Seminario – Taller

IDENTIFICACION Y ANALISIS DE RIESGOS PARA AUDITORES

Contenido:	Pág

PRESENTACIÓN

La **identificación y análisis de riesgos inherentes** son actividades críticas en el desarrollo de las Auditorías Basadas en Riesgos, porque establecen una base sólida para evaluar el diseño y efectividad de los controles establecidos y diseñar las pruebas de auditoría que se consideren necesarias y apropiadas, en los procesos de la cadena de valor y los servicios de tecnología de información de la Empresa.

La criticidad de estas actividades se manifiesta cuando los auditores, para desarrollar sus auditorías basadas en riesgos, se apoyan en el contenido de las *matrices o mapas de riesgos existentes en la empresa y éstas presentan deficiencias en el planteamiento de los riesgos, su análisis y los controles establecidos para mitigarlos.*

En el planteamiento de los riesgos inherentes identificados en las matrices, con frecuencia no se utilizan correctamente las expresiones *evento de riesgo negativo, agente generador del riesgo, causas de riesgo y vulnerabilidades.* Como consecuencia, los eventos *de riesgo negativos* se describen como *debilidades de control, carencia de controles o agentes generadores del riesgo.* También es frecuente encontrar ***ambigüedades*** *en la descripción de los riesgos identificados, lo cual* ***dificulta el análisis de los mismos y la selección de los controles para mitigarlos.***

Estas confusiones y deficiencias en la identificación de los riesgos conducen a fallas y grietas en etapas posteriores del proceso de gestión de riesgos, particularmente **en el análisis de riesgos y el diseño de los controles requeridos**. Por consiguiente, estas fallas generan sistemas de gestión de riesgos que algunas veces solo están disponibles para cumplir requerimientos de los organismos de supervisión y control del Estado y **no satisfacen los requerimientos de seguridad de los procesos y de las empresas.**

En la **etapa de Análisis de Riesgos,** como consecuencia de los problemas mencionados y los procedimientos empleados para realizar el análisis, también se presentan fallas y deficiencias. Con frecuencia el análisis individual de los eventos de riesgo identificados, **omite** describir las ***vulnerabilidades*** *(causas o debilidades o deficiencias de control)* que generan el ambiente propicio para que ocurran los riesgos y los ***agentes generadores*** **del riesgo** que pueden explotar las vulnerabilidades para hacer que el riesgo se materialice. Posiblemente se ignora que *"un evento de riesgo se materializa solo cuando existen vulnerabilidades y al menos un agente generador que explote esas vulnerabilidades"*

Finalmente, las deficiencias mencionadas en la identificación y análisis de riesgos, impactan el diseño y efectividad de los controles para mitigarlos, puesto que se carece de materia para definir los requisitos que deben satisfacer los controles: ***estos deben servir para eliminar las vulnerabilidades y/o neutralizar a los agentes generadores del riesgo.*** La importancia de efectuar correctamente las actividades de identificación y análisis de los riesgos, consiste en que éstas etapas producen como entregable *"las medidas del traje denominado* ***Diseño de Controles requeridos*** *para los procesos y servicios de sistemas de las organizaciones".*

Por lo anterior, este seminario - taller se propone presentar los fundamentos para *identificar y analizar correctamente los eventos de riesgo potenciales que podrían presentarse en los procesos y servicios de sistemas de las organizaciones.* También se propone proveer ayudas para elaborar el plan anual de la Auditoría Interna y de Sistemas, *basado en la exposición a riesgos potenciales de cada uno de los ítems o entes auditables que componen el universo auditable.*

PROPUESTA DE VALOR

Al finalizar el seminario los participantes estarán en capacidad de:

a) Identificar eventos de riesgo negativos con expresiones libres de ambigüedades, individualmente para las clases o categorías de riesgo del Sistema de Administración de Riesgos Operacionales (SARO), sistema de administración de lavado de activos y financiación del terrorismo (SARLAFT), y los tipos de riesgos financieros.

b) Realizar análisis cualitativo y cuantitativo de los eventos de riesgo negativo, utilizando **seis elementos del riesgo**: Activos impactados, vulnerabilidades, agentes generadores del riesgo, factor de exposición al riesgo, frecuencia anual de ocurrencia (FAO) y pérdida anual estimada (PAE).

c) Elaborar cuestionarios para evaluar la exposición a riegos potenciales de los items del universo auditable, como base para elaborar el plan anual de auditoria interna y de sistemas basado en la exposición a riesgos.

1. OBJETIVOS DEL SEMINARIO

- Presentar los fundamentos para desarrollar las etapas de identificación y análisis de riesgos, de acuerdo con los estándares ISO 31000 y el marco ERM 2017.

- Sensibilizar a los participantes sobre el uso de procedimientos apropiados para identificar y analizar correctamente los eventos de riesgo negativos en los procesos y los servicios de sistemas de la Empresa.

- Desarrollar habilidades en los participantes para identificar, analizar y documentar correctamente los eventos de riesgo negativos en procesos de la cadena de valor y en el ambiente de Tecnología de Información (TI).

2. A QUIÉN VA DIRIGIDO.

El seminario está dirigido a Auditores Internos, Externos y de Sistemas, funcionarios responsables de implementar Sistemas de Administración del Riesgo en entidades públicas y privadas, personal de seguridad de la información y otros interesados en gestión de riesgos y diseño de controles.

3. TEMAS DEL SEMINARIO

DIA 1: Identificación de Riesgos Inherentes.

- Conceptos de Riesgos y Gestión de Riesgos según ISO 31000 y ERM
- Subsistemas del Sistema de Gestión Integral de Riesgos (SARO, SARLAFT, Crédito, de mercado y otros).
- Requisitos de conocimiento, para identificar y analizar los eventos de riesgos de un proceso o servicio de sistemas.
- Metodología para identificar eventos de riesgo negativos, por clase de riesgo.
- Errores más frecuentes que se presentan en la identificación de riesgos.
- Taller 1: Identificación de eventos de riesgo negativos para las clases de riesgo del SARO.
- Taller 2: Identificación de eventos de riesgo negativos para clases de riesgo del SARLAFT
- Taller 3: Identificación de eventos de riesgo negativos para el sistema de gestión de seguridad de la información (SGSI – ISO 27001).

DIA 2: Análisis de Eventos de Riesgo Inherente.

- Metodología para Analizar los seis (6) elementos del riesgo por cada evento de riesgo negativo.
- Errores más frecuentes que se presentan en el análisis de riesgos.
- Criterios para estimar la frecuencia anual de ocurrencia (FAO) y la probabilidad de ocurrencia de los riesgos.
- Criterios para estimar el impacto de los riesgos.
- Análisis cualitativo de eventos de riesgos negativos .
- Taller 4: Análisis cualitativo de eventos de riesgo.
- Análisis cuantitativo de eventos de riesgos negativos .
- Taller 5: Análisis cuantitativo de eventos de riesgo negativos.
- Mapas de riesgo inherente por proceso y consolidados de la empresa

DÍA 3: Planeación Anual de la Auditoría Interna y de Sistemas, Basada en Riesgos.

- Identificación del Universo Auditable, en Auditoría Interna y de Sistemas.
- Estructura y Diseño de cuestionarios para estimar la exposición a clases de riesgo del SARO, en los procesos de la cadena de valor.
- **Taller 6:** Procesamiento de cuestionarios para estimar exposición a riesgos, en los procesos de la cadena de valor.
- Estructura y Diseño de cuestionarios para estimar la exposición a clases de riesgo del SARO, en el ambiente de Tecnología de Información (TI).
- **Taller 7:** Procesamiento de cuestionarios para estimar exposición a riesgos en los procesos de TI y los Sistemas de Información de Negocios (Aplicaciones de Computador).
- Tipos de Trabajos de auditoría a realizar durante el año.
- Contenido del Plan Anual de Auditoría Interna y de Sistemas

4. METODOLOGÍA.

El seminario está estructurado en la modalidad de Taller y se desarrollará de manera interactiva entre los facilitadores y los participantes, con presentaciones de los temas apoyados en casos y experiencias del mundo real.

Los talleres del seminario se desarrollarán alrededor de la implantación del Sistema de Administración de Riesgos Operacionales (SARO) para un proceso del modelo de operación de la Empresa.

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 medios magnéticos, con las ideas claves del seminario, formatos de la metodología de administración de riesgos y enunciados de los ejercicios y talleres.

6. CERTIFICACIÓN.

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

7. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- Deseable: Conocimientos básicos de riesgos, controles y auditoría.
- Disponibilidad de computadores portátiles 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 Empresariales) y AUDIRISK (Auditoria Interna y de Sistemas basada en riesgos). 40 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 (Bogota 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

9. PROCEDIMIENTO DE INSCRIPCIÓN

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

10. FECHAS Y DURACIÓN

FECHAS: Abril 19, 20 y 21 de 2023.
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

VALOR SEMINARIO VIRTUAL

Pagos antes del Seminario	Pagos después del Semina-
COL $ 1.600.000 + IVA	$ 1.651.400 + IVA

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

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 personas inscritas.

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 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, 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.

- Auditoria a sistemas de Gestión de riesgos (SARO, SARLAFT, financieros, otros).
- Auditoria al proceso de Gobierno Corporativo.
- Consultoría para implementar la Auditoria 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 Auditoria 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 (Enterprice 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.