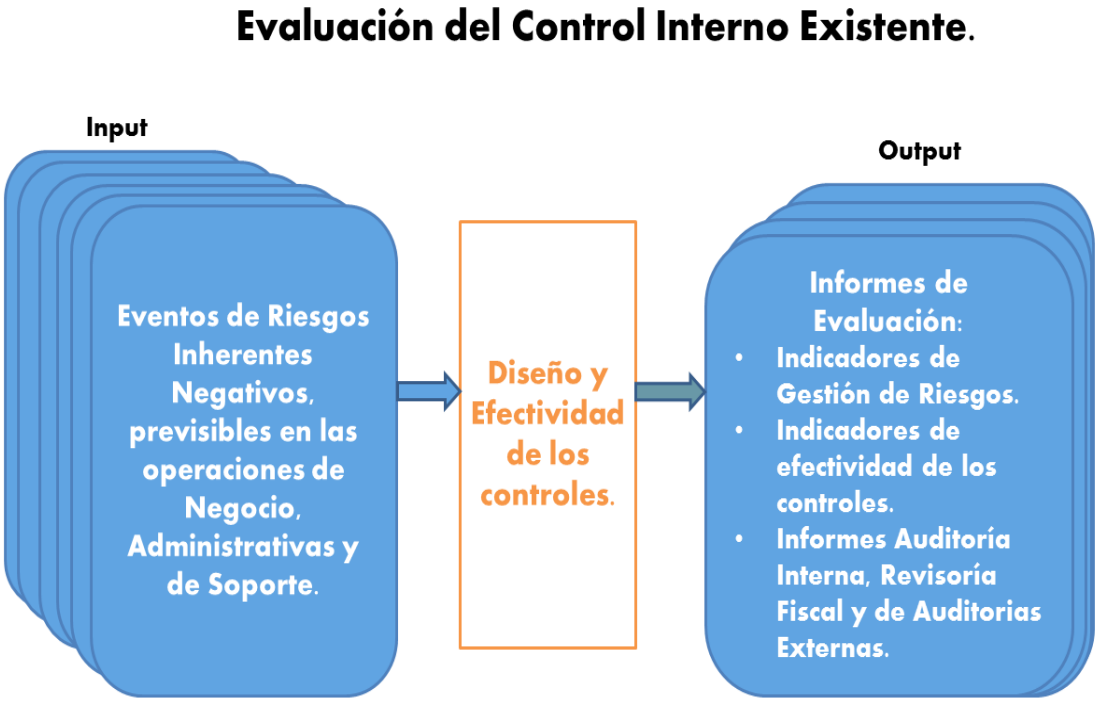
Seminario – Taller
EVALUACIÓN DEL CONTROL INTERNO EXISTENTE.

Contenido:	Pág

PRESENTACIÓN

Evaluar el diseño y la Efectividad del Control Interno existente en las empresas, por los auditores internos y externos y los administradores de riesgos, es una *actividad crucial* para confirmar que el *control interno* ofrece **seguridad razonable** para el manejo de las operaciones de negocio, administrativas y de soporte, es decir, en los procesos del modelo de operación, la infraestructura de Tecnología de Información y los sistemas de información automatizados (aplicaciones de computador).



Esta evaluación *es crucial* porque el éxito de las organizaciones depende *de la capacidad de los controles establecidos para asegurar razonablemente la consecución de sus objetivos y metas.* Los resultados de la evaluación deberían ***revelar los niveles reales de protección ofrecida*** **y de** ***riesgo residual*** a nivel general de la toda la organización, en cada uno de los procesos y sistemas de información automatizados e individualmente para los eventos de riesgo inherente que pueden presentarse e impactar negativamente a las operaciones de negocio y administrativas. La comunicación de los resultados de esta evaluación, es necesaria como retroalimentación para permitir *a la Gerencia y los responsables de los procesos auditados, efectuar de manera oportuna los ajustes necesarios para asegurar que la organización continúe funcionando dentro de límites aceptables de seguridad y confiabilidad.*

Los resultados de estas evaluaciones, con la *confirmación que los controles internos ofrecen seguridad razonable* o de la *revelación del nivel de seguridad real existente,* se divulgan en informes periódicos de las Gerencias de Riesgos que contienen *indicadores de gestión de riesgos y de efectividad de los controles* y en informes de Auditoría con los resultados de la evaluación del control interno existente realizadas por Auditores Internos y externos y la Revisoría Fiscal; algunas veces también se reciben evaluaciones en los diagnósticos emitidos por profesionales independientes especializados en seguridad de la información y certificadores de fraude. Normalmente, los destinatarios de estos informes son la Gerencia, la Junta Directiva, los accionistas de las Empresas, los stakeholders y las entidades de control del Estado.

La evaluación también debería realizarse por cada una de las clases de riesgo que integren el universo de riesgos de la Empresa, en cada una de las áreas del organigrama de la empresa, en los terceros que intervienen en el manejo de las operaciones de la empresa y servir de base para determinar la *evolución de los perfiles de protección existente y riesgo residual* en las organizaciones.

Este seminario - taller presenta los fundamentos para *evaluar el diseño y la efectividad de los controles internos establecidos en los procesos, la infraestructura de tecnología de información y las aplicaciones de computador de las Empresas*, utilizando un **enfoque proactivo y preventivo,** en concordancia con normas y procedimientos de auditoría de aceptación general, estándares internacionales y nacionales de gestión de riesgos y de control interno y las "buenas y mejores prácticas" de evaluación de controles y seguridad en tecnología de información.

PROPUESTA DE VALOR

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

a) Contribuir a mejorar la cultura de control de la organización, mediante la aplicación del enfoque Proactivo / preventivo del Control Interno.

b) Aplicar los *estándares y buenas prácticas de seguridad y control interno q*ue se utilizan como marcos de referencia para evaluar el diseño y efectividad de los controles internos establecidos en los procesos y la tecnología de información de las empresas (ley SOX, COSO, COBIT, MECI, ISO 27001 y normas de los organismos de control del Estado).

c) Aplicar diferentes alternativas para identificar los controles establecidos en los componentes del sistema de control interno y evaluar su diseño y efectividad.

d) Aplicar un enfoque Proactivo / Preventivo de los controles para evaluar *el diseño y efectividad* de los controles establecidos en la organización, por evento de riesgo inherente.

e) Aplicar el enfoque de las "tres barreras o anillos de seguridad" y otros criterios para evaluar *la eficacia y la eficiencia de los controles* establecidos por evento de riesgo inherente en los procesos y sistemas de información de la organización.

f) Aplicar criterios para *medir la protección existente y el riesgo residual* en las evaluaciones del control interno existente por eventos de riesgo inherente, por proceso, por área organizacional y a nivel de toda la organización. *Lo que no se mide no se puede administrar.*

g) Aplicar criterios para determinar los *perfiles de protección existente y riesgo residual de las organizaciones, por diferentes conceptos (por clase de riesgo, por proceso y por área organizacional), en cada uno* de los monitoreos periódicos que deben efectuarse en los diferentes sistemas de gestión de riesgos de la organización.

h) *Elaborar informes de auditoría efectivos con los resultados de la evaluación de control interno* a los procesos y sistemas por parte de los auditores internos de la Empresa, los Revisores Fiscales y las Auditorías de tecnología de información.

1. A QUIENES ESTA DIRIGIDO?

El seminario está dirigido a 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).

2. OBJETIVOS DEL SEMINARIO

1) Transferir conocimientos sobre aspectos claves de los *estándares y buenas prácticas de seguridad y control interno q*ue se utilizan como marcos de referencia para evaluar el diseño y efectividad de los controles internos establecidos en los procesos y la tecnología de información de las empresas (ley SOX, COSO, COBIT, MECI, ISO 27001 y normas de los organismos de control del Estado).

2) Transferir los conocimientos necesarios en los participantes para diseñar y aplicar procedimientos eficaces de *evaluación del control interno existente* en la organización, de acuerdo con las normas y procedimientos de auditoría de aceptación general, las normas del IIA y las normas de ISACA.

3) Estimular y reforzar consciencia sobre la necesidad de evaluar el diseño y la efectividad del control interno existente en los procesos y la tecnología de información, como medio de asegurar que las empresas disponen de un nivel de seguridad razonable para el desarrollo de sus operaciones de negocio y administrativas y la consecución de los objetivos y metas de las organizaciones.

4) Desarrollar habilidades en los participantes para evaluar el diseño y la efectividad de los controles y para generar informes de auditoría con los resultados de la evaluación del control interno existente.

3. TEMAS DEL SEMINARIO

DIA 1.
Fundamentos sobre Controles Internos.

- Concepto y componentes del Sistema de Control Interno de las organizaciones, según marcos de referencia nacionales e internacionales (COSO 2013, COBIT y MECI).
- Conceptos de riesgos y controles según marcos de referencia internacionales y nacionales de gestión de riesgos y de *buenas prácticas de seguridad y control interno* (ISO 31000, ERM, SOX, ISO 27001, ISO 22301 y otras).
- Normas de Auditoría que obligan a los Auditores a evaluar el sistema de Control Interno Existente.

- Clasificaciones de los Controles.
- Enfoque Reactivo Vs Enfoque Proactivo de los Controles.
- Taller 1: Presentación de Buenas prácticas de *Controles Generales de TI.*
- Taller 2: Presentación de Buenas prácticas de *Controles Específicos de Aplicaciones de Computador.*
- Taller 3: Presentación y análisis de las buenas prácticas de control exigidas por SOX
- Presentación del Caso de Estudio del Seminario: *Evaluación de Controles para un proceso.*

DIA 2.
Evaluación del Diseño y Efectividad de los Controles – Parte 1

- Etapas de la Metodología para evaluar el control Interno por parte de las Auditorías.
- Clasificación de los riesgos según Sistemas de Gestión de Riesgos utilizados en el mercado (SARO, SARLAFT, MECI, SARM y otros).
- ¿Qué se evalúa a los Controles?
- ¿Cuándo evaluar los Controles?
- Análisis de los Métodos más utilizados para evaluar el sistema de Control Interno en las organizaciones
- **Evaluación de Controles por Eventos de Riesgo Inherente para las Categorías de Riesgos Críticos de un proceso ó sistema.**
    - Cómo identificar y priorizar las categorías o clases de riesgo críticos para un proceso o sistema.
    - **Taller 4:** Cómo identificar los eventos de riesgo inherentes asociados a las clases de riesgos críticos de un proceso o sistema.
    - **Taller 5:** Cómo analizar los eventos de riesgo inherentes, como requisito para evaluar el diseño de los controles.
    - 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.
    - Escala cualitativa para determinar la efectividad de los controles por Riesgo Inherente
    - **Taller 7:** Evaluación de la efectividad de los controles

DIA 3.
Evaluación del Diseño y Efectividad de los Controles – Parte 2.

- Evaluación de Controles por Eventos de Riesgo Inherente para las Categorías de Riesgos Críticos de un proceso ó sistema (Cont).
    - **Taller 8:** Identificación y Análisis de Hallazgos de Auditoría sobre el Control Interno Existente.
    - **Taller 9:** Cómo elaborar informes de Auditoría efectivos, con los resultados de la Evaluación del Control Interno Existente.
- Evaluación de Controles por proceso, en la etapa de Monitoreo de los Sistemas de Gestión de Riesgos.
    - Herramientas utilizadas.
    - Indicadores de Gestión de Riesgos de Control Existente.

- El perfil profesional de los *Evaluadores de los 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 de los temas por parte del facilitador, apoyadas en casos y experiencias del mundo real.
Los talleres y ejercicios del seminario se desarrollan alrededor de un caso de estudio de un proceso del modelo de operación de la Empresa, especialmente diseñado para el seminario.

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

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 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.— GHL Hotel Capital.

FECHAS: Marzo 4, 5 y 6 de 2019.

Agosto 12, 13 y 14 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 $ 1.450.000 + 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%

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

♦ **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.

♦ **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.