Seminario – Taller
AUDITORÍA DE CONTROLES GENERALES DE TI Y APLICACIONES DE COMPUTADOR.

Contenido:	Pág

PRESENTACIÓN

Las Auditorías de Sistemas de Información, internas ó externas, realizan un examen objetivo e independiente de los procesos y operaciones de tecnología de información, con el fin de evaluar, verificar e informar a la Gerencia y otras partes interesadas, sobre la efectividad y eficiencia de las operaciones, el cumplimiento y efectividad del Sistema de Control Interno (SCI) establecido en los servicios Informáticos de la Empresa y la seguridad y confiabilidad de la información que generan los sistemas de información.

La **Auditoría Basada en Riesgos** es una forma de conducir las auditorías internas y externas de diferentes tipos (Operativa, de estados financieros y de sistemas de información), basando su planeación y desarrollo en los **riesgos** que pueden generar el mayor impacto negativo en las operaciones de negocio y actividades económicas de las Empresas, para confirmar si las operaciones se ajustan a lo fijado por las leyes, las reglas del negocio y las buenas y mejores prácticas de gestión de riesgos, control interno y seguridad.

La auditoría de Sistemas Basada en Riesgos Críticos es una revisión independiente y objetiva, que evalúa la *efectividad de los controles* establecidos en la Tecnología Información y Comunicaciones (TICs) y los Sistemas de Información Automatizados (ERPs y aplicaciones de computador) para reducir los riesgos potenciales (inherentes) que pueden causar el mayor impacto negativo en las operaciones de la empresa, a niveles aceptables de riesgo residual. También verifica la operación de los controles, la seguridad en los servicios de sistemas de la empresa y el cumplimiento con las normas legales vigentes relacionadas con la información, los datos, el software y las redes de comunicación de datos.

Este seminario presentará la metodología para realizar auditorías de sistemas, alineadas con las normas de auditoria de aceptación general (NAGAs) y las normas de auditoría de TI promulgadas por el IIA e ISACA y las buenas y mejores prácticas de gestión y seguridad de TI vigentes en el mundo (COBIT, ITIL, ISO 27001:2013, ISO 20000, ISO 22301 e ISO 38500).

Durante el seminario, los participantes desarrollarán una Auditoría de sistemas a los Controles Generales de TI bajo la orientación de los instructores.

PROPUESTA DE VALOR

Al finalizar el seminario, los participantes en este seminario estarán en capacidad de:

a) Elaborar el **plan anual de la auditoría de sistemas "basado en valoración de riesgos"**, para los procesos de TI y las aplicaciones de computador que soportan los procesos del modelo de operación de la empresa.

b) Planear y desarrollar **auditorías de sistemas basadas en riesgos críticos**, de acuerdo con estándares internacionales de auditoria generalmente aceptados y las normas de auditoria promulgadas por IIA e ISACA.

c) Desarrollar Auditorías de Sistemas "Basadas en Riesgos Críticos" a los Controles Generales de TI, la Gestión de servicios de TI, las Aplicaciones de Computador y el Desarrollo de Sistemas utilizando el marco de referencia COBIT.

d) Identificar, analizar y evaluar los eventos de riesgo negativos (amenazas) sobre los que se desarrollará la evaluación de control interno y las pruebas de auditoría (de cumplimiento y sustantivas).

e) Evaluar y verificar la efectividad (eficacia + eficiencia) de los controles internos establecidos en la Gestión de Servicios de TI y las Aplicaciones de Computador de la Empresa, para reducir los riesgos potenciales críticos a niveles aceptables de riesgo residual.

f) Diseñar y ejecutar pruebas de auditoria de sistemas (de cumplimiento y sustantivas) con base en los resultados de la evaluación de la efectividad de los controles establecidos para los eventos de riesgo negativos (amenazas).

g) Elaborar y organizar papeles de trabajo de la Auditoría de Sistemas.

h) Elaborar informes eficaces de Auditoría de Sistemas, con los resultados de la Auditoria Basada en Riesgos Críticos.

1. OBJETIVOS DEL SEMINARIO

α) Presentar la metodología para realizar Auditorías de Tecnología de Información (TI), en aspectos de planeación y ejecución "basada en riesgos críticos", de acuerdo con las normas de auditoría generalmente aceptadas, las normas de Auditoría Interna del IIA, las normas de auditoría de sistemas emitidas por ISACA y normas locales expedidas por los organismos de supervisión y control del Estado.

β) Desarrollar habilidades en los participantes para planear y desarrollar **auditorías de sistemas basadas en riesgos críticos**, en los Servicios de tecnología de Información y las aplicaciones de computador que soportan el desarrollo de las operaciones de las empresas.

χ) Presentar y analizar las técnicas y herramientas de auditoria asistidas por computador para apoyar la planeación y desarrollo de las **auditorías de tecnología de información basadas en riesgos críticos**.

2. A QUIÉN VA DIRIGIDO (PARTICIPANTES)

El seminario está dirigido a Auditores de Sistemas, Auditores Internos y Externos, Revisores Fiscales, Contralores, Funcionarios de Oficinas de Control Interno y consultores en auditoría que deseen actualizar o profundizar sus conocimientos sobre auditoría de sistemas de información.

3. TEMAS DEL SEMINARIO

DIA 1.

1. INTRODUCCION.

- Objetivos y alcance de la Auditoría de Sistemas de Información.
- Normas de Auditoria de Aceptación General y su aplicabilidad en Auditoria de Sistemas .
- Normas de Auditoría de Sistemas promulgadas por ISACA, Análisis de los Enfoques de Auditoría proactivo y reactivo.

2. PLANEACION ANUAL DE AUDITORIA DE SISTEMAS, BASADA EN VALORACION DE LA EXPOSICION A RIESGOS de los procesos de TI y las aplicaciones de computador.

- Definición del Universo de Servicios de TI Auditable en la Empresa.
- Definición del Universo de Categorías de Riesgos que podrían afectar negativamente las operaciones de Negocio y Servicios de la Empresa a través de la tecnología de información.
- Elaboración y procesamiento de cuestionarios con factores de riesgo para evaluar exposición a riesgos de los procesos de TI y las aplicaciones de computador en producción.
- Taller 1: Planeación de la Auditoría a los procesos de Control General de TI.
- Taller 2: Planeación de la Auditoría de Aplicaciones.

3. MARCO DE REFERENCIA PARA EL DESARROLLO DE AUDITORIAS DE SISTEMAS "BASADAS EN RIESGOS CRITICOS".

- Fases y Etapas de la metodología de Auditoría de Sistemas basada en Riesgos Críticos.
- Productos entregables de cada etapa de la metodología.

DIA 2.

4. METODOLOGIA DE DESARROLLO DE LA AUDITORIA – PARTE 1: PLANEACIÓN BASADA EN RIESGOS.

- Memorando de planeación, comprensión del proceso o sistema objeto de la Auditoría, identificación y análisis de la muestra de riesgos inherentes para los cuales se evaluará el control interno y se ejecutaran pruebas de auditoría.
- Taller 3: Identificación de Riesgos Inherentes para áreas de Controles Generales de TI.
- Taller 4: Análisis y Evaluación de la Severidad de los riesgos inherentes para áreas de Controles Generales de TI.

5. METODOLOGIA DE DESARROLLO DE LA AUDITORIA – PARTE 2: EVALUACIÓN DEL DISEÑO Y EFECTIVIDAD DE LOS CONTROLES ESTABLECIDOS.

- Conceptos sobre controles, tipos de controles y alternativas utilizadas por los Auditores para evaluar la efectividad del sistema de control interno.
- El Enfoque Proactivo / preventivo de los controles.
- Cómo Identificar y documentar los controles establecidos en la organización para reducir la severidad de los riesgos inherentes.
- Criterios para evaluar la el diseño y la efectividad de los controles establecidos.
- Taller 4: Evaluación de controles por eventos de riesgo críticos, para áreas de Controles Generales de TI.

6. **METODOLOGIA DE DESARROLLO DE LA AUDITORIA – PARTE 3: DISEÑO Y EJECUCIÓN DE PRUEBAS DE AUDITORIA.**

- Diseño, planeación y ejecución de Pruebas de Cumplimiento y sustantivas con base en los resultados de la evaluación del control interno por eventos de riesgo.
- Taller 5: Diseño de Pruebas de cumplimiento y sustantivas, para áreas de Controles Generales de TI.

DIA 3.

7. **METODOLOGIA DE DESARROLLO DE LA AUDITORIA – PARTE 4: AUDITORIA DE APLICACIONES DE COMPUTADOR EN PRODUCCION, BASADA EN RIESGOS CRITICOS.**
   - Planeación detallada de la Auditoría (objetivos, alcance, puntos de interés, asignación de recursos).
   - Comprensión (Caracterización) del ambiente técnico, administrativo y operativo de la Aplicación sujeta a auditoría.
   - Taller 6: Identificación, análisis y Evaluación de Riesgos inherentes (eventos de riesgo negativos) a considerar por la auditoria.
   - Taller 7: Evaluación del diseño y Efectividad del control interno existente para los eventos de riesgo negativos.
   - Taller 8: elaboración del informe de la Auditoría con los resultados de la evaluación de controles.
   - Diseño, planeación y ejecución de Pruebas de Cumplimiento y sustantivas con base en los resultados de la evaluación de control interno por eventos de riesgo negativos (amenazas).

8. **METODOLOGIA DE DESARROLLO DE LA AUDITORIA - PARTE 5: PAPELES DE TRABAJO DE LA AUDITORÍA DE SISTEMAS.**
   - Criterios y procedimientos para elaboración y conservación de los papeles de trabajo.
   - Archivos permanentes (forma y contenido).
   - Archivos Corrientes (Forma y Contenido).

9. **METODOLOGIA DE DESARROLLO DE LA AUDITORIA – PARTE 6: INFORMES DE AUDITORIA DE SISTEMAS**.
   - Importancia de las comunicaciones eficaces en Auditoria.
   - Criterios y procedimientos para redactar informes de auditoría eficaces.
   - Taller 9: Redacción de Informes de Auditoria de Sistemas .

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores y desarrollo progresivo de talleres preparados para ejecutar las etapas de la metodología de auditoría de Tecnología de información basada en riesgos.

5. MATERIAL PARA LOS PARTICIPANTES

Se entregará material escrito en medio magnético con las ayudas utilizadas por los expositores, los casos de estudio y talleres.

6. CERTIFICACIÓN DE APROBACIÓN Ó ASISTENCIA

A los participantes que participen en el 80% o más de las sesiones del seminario se entregará certificación de asistencia.

7. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- **Obligatorios**: Conocimientos básicos de Sistemas de Información y metodologías de gestión de riesgos.

- **Deseables:** Llevar un computador portátil (Windows,32 MB en RAM, 60MB en disco duro y unidad de entrada para acceder a los materiales de trabajo, casos de estudio y realizar los talleres.

8. INSTRUCTORES

Euclides Cubillos M. – **Gerente de Auditoría / Consultoría de AUDISIS**., Ingeniero de Sistemas. Maestría en Dirección y Administración de Empresas. Título de Posgrado en Auditoría de Sistemas, Certificaciones CISA (Certified Information Systems Auditor), COBIT, Auditor ISO 27001, Auditor Líder de Calidad. Experto en Gestión de Riesgos, Seguridad y Auditoría de sistemas. Autor de dos herramientas de software para asistir las actividades de gestión de riesgos y auditoría: CONTROLRISK (Gestión integral de riesgos y diseño de controles) y AUDIRISK (Auditoria basada en riesgos para procesos y sistemas de información). 35 años de experiencia profesional. Ex presidente de la Asociación Colombiana de Auditores de Sistemas (ACDAS) y fundador y ex presidente del ISACA Capítulo de Bogotá. Fue fundador y Director de la Especialización en Auditoría de Sistemas de la Universidad Católica de Colombia y catedrático en Postgrados de Auditoría y Revisoría Fiscal en las Universidades Nacional de Colombia, América, Central de Bogotá, Antonio Nariño, El Rosario, Santo Tomás de Aquino (Bucaramanga), Universidad Militar, UNAB, FUNDEMA (Manizales), Santiago de Cali, Libre de Colombia (Bogotá y Cali), Jorge Tadeo Lozano y Corporación Universitaria de la Costa (Barranquilla). Autor de varias publicaciones sobre Controles y Auditoría de Sistemas. Ha sido conferencista invitado a las Jornadas de ISACA y al LATINCACS de México.

Alvaro Mauricio Romero -Lead Auditor BS ISO/IEC 27001:2013 -Certified Ethical Hacking CEH Profesional experto en Tecnología y Seguridad de la información con certificaciones como auditor líder BS ISO/IEC 27001:2013 Information Security Management System otorgada por el BSI British Standards Management System, CEH (Certified Ethical Hacker & Countermeasures) otorgada por el organismo internacional ECCOUNCIL y en proceso de certificación como profesional de continuidad del negocio CBCP, CISSP (Certified Information Systems Security Professional) y auditor interno norma ISO 9001 versión 2000. Cuenta con más de 20 años de experiencia en administración y auditoria de plataformas de Tecnología y seguridad informática en entidades financieras nacionales e internacionales. Ha participado en la gerencia de proyectos relacionados con el Diseño, implementación y administración de Sistemas de Gestión de Seguridad de la Información, Sistemas de gestión de Riesgos, Planes de Continuidad de Negocios y Recuperación ante desastres, auditorias basadas en riesgos, pruebas de ethical hacking y análisis de vulnerabilidades en Organizaciones nacionales e internacionales del sector servicios y financiero.
Por más de 15 años docente en Seminarios, diplomados y especializaciones de Seguridad Informática y análisis forense informático en varias Universidades y empresas como la Pontificia Universidad Javeriana, Universidad Manuela Beltrán, Universidad Autónoma, Universidad Piloto, Universidad Militar Nueva Granada y la Escuela de Comunicaciones del Ejercito ESCOM.

9. PROCEDIMIENTO DE INSCRIPCIÓN

Descargar de la página **http://www.audisis.com/FormularioSeminariosAUDISIS.docx** el formulario de inscripción, diligenciarlo y enviar a AUDISIS al correo **audisis@audisis.com**.

10. FECHAS, LUGAR Y DURACIÓN

LUGAR: Bogotá, D.C. - GHL Hotel Capital

FECHA: Abril 24, 25 y 26 de 2019.

Octubre 1, 2 y 3 de 2019.

DURACIÓN: 24 Horas.

HORARIO: De 8:00 AM a 12:00 M y de 1:00 PM a 5:00 PM.

11. FORMA DE PAGO

En cheque a nombre de AUDISIS o transferencia de fondos a la cuenta corriente número **07511792-9** del Banco de Bogotá. Sucursal Galerías.

12. VALOR INVERSIÓN POR PARTICIPANTE

Pagos antes del Seminario	Pagos **después del Seminario**
COL $ 1.450.000 + IVA	$ 1.515.000 + IVA

Descuentos por Participantes de la misma Empresa	
3 Participantes	5 %
4 y 5 Participantes	7.5 %
Más de 6 Participantes	10 %

Miembros de ISACA y DEL IIA: Descuento del 5%

13. PLAZO PARA ANULAR LAS INSCRIPCIONES

Se acepta anulación de inscripciones por escrito, hasta 4 días hábiles antes de la realización del seminario. Después de esta fecha, únicamente se aceptará el cambio de participantes inscritos.

14. PLAZO PARA CANCELAR LA REALIZACIÓN DEL SEMINARIO

AUDISIS se reserva el derecho de cancelar el seminario en caso de no completarse el número mínimo de participantes requerido.

15. EL SEMINARIO DENTRO DE SU EMPRESA

Ofrecemos la posibilidad de desarrollar el seminario para grupos de funcionarios de su empresa, en sus instalaciones o en el sitio que la empresa seleccione.

Contáctenos: audisis@audisis.com
Tels: (571) 2556717- **PBX:** (571) 3470022 (571) 3099764

16. NUESTROS PRODUCTOS Y SERVICIOS PROFESIONALES

NUESTROS SERVICIOS

AUDISIS presta sus servicios profesionales con un enfoque PROACTIVO y PREVENTIVO, orientado a LA PREVENCION DE RIESGOS CRITICOS y la implantación de la cultura de AUTOCONTROL. De esta manera ayuda a modernizar el control interno y la auditoría de los servicios y productos de las empresas.

El enfoque preventivo de nuestros servicios se transfiere a nuestros clientes a través de todos nuestros servicios y productos, buscando siempre la modernización de la cultura de control, el establecimiento de una sólida conciencia de seguridad y la creación de una actitud positiva en los empleados, como base para emprender la transición hacia el autocontrol y el mejoramiento continuo de la calidad.

1. CONSULTORÍA EN CONTROL INTERNO, GESTION DE RIESGOS EMPRESARIALES Y SEGURIDAD EN TECNOLOGIA DE LA INFORMACION (TI).

- Implantación de Sistemas de Control Interno (COBIT, MECI, COSO).
- Implantación de Gestión de Seguridad de la Información (ISO 27001).
- Implantación de Gestión de Riesgos empresariales con base en ISO 31000:2009 (SARO, SARLAFT, Salud y otros).
- Implantación de Planes de Continuidad del Negocio y de Tecnología de Información (ISO 22301).
- Diseño de controles para Sistemas de Información y Procesos de negocio.
- Prevención, detección e investigación de fraudes y delitos informáticos. D
- Desarrollo de programas Antifraude.

2. AUDITORÍAS DE SISTEMAS Y DE PROCESOS DEL NEGOCIO.

- Auditorías de Sistemas de Información "Basada en Riesgos Críticos".
- Pruebas de Hacking Ético.
- Auditoría Forense.
- Auditoría Basada en Riesgos críticos a procesos de Negocio.

3. OUTSOURCING DE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN PARA AUDITORIAS INTERNAS, REVISORIAS FISCALES U AUDITORIAS FINANCIERAS.

4. AUTOMATIZACIÓN DE PRUEBAS DE AUDITORÍA A LA MEDIDA DE LAS NECESIDADES DE LA EMPRESA (Desarrollo de CAATs e implementación).

5. INTERVENTORIA EN PROYECTOS DE SISTEMAS, SEGURIDAD Y AUDITORÍA DE SISTEMAS

6. PERITAZGOS EN LITIGIOS DE CONTRATOS DE SERVICIOS PROFESIONALES EN TECNOLOGÍA DE INFORMACIÓN.

7. EDUCACIÓN Y DESARROLLO PROFESIONAL EN CONTROL INTERNO, ADMINISTRACIÓN DE RIESGOS, SEGURIDAD DE TI Y AUDITORÍA DE SISTEMAS.

NUESTROS PRODUCTOS

- Seminarios abiertos virtuales para para participantes de diferentes empresas.
- Seminarios cerrados presenciales o virtuales, dentro de las empresas.

- **AUDIRISK:** Software de Auditoría Basada en Riesgos críticos para Procesos de Negocio, Sistemas y Tecnología de Información.

- **AUDIT IP:** Software de Gestionar el seguimiento a Planes de Mejoramiento Institucional.

- **CONTROLRISK:** Software de Gestión de Riesgos y Diseño de Controles para Procesos de Negocio, Sistemas y Tecnología de Información**.**

- **IDEA**: Software para Análisis, Extracción, Auditoría de Datos y Desarrollo de CAATTs.

- **WORKING PAPERS:** Software de Papeles de Trabajo de Auditoria Financiera.

- **MONITOR:** Software de Monitoreo Continuo y Auditoría Continua de Riesgos y Controles.