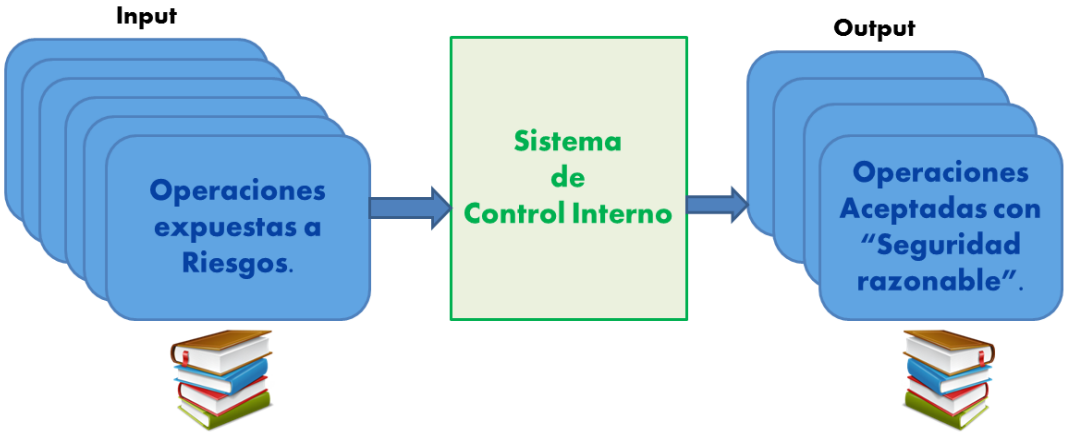
Seminario – Taller
DISEÑO DE CONTROLES INTERNOS EN PROCESOS Y TECNOLOGÍA DE INFORMACIÓN

Contenido:	Pá

PRESENTACIÓN

El diseño de los controles debería realizarse con base en las políticas de operación de la Empresa[1] y en el análisis de los *eventos de riesgo inherentes negativos* que pueden presentarse en el desarrollo de sus actividades, con el propósito de *reducir la severidad de los riesgos a nivel aceptable o tolerable*, de tal manera que los controles establecidos aseguren razonablemente la consecución de los objetivos esperados y evidencien su efectividad para la gestión adecuada de los riesgos.

Sistema de Control Interno como FILTRO PREVENTIVO



El **enfoque proactivo y preventivo** de los controles debería prevalecer sobre el **enfoque Reactivo o A posteriori**. Esto significa que los controles *deberían diseñarse para anticiparse a la ocurrencia de los eventos de riesgo, más que orientarse a detectar la ocurrencia de errores e irregularidades después que estas ocurren,* cuando lo único que puede hacerse es establecer los controles como una reacción a hechos ocurridos (Ex post Facto) o como remedio para que no estos no vuelvan a presentarse.

Los controles internos deberían diseñarse antes de iniciar la operación de los procesos y proyectos de la Empresa, durante las fases de planeación y construcción, no después, cuando los procesos están en operación y se detecta la ocurrencia de errores, irregularidades o después que se presentan desastres por actos de la naturaleza o provocados por terceros. Por consiguiente, los controles deberían diseñarse e implantarse para reducir la posibilidad de que se materialicen los eventos de riesgo o para reducir su impacto si no pueden evitarse, es decir, *para que actúen antes de que los riesgos ocurran.*

[1]Las políticas de Operación son guías de acción que definen los límites y parámetros necesarios para ejecutar los procesos y actividades en cumplimiento de la función, planes, programas, proyectos y políticas de la administración del riesgo, previamente definidos por la organización. http://www.cali.gov.co/cinterno/publicaciones/44199/polticas_de_operacin_del_proceso_control_interno_a_la_gestin/

Algunas inquietudes que surgen respecto a la cultura de control existente en las organizaciones y al enfoque proactivo de los controles, son las siguientes:

a. En el personal de las organizaciones existe conciencia que todos los controles (preventivos, detectivos y correctivos) deben actuar *antes de que se materialicen los riesgos*? Que todos los controles deben actuar como alertas tempranas respecto a la ocurrencia de eventos accidentales o intencionales que afecten negativamente el patrimonio y la continuidad de las organizaciones?

b. *Los eventos de riesgo ocurridos o materializados recientemente en la empresa*, estaban en la lista o portafolio de riesgos inherentes identificados como probables en el sistema de gestión de riesgos diseñado para el manejo de las operaciones en la Empresa?

c. Los controles establecidos en la Empresa para reducir la severidad de los *riesgos materializados recientes,* fueron efectivos para reducir la posibilidad y el impacto de su ocurrencia?.

d. Los auditores internos, Revisores Fiscales y Auditores externos de la Empresa advirtieron oportunamente a la Gerencia o la Junta Directiva sobre la propensión y la vulnerabilidad de la Empresa a los riesgos materializados recientes, antes que estos ocurrieran ?

e. Es aceptable que los organismos de control y vigilancia del Estado (Contralorías, Superintendencias y oficinas de Control Interno) *se pronuncien sobre los riesgos materializados varios años después de su ocurrencia?.*

f. Para el diseño de controles internos, la Empresa dispone de un marco de referencia (framework) alineado con los estándares internacionales y las buenas y mejores practicas de gestión de riesgos y seguridad?

g. Son apropiadas las Guías o instructivos y las metodologías 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) Interpretar y aplicar correctamente los principios definidos para implantar los componentes del sistema de control interno en el marco de referencia COSO 2013 y otros estándares vigentes, en los procesos del modelo de operación de la empresa y en los servicios de Tecnología de Información.

b) Diseñar controles efectivos para reducir la severidad de los riesgos inherentes asociados con las actividades del ciclo PHVA de los procesos del modelo de operación de la Empresa, de la infraestructura de Tecnología de Información (TI) y de las aplicaciones de computador que soportan el core del negocio.

c) Aplicar un **enfoque proactivo[2] y preventivo** Identificar, diseñar, documentar e implantar los controles necesarios durante la planeación e implementación del Ciclo PHVA de los procesos, proyectos y sistemas, para reducir la severidad de los riesgos inherentes en los procesos del modelo de operación de la empresa, de la infraestructura de TI y de los sistemas de información (aplicaciones de computador).

[2] Proactivo: Que tiene iniciativa y capacidad para anticiparse a problemas o necesidades futuras.

d) Aplicar criterios para determinar y medir el nivel de protección que ofrecen los controles (efectividad) establecidos por cada evento de riesgo inherente y decidir o recomendar sobre 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.

f) Diseñar e implantar un programa antifraude en la organización.

1. A QUIENES ESTA 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, 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 efectivos y eficientes sobre los eventos de riesgo inherente que pueden presentarse en las actividades de los procesos del modelo de operación de las empresas y los servicios de Tecnología de Información, de acuerdo con estándares de gestión de riesgos nacionales e internacionales vigentes (ISO 31000: 2009, 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, para eliminar las vulnerabilidades que crean el ambiente propicio para la ocurrencia de los eventos de riesgo y neutralizar los agentes (factores de riesgo) que pueden explotar tales vulnerabilidades.

3) Desarrollar habilidades en los participantes para diseñar, documentar e implantar los controles necesarios por evento de riesgo, para reducir la severidad del riesgo inherente a nivel aceptable de riesgo residual.

3. TEMAS DEL SEMINARIO

DIA 1.
Generalidades sobre 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 - Ejercicios.
- Enfoque Reactivo Vs Enfoque Proactivo de los Controles.
- **Taller 1:** Presentación y análisis de Buenas prácticas de *Controles Generales de TI.*
- ***T*aller 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.
Metodología de Diseño de Controles por Eventos de Riesgo Inherente para las Categorías de Riesgos Críticos de un proceso ó sistema – Parte 1.

- Etapas de la Metodología de diseño de Controles en procesos y sistemas de información
- Caracterización del Proceso.
- Cómo identificar las categorías o clases de riesgo críticos para un proceso o sistema.
- **Taller 4:** identificación de los eventos de riesgo inherentes asociados a las clases de riesgos críticos de un proceso o sistema.
- **Taller 5:** Análisis de los eventos de riesgo inherentes, como requisito para diseñar los controles.
- 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.
Metodología de Diseño de Controles por Eventos de Riesgo Inherente para las Categorías de Riesgos Críticos de un proceso ó sistema – Parte 2.

- Escala cualitativa para determinar la efectividad 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.
- El perfil profesional de los diseñadores de controles.

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 presentaciones conceptuales de los temas por parte del facilitador, apoyadas en casos y experiencias del mundo real.
Los ejercicios individuales y grupales se realizaran 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 COMPUTADOR

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

8. CONFERENCISTAS

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.

FECHAS: Febrero 11, 12 Y 13 de 2019.

Julio 29, 30 y 31 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 $ 1.360.000 + IVA	$ 1.430.000 + 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%

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

SUMINISTROS DEL SOFTWARE

- **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 que resultan de Auditorias efectuadas por terceros.

- **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.