

Seminario – Taller Virtual PLANEACION ANUAL DE LA AUDITORIA INTERNA Y DE SISTEMAS BASADA EN RIESGOS.

Contenido:	Pág
Presentación	1
Propuesta de Valor	2
1. A quién va dirigido	2
2. Objetivos	2
3. Temas del Seminario	3
4. Metodología	4
5. Material para los Participantes	4
6. Certificación	4
7. Requisitos	4
8. Instructores	4
9. Procedimiento de Inscripción	5
10. Fechas y duración	5
11. Forma de pago	5
12. Valor Inversión	6
13. Plazo para Anular Inscripciones	6
14. Plazo para cancelar realización del seminario	6
15. El seminario dentro de su empresa	6
16. Nuestros Servicios Profesionales y Productos	7

PRESENTACIÓN

Este seminario presentará los fundamentos teórico – prácticos para elaborar el PLAN ANUAL DE LA AUDITORÍA INTERNA, con base en la estimación de la exposición a riesgos potenciales de los ítems del universo de auditoría interna y de conformidad con los Estándares y Normas para el ejercicio profesional de la Auditoría Interna, promulgadas por el Instituto de Auditores Internos e ISACA.



El seminario presentará alternativas y procedimientos para estimar las necesidades de seguridad de cada ente auditable, **en los tres (3) componentes del Universo Auditable de la Auditoría Interna:** a) los procesos de la cadena de valor; b) los procesos de la infraestructura de servicios de Sistemas; y c) las aplicaciones de computador que soportan los procesos del core del negocio y administrativos de la empresa.

También presentará procedimientos para valorar, por cada ente auditable, la exposición a las siete (7) categorías o clases de riesgo operativo y generar *Panoramas de Riesgo* que indican las *clases de riesgo* sobre las cuales se deberá enfatizar el desarrollo de los trabajos de auditoría por cada ente auditable que se seleccione para el plan anual de la Auditoría Interna.

Paralelamente con el desarrollo de los conceptos mencionados, se realizarán ejercicios para aplicar los conceptos y desarrollar habilidades para elaborar el plan anual de la Auditoría Interna.

PROPUESTA DE VALOR

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

- Aplicar criterios y procedimientos para estimar y expresar porcentualmente las necesidades de seguridad de los entes auditables que componen el Universo Auditable de la Auditoría Interna.
- Aplicar criterios y procedimientos para estimar y expresar porcentualmente la exposición de los entes auditables a las categorías o clases de riesgo que representen el Universo de Riesgos aplicables a la Empresa.
- Elaborar la matriz de Planeación Anual de la Auditoría con los entes auditables priorizados según su exposición a riesgos, por componente del universo de auditoría.
- Definir y programar la ejecución de los trabajos de auditoría a realizar en el año, por cada ente auditable, basados en riesgos críticos.
- Identificar y justificar las necesidades de personal y recursos de tiempo y tecnológicos requeridos para desarrollar el plan anual de la auditoría basado en riesgos críticos.
- Presentar y sustentar el Plan Anual de Auditoría a la Gerencia y el Comité de Auditoría.

1. A QUIENES VA DIRIGIDO?

Este seminario está dirigido a Directivos de Auditoría Interna, Jefes de Control Interno de Entidades del Sector Público, Auditores de Sistemas, Auditores Externos, Revisores Fiscales, Funcionarios de Contralorías de empresas públicas y privadas y Auditores de Sistemas de Gestión (ISO 9001, ISO 27001, etc) .



2. OBJETIVOS DEL SEMINARIO

- Presentar y analizar la metodología para elaborar el PLAN ANUAL DE AUDITORÍA INTERNA basado en la estimación de las necesidades de seguridad y la exposición a riesgos operacionales de los entes auditables.
- Presentar y analizar el uso de las Matrices de Riesgo Operativo de la Empresa para estimar las necesidades de seguridad de los entes auditables que componen el Universo de Auditoría.
- Desarrollar habilidades en los participantes para aplicar los conceptos de seguridad, riesgos y exposición a riesgos en la elaboración del Plan Anual de Auditoría Interna.

3. TEMAS DEL SEMINARIO

1. Normas de Auditoria relativas planeación anual de las auditorías internas y de Sistemas basada en riesgos
 2. Uso de la matriz de riesgos de la empresa para elaborar el plan anual de auditoría interna.
 3. Identificación del Universo de Entes Auditables para la Auditoría Interna.
 4. Identificación Universo de clases o categorías de Riesgo Aplicables.
 5. Criterios y Factores a considerar para valorar la Exposición a Riesgos en los Entes Auditables.
 6. Procedimientos para elaborar el plan anual de auditoría basado en riesgos.
- Cómo medir (estimar) la Seguridad Requerida / Exposición a Riesgos de los Entes Auditables, basándose en las Matrices de Riesgos de la Empresa.
 - Diseño de cuestionarios de Factores de Riesgo para evaluar las necesidades de Seguridad (Exposición a Riesgos) por Componente del Universo de Auditoría y Ente Auditable.
 - Cómo medir la Exposición de los Entes Auditables a las siete (7) Clases de Riesgo Operativo.
 - Aplicación y procesamiento de cuestionarios para valorar exposición a las clases de riesgo operativo, por Componente del Universo de Auditoría y entes auditables.
 - Elaboración de Matriz de Planeación Anual por Componentes Universo de Auditoría - Seguridad Requerida de los entes auditables Vs. Exposición a Riesgos a Riesgos Operativos -
 - Priorización de Entes Auditables según necesidades de Seguridad, por Componentes del Universo Auditable.
 - Elaboración de Matriz de Exposición a Riesgos Operativos por Componente del Universo Auditable - Clases de Riesgo Operativo Vs Entes Auditables.
 - Priorización de Clases de Riesgo operativo por Entes Auditables y Componente del Universo de Auditoría..
 - Selección de Entes Auditables para elaborar el Plan Anual de Auditoría.
 - Selección y programación de Trabajos de Auditoría a realizar durante el año, por Ente Auditable.
 - Definición de objetivos, alcance y recursos requeridos para el desarrollo de los trabajos del Plan Anual de la Auditoría.
 - Elaboración de Cronograma para el desarrollo del Plan Anual de Auditoría.
 - Presentación del Plan Anual de Auditoría a la Gerencia y el Comité de Auditoría.

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

El seminario está estructurado en la modalidad de Taller y se desarrollará de manera interactiva entre el instructor y los participantes, con presentaciones de los temas por parte del instructor y descripción de casos y experiencias del mundo real.

Los talleres del seminario se desarrollarán alrededor de la implantación del Sistema de Administración de Riesgos para un proceso del modelo de operación de la Empresa. Eliminar este párrafo.

Se realizarán también ejercicios para afianzar los conceptos y desarrollar habilidades para aplicarlos utilizando y formatos diseñados para el uso de la metodología.

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 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

Deseables: Conocimientos básicos de auditoría, riesgos y controles.

Disponibilidad de un computador portátil para instalar los casos de estudio y realizar los talleres.

8. DIRECTOR E INSTRUCTORES.

El seminario será dirigido por Euclides Cubillos Moreno, socio director de AUDISIS y desarrollado por expertos en los temas del seminario.

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 (Auditoría 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 auditoría 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, auditorías 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 Ejército ESCOM.

9. PROCEDIMIENTO DE INSCRIPCIÓN

Descargar de la página <http://www.audisis.com/FormularioSeminariosAUDISIS.docx> el formulario de inscripción,

10. FECHAS Y DURACIÓN

FECHAS: Julio 26 y 27 del 2023

DURACIÓN: 16 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

VALOR SEMINARIO VIRTUAL

Pagos antes del Seminario	Pagos después del Seminario
COL \$ 1.000.000 + IVA	COL \$ 1.067.000 + IVA

Descuentos por Inscripción.	
Clientes de servicios y productos de AUDISIS	5%
Tres o más inscritos de la misma empresa	7.5%
Miembros de ISACA e IIA	5%

13. PLAZO PARA ANULAR LAS INSCRIPCIONES

La anulación de inscripciones solo se aceptará por escrito, hasta cinco (5) días calendario antes de la realización del seminario. Después de este plazo, solamente se aceptará cambio de las

14. PLAZO PARA CANCELAR LA REALIZACIÓN DEL SEMINARIO

La realización del seminario estará sujeto a la inscripción de un número mínimo de participantes. Cuando este número no se obtenga, AUDISIS informará con anticipación de 3 días hábiles la no realización o aplazamiento del seminario.

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

Celular: 3173638828



16. NUESTROS PRODUCTOS Y SERVICIOS PROFESIONALES

NUESTROS SERVICIOS

AUDISIS presta sus servicios profesionales con un enfoque PROACTIVO y PREVENTIVO, orientado a LA PREVENCIÓN DE RIESGOS CRÍTICOS 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, el mejoramiento continuo de la calidad, de la seguridad y el control interno.

1. CONSULTORÍA EN CONTROL INTERNO, GESTIÓN DE RIESGOS EMPRESARIALES Y SEGURIDAD EN TECNOLOGÍA DE LA INFORMACIÓN (TI)

- Implantación de Sistemas de Control Interno (COBIT, MECI, COSO).
- Implantación del sistema de Gestión de Seguridad de la Información (ISO 27001).
- Implantación de sistemas de Gestión de Riesgos Empresariales con base en ISO 31000 (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.
- Consultoría en Gestión de Riesgos de Ciberseguridad.
- Evaluación Arquitectura de Seguridad en TI.

2. AUDITORÍAS DE SISTEMAS Y DE PROCESOS DE NEGOCIO.

- Auditorías de Sistemas de Información "Basadas en Riesgos Críticos".
- Pruebas de Hacking Ético.
- Análisis Forense digital.
- Auditorías a procesos de Negocio Basadas en Riesgos críticos.
- Auditoría a sistemas de Gestión de riesgos (SARO, SARLAFT, financieros, otros).
- Auditoría al proceso de Gobierno Corporativo.
- Consultoría para implementar la Auditoría de sistemas.
- Auditoría a la Gestión de Riesgos de Ciberseguridad.

3. OUTSOURCING DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA AUDITORÍAS INTERNAS, REVISORÍAS FISCALES Y AUDITORÍAS FINANCIERAS.

Servicios ofertados por anualidad.

4. OUTSOURCING DE SEGURIDAD DE LA INFORMACIÓN (CISO), DE CONFORMIDAD CON ISO 27000.

Servicio por contrato anual.

5. DESARROLLO Y EJECUCIÓN DE TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAATS) UTILIZANDO EL SOFTWARE IDEA.

Por demanda y por anualidad.

6. AUTOMATIZACIÓN DE FUNCIONES DE ANÁLISIS DE DATOS (DATA ANALYTICS) Y GENERACIÓN DE REPORTES ADMINISTRATIVOS, UTILIZANDO EL SOFTWARE IDEA.

Por demanda o contrato anual.

7. INTERVENTORÍA A CONTRATOS DE DESARROLLO DE SISTEMAS, SEGURIDAD DE TI Y AUDITORÍA DE SISTEMAS.

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

9. EDUCACIÓN Y DESARROLLO PROFESIONAL EN CONTROL INTERNO, ADMINISTRACIÓN DE RIESGOS, SEGURIDAD DE TI Y AUDITORÍA DE SISTEMAS. MODALIDAD VIRTUAL Y PRESENCIAL.

Tenemos disponibles numerosos cursos y seminarios, para ser desarrollados "In Company" o abiertos para personas de diferentes empresas.

NUESTROS PRODUCTOS

• AUDIRISK WEB: Software de Auditoría Interna y de Sistemas "Basada en Riesgos"

Es un software en tecnología WEB (Cloud Computing) diseñado para conducir las siguientes actividades de Auditoría, de conformidad con normas de Auditoría de aceptación general y con estándares del IIA e ISACA:

- a) Elaborar el Plan Anual de la Auditoría, basado en la "Valoración de la exposición a Riesgos" de los componentes del Universo de posibles trabajos de Auditoría interna.
- b) Desarrollo de Auditorías "Basada en Riesgos Críticos" a procesos de negocio y sistemas de información con un enfoque **Proactivo** y **Preventivo**.
- c) Seguimiento a Hallazgos de Auditoría.
- d) Generar informes con Indicadores de Gestión de la Auditoría Interna y control de Calidad, según Noma 1300 del IIA.

- **AUDIT IP: Aplicación Web para seguimiento de Hallazgos de Auditoria.**

Planeación y Ejecución del Seguimiento a planes de Mejoramiento que se elaboran para atender hallazgos y recomendaciones de auditorías efectuadas por terceros y para terceros.

Provee dos tipos de perfiles de usuario:

- Coordinadores del Plan de Mejoramiento (Auditores)
- Implantadores del Plan de Mejoramiento (Auditados)

- **CONTROLRISK WEB: Software para Administración Integral de Riesgos Empresariales.**

Es un software en Tecnología Web (Cloud Computing), para conducir con enfoque preventivo y proactivo, la implantación de diferentes componentes (subsistemas) del Sistema Integral de Administración de Riesgos Empresariales y soportar su evolución y mejoramiento continuo (ciclo PHVA), de acuerdo con las buenas y mejores prácticas de Administración de Riesgos, la norma ISO 31000 y el marco de referencia ERM (Enterprise Risk Management).

Soporta la gestión de ocho (8) Subsistemas de gestión de riesgos (SARO, SARLAFT, Riesgos Financieros y otros) y provee tres tipos de perfiles de usuario **Administradores de Riesgo, Dueños de Procesos y Auditores.**

- **ASD AUDITOR:**

Es una poderosa herramienta Auditoría Financiera y análisis financiero, de origen Español, que permite trabajar y dirigir de forma ordenada, eficiente y ágil el proceso de auditoría desde las actividades previas hasta la finalización y emisión del correspondiente informe. Las auditorías con ASD Auditor se desarrollan de acuerdo con las NIAs, en base a riesgos y en los requerimientos de Control de Calidad NICC1.

ASD AUDITOR, también provee soporte al análisis financiero de la organización, realizando de forma automática el cálculo y preparación de las cuentas anuales (Balance, cuenta de pérdidas y ganancias y estado de flujo de efectivo) gracias a su sistema de importación de archivos contables y extracontables.

- **IDEA (Interactive Data Extraction and Analysis):**

Es una poderosa herramienta para análisis, Extracción y Auditoría de datos, contenidos en Archivos de Computador (bases de datos relacionales) y en formatos txt, cvs, pdf, prn; que provee funcionalidades para aplicar numerosas "buenas y mejores prácticas de Auditoría Universalmente aceptadas" para Auditorías Internas, Financieras y Revisoría Fiscal. También es útil para automatizar el análisis de datos, pruebas de auditoría y generación de reportes para SARLAFT.

IDEA es un software líder en el mundo para análisis y extracción de datos que permite desarrollar, implementar y automatizar CAATs (Técnicas de Auditoría Asistidas por Computador) a la medida de las necesidades de la Auditoría.

(*) Smart Analyzer Financial:

Es un complemento de IDEA, ofrece una recopilación de pruebas de auditoría financiera y reportes básicos que pueden ser utilizados por cualquier auditor con un mínimo de entrenamiento sobre archivos del balance general, inventarios, activos, cuentas por cobrar y cuentas por pagar. Software complemento y compatible con IDEA.

SmartAnalyzer es una herramienta poderosa, sin importar si es un auditor experimentado o un usuario novato. Al trabajar con SmartAnalyzer se beneficiará al contar con la forma más eficiente para ejecutar un análisis de datos. Las pruebas de auditoría predefinidas y de calidad comprobada le ayudarán a ahorrar tiempo, ya que no tiene que definir sus propias pruebas desde cero.

(*) SmartExporter®:

Es una solución de software que le permite acceder de forma fácil y flexible a todos los datos relevantes de un sistema SAP®. Gracias a SmartExporter®, los usuarios pueden extraer ellos mismos los datos de SAP® que necesitan mientras el departamento de TI conserva el control de los datos y de los derechos de acceso. Software compatible con IDEA.

Con el modo en línea, el usuario está conectado al sistema SAP®, por lo que puede extraer los datos directamente o si lo prefiere puede programar la extracción de los datos para una hora no pico, por ejemplo, durante la noche o los fines de semana.

SmartExporter® es una de las primeras aplicaciones del mundo en recibir una certificación ABAP para SAP® NetWeaver® ejecutado sobre HANA.

(*) Requiere tener instalado el Software IDEA.