Seminario – Taller
DISEÑO DE CONTROLES PARA PROCESOS DE NEGOCIO Y SERVICIOS DE TECNOLOGIA DE LA INFORMACION

Contenido:

PRESENTACIÓN

El **enfoque proactivo y preventivo** de los controles debería prevalecer sobre el **enfoque Reactivo o A Posteriori**. Esto significa que los controles deberían diseñarse e implantarse en los procesos y sistemas antes de que ocurran los riesgos, con el propósito de ***eliminar*** las vulnerabilidades que pueden causarlos y/o de **neutralizar** a los agentes generadores que pueden explotar las vulnerabilidades existentes (deficiencias, debilidades de seguridad que crean ambiente propicio para que los riesgos se materialicen) para hacer que los riesgos ocurran

Los controles internos en los procesos, sistemas y proyectos de la Empresa deberían diseñarse e implantarse antes de iniciar su operación, en *las fases de planeación, diseño y construcción,* ***no después***, en la fase de operación, como respuesta a la ocurrencia de errores, irregularidades o desastres causados por actos de la naturaleza o provocados por terceros.

Algunas inquietudes que surgen respecto a los procedimientos y estándares de diseño de controles existentes en las organizaciones y al enfoque proactivo - preventivo de los controles, son las siguientes:

1. ¿Dentro de las organizaciones, las personas están conscientes que todos los controles (llámense preventivos, detectivos ó correctivos) deben actuar antes de materializarse los riesgos?. Que todos los controles deben actuar como alertas tempranas respecto a la ocurrencia de eventos accidentales o intencionales que pudieran afectar negativamente el patrimonio y la continuidad de las organizaciones?

2. ¿Los eventos de riesgo ocurridos o materializados recientemente en su empresa, estaban en la lista o inventario de riesgos inherentes identificados como probables en la matriz de riesgos diseñada para el manejo del riesgo en las operaciones en la Empresa?

3. ¿Los controles establecidos en la Empresa para reducir la severidad de los *riesgos recientemente materializados, fueron o no* efectivos para reducir la frecuencia y el impacto de su ocurrencia? ¿Estos controles fueron eludidos (omitidos) por los agentes generadores o causantes del riesgo?

4. ¿Los Auditores Internos, Revisores Fiscales y Auditores externos de la Empresa advirtieron a la Gerencia o la Junta Directiva sobre la propensión y/o vulnerabilidad de la Empresa a los riesgos materializados recientemente, antes que estos ocurrieran?

5. ¿Es aceptable que los organismos de control y vigilancia del Estado (Contralorías, Superintendencias y oficinas de Control Interno), en revisiones posteriores a los hechos (detrás de lo conocido) sean quienes descubren y *se pronuncian sobre cuantiosas pérdidas por fraudes materializados, varios años después de su ocurrencia? ¿Por qué los Jefes de Control Interno o Auditores Internos no advirtieron su probable ocurrencia o los detectaron en sus revisiones?*

6. ¿Para diseñar los controles internos, la Empresa dispone de un marco de referencia alineado con las buenas y mejores prácticas de gestión de riesgos y seguridad?

7. ¿Son apropiadas las metodologías, Guías o instructivos actualmente utilizadas para diseñar y documentar los controles internos en las Empresas?

PROPUESTA DE VALOR

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

a. Aplicar el enfoque **proactivo y preventivo** de diseño de controles para reducir la severidad de los riesgos inherentes en los procesos del modelo de operación de la empresa, en la infraestructura de Gestión de Servicios de TI y en los sistemas de información (aplicaciones de computador).

b. Aplicar una metodología de análisis de riesgos que conduzca a identificar las vulnerabilidades que deben eliminarse y los agentes generadores del riesgo que deben neutralizarse con los controles

c. Interpretar y aplicar correctamente los principios definidos en el marco de referencia COSO 2013 y otros estándares vigentes, relativos al análisis de riesgos, para implantar los componentes del sistema de control interno en los procesos del modelo de operación de la empresa y los servicios de Tecnología de Información.

d. Aplicar criterios para estimar (medir) el nivel de protección que ofrecen los controles (efectividad) por cada riesgo inherente y decidir o recomendar su aceptación.

e. Aplicar correctamente los conceptos de controles preventivos, detectivos, correctivos, manuales, automatizados, discrecionales y no discrecionales para reducir los riesgos y para medir la efectividad de los controles que se establezcan

1. A QUIENES VA DIRIGIDO?

Gerentes y Analistas de Riesgos, Gerentes y Analistas de Seguridad en Tecnología de Información, Auditores Internos y Externos, Jefes de Oficinas de Control Interno, Auditores de Tecnología de Información y Auditores de Sistemas de Gestión (de Calidad, ambiental, de salud ocupacional, de seguridad de la información - ISO 270O1, y de gestión de continuidad del negocio - ISO 22301).

2. OBJETIVOS DEL SEMINARIO

1. Transferir conocimientos y experiencias a los participantes para diseñar, documentar e implantar controles eficaces y eficientes por cada evento de riesgo potencial que pueda presentarse en las actividades de los procesos del modelo de operación de las empresas y la Gestión de Servicios de Tecnología de Información, de acuerdo con estándares de gestión de riesgos nacionales e internacionales vigentes (ISO 31000: 2018, ERM, DAPF y Superintendencias de Control del Estado) y los marcos de control interno COSO 2013, MECI, COBIT e ISO 27001.

2. Estimular y reforzar la conciencia sobre la necesidad de aplicar criterios apropiados en el diseño de los controles, considerando **eliminar** las vulnerabilidades identificadas que crean el ambiente propicio para la ocurrencia de los eventos de riesgo y **neutralizar** los agentes generadores del riesgo (factores de riesgo) que pueden explotar las vulnerabilidades.

3. Desarrollar habilidades en los participantes para diseñar, documentar e implantar los controles necesarios por evento de riesgo.

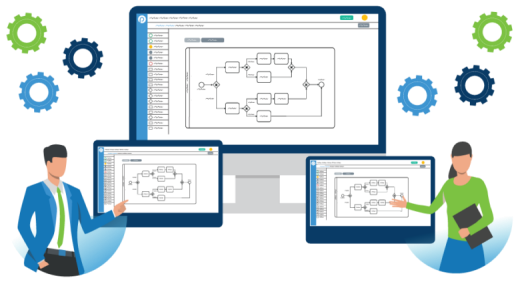
3. TEMAS DEL SEMINARIO

DIA 1.

Fundamentos para el Diseño de Controles.

- Marcos de referencia de Control Interno COSO 2013, COBIT y MECI.
- Marcos de Referencia de la Gestión de Riesgos Empresariales ISO 31000: 2018 y ERM.
- Clasificaciones de los riesgos según Sistemas de Gestión de Riesgos utilizados en el mercado - SARO, SARLAFT, MECI, SARM, etc.
- Conceptos de Controles y Seguridad según marcos de referencia internacionales.
- Clasificaciones de los Controles.
- Enfoque Reactivo Vs Enfoque Proactivo de los Controles.

- **Taller 1:** Presentación y análisis de Buenas prácticas de *Controles Generales de de TI.*
- ***Taller 2:*** Presentación y análisis de Buenas prácticas de *Controles Específicos de Aplicaciones de Computador.*
- **Taller 3:** Presentación del Caso de Estudio del Seminario: *"Diseño de Controles para el proceso de Gestión de Recursos Humanos"*



DIA 2.

Diseño de Controles por Evento de Riesgo Inherente y Clase (categoría) de Riesgo Operativo en procesos ó servicios de sistemas – Parte 1.

- Etapas de la Metodología de diseño de Controles en procesos y sistemas de información
- Caracterización del Proceso.
- Cómo identificar las clases de riesgo críticos para un proceso o sistema.
- Cómo identificar los eventos de riesgo negativos críticos, asociados a las clases o categorías de riesgo dentro de un proceso o sistema.
- **Taller 4:** identificación de los eventos de riesgo inherentes asociados para las clases de riesgos críticos de un proceso o sistema.
- **Taller 5:** Identificación de vulnerabilidades que crean ambiente propicio para la ocurrencia de los eventos de riesgo**.**
- Identificación de agentes generadores del riesgo por evento de riesgo.
- Criterios para identificar y documentar los Controles Necesarios.
- Criterios para evaluar el diseño de los controles por evento de riesgo inherente.
- **Taller 6:** Evaluación del Diseño de los Controles.
- Criterios para evaluar la efectividad de los controles por riesgo inherente.
- El Enfoque de los tres anillos o barreras de control por evento de riesgo inherente

DIA 3.

Diseño de Controles por Evento de Riesgo Inherente y Clase (categoría) de Riesgo operativo en un proceso ó servicio de sistemas – Parte 2.

- Escala cualitativa para estimar (medir) la efectividad individual de los controles por Riesgo Inherente.
- Escala cualitativa para estimar (medir) la efectividad colectiva de los controles por Riesgo Inherente.
- **Taller 7:** Evaluación de la efectividad de los controles
- Orientaciones para el diseño e implantación del programa Antifraude en las Empresas.
- **Taller 8:** Análisis de Controles Antifraude.
- Cómo se distribuyen las responsabilidades por los controles en la organización.

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

El seminario está estructurado en la modalidad de taller y se desarrollará de manera interactiva entre el facilitador y los participantes, con presentación de los temas por parte del facilitador, apoyadas en casos y experiencias del mundo real.

Los ejercicios individuales y grupales se realizarán alrededor de un caso de estudio especialmente preparado para el seminario con el propósito de afianzar los conceptos y desarrollar habilidades para aplicarlos utilizando 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

Para la realización de los ejercicios y talleres, es necesario que los participantes dispongan de un computador portátil con sistema operativo Windows.

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 (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,

10. FECHAS Y DURACIÓN

FECHAS: Abril 26, 27 y 28 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 Seminario
COL $ 1.600.000 + IVA	$ 1.651.400 + IVA

Descuentos por inscripción.	
Para clientes de seminarios y productos de AUDISIS.	5%
Miembros de ISACA e IIA	5%
Tres o más inscritos de la misma empresa.	7.5%

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 personas inscritas.

14. PLAZO PARA CANCELAR LA REALIZACIÓN DEL

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

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.