiencia del Gobierno Brasileño ▲

Carlos Renato Araujo Braga, CISA
Tribunal de Cuentas de la Unión
Brasil

El participante aprenderá más sobre:

- La situación del outsourcing en el Gobierno Federal brasileño
- Los desafíos de cumplimiento para las contrataciones de TI en el sector público brasileño
- La relación entre outsourcing y gobierno de TI
- Evaluación del gobierno de TI en el sector público
- Evaluación de outsourcing en el sector público
- La importancia del cumplimiento para el sector público brasileño

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Pista 2—Auditoría de Sistemas de Información (IT Assurance)

Cómo ejecutar un análisis de riesgos y amenazas de TI: Caso práctico y matriz de riesgos ▲

Mario Ureña Cuate, CISA, CISM
Secure Information Technologies
México

El participante aprenderá más sobre:

- Cuáles son los componentes que conforman los riesgos de TI
- Cómo ejecutar un análisis de riesgos y amenazas de TI
- Quiénes deberían ejecutar el análisis de riesgos y amenazas de TI
- Técnicas de diagramación para identificar activos de TI dentro de los procesos del negocio
- Diferentes opciones para el tratamiento de riesgos
- Factores críticos de éxito en la ejecución del análisis de riesgos y amenazas de TI

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Tendencia actual: Auditoría integrada ▲

Fernando Nikitin, CGEIT, CISA, CISM
Banco Interamericano de Desarrollo (BID)
Uruguay

El participante aprenderá más sobre:

- Organización óptima de la función de Auditoría Tecnológica
- Tipos de auditorías, interrelación, coordinación e integración de auditorías de TI con auditorías no-TI
- Planeamiento integrado
- Trabajo colaborativo y sinergia multidisciplinaria
- El perfil requerido de conocimientos, habilidades y comportamientos
- Opinión integrada, valor agregado, eficacia y eficiencia

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.



Experiencias SAS 70: Lecciones aprendidas— La visión del cliente y del auditor: Panel de discusión ▲

Jorge Serrano, CISA, Moderador
Combanc SA
Chile

María Eugenia Solovioff L
SINACOFI SA
Chile

Humberto Salicetti
KPMG
Chile

Dario Rojas A, CISA
Ernst & Young Servicios de Riesgo y Gestión
Chile

El participante aprenderá más sobre:

- Cómo enfrentar una revisión SAS 70 desde la perspectiva del auditor y del auditado
- Los objetivos de la Auditoría SAS 70, origen y consideraciones al enfrentar esta revisión
- Cómo llevar adelante un proceso de Auditoría SAS 70, considerando aspectos metodológicos, culturales, de gestión del cambio, de gestión de riesgos, y de la naturaleza del negocio
- La detección de oportunidades de mejora, que agreguen valor a la organización a través de las observaciones de la auditoría
- Los problemas más típicos a considerar durante un proceso SAS70

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Auditoría de los requerimientos legales para TI—Diversidad del enfoque ▲

Marina Touriño, CISA, CISM
Marina Touriño & Asociados SL
España

El participante aprenderá más sobre:

- La tendencia globalizadora en la promulgación de regulación sobre TI
- Concepto de eficiencia en alcances de auditoría que incluyan requerimientos legales para TI
- Reseña de experiencias prácticas en el aseguramiento de requerimientos legales para TI
- Complejidad en el enfoque interpretativo de aspectos concretos de las regulaciones para TI

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Opcionalmente, deberá contar con algunos conocimientos sobre requerimientos legales para TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Cómo enfrentar una Auditoría de TI: Perspectiva del auditado ▲

Alfonso Mateluna, CISA
KPMG Auditores Consultores Ltda
Chile

El participante aprenderá más sobre:

- El proceso de ser auditado
- El rol de la Auditoría, ver las oportunidades que hay detrás de una auditoría, como la concienciación mayor de ejecutivos reacios a discutir presupuesto para una inversión en TI

- El énfasis que se debe poner sobre aspectos como la comunicación con un lenguaje común, abordar y dejar atrás viejos mitos
- Qué hacer una vez que somos auditados, a fin de poder priorizar los planes de acción

Prerrequisitos:

El participante debe contar con al menos un año de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

232

Desarrollo Profesional del Auditor de TI ▲

Carlos Kingweres Castrejón

*Pinchale Vision Sc—México y LATAM
México*

El participante aprenderá más sobre:

- Entendimiento de los paradigmas laborales que limitan el desarrollo profesional así como el logro de objetivos personales
- Reconocimiento de las variables que llevan a las compañías a tomar decisiones sobre la contratación de talento en el mercado laboral latinoamericano
- Elaboración del CV y como destacar aquellos elementos que hacen a un candidato más atractivo sobre su competencia para vender el activo más importante como profesionista: uno mismo
- Consejos genéricos y prácticos de cómo conducir una entrevista de trabajo

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

312

Racionalización de controles basándose en el estándar 5 del PCAOB ▲

Salomón Rico, CISA, CISM

*Deloitte Monterrey
México*

El participante aprenderá más sobre:

- Las oportunidades que ofrece el estándar 5 del PCAOB para racionalizar el marco de controles de una organización
- Enfoque top-down para la racionalización de controles
- ¿Cuáles son algunas lecciones aprendidas en la aplicación de este estándar?
- Casos de éxito que sirvan de referencia en cuanto a los logros obtenidos en la aplicación de un enfoque de racionalización de controles

Prerrequisitos:

El participante deberá estar familiarizado con tareas de cumplimiento para Sarbanes-Oxley u otras regulaciones similares desde un punto de vista dentro de una empresa o como consultor o auditor en cumplimiento con estas regulaciones. Sería deseable que hayan pasado por experiencias con el estándar 2 y el estándar 5 del PCAOB. El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

▲ Básico ▲ Intermedio ▲ Avanzado

Nota: El nivel básico de una persona, puede ser el nivel avanzado de otra. Por favor revise la descripción y prerrequisitos de la sesión para determinar si la sesión es apropiada para usted.

322

Caso de implementación de integridad y seguridad de datos en un ambiente de outsourcing ▲

Ernesto Aguilar, CISA

*Federal Reserve Bank
Estados Unidos*

El participante aprenderá más sobre:

- Cómo las entidades financieras están sujetas a estrictas leyes federales y locales en materia de privacidad, además de varias leyes que regulan su operación desde el punto de vista financiero y contable, incluyendo US Sarbanes-Oxley Act
- La implementación de un esquema diseñado para evaluar, monitorear y asegurar la totalidad, exactitud, consistencia, autorización, disponibilidad y confidencialidad de datos en una empresa que opera principalmente a través de una red de más de veinte proveedores de servicios de procesamiento de datos
- El esquema de este ejercicio, el cual está basado en un repositorio de meta-data para vigilar trayectorias de información y asegurar un control adecuado en los varios flujos operativos

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

332

CobIT 4.1 en el nuevo Marco de Referencia para el Aseguramiento de TI ▲

Gustavo Adolfo Solís Montes, CISA, CISM

*Grupo Cynthus, SA de CV
México*

El participante aprenderá más sobre:

- La importancia del diseño y efectividad de los controles de tecnología de información
- La necesidad de informar a stakeholders sobre los sistemas de control existentes
- Las Guías para realizar auditorías de forma eficiente, efectiva y en cabal cumplimiento de las obligaciones normativas
- El ITAF (Information Technology Assurance Framework)
- Los Lineamientos de Aseguramiento de CobIT 4.1

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

342

Riesgo tecnológico y fraude en la comunidad de los negocios ▲

Rubén Bareiro

*Ernst & Young
Argentina*

Luciano Fain

*Ernst & Young
Argentina*

El participante aprenderá más sobre:

- Tipos de fraude y sus características
- Estadísticas de fraude
- El involucramiento de TI en la ejecución de fraudes
- Consecuencias del fraude
- Enfoques modernos para combatir al fraude

Prerrequisitos:

El participante debe contar con al menos un año de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

Pista 3—Gestión de Seguridad de Sistemas de Información (IT Security Management)

113

Administración de la Identidad y Accesos (IAM)— El próximo desafío ▲

Nihat Guven

KPMG Auditores Consultores Ltda
Chile

Ricardo Gadea

Assertiva
Chile

El participante aprenderá más sobre:

- Conceptos básicos de la administración de la Identidad y Acceso (Identity and Access Management—IAM)
- Ciclo de vida de gestión de la identidad
- Beneficios de la IAM
- Metodología y mejores prácticas para la ejecución de un proyecto IAM
- El funcionamiento en vivo de una solución de IAM, a través de una demostración orientada a ejemplificar los conceptos aprendidos en la sesión

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

123

Tensiones en la organización: El impacto generacional sobre la seguridad de la información ▲

Alberto Enrique Orgeira, CISA

Standard Bank Argentina
Argentina

El participante aprenderá más sobre:

- El marco conceptual y los arquetipos de las generaciones sociales actuales
- Los usos y motivaciones generacionales sobre las tecnologías de información a su disposición
- Los riesgos en vigor, tendencias y potenciales mitigantes tecnológicos y sociales
- El desafío que presenta gestionar y aprovechar los beneficios de grupos Wikis

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

133

Modelo de negocio de seguridad de información ▲

Cilliam Cuadra, CISA, CISM

Banco Nacional de Costa Rica
Costa Rica

El participante aprenderá más sobre:

- Las necesidades generales en las organizaciones para garantizar un adecuado gobierno de la seguridad de la información
- Cómo los encargados de esta función reclaman por la existencia de modelos de negocio que les permitan superar las barreras del entendimiento con la administración
- El modelo de Negocio para la Seguridad de la Información que ha considerado ISACA dentro de sus programas de investigación, supliendo esta necesidad
- La cobertura global de la organización del modelo y su uso en nuestra región como soporte a la gestión de seguridad

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.



213

Implementación de ISO 27001—Casos prácticos sector gobierno y privado: Panel de discusión ▲

Luis Guillermo Budge Soriano, CISA, CISM, Moderador

Deloitte
Perú

Carlos Samaniego, CISA, CISM

Orion 2000
Perú

Miguel Cisterna Landaeta

Orion 2000
Chile

El participante aprenderá más sobre:

- Las organizaciones con diferentes realidades que desean implementar un Sistema de Gestión de Seguridad de la Información, certificarlo y demostrar al mercado sus elementos de valor con esta iniciativa
- Identificar las diferentes realidades y los distintos caminos para lograrlo
- Diferentes regulaciones y exigencias, que han obligado a muchas organizaciones a cumplir con la estándar ISO 27001, asumiendo costos económicos importantes y múltiples proyectos por gestionar
- La experiencia práctica que se ha tenido en proyectos de implementación y certificación del estándar, en distintas organizaciones dentro del sector gubernamental como en el sector privado

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

223

Islas de alta seguridad dentro de redes corporativas ▲

Victor M. Chapela

Sm4rt Solutions
México

El participante aprenderá más sobre:

- Cómo al aumentar la interconectividad aumenta el riesgo
- Reducción de riesgo implantando islas de alta seguridad para áreas de tesorería, administradores, altos directivos y personal clave
- Métricas para medir el riesgo de los individuos y sus equipos personales
- Comparación de los niveles de riesgo antes y después de implantadas las islas
- El balance entre interoperabilidad, facilidad de uso y seguridad
- Definición de los aspectos técnicos y humanos más relevantes
- Un caso práctico de implantación de islas de seguridad en varios corporativos

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en auditoría de TI, 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.

Talleres

Sábado, 16 de Agosto, 2008	Domingo, 17 de Agosto, 2008	Lunes, 18 de Agosto, 2008					Martes, 19 de Agosto, 2008						
9.00-17.00	9.00-17.00	8.30-10.00	10.30-12.00	13.30-15.00	15.30-17.00	17.30-19.30	8.30-10.00						
WS1 Curso de Fundamentos de CoBIT ▲ <i>Gustavo Adolfo Solís Montes, CISA, CISM (México) y Jorge Medín Hidalgo, CGEIT, CISA, CISM (Argentina)</i> ▲		Pista 1 Gobierno y Control de TI (IT Governance and Control) Pista 2 Auditoría de Sistemas de Información (IT Assurance) Pista 3 Gestión de Seguridad de Sistemas de Información (IT Security Management)		Presentación Inaugural—El nuevo papel del CISO—Santiago Moral Rubio, CISA, CISM (España)					211 Automatizando e integrando el GRC - Gobierno, Riesgo y Cumplimiento ▲ <i>Alberto Bastos (Brasil)</i>				
WS2 Curso de Preparación al Examen CISA ▲									111 Caso práctico de implantación de Gobierno de TI en la banca ▲ <i>Francisco Siexas Neto, CISA (Brasil)</i>	121 Val IT-El valor integrado en el negocio—pronóstico, medición y sustentación: Panel de discusión ▲ <i>Jose Luis Diniz (Brasil) y Fernando Ferrer Olivares, CISM (Colombia)</i>	131 Gestión automatizada de riesgos de IT compliance ▲ <i>Nathaly Rey y José Luis Sánchez, CISA, CISM (España)</i>	Sesiones Educativas de Proveedores y Recepción de Proveedores	212 Auditoría de los requerimientos legales para TI—Diversidad del enfoque ▲ <i>Marina Touriño, CISA, CISM (España)</i>
WS2 Curso de Preparación al Examen CISA ▲ <i>Salomón Rico, CISA, CISM (México) y Carlos E. Villamizar Rodríguez, CISA (Colombia)</i> ▲									112 Cómo ejecutar un análisis de riesgos y amenazas de TI: Caso práctico y matriz de riesgos ▲ <i>Mario Ureña Cuate, CISA, CISM (México)</i>	122 Tendencia actual: Auditoría integrada ▲ <i>Fernando Nikitin, CGEIT, CISA, CISM (Uruguay)</i>	132 Experiencias SAS 70: Lecciones aprendidas - La visión del cliente y del auditor: Panel de discusión ▲ <i>Humberto Salicetti, Darío Rojas A., CISA, Jorge Serrano, CISA y María Eugenia Soloviof L. (Chile)</i>		213 Panel: Implementación de ISO 27001—Casos Prácticos Sector gobierno y privado ▲ <i>Luis Guillermo Budge Soriano, CISA, CISM y Carlos Samaniego, CISA, CISM (Perú) y Miguel Cisterna Landaeta (Chile)</i>
		113 Administración de la Identidad y Accesos (IAM) El proximo desafío ▲ <i>Ricardo Gadea y Nihat Guven (Chile)</i>	123 Tensiones en la organización: El impacto generacional sobre la seguridad de la información ▲ <i>Alberto Enrique Orgeira, CISA (Argentina)</i>	133 Modelo de negocio de seguridad de información ▲ <i>Cilliam Cuadra, CISA, CISM (Costa Rica)</i>									

▲ Básico ▲ Intermedio ▲ Avanzado

Nota: El nivel básico de una persona, puede ser el nivel avanzado de otra. Por favor revise la descripción y prerrequisitos de la sesión para determinar si la sesión es apropiada para usted.

Talleres

Martes, 19 de Agosto, 2008			Miércoles, 20 de Agosto, 2008				Jueves, 21 de Agosto, 2008	Viernes, 22 de Agosto, 2008
10.00-12.00	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	9.00-17.00
221			231	311	321	331	341	WS3
Modelo para la implementación de procesos de TI bajo CobiT 4.1 ▲ <i>Olga Botero Peláez (Colombia)</i>			Alineación de procesos operacionales a CobiT para el Gobierno de TI en una empresa postal ▲ <i>João Souza Neto (Brasil)</i>	El Estado digital, un desafío para el gobierno de TI ▲ <i>Jorge Mérida Muñoz (Chile)</i>	Estrategia de control interno en una implementación de una ERP y GRP— Soluciones Exitosas: Panel de discusión ▲ <i>Pedro Hernández y José Antonio Lagos Melo, CISA, (Chile)</i>	Implementación de un sistema de gestión de servicios de TI basado en ISO 20000, CobiT e ISO 270001 ▲ <i>Juan Carlos Martínez Ventura, CISA (México)</i>	Evaluación de outsourcing y Gobierno de TI en el sector público: Experiencia del Gobierno Brasileño ▲ <i>Carlos Renato Araujo Braga, CISA (Brasil)</i>	Implementación de Gobierno de TI Utilizando CobiT y Val IT ▲ <i>Gloria Elena Cárdenas Soto, CISA (Colombia) y Alexander Zapata Lenis, CISA (México)</i>
222			232	312	322	332	342	WS4
Cómo enfrentar una Auditoría de TI: perspectiva del auditado ▲ <i>Alfonso Mateluna, CISA (Chile)</i>			Desarrollo Profesional del Auditor de TI ▲ <i>Carlos Kigwergs Castrejón (México)</i>	Racionalización de controles basándose en el estándar 5 del PCAOB ▲ <i>Salomón Rico, CISA, CISM (México)</i>	Caso de implementación de integridad y seguridad de datos en un ambiente de outsourcing ▲ <i>Ernesto Aguilar, CISA (EUA)</i>	CobiT 4.1 en el nuevo Marco de Referencia para el Aseguramiento de TI ▲ <i>Gustavo Adolfo Solís Montes, CISA, CISM (México)</i>	Riesgo tecnológico y fraude en la comunidad de los negocios ▲ <i>Luciano Fain y Rubén Bareiro (Argentina)</i>	Curso de Preparación al Examen CISM ▲ <i>Fernando Ferrer Olivares, CISM (Colombia) y Marcelo Melro, CISA, CISM (Brasil)</i>
223			233	313	323	333	343	WS5
Islas de alta seguridad dentro de redes corporativas ▲ <i>Victor M. Chapela (México)</i>			Aspectos y Experiencias en Seguridad en Ambientes VoIP ▲ <i>Marcelo F. Melro, CISA, CISM (Brasil)</i>	Seguridad en equipos de ejecutivos: Caso de ambientes MAC OS X ▲ <i>Aureo Monteiro Tavares Da Silva (Brasil)</i>	Desde el eslabón débil al eslabón fuerte ▲ <i>Lucas Adrián Gómez (Chile) y Diego Andrés Zuluaga, CISM (Colombia)</i>	Aspectos prácticos de implementación de un sistema de gestión de seguridad de la información ▲ <i>Oscar Viniestra, CISA (México)</i>	Fuga de datos por dispositivos móviles ▲ <i>Ezequiel Sallis (Argentina)</i>	Cómputo Forense en la Organización ▲ <i>Andrés Velázquez Olavarrieta (México)</i>

233

Aspectos y Experiencias en Seguridad en Ambientes VoIP ▲

Marcelo F. Melro, CISA, CISM

*Siemens Enterprise Communications
Brasil*

El participante aprenderá más sobre:

- La actual tendencia orientada al uso de tecnologías VoIP y el amplio despliegue que está teniendo
- La evaluación de los diferentes riesgos, amenazas y aspectos de seguridad para garantizar un ambiente seguro en el ámbito de las comunicaciones VoIP
- Los riesgos, amenazas, aspectos de seguridad relacionados con Ambientes VoIP
- El estado actual de madurez en seguridad para Redes VoIP y las soluciones e implementaciones e experiencias actuales de seguridad en Ambientes VoIP
- Tendencias futuras en seguridad de Ambientes VoIP

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

313

Seguridad en equipos de ejecutivos: Caso de ambientes MAC OS X ▲

Aureo Monteiro Tavares Da Silva

*URBTEC™ INFORMATION SECURITY
Brasil*

El participante aprenderá más sobre:

- Los nuevos paradigmas en la computación móvil
- Utilización de equipos Apple en el ambiente de la empresa
- El Mac OS X
- Comparación con ambientes Windows
- Riesgos e amenazas asociados
- Configuraciones de seguridad

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

323

Desde el eslabón débil al eslabón fuerte ▲

Lucas Adrián Gómez

*KPMG Auditores Consultores Ltda
Chile*

Diego Andrés Zuluaga, CISM

*ISAGEN SA ESP
Colombia*

El participante aprenderá más sobre:

- El eslabón más débil de la cadena de seguridad de información dentro de las distintas organizaciones, se sabe normalmente que son las personas
- La forma de identificar la diferencia entre el aprendizaje de las normas de seguridad y el desarrollo de hábitos de seguridad en información y como desarrollarlos en la empresa, mediante estrategias adaptadas a los recursos y entornos de cada organización

Prerrequisitos:

El participante debe contar con al menos un año de experiencia en auditoría de TI, 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.

333

Aspectos prácticos de implementación de un sistema de gestión de seguridad de la información ▲

Oscar Viniegra, CISA

*ISM
México*

El participante aprenderá más sobre:

- La información como una necesidad de negocio
- La necesidad de contar con sistemas de información confiables que ha fomentado la mención de diferentes normas y marcos de referencia internacionales en literatura especializada y en revistas de negocios
- El desconocimiento en las PYMES donde no existe una persona dedicada a la seguridad de la información y en ocasiones ni siquiera alguien de tiempo completo dedicado a TI
- Una visión práctica de qué es seguridad de la información, por qué es necesaria y cómo abordar su implementación de manera práctica no-nonsense

Nota: La visión que se presentará está alineada con ISO 27001, ISO 17799 y CoBIT® Security Baseline

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

343

Fuga de datos por dispositivos móviles ▲

Ezequiel Sallis

*Root-Secure
Argentina*

El participante aprenderá más sobre:

- El rol de los dispositivos móviles en la organización
- Cuál es la problemática en lo referente a la fuga de información y las nuevas tecnologías.
- Riesgos y ataques –casos prácticos
- U3 y Non U3 USB Hacks
- Bluetooth BlueLine Attack

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

▲ Básico ▲ Intermedio ▲ Avanzado

Nota: El nivel básico de una persona, puede ser el nivel avanzado de otra. Por favor revise la descripción y prerrequisitos de la sesión para determinar si la sesión es apropiada para usted.

Talleres

WS1

Curso de Fundamentos de CobIT ▲

sábado y domingo 16 y 17 de agosto 2008

Jorge Medin Hidalgo, CGEIT, CISA, CISM

*Gobierno de la provincia de Mendoza
Argentina*

Gustavo Adolfo Solís Montes, CISA, CISM

*Grupo Cynthus
México*

Dada la popularidad del Curso de Fundamentos de CobIT (CobIT Foundation Course™) ISACA presenta este taller para quienes desean conocer la forma efectiva de llevar a cabo el gobierno de la tecnología de información utilizando el marco de CobIT.

Este taller es interactivo, basado en una experiencia en un salón de clases. Este curso explica el marco de CobIT utilizando ejemplos prácticos y casos de estudio y proporcionará todos los componentes de CobIT, incluyendo los objetivos de control, las directrices gerenciales y los modelos de madurez. El curso ayudará a los profesionistas, comprender cómo utilizar CobIT en una forma lógica y validará este conocimiento en un ambiente de aprendizaje interactivo.

Nota: El curso finalizará con el Examen de Fundamentos de CobIT (CobIT® Foundation Exam), el cual es opcional, para quienes deseen obtener el Certificado de Fundamentos de CobIT (CobIT® Foundation Certificate).

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

WS2

Curso de Preparación al Examen CISA ▲

sábado y domingo 16 y 17 de agosto 2008

Salomón Rico, CISA, CISM

*Deloitte
México*

Carlos E. Villamizar Rodríguez, CISA

*Consultor Independiente
Colombia*

Este curso de preparación de dos días está diseñado para apoyar y mejorar el proceso de estudio de los candidatos a presentar el examen Certified Information Systems Auditor™ (CISA®) y también será muy útil para el profesional que desee tener una visión de los principales temas relacionados con la auditoría de sistemas. En este curso se revisarán los principales temas, conceptos y prácticas de auditoría de sistemas. El material del curso complementará el material que ISACA ha desarrollado para el estudio de preparación al examen CISA. Este curso es complementario a los cursos intensivos de varias semanas que se ofrecen en diversos capítulos de ISACA como preparación al examen CISA. El participante recibirá un *Manual de Preparación al Examen CISA® 2008* en español como parte de su material del curso.

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para auditar el ambiente de TI. Experiencia gerencial sería deseable, pero no es requerida para esta sesión.

WS3

Implementación de Gobierno de TI Utilizando CobIT y Val IT ▲

jueves y viernes 21 y 22 de agosto 2008

Gloria Elena Cárdenas Soto, CISA

*Bancolombia
Colombia*

Alexander Zapata Lenis, CISA

*Grupo Cynthus
México*

Como respuesta a las necesidades de orientación sobre cómo implementar el Gobierno de TI utilizando CobIT, el ITGI creó la segunda edición de la *Guía de Implementación de Gobierno de TI*. Este importante documento ayuda a las organizaciones a evaluar e implementar el Gobierno de TI usando modelos de madurez, marcos de referencia para la medición de desempeño, objetivos y prácticas de control. Este taller de dos días se basa en la guía de implementación y su mapa

de ruta para las actividades de implementación de Gobierno de TI. El taller ofrece lecturas, casos de estudio y ejercicios grupales con el fin de explorar los conceptos de Gobierno de TI y resaltar mejores prácticas y factores críticos de éxito para el proyecto. El Taller también incluye referencias a la iniciativa de Val IT del ITGI con el fin de optimizar la creación de valores de las inversiones de TI y se explicará cómo el marco de referencia de Val IT soporta el proyecto de implementación de Gobierno de TI.

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en gobierno de TI, auditoría de TI y/o experiencia en gestión de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para gobernar el ambiente de TI. La experiencia gerencial sería deseable, pero no es requerida para esta sesión.

WS4

Curso de Preparación al Examen CISM ▲

jueves y viernes 21 y 22 de agosto 2008

Fernando Ferrer Olivares, CISM

*Banco de la República/Estérganos International Group
Colombia*

Marcelo F. Melro, CISA, CISM

*SIEMENS
Brasil*

Este es un curso diseñado para apoyar y mejorar el proceso de estudio de los candidatos a presentar el examen Certified Information Security Manager® (CISM®). También servirá para aquellos profesionales interesados en conocer los conceptos fundamentales de la Gestión de la seguridad de la información. En este curso se revisarán los conceptos clave de la gestión de la seguridad de la información. Se enfatizarán las prácticas gerenciales y los tópicos y conceptos relacionados con el temario de preparación para el examen CISM. Este curso es complementario a los cursos intensivos de varias semanas que se ofrecen en diversos capítulos de ISACA como preparación al examen CISM. El participante recibirá un *Manual de Preparación al Examen CISM® 2008* en español como parte de su material del curso.

Prerrequisitos:

El participante debe contar con al menos tres años de experiencia en auditoría de TI, 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.

WS5

Cómputo Forense en la Organización ▲

jueves 21 de agosto 2008

Andrés Velázquez Olavarrieta

*Director Investigaciones Digitales/Mattica
México*

Según estadísticas, cada vez es más notorio el uso de las tecnologías de la información dentro de las organizaciones para la extracción de información, mejor conocido como la inteligencia competitiva. Si bien el cómputo forense es una disciplina completamente reactiva, es importante tener los mecanismos necesarios preventivos para que a la aplicación del mismo, se pueda obtener la mayor cantidad de información para encontrar al responsable.

Este taller está orientado a explicar las mejores prácticas internacionales para la realización de las investigaciones digitales dentro de la organización, no importando si van a ser usadas o no dentro de un procedimiento legal, considerando la evidencia digital, el proceso del cómputo forense, las herramientas usadas en el mercado y el manejo de la prueba digital. Cupo limitado a 25 participantes.

Prerrequisitos:

El participante debe contar con al menos cinco años de experiencia en seguridad y auditoría de TI o conocimiento equivalente y estar familiarizado con la terminología, enfoques, metodologías y técnicas para la gestión de seguridad y para auditar el ambiente de TI.



Información General

Límite de Responsabilidad

Los datos sobre los ponentes/expositores, temas y eventos, son correctos hasta el momento de la publicación de este documento. Si existiera alguna eventualidad, ISACA se reserva el derecho de alterar o borrar algún elemento de la conferencia Latin América CACS 2008. Los conferencistas han preparado su material para el desarrollo profesional de la membresía de ISACA y otros interesados en la comunidad de Auditoría y Control de Sistemas de Información. Aún cuando ellos confían en que tal material será útil para tal efecto, ni los conferencistas ni la ISACA pueden garantizar que el uso de este material sea adecuado para descargar la responsabilidad legal o profesional de los miembros en el ejercicio de sus prácticas.

Beneficios de la Conferencia

Las cuotas de inscripción al Latin America CACS incluyen:

- Asistencia a las sesiones que desee de las 30 que se llevarán a cabo en la conferencia
- Memoria impresa de las presentaciones de los conferencistas, de las sesiones recibidas al tiempo de la impresión
- Entrada sin restricción alguna a las sesiones de intercambio de información InfoExchange el lunes y el martes, 18 y 19 de agosto
- Asistencia a las sesiones educativas que elija de los proveedores de InfoExchange
- Almuerzos/comidas de cortesía desde el lunes 18 de agosto, hasta el miércoles 20 de agosto
- Refrescos gratuitos durante los descansos de la mañana y la tarde durante los tres días de la conferencia
- Invitaciones a los siguientes eventos sociales:
 - Recepción de Bienvenida, el domingo 17 de agosto
 - Recepción de Proveedores, el lunes 18 de agosto
 - Velada Especial, el martes 19 de agosto
- Posibilidad de obtener hasta 40 horas de CPE

Fechas y Horarios de la Conferencia y de los Talleres

Conferencia

Del Lunes 18 de Agosto al Miércoles 20 de agosto de 2008, 8.30 a 17.00

Talleres

WS1 y WS2 el Sábado y Domingo 16 y 17 de agosto de 9.00 a 17.00 hrs.
 WS3 y WS4 el Jueves y Viernes 21 y 22 de agosto de 9.00 a 17.00 hrs.
 WS5 el Jueves 21 de agosto de 9.00 a 17.00 hrs.

Conferencia y Talleres

Fechas y Horarios de Inscripción

Inscripción a la Conferencia

domingo, 17 de agosto de 15.00 a 19.30
 lunes, 18 de agosto de 7.00 a 17.00
 martes, 19 de agosto de 8.00 a 17.00
 miércoles, 20 de agosto de 8.00 a 17.00

Fechas y horarios de InfoExchange

lunes, 18 de agosto de 17.00 a 19.30
 martes, 19 de agosto de 10.00 a 13.30

Inscripción a los talleres antes o después de la conferencia

Talleres WS1 y WS2 sábado 16 de agosto de 7.30 a 12.00
 Talleres WS3, WS4 y WS5 jueves 21 de agosto de 7.30 a 12.00

Eventos Especiales

Recepción de Bienvenida

Domingo 17 de agosto de 17.30 a 19.30

Participe en el acto de apertura de la conferencia Latin America CACS. Reúnase con sus antiguos y nuevos compañeros de todo el mundo, así como con los ponentes. Este es el momento propicio para comenzar a hacer contactos en el mundo de los negocios.

Recepción de Proveedores e InfoExchange

Lunes, 18 de agosto de 2008, de 17.00 a 19.30—Recepción de Proveedores

Martes, 19 de agosto de 2008, de 10.00 a 13.30—Apertura de exhibiciones

La Recepción de Proveedores marca la apertura oficial de las sesiones de intercambio de información InfoExchange. Acérquese a tomar un refresco y a evaluar los últimos productos y servicios disponibles para los profesionales de TI. Los proveedores estarán a su disposición para mostrar productos y responder a sus preguntas. Deje su tarjeta de presentación en cada uno de los puestos de exhibición y opte a los premios que ofrecen. El gran premio es una inscripción gratuita a la conferencia Latin America CACS 2009 en Costa Rica.

Sesiones Educativas de Proveedores

Lunes, 18 de agosto de 17.30 a 19.30

Martes, 19 de agosto de 10.45 a 12.30

ISACA ofrece sesiones educativas especiales de media hora, presentadas por los proveedores de InfoExchange. Usted podrá obtener créditos de CPE por su asistencia a estas sesiones. Las sesiones educativas de proveedores facilitan la gran posibilidad adicional de interactuar con los proveedores o ver una demostración de los productos y servicios que ofrecen. En la conferencia se anunciarán las sesiones, con su lugar y horario específico.

Velada Especial

Martes, 19 de agosto de 18.30 a 23.00

Reúnase con sus compañeros de Latin America CACS para un evento especial por la noche. El sitio agasajará a los delegados con comida gourmet, bebidas, música, baile y una vista panorámica espectacular de Santiago. Se proporcionará transporte de ida al evento y de regreso al hotel. Los delegados de la conferencia dispondrán de acceso gratuito al evento con su inscripción. Las entradas adicionales para su pareja e invitados se pueden comprar por Internet en el website de ISACA o en la misma conferencia.

Lugar de la Conferencia y Alojamiento

Escollado por la Cordillera de los Andes y sobre un gran valle, se encuentra Santiago, capital de Chile, fundada en 1541 por el conquistador español Pedro de Valdivia a los pies del, hasta entonces, cerro Huelén y actual Santa Lucía. La posición geográfica marítima de Santiago le da un carácter de puerta de entrada y vínculo entre la cultura latinoamericana y el mundo entero. La Conferencia Latin America CACS 2008 se llevará a cabo en el Santiago Marriott Hotel, en Santiago de Chile. Las Condes, Santiago, Chile, una de las principales avenidas de Santiago, cercano a centros comerciales como Parque Arauco.

Usted podrá reservar su habitación en el hotel del evento contactando directamente a:

Santiago Marriott Hotel

Avenida Presidente Kennedy 5741

Santiago de Chile

Teléfono: +56.2.426.2100

Fax: +56.2.426.2001

Web site: www.marriott.com

Fecha límite para las reservaciones de hotel: 31 de julio de 2008.

Por favor mencione la Conferencia de ISACA Latin America CACS 2008 cuando haga sus reservaciones. Los huéspedes extranjeros no residentes en Chile, quedan exentos de pagar el 19 por ciento de impuesto Local (IVA) en sus cuentas.

Tarifa del Hotel:

Precio de la habitación: US \$120 por noche en habitación sencilla/doble e incluye bufet de desayuno americano. La tarifa del hotel estará disponible tres (3) días antes y tres (3) días después de la fecha de la conferencia, dependiendo de su disponibilidad.

Invitación Para Unirse a ISACA

¿Aún no es socio? Si se asocia a ISACA, podrá solicitar la diferencia entre las cuotas de conferencia a asociado y no asociado. 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 asociación. Los no asociados pagarán la cuota de conferencia de no asociados al inscribirse; la diferencia entre la cuota de asociado y no asociado se aplica a los asociados. Marque el cuadro del formulario de inscripción para aceptar nuestra invitación. Para más información acerca de la membresía de ISACA, póngase en contacto con el departamento de membresía por email en membership@isaca.org o visite la página web de ISACA (www.isaca.org/membership). Esta oferta vence 30 días después de que termine el evento.

Descargo de responsabilidad de membresía: Mediante la solicitud para formar parte de ISACA, los asociados se comprometen a proteger a la asociación y al IT Governance Institute (ITGI), sus dignatarios, directores, agentes, administradores, miembros y empleados de todas actuaciones o mala actuación mientras llevan a cabo la finalidad de la asociación y del instituto, expuestos en sus respectivos estatutos, así como a certificar que se apegarán al código de ética profesional de la asociación (www.isaca.org/ethics).

Vestimenta

La vestimenta apropiada para la conferencia es business casual, si lo desea puede usar trajes de varias piezas, se recomienda el uso de ropa abrigada para la estación, además de ropa adecuada para la lluvia.

Créditos CPE

Todos los participantes de Latin America CACS tienen derecho a recibir hasta 40 créditos de CPE (19 por asistir a la conferencia y 7 por cada día de un taller). Estos créditos están reconocidos por ISACA como horas CPE de CGEIT, CISA y CISM (en conformidad de las Políticas de Educación Profesional Continua de CGEIT, CISA y CISM), y en su caso, por otras organizaciones profesionales.

Política de Cancelación

Si se recibe una cancelación indicando que no podrá asistir a la conferencia, por teléfono, e-mail o fax antes del 23 de junio de 2008, le reembolsaremos sus cuotas de inscripción a la conferencia menos una tasa de cancelación de US \$100, una tasa de cancelación de US \$50 de la inscripción a talleres y (si procede) se le deducirá la cantidad de derechos de asociado aplicada como resultado de aceptar el cuadro que aparece a continuación: "Deseo solicitar la diferencia entre cuota de conferencia de asociado y no asociado haciéndome socio de ISACA." Después del 23 de junio de 2008, no se realizará ningún reembolso. No hay fecha límite para llevar a cabo las sustituciones de asistentes hasta el día de la conferencia. Si se sustituye un no asociado por un asociado, se seguirán cargando las cuotas de conferencia para no asociado.

Aviso: La inscripción y la entrega de los materiales de la conferencia está condicionada al pago total de la cuota de inscripción. Para garantizar su inscripción, las cuotas del evento o curso deben recibirse antes del plazo publicado. Los giros telegráficos y los formularios enviados por e-mail pueden requerir 10 o más días laborables en llegar a ISACA, de modo que debe prever este plazo en su inscripción. En caso de que por cualquier razón ISACA deba cancelar un curso o evento, se hará responsable únicamente de la cuota de inscripción pagada. ISACA no se hace responsable de otros gastos incurridos, incluidos los gastos de viaje y de alojamiento.



Para más información concerniente a las políticas de administración, tales como quejas y reembolsos, póngase en contacto con el departamento de conferencia de ISACA:
Teléfono: +1.847.660.5585
Fax: +1.847.253.1443
E-mail: conference@isaca.org

Precios

Cuotas de inscripción

(Las cuotas de inscripción están indicadas en dólares americanos)

Inscripción a la conferencia:

Asociado de ISACA (Hasta el 5 de junio de 2008).....	US \$800
Asociado de ISACA (Después del 5 de junio de 2008).....	US \$850
No asociados.....	US \$1,050

Inscripción a talleres:

WS 1—Curso de Fundamentos de COBIT (dos días)	
Asociado de ISACA.....	US \$550
No Asociados.....	US \$750
WS 2—Curso de Preparación al Examen CISA (dos días)	
Asociado de ISACA.....	US \$550
No Asociados.....	US \$750
WS 3—Implementation de Gobierno de TI Utilizando COBIT y Val IT (dos días)	
Asociado de ISACA.....	US \$550
No Asociados.....	US \$750
WS 4—Curso de Preparación al Examen CISM (dos días)	
Asociado de ISACA.....	US \$550
No Asociados.....	US \$750
WS 5—Cómputo Forense en la Organización (un día)	
Asociado de ISACA.....	US \$350
No Asociados.....	US \$450

Impuesto IVA (VAT): Las cuotas de inscripción que aquí se indican no incluyen el impuesto al valor agregado (IVA) ó (Value Added Tax [VAT]) y las cuotas de IVA (VAT) no se pueden deducir de las cuotas de inscripción remitidos.

Nota: Por favor tenga en cuenta que todas las obligaciones de pagos de impuestos, son responsabilidad de la persona o organización que está realizando el pago y no de ISACA. Adicionalmente, ISACA debe recibir la cantidad total de cuotas de inscripción indicada, antes de considerar que su inscripción ha sido pagada por completo.

Conferencia y Talleres de Latin America CACS Página 1 de 2

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

INSCRÍBASE AHORA

¿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												TALLERES	
	Sábado, 16 de Agosto 2008	Domingo, 17 de Agosto 2008	Lunes, 18 de Agosto 2008			Martes, 19 de Agosto 2008			Miércoles, 20 de Agosto 2008				Jueves, 21 de Agosto 2008	Viernes, 22 de Agosto 2008
	9.00-17.00	9.00-17.00	10.30-12.00	13.30-15.00	15.30-17.00	8.30-10.00	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	9.00-17.00
Gobierno y Control de TI	WS1		111	121	131	211	221	231	311	321	331	341	WS3	
Auditoría de Sistemas de Información	WS2		112	122	132	212	222	232	312	322	332	342	WS4	
Gestión de Seguridad de Sistemas de Información			113	123	133	213	223	233	313	323	333	343	WS5	

Conferencia y Talleres de Latin America CACS

Página 2 de 2

Nombre _____

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

(todas las cuotas están indicadas en dólares americanos)

Inscripción a la conferencia

Asociado de ISACA (pago hasta el 5 de junio de 2008) US \$800

Asociado de ISACA (pago después del 5 de junio de 2008). US \$850

No asociado US \$1,050

Inscripción a talleres (dólares americanos)

Talleres antes o después de la conferencia

	Asociado	No-Asociado
WS1 Curso de Fundamentos de CoBIT [dos días]	US \$550	US \$750
WS2 Curso de Preparación al Examen CISA [dos días] . . .	US \$550	US \$750
WS3 Implementación de Gobierno de TI Utilizando CoBIT y Val IT [dos días]	US \$550	US \$750
WS4 Curso de Preparación al Examen CISM [dos días] . . .	US \$550	US \$750
WS5 Cómputo Forense en la Organización [un día]	US \$350	US \$450

Boleto para Velada Especial (sólo para acompañantes [El boleto para asistentes a la conferencia ya está incluido en la cuota de su inscripción a la conferencia]) US \$120.

TOTAL (Sume todos los importes que apliquen.) US \$ _____

Impuesto IVA (VAT): Las cuotas de inscripción que aquí se indican no incluyen el impuesto al valor agregado (IVA) ó (Value Added Tax [VAT]) y las cuotas de IVA (VAT) no se pueden deducir de las cuotas de inscripción remitidos.

Nota: Por favor tenga en cuenta que todas las obligaciones de pagos de impuestos, son responsabilidad de la persona o organización que está realizando el pago y no de ISACA. Adicionalmente, ISACA debe recibir la cantidad total de cuotas de inscripción indicada, antes de considerar que su inscripción ha sido pagada por completo. La inscripción y la entrega de los materiales de la conferencia está condicionada al pago total de la cuota de inscripción.

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 a la vez 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: **Conferencia Latin America CACS 2008**)

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 de la Tarjeta de Socio

5. Métodos de inscripción

- A.  **Inscripción electrónica en el web site de ISACA:**
www.isaca.org/latincacs.
- 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, IL 60674 USA.
- D.  **Transferencias electrónicas/Giros bancarios:** Enviar pagos electrónicos en dólares americanos a:
Bank of America, ABA n° 071000505,
cuenta de ISACA n° 22-71578, código SWIFT LASLUS44
[Incluir el nombre del asistente y **Latin America CACS** en la descripción o notificación de la transferencia.]

6. Política de cancelación

Si se recibe una cancelación por teléfono, e-mail o fax antes del 23 de junio de 2008, le reembolsaremos sus gastos de inscripción a la conferencia descontándole una cuota de cancelación de US \$100, un importe de cancelación de US \$50 de la inscripción a talleres y (si procede) se le deducirá la cantidad de derechos de asociado aplicada como resultado de aceptar el cuadro que aparece a continuación: "Deseo aplicar la diferencia de cuota de la conferencia entre el costo de asociado y el de no asociado hacia la membresía de la ISACA." Después del 4 de junio de 2008, no se realizará ningún reembolso. No hay fecha límite para llevar a cabo las sustituciones hasta la conferencia. Si se sustituye un no asociado por un asociado, se seguirán cargando las cuotas de conferencia a no asociado.

Descargo de responsabilidad/Notas:

Las transferencias electrónicas/giros telegráficos y los formularios enviados en forma electrónica pueden requerir 10 o más días laborables en llegar a ISACA y ser tramitados, de modo que debe prever su inscripción. En caso de que por cualquier razón ISACA deba cancelar un curso o evento, se hará responsable únicamente de la cuota de inscripción. ISACA no se hace responsable de otros gastos incurridos, incluidos los gastos de viaje y alojamiento.

Aviso: Todo aquel que se inscriba en forma electrónica y cuya inscripción no quede pagada hasta el comienzo del evento no se le garantizará la entrega de los materiales de la conferencia. Para más información concerniente a las políticas de administración, como quejas y reembolsos, póngase en contacto con el departamento de conferencias de ISACA:

Teléfono: +1.847.660.5585

Fax: +1.847.253.1443

E-mail: conference@isaca.org

7. Arreglos Especiales

Requisitos de dieta especiales _____

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

La responsabilidad para obtener una VISA corre a cuenta del participante. Para más detalles, póngase en contacto con el gobierno local del país anfitrión. Una vez que se reciba una inscripción pagada, ISACA le enviará una carta de invitación, a petición.

Conferencia Latinoamericana de Auditoría, Control y Seguridad (Latin America CACSSM)

Comité del Programa Latin CACS 2008

Jorge Serrano, CISA

ComBanc S.A
Capítulo de Santiago, Chile
Presidente del Comité

Alexander Zapata Lenis, CISA

Grupo Cynthus
Capítulo Ciudad de México, México

Gloria Elena Cárdenas Soto, CISA
Organización Bancolombia, Colombia
Capítulo de Bogotá, Colombia

Alberto Enrique Orgeira, CISA

Standard Bank
Capítulo Buenos Aires, Argentina

Víctor M. Chapela

Sma4rt Security Services
Capítulo Ciudad de México, México

Marcelo F. Melro, CISA, CISM

Siemens
Capítulo de Sao Paulo, Brasil

Luis Guillermo Budge Soriano, CISA, CISM

Deloitte
Capítulo de Lima, Perú

Cilliam Cuadra, CISA, CISM

Banco Nacional de Costa Rica
Capítulo de San José, Costa Rica

Elia Fernández Torres, CISA

ISACA
Estados Unidos



Comité Del Capítulo Anfitrión

Alfonso Mateluna Concha, CISA,
Presidente del Comité

Pablo José Caneo Gutiérrez, CISA

David Varas, CISA

Edson Vittoriano Piuze, CISM

Alfonso Fuentes Morán

Hugo Mejias Quintana, CISA

Víctor Hugo Muñoz, CISA

Michael G. Davis, CISA



3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008-3105, USA

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 cumplimiento