

TÉCNICAS Y HERRAMIENTAS DE AUDITORÍA ASISTIDA POR COMPUTADOR (CAATTS).

Alineado con la NIA 1009 y Normas de IIA e ISACA

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

PRESENTACIÓN

El uso del computador como herramienta de auditoría ya no es una opción, es una necesidad incuestionable para incrementar la productividad, eficiencia y valor agregado de las auditorías, principalmente en las modalidades de auditorías internas, de estados financieros, de sistemas de información y forenses.

Las Tecnologías de Información y comunicaciones (TICs), al tiempo que plantean retos a los auditores (internos, externos y Revisores Fiscales) para evaluar el control interno y verificar la integridad de la información de las empresas, ofrecen oportunidades para realizar trabajos de auditoría más eficientes y eficaces e incrementar la productividad de los auditores, mediante el uso de Técnicas de Auditoría Asistidas por Computador (CAATs).



Según NIA 1009, las CAATs son programas y datos de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes contenidos en los sistemas de información de una entidad. Los datos pueden ser transacciones sobre las que el auditor desea realizar pruebas de controles o procedimientos sustantivos, o pueden ser otros tipos de datos.

Algunos ejemplos de CAATs que los auditores deberían tener disponibles y reutilizar frecuentemente en sus revisiones son los siguientes: a) Comprobación de cálculos efectuados por las aplicaciones de computador de la empresa (también denominada simulación paralela) para operaciones de facturación, liquidación de intereses y cuotas de capital, causaciones, provisiones, indicadores de gestión, etc); b) validar cumplimiento de reglas del negocio; c) extraer muestras estadísticamente validas de transacciones o de registros de cuentas por cobrar y por pagar ; d) para fines de planeación de la auditoría de procesos, clasificar y analizar la información de archivos de computador por rangos de valor (por ejemplo clasificación de la cartera por edades, estratificación de la información de compras y de contratos); e) Generar estadísticas de información de los archivos de computador por campos tipo fecha, numéricos y hora; f) generar alertas sobre situaciones sospechosas de fraude; y otras funciones orientadas a detección de excepciones a políticas e inconsistencias en los archivos de computador de la empresa.

PROPUESTA DE VALOR.

Al finalizar el seminario los participantes estarán en capacidad de:

- a) Planear el desarrollo o la adquisición de software de auditoría.
- b) Definir e implantar los CAATs que se utilizarán en las auditorías de estados financieros.
- c) Diseñar e implantar CAATs para apoyar la elaboración del Plan Anual de Auditoría Interna basada en riesgos.
- d) Definir e implantar CAATs que se utilizarán en la ejecución de auditorías internas y de aseguramiento a los procesos del modelo de operación de la empresa y las aplicaciones de computador (o módulos de ERPs) que soportan las operaciones de negocio y administrativas de la empresa.
- e) Definir e implantar CAATs que se utilizarán en la ejecución de auditorías a Controles Generales en la infraestructura de TI y de Controles Específicos en las aplicaciones de Computador.

Este seminario presentará una visión general sobre las CAATs y la oportunidad de conocer y ampliar sus conocimientos sobre *herramientas de software disponibles en el mercado* para evaluar y verificar los controles internos, revisar la seguridad en el ambiente de las TICs (por ejemplo, análisis de vulnerabilidades a través de pruebas de Ethical Hacking) y verificar la integridad de la información contable y financiera de las empresas que reside en grandes Bases de Datos y archivos de computador, a través “Auditorías basadas en datos”, análisis foren-

1. OBJETIVOS DEL SEMINARIO

- Transferir conocimientos sobre técnicas de auditoría asistidas con el Computador (CAATs) aplicables a las auditorías internas y de estados financieros, de acuerdo con normas de auditoría generalmente aceptadas, las NIAs, los estándares del IIA aplicables a las Auditorías Internas y los estándares de ISA-CA aplicables a la auditorías de Sistemas de Información.
- Presentar y analizar alternativas para planear e implantar el uso constante y reutilizable de CAATs en las auditorías, como requisito para mejorar la productividad y calidad de las auditorías internas y externas.
- Desarrollar habilidades en los auditores para planear, diseñar y ejecutar la función de auditoría apoyándose en técnicas y herramientas asistidas por computador (CAATs).

2. A QUIÉN VA DIRIGIDO (PARTICIPANTES)



A personal de auditorías internas, auditorías externas, auditores de sistemas y Revisores Fiscales

3. TEMAS DEL SEMINARIO

DIA 1.

1. **Objetivos y Beneficios de las CAATs.**
2. **Normas de Auditoría que se refieren al uso de CAATs en las auditorías.**

- Normas Internacionales de Auditoría (NIAs).
- Normas aplicables a las Auditorías Internas según estándares del IIA.
- Normas aplicables a las Auditorías de TI según estándares de ISACA.

3. CAATs MÁS USUALES.

- Para Planeación de la Auditoría.
- Para verificar la operación de los controles establecidos en los programas de las aplicaciones de computador
- Para verificar la exactitud de los datos de los archivos y bases de datos.
- Para verificar el cumplimiento de las políticas y reglas de control de acceso a los datos y los programas.
- Para verificar el licenciamiento del software y el inventario de software.
- Para verificar la seguridad en las redes de computadores.

DIA 2.

4. ANALISIS DE ALTERNATIVAS PARA SATISFACER LAS NECESIDADES DE CAATs.

- Software generalizado de auditoría (paquetes).
 - Desarrollo de software a la medida de las necesidades de la empresa.
 - Utilización del software del sistema (Utilitarios, software y funciones del sistema).
 - Uso de herramientas comerciales de seguridad y análisis forense informático.
 - Criterios para seleccionar herramientas de Análisis y Extracción de Datos para Auditoría.
 - Características de las herramientas de Software de Auditoría disponible en el mercado.
5. **Taller 1:** Planeación de la Auditoría Interna Basada en Valoración de la Exposición a Riesgos, utilizando hojas electrónicas.
 6. **Taller 2:** Definición y uso de CAATs para auditar Cuentas por Cobrar, utilizando el software IDEA.
 7. Taller 3: Definición de CAATs para auditar la Aplicación de NOMINA, utilizando el software IDEA.

DIA 3.

8. **Taller 4:** CAATs para realizar Muestreo Estadístico en Auditoría, utilizando el software IDEA.
9. **Análisis de Vulnerabilidades y Pruebas de Ethical Hacking:** Ataques típicos a los recursos de computador. Planeación, ejecución y evaluación de resultados de las pruebas. Informe con los resultados de las pruebas. Herramientas disponibles para análisis de vulnerabilidad y evaluación de la seguridad en Redes.
10. **Análisis Forense Informático:** Introducción a la informática Forense y la evidencia digital. Planeación, ejecución y evaluación del análisis forense. Informe con los resultados del Análisis.

4. METODOLOGÍA

Presentación de los temas por parte de los instructores utilizando diapositivas, el desarrollo de talleres utilizando microcomputadores y el software IDEA para análisis y extracción de datos.

5. MATERIAL PARA LOS PARTICIPANTES

Antes de iniciar el seminario, los participantes recibirán material escrito en medio magnético. Se entregará material escrito en medio magnético con las ideas claves del seminario, los textos de los talleres, formatos para el diseño de pruebas de auditoría asistidas por computador y la versión demostrativa



6. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- Conocimientos o experiencia en auditoría financiera, operativa, de gestión o de sistemas.
- Conocimientos básicos de software de microcomputadores (Windows, MS-office).
- Los participantes deberán tener disponible 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.

7. CERTIFICACIÓN DE ASISTENCIA

A los participantes que asistan al 80% o más del seminario se entregará certificado de asistencia.

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 (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, 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. – Consultor Seguridad Informática y análisis forense, AUDISIS. Profesional experto en Tecnología y Seguridad Informática con certificaciones como auditor líder BS ISO/IEC 27001:2005 Information Security Management System otorgada por el BSI British Standards Management System, CEH (Certified Ethical Hacker & Countermeasures), y la plataforma de seguridad de checkpoint, auditor interno ISO 9001 versión 2000. Cuenta con 18 años de experiencia en administración y auditoría de plataformas de Tecnología y seguridad informática en entidades financieras nacionales e internacionales. Experiencia en el diseño, implementación y administración de sistemas de Gestión de Seguridad de la Información y del Plan de Continuidad del Negocio y Recuperación del sistema en multinacionales del sector servicios con sucursales a nivel nacional con más de 1600 Empleados. Ha participado en los Diplomados de Seguridad informática y Análisis forense en las universidades Javeriana, Militar Nueva Granada, Manuela Beltrán, Autónoma y CIDE.

9. FECHAS, DURACIÓN Y HORARIO DEL SEMINARIO

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

FECHAS: Julio 2, 3 y 4 de 2019.

Diciembre 2, 3 y 4 de 2019.

DURACIÓN: 24 Horas

HORARIO: De 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm.

10. 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	
Hasta 3 Participantes	5 %
4 y 5 Participantes	7.5 %
Más de 6 Participantes	10 %

Miembros de ISACA y DEL IIA: Descuento del 5%

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. 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.

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.

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 requeridos.

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: 2556717—2556757—2556816
PBX: 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 y el mejoramiento continuo de la calidad.

1. CONSULTORÍA EN GESTIÓN DE RIESGOS, SEGURIDAD Y CONTROL INTERNO EN PROCESOS DE NEGOCIO Y TECNOLOGÍA DE INFORMACIÓN.

- 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).

- Diseño de controles para Sistemas de Información y Procesos de negocio.
- Prevención, detección e investigación de fraudes y delitos informáticos. 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 INTERNAS DE SISTEMAS DE INFORMACIÓN.

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

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

- Interventoría al diseño y/o estrategias de tecnología.
- Interventoría a la implantación de soluciones de tecnología.
- Interventoría al desarrollo de soluciones de tecnología.
- Interventoría a la gerencia de proyectos de tecnología.

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.

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

NUESTROS PRODUCTOS

- **AUDIRISK:** Software de Auditoría Basada en Riesgos críticos para Procesos de Negocio, Sistemas y Tecnología de Información.
- **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 CAATs.
- **WORKING PAPERS:** Software de Papeles de Trabajo de Auditoria Financiera.
- **MONITOR:** Software de Monitoreo Continuo y Auditoría Continua de Riesgos y Controles.