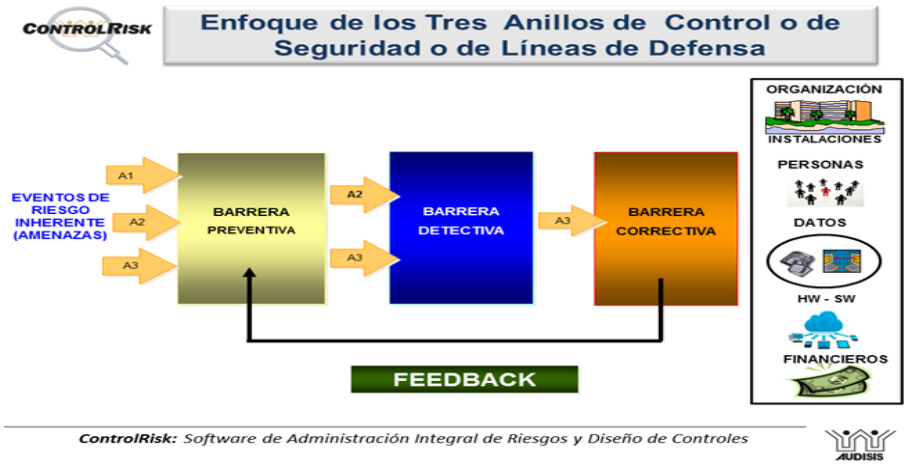
Seminario Taller
DISEÑO DE CONTROLES INTERNOS, BASADO EN RIESGOS
Bogotá D.C, Abril 20 Y 21 de 2017
GHL HOTEL CAPITAL

Contenido:	Pág

PRESENTACIÓN

El diseño de Controles es un tema sobre el que existen pocas referencias bibliográficas, se aborda superficialmente en la mayoría de las Universidades y sobre el que la opinión pública y los medios de comunicación nunca se pronuncian cuando se descubren irregularidades y actos de corrupción en el ámbito empresarial, en los sectores público y privado. *El análisis que se hace a estos eventos casi nunca se refiere a la capacidad o incapacidad de los controles establecidos para evitarlos, o la elusión de los mismos para posibilitar su ocurrencia o la efectividad de la gestión que realizan o dejan de hacer los organismos de control del Estado y las auditorías de las empresas.*



Algunas inquietudes que surgen en sectores de la opinión pública y en ciudadanos que prestan servicios profesionales independientes en Seguridad, Control Interno y Auditoría frente a los mencionados actos de corrupción y los fraudes son: a) Los riesgos ocurridos o materializados estaban en la lista o portafolio de riesgos inherentes identificados como probables por los Gerentes de Riesgos y los responsables del manejo de las operaciones en la Empresa?; b) Los auditores internos, Revisores Fiscales y Auditores externos de la Empresa advirtieron formalmente a la Gerencia o la Junta Directiva sobre la propensión y la vulnerabilidad de la Empresa a los riesgos ocurridos, antes que estos ocurrieran ?; c) La Empresa tenía formalmente establecidos los controles necesarios para reducir la posibilidad de ocurrencia de los riesgos; d) Los controles establecidos en la empresa para mitigar los riesgos ocurridos se eludieron intencionalmente o no fueron efectivos para evitar que ocurrieran los riesgos?; e) Es aceptable que las auditorías de la Contraloría General de la República, las Contralorías Departamentales y de las principales ciudades y las Superintendencias del Estado se pronuncien sobre estos actos de corrupción y dolo varios años después de la ocurrencia de los eventos de riesgo?; y f) Es aceptable que los Auditores Internos y Externos o los Jefes de Control Interno de las Empresas no se pronuncien sobre la propensión a estos actos de corrupción antes de la ocurrencia de los eventos de riesgo?

Las respuestas a estos cuestionamientos seguramente reflejan numerosas *deficiencias y grietas (fisuras) existentes en la estructura organizacional y en los estándares de gestión de riesgos empresariales y de diseño de controles internos,* los cuales se analizarán en este seminario*,* como las siguientes: *a) S*on apropiados los perfiles académicos, habilidades y competencias exigidas a los responsables de diseñar los controles y realizar las auditorías internas en las Empresas?; b) Están definidos o tipificados los conflictos de interés que constituyen inhabilidades para desempeñar esos cargos?; c) 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

1. PROPUESTA DE VALOR:

La *propuesta de valor percibido - Beneficios -* que obtendrán los participantes al finalizar este seminario se resume a continuación:

- Estarán en capacidad de interpretar y aplicar los principios definidos para implantar los siguientes tres (3) componentes del sistema de control interno COSO 2013 : EVALUAR RIESGOS, ACTIVIDADES DE CONTROL e INFORMACION Y COMUNICACIONES en los procesos del modelo de operación de la empresa y en los servicios de Tecnología de Información.

- Aprenderán a aplicar *el enfoque de los tres anillos o niveles de seguridad en el diseño de* los controles necesarios y efectivos por cada riesgo inherente, para reducir su severidad a niveles de riesgo residual tolerables.

- Aprenderán a aplicar criterios para determinar la eficacia y eficiencia de los controles que se diseñen e implanten para gestionar cada riesgo inherente.

- Estarán en capacidad de definir los 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.

2. A QUIENES ESTA DIRIGIDO

Auditores Internos y Externos, Jefes de Control Interno, Gerentes y Analistas de Riesgos, *Auditores* de Sistemas, Gerentes y Analistas de Seguridad en Tecnología de Información, 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).

3. OBJETIVOS DEL SEMINARIO

◊ Capacitar a los participantes para llevar a la práctica los Principios de COSO 2013 relativos a los componentes del sistema de control interno EVALUACION DE RIESGOS, ACTIVIDADES DE CONTROL y INFORMACION Y COMUNICACION.

◊ Capacitar a los participantes para definir la mezcla de controles requeridos para aplicar el enfoque de los tres anillos o niveles de seguridad en el diseño de controles por riesgo inherente.

◊ Capacitar a los participantes para IDENTIFICAR, ANALIZAR, DOCUMENTAR, EVALUAR y CONTROLAR en forma eficaz y eficiente los riesgos inherentes en los procesos del modelo de operación de las empresas y los servicios de Tecnología de Información que soportan el desarrollo de las operaciones de negocio y administrativas de las empresas, de acuerdo con los estándares de gestión de riesgos nacionales e internacionales vigentes (ISO 31000: 2009, DAPF, Superintendencias del Estado) y los marcos de control interno COSO 2013, MECI, COBIT e ISO 27001.

4. TEMAS DEL SEMINARIO

DIA 1.

1. Generalidades sobre los marcos de referencia de Control Interno COSO 2013, COBIT y MECI.
2. Generalidades sobre Marcos de Referencia de la Gestión de Riesgos Empresariales ISO 31000: 2009 y ERM.
3. El proceso de Gestión de Riesgos Empresariales según ISO 31000:2009.
4. La Gestión de riesgos como motor del Sistema de Control Interno.
5. Conceptos de Control según marcos de referencia internacionales.
6. Clasificaciones de los Controles - Ejercicios.

DIA 2.

1. El Enfoque de los tres anillos o barreras de control para reducir los riesgos.
2. Metodología de diseño de controles en los procesos del modelo de operación de la Empresa
3. Análisis del riesgo, como base para diseñar los controles requeridos - Ejercicios.
4. Clasificaciones de los riesgos según Sistemas de Gestión de Riesgos utilizados en el mercado - SARO, SARLAFT, MECI, SARM, etc.
5. Concepto, análisis y diseño de controles para el Riesgo de Fraude – Ejercicios.
6. Cómo se distribuyen las responsabilidades por los controles en la organización.
7. El perfil profesional de los diseñadores de controles.

5. 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. Realización de ejercicios individuales y grupales para afianzar los conceptos y desarrollar habilidades para aplicarlos utilizando y formatos diseñados para el uso de la metodología. Para la realización de ejercicios y talleres , es necesario que los participantes dispongan de un computador portátil con sistema operativo Windows.

6. 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.

7. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- Deseables**:** Conocimientos básicos de auditoria, riesgos y controles.

8. CERTIFICACIÓN DE ASISTENCIA

AUDISIS entregará certificación de asistencia a los participantes que asistan al 80% o en adelante de las horas programadas.

9. 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 (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, 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.

10. FECHAS, DURACIÓN Y HORARIO DEL SEMINARIO

FECHAS: Abril 20 y 21 de 2017
DURACIÓN: 16 Horas
HORARIO: De 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm.

FORMA DE PAGO

- En cheque a nombre de AUDISIS o transferencia de fondos a la cuenta corriente de AUDISIS.
- transferencia de fondos a la cuenta corriente Numero 075 11792-9 del Banco de Bogotá, Sucursal Galerías.

11. VALOR INVERSIÓN POR PARTICIPANTE

Pagos antes del Seminario	Pagos después del Seminario
COL $ 1.610.000 + IVA Extranjeros: USD 537	$ 1.660.000 + IVA USD 554

Descuentos por Participantes de la misma Empresa	
Hasta 3 Participantes	3 %
4 y 5 Participantes	5 %
Más de 6 Participantes	7.5 %

El valor de la inscripción incluye almuerzos, refrigerios y materiales.

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 IN-HOUSE

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.

E-mail : audisis@audisis.com
Teléfono: 255 67 17
PBX: 347 002 2
Celular: 3163638828

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 GESTION DE RIESGOS, SEGURIDAD Y CONTROL INTERNO EN PROCESOS DE NEGOCIO Y TECNOLOGIA DE INFORMACION.

- 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. 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.

2. 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 CAATTs.

- **WORKING PAPERS:** Software de Papeles de Trabajo de Auditoria Financiera.

- **MONITOR:** Software de Monitoreo Continuo y Auditoría Continua de Riesgos y Controles.

(*) La integración de **AUDIRISK** con **CONTROLRISK** permite a los auditores y administradores de riesgos compartir la **base de conocimientos o metadata de la empresa** que contiene la definición de categorías de riesgo, amenazas, activos impactados, vulnerabilidades, agentes generadores de riesgo, controles, objetivos de control y escenarios riesgo.