

Cómo Hacer una Revisión de Controles Generales en el Area de Informática

El Uso de COBIT® Para Auditar los Componentes de la Infraestructura de Informática

- Identificar los componentes que se deben enfrentar para asegurar la integridad, confiabilidad y buena marcha de los sistemas
- Definir los componentes críticos que requieren revisión en la estructura de informática
- Repasar el cuadro COBIT 4.1 y determinar como se usa para evaluar la eficacia de los controles generales
- Desarrollar estrategias para evaluar los controles claves en la infraestructura de sistemas
- Aprender como se conduce un análisis de impacto a la empresa para asegurar sobrevivencia ante un evento perjudicial.

San José, Costa Rica

6-8 Febrero

Hotel Real
InterContinental

Miembros
de ISACA
reciben un
descuento
de 10%



El líder internacional en
capacitación de auditoría
y seguridad de informática



Al servicio de los profesionales encargados de la
gobernabilidad de la tecnología de la información
Capítulo 31 - Costa Rica

www.misti.com

Enfoque y Destacues del Seminario

En este seminario de tres días, se analizarán las áreas de revisión para asegurar la integridad, confiabilidad y fiabilidad de valores de información. Se explorarán aspectos críticos del medio ambiente de la informática, tales como buen manejo, controles de la infraestructura, seguridad sobre la información, seguridad física, recuperación después de un desastre, manejo de cambios, y seguridad sobre el perímetro de la red. También se aprenderá como desarrollar estrategias para evaluar controles claves en el sistema de informática.

Además, porque COBIT (Control Objectives for Information and related Technology) nos ofrece un cuadro efectivo de controles, tanto para el manejo, como para la auditoría de informática, se estudiará el cuadro COBIT 4.1. A través del seminario habrá un enfoque sobre como se puede usar este cuadro reconocido como estándar para evaluar la eficacia de los controles internos en los sistemas de informática. Se prestará gran atención al uso de objetivos y prácticas de control según COBIT para apoyar controles de informática y se usará COBIT como medio de planificación, alcance y evaluación de cumplimiento de controles.

Pre-requisito: Auditoría y Controles de Informática (ITGI01) o experiencia equivalente.

Nivel de Capacitación: Básico

Quién Debe Asistir?

Audidores Internos Tanto Como Externos – Auditores Financieros; de Operaciones; de Sistemas; de Módulos de Negocios; de Informática; Aquellos Encargados del Sistema de Calidad; Gerentes y Directores de Auditoría; Gerentes y Analistas de Seguridad de Informática.

Lo que se Aprenderá

1. Planificación de Auditoría de Controles Generales de Informática Basado en Análisis de Riesgos

- **introducción a controles generales de informática**
- la relación entre controles generales y controles de aplicación (sistema específico)
- riesgos/controles
- medio ambiente centralizado o disperso
- Sarbanes-Oxley y controles de informática

2. Criterios y Cuadros de Controles de Informática

- COSO
- ISO-17799 / ISO-27001
- COBIT 4.1
 - que significa COBIT?
 - objetivos/componentes de COBIT
 - requisitos de información de COBIT
 - recursos de informática
 - siguiendo las bases de COBIT
 - Modelo de métrica y madurez o vencimiento

- jeraquía de controles en COBIT
- guía de auditoría y prácticas de controles en COBIT
- auditando a través de COBIT

3. Manejo de la Informática y Gerencia de Operaciones

- objetivos de control de COBIT
- estructura de la organización de informática
- políticas y procedimientos
- planificación estratégica
- manejo de riesgos
- prácticas de recursos humanos dentro de la informática
- manejo de calidad
- separación de responsabilidades
- servicios contratados
- pasos de un programa de auditoría

4. Infraestructura de Computadoras y Sistemas (hardware/software)

- objetivos de control de COBIT
- infraestructura de computadoras (hardware)
 - central vs. dispersa
 - adquisición, contratos e inventarios
 - uso y mantenimiento del equipo
 - auditorías del equipo
- infraestructura de sistemas (software): operativo
 - componentes
 - riesgos
 - manejo de parches
 - auditoría de sistemas operativos
- infraestructura de sistemas (software): manejo de base de datos
 - componentes
 - re-arranque/recuperación/fiabilidad
 - ventajas de la base de datos/desventajas
 - base de datos dispersa
 - controles sobre la administración de base de datos
 - auditoría de base de datos
- pasos de un programa de auditoría de software operativo

5. Controles Sobre el Acceso a la Lógica

- objetivos de control de COBIT
- componentes de controles de acceso
- autenticación: contraseñas, fichas, biométricas
- autorización de los derechos del usuario
- manejo de la cuentas de usuarios
- sistemas de control de acceso
- pista de auditoría
- monitoreo de seguridad
- acceso remoto
- información confidencial en PCs y en estaciones de trabajo
- administración de la seguridad
- autenticación de entrada única (SSN single sign-on)
- mejores prácticas de controles de acceso

6. Controles Físicos y Medioambientales

- objetivos de control de COBIT

- objetivos de seguridad física, riesgos y valores expuestos a pérdida
- controles sobre seguridad física
- riesgos medioambientales
- controles medioambientales

7. Seguridad del Perímetro de la Red

- objetivos de control de COBIT
- análisis de riesgos de la red
- estrategias para mantener seguridad
- programas (software) de comunicación de datos
- Modelo OSI
- TCP/IP
- pared cortafuegos/DMZ
- sistemas para detectar acceso no autorizado
- acceso remoto/acceso inalámbrico
- riesgos del internet

8. Manejo de Cambios

- objetivos de control de COBIT
- riesgos del manejo de cambios
- traducción del lenguaje fuente a módulos de ejecución
- proceso de manejo de cambios
- lenguaje fuente del proveedor
- programas (software) para controlar cambios
- control de versiones de distribución
- pasos de un programa de auditoría

9. Recuperación de un Desastre y Planificación Para Continuar en Marcha

- objetivos de control de COBIT
- eventos desastrosos
- recuperación y planificación para continuar
- análisis del impacto a la empresa
- objetivos de tiempo para recuperación
- estrategia de recuperación
- estrategia de continuidad
- lugares para efectuar la recuperación
- equipos que participarán en la recuperación
- almacenaje remoto
- respaldo y recuperación de datos
- red de telecomunicaciones
- prueba del plan de recuperación
- mantenimiento del plan de continuidad
- requisitos de contratos
- pasos de un programa de auditoría

10. Planificación y Ejecución de Revisiones de Controles Generales

- evaluación de riesgos
- planificación y estrategia de la auditoría
- memorandum de planificación
- documentos claves necesarios para desarrollar la auditoría
- programas de auditoría
- controles sobre pruebas
- papeles de trabajo
- reporte de auditoría

Información para el Registro

Formulario: Envíe el formulario de inscripción debidamente completo a nuestra dirección electrónica administracion@acaicr.org o al fax +506 241 0393

Teléfonos: +506 240 0100 ó TelFax +506 241 0393

IMPORTANTE: Por favor, al inscribirse en el curso, haga referencia al código de inscripción que se encuentra en este boletín.

Inversión: Es de \$1.695,00 (un mil seiscientos noventa y cinco dólares). Miembros de ISACA reciben un descuento de 10%. La inversión cubre: material, refrigerios, y certificado de participación.

Forma de Pagos: Realice su pago mediante *Cheque* a nombre de ACAI "Asociación Costarricense de Auditores en Informática. *Tarjeta de Crédito* (VISA) en nuestras oficinas o por medio de *transferencia electrónica* a nuestras cuentas con el Banco de Costa Rica, Cuenta Colones No.138608-5, Cuenta Dólares No.223389-4.

Importante: Su inscripción al evento queda confirmada al recibo de la inversión total.

Horario: Diariamente de 8.30 am a 5.30 pm. Concluye a la 1pm el último día.

Hora CPE's: Obtenga hasta 22 horas de actualización Profesional.

Política de Cancelación: 1. Para recibir la devolución total del monto pagado, el interesado responsable debe comunicar que no participará en el curso antes del 03 de agosto. Si cancela entre el 06 y el 10 de agosto recibirá un 50% de devolución del monto pagado. Cancelaciones posteriores a esta fecha no se hará devolución alguna.

2. ACAI, se reserva el derecho de cambiar la fecha o cancelar el seminario si no se completa el cupo mínimo, devolviendo en este último caso, las sumas recibidas por concepto del presente seminario y dentro de los 10 días naturales siguientes a la cancelación del evento.

Información Sobre el Hotel: Para interesados que deseen viajar a Costa Rica, debe hacer reservaciones en el hotel lo más pronto posible después de la inscripción en el seminario para recibir la tarifa más baja. Favor de contactar el hotel directamente (números telefónicos aparecen debajo) y pedir el descuento relacionado a este curso.

Cambios de Horario/Cancelación: De vez en cuando, MIS se ve en la necesidad de cambiar los días del curso o de cancelarlo totalmente. Si esto sucediera, se daría aviso con amplio plazo. MIS no se responsabiliza por multas de aerolíneas u hoteles que un cambio tal pudiera causar.

MIS ofrece
este y otros cursos
en particular a su
empresa.
Favor llamar a
Daniel Carney al
+1 508 532 3629
part más detalles.

Cómo Hacer una Revisión de Controles Generales en el Area de Informática

CAPACITACION Formulario de Inscripción

Lugar: San José, Costa Rica, Hotel Real InterContinental

Tel: +506 208 2100 **Fax:** +506 208 2102

Email: inter.sjo@realhotelsandresorts.com

Inversion: USD\$ 1695.00. Miembros de ISACA reciben un descuento de 10%.

Fecha: 6-8 febrero

Horario: Desde las 8:30 am hasta las 5:00 pm diario, excepto el último día cuando la sesión se terminará a la 1:00 pm.

Incluye: Material oficial, refrigerio, certificado de participación

DATOS DE LOS PARTICIPANTES

Nombre Completo:

Tel:

Email:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Total a pagar: \$ _____ **Para pagos en colones consultar tipo cambio vigente**

DATOS DE FACTURACION Y PAGO

Nombre Contacto:

Tel:

Email:

Nombre Empresa:

Tel:

Fax:

Dirección:

Forma de Pago:

Transferencia a cuenta corriente

Cheque

Cuenta Dólares No.223389-4

A nombre de:ACAI

Cuenta Cliente No.15201001022338943

Cuenta Colones No.138608-5

Cuenta Cliente No.15201001013860853

Del Banco de Costa Rica, a nombre de la Asociación Costarricense de Auditores en Informática

Tarjeta de Crédito: Visa (Pago con tarjeta de crédito o cheque en nuestras oficinas de 8 am a 5 pm)

Firma Responsable: _____ (Indispensable)

Notas:

1. Para pagos en moneda local (Colones), consultar tipo de cambio a aplicar
2. La inscripción queda confirmada al momento de hacer efectivo el pago completo del seminario.
3. Consulte tarifa por 3 ó más participantes de una misma empresa.

Política de cancelación

1. Para recibir la devolución total del monto pagado, el interesado responsable debe cancelar la participación en el curso antes del 03 de agosto. Si cancela entre el 06 y el 10 de agosto recibirá un 50% de devolución del monto pagado. Cancelaciones posteriores a esta fecha no se hará devolución alguna.
2. ACAI, se reserva el derecho de cambiar la fecha o cancelar el seminario si no se completa el cupo mínimo, devolviendo en este último caso, las sumas recibidas por concepto del presente seminario y dentro de los 10 días naturales siguientes a la cancelación del evento.

Nombre y Firma

Fecha:



El líder internacional en
capacitación de auditoría
y seguridad de informática



Teléfono +506 240 0100 / TelFax +506 241 0393

administracion@acaicr.org / www.acaicr.org

ITG201CR-M