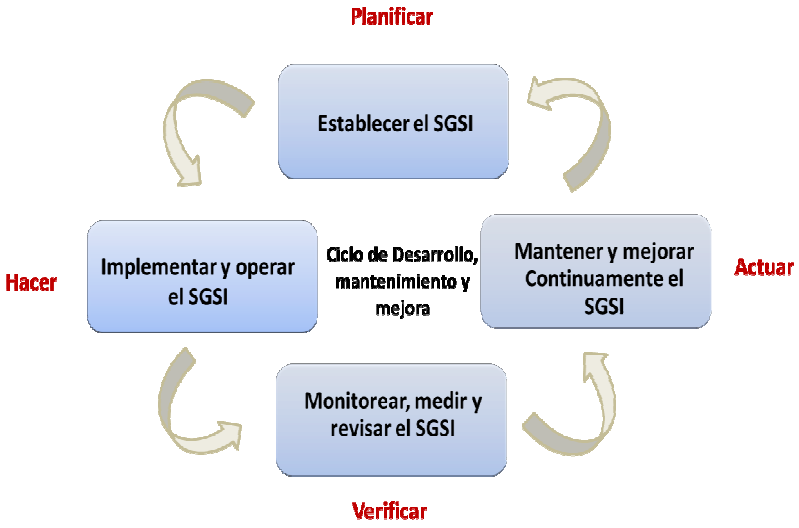
Seminario - Taller por INTERNET

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001:2013) – Implantación y Auditoría

Contenido:	Pág

PRESENTACIÓN

La información es el activo más valioso de cualquier organización, no precisamente por su valor en los libros de contabilidad (puesto que no está contabilizada), sino por lo que representa. Como sistema nervioso de cualquier organización, la información es indispensable para soportar la toma de decisiones, el control y el manejo de las operaciones de negocio de las organizaciones y como tal debe protegerse. Sin la información sería imposible el funcionamiento y la operación de las Empresas.



Para satisfacer las necesidades de seguridad de la información, surgieron los estándares ISO / IEC 27001:2013, ISO 27003: 2010 e ISO 27005: 2011. El primero proporciona un modelo para establecer, implementar, operar, monitorear y mejorar un **Sistema de Gestión de seguridad de la información (SGSI)** en los procesos de la organización, armonizado con otros sistemas de gestión.

La ISO 27003 provee una guía práctica para desarrollar el plan de implementación del SGSI dentro de las organizaciones. La ISO 27005:2011 provee guías para la Gestión de Riesgos de Seguridad de la Información (ISRM), específicamente soportando los requerimientos del sistema de gestión de seguridad de la información definida por ISO 27001.

La aplicación de estos estándares posibilita a las Organizaciones sin importar su tamaño o sector al cual

pertenecen, alcanzar un nivel adecuado de seguridad de la información mediante la aplicación de un sistema de gestión basado en la implementación de políticas de seguridad de la información, gestión de riesgos, controles y mejora continua que les permita garantizar la confidencialidad, integridad y disponibilidad de su información y la de sus Clientes.

PORQUÉ ASISTIR AL SEMINARIO?

Este seminario permitirá a los asistentes conocer la metodología y los factores de éxito necesarios para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001: 2013.

Durante 3 días, los conferencistas compartirán experiencias y vivencias sobre teoría y la práctica de la implementación de un SGSI en empresas de diferentes tamaños y grados de sofisticación, y darán respuesta a las inquietudes de los participantes respecto a los problemas y desafíos que se presentan en la ejecución del proyecto.

Algunos interrogantes que podrán resolver los participantes en este seminario son:

- Como preparar el plan de implementación del SGSI, definir la estructura del proyecto y obtener la aprobación de la Gerencia.
- Cómo soportar y documentar las actividades críticas del proyecto de implantación del SGSI.
- Cómo identificar, medir, controlar y monitorear los riesgos asociados con los activos de información para asegurar que estos activos se mantienen dentro de unos límites aceptables de seguridad de la información?.
- Cómo definir políticas y procedimientos del SGSI?
- Cómo administrar el cambio de cultura organizacional en la empresa con respecto a la Seguridad de la Información ?.
- Cómo realizar las auditorías internas del SGSI y mejoramiento continuo?
- Como obtener la certificación del SGSI?.

1. OBJETIVOS DEL SEMINARIO

- Presentar la metodología para desarrollar el plan de implementación del Sistema de Gestión de seguridad de la información (SGSI) dentro de la organización, en concordancia con la norma ISO / IEC 27001:2013.

- Desarrollar habilidades en los participantes para realizar una adecuada administración de riesgos de seguridad de los activos de información y la elección de los controles más eficaces y eficientes para mitigarlos.
- Desarrollar habilidades para definir y documentar políticas y procedimientos del SGSI.
- Conocer herramientas de software que apoyan la implementación de un SGSI.

2. A QUIÉN VA DIRIGIDO (PARTICIPANTES)

El seminario está dirigido a Gerentes de Tecnología de Información y Comunicaciones, Gerentes de Riesgos, Jefes de Planeación , Administradores de Seguridad Informática, Oficiales de Seguridad, Auditores de Sistemas, Organizaciones en proceso de implementación sistemas de gestión de seguridad.

3. TEMAS DEL SEMINARIO

DIA 1.

1. INTRODUCCIÓNAL SGSI – 3 horas.

- La Familia de Normas ISO 27000.
- Definición y elementos del sistema de gestión de seguridad de la información (SGSI).
- Los 14 dominios de la Norma ISO 27001: 2013.
- Razones y beneficios de adoptar la ISO 27003 .
- El modelo PHVA del SGSI.

2. METODOLOGIA PARA IMPLANTACION DEL SGSI – Parte 1 (5 Horas).

- Fases y actividades de la metodología para implementar el SGSI (Norma ISO 27003).
- Obtener aprobación de la Gerencia para implantar el SGSI.
- Definir Alcance, Límites y Política del SGSI.

DIA 2.

3. METODOLOGIA PARA IMPLANTACION DEL SGSI – Parte 2 (8 horas).

- Análisis de Requerimientos de Seguridad de la Información.
- Evaluación de Riesgos y Planeación del Tratamiento de Riesgos.
- Selección de Objetivos de Control y Controles requeridos – Norma ISO 27001: 2013.
- Determinar Efectividad de los controles y las métricas.

DIA 3.

4. METODOLOGIA PARA IMPLANTACION DEL SGSI – Parte 3. (6 horas).

- ♦ Plan de Implementación del SGSI.
- ♦ Monitoreo y Auto- aseguramiento del SGSI.
- ♦ Desarrollo de Competencias Organizacionales.
- ♦ Planeación de la Auditoría Interna al SGSI.
- ♦ Redacción del manual de Seguridad de Información.

5. El PROCESO DE CERTIFICACION INTERNACIONAL (2 horas).

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores utilizando filminas, desarrollo de ejercicios de aplicación y recapitulación de las principales ideas de cada tema.

5. MATERIAL PARA LOS PARTICIPANTES

Se entregará material escrito en medio magnético con las ayudas utilizadas por los expositores y los talleres y casos de estudio.

6. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- ♦ Conocimientos básicos de seguridad de la información.
- ♦ Disponibilidad de un computador portátil para instalar los casos de estudio y realizar los talleres.

7. CERTIFICACIÓN DE ASISTENCIA

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

8. 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 in-

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.

Alvaro Mauricio Romero. – Consultor Seguridad Informática y análisis forense., de AUDISIS. Experto en Tecnología y Seguridad Informática con certificaciones como auditor líder BS ISO/IEC 27001:2005 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 y CISSP. Auditor interno norma ISO 9001 versión 2000. Cuenta con más de 18 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 del sistema, y auditorias basadas en riesgos en Organizaciones nacionales e internacionales del sector servicios y financiero

Se ha desempeñado por más de 10 años como docente en Seminarios, diplomados y especializaciones de Seguridad Informática y Análisis Forenses 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. Entre otros, los seminarios dictados son:

- Seminario taller Implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013.
- Seminario para auditores internos del SGSI.
- Seminario taller de implementación del plan de continuidad del Negocio BCP.
- Seminario taller de control interno y diseño de controles con énfasis en el cumplimiento de la CE038 SFC y CE023 SSF.
- Seminario talle de auditoria basada en riesgos.
- Seminario taller de Ethical hacking y análisis forense informático.

Actualmente es docente en la ESCUELA DE COMUNICACIONES DEL EJERCITO NACIONAL en la especialización de seguridad física y de la información dictando las cátedras de seguridad en sistemas operativos, plan de continuidad del negocio, Ethical hacking y análisis forense informático.

Como consultor de AUDISIS ha participado en proyectos de seguridad realizados para FUNDACION DE LA MUJER, FINAGRO, COMFENALCO TOLIMA, FIDUCIARIA BOGOTA, SEGUROS GENERALI, LAFAYETTE, PROENFAR, INIF, HOSPITAL SAN IGNACIO, BOLSA MERCANTIL DE COLOMBIA, TERMINAL DE TRANSPORTES, UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA Y EL ICFES. También ha sido instructor en cursos y seminarios organizados por AUDISIS.

9. FECHAS, DURACIÓN Y HORARIO DEL SEMINARIO

FECHAS: Noviembre 16, 17 y 18
DURACIÓN: 24 Horas
HORARIO: De 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm—Hora de Colombia

FORMA DE PAGO
En cheque a nombre de AUDISIS o transferencia de fondos a la cuenta corriente de AUDISIS.

10. VALOR INVERSIÓN POR PARTICIPANTE

Pagos antes del Seminario	Pagos después del Seminario
COL $ 1.000.000 + IVA Extranjeros: USD 350	$ 1.050.000 + IVA USD 370

Descuentos por Participantes de la misma Empresa	
Hasta 3 Participantes	5 %
4 y 5 Participantes	7.5 %
Más de 6 Participantes	10 %

11. 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.

12. 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.

13. 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.

14. 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: 2556717—2556757—2556816
PBX: 3470022

15. NUESTROS PRODUCTOS Y SERVICIOS PROFESIONALES

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.

NUESTROS SERVICIOS

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.

3. 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.