Seminario – Taller

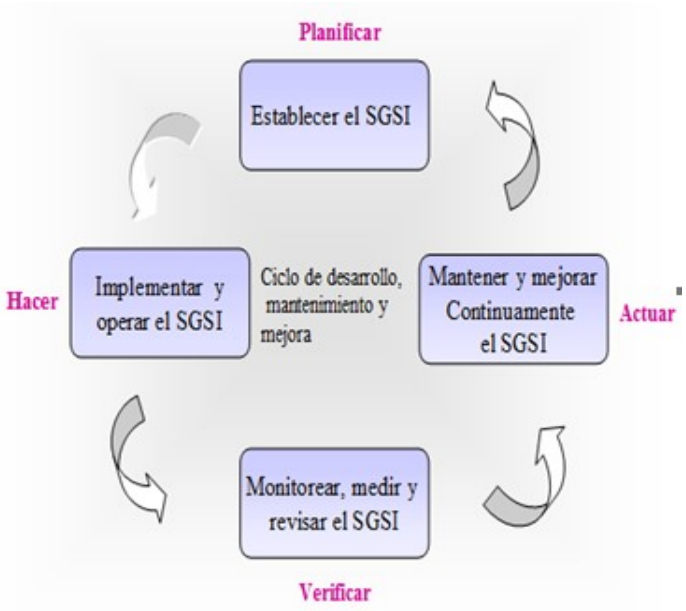
IMPLANTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD—ISO 27001

Contenido:	Pág

PRESENTACIÓN

La información es el activo más valioso de cualquier organización, no por su valor registrado en los libros de contabilidad (puesto que no está registrada como un activo en la contabilidad), 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 en sus componentes de integridad, disponibilidad y confidencialidad.

Ciclo PHVA del Sistema de Gestión de Seguridad de la Información (SGSI)"



Sin información no es posible la continuidad de las operaciones y si la **información no es confiable y segura,** la toma de decisiones, el control y otras actividades administrativas se exponen a riesgos de la mayor severidad y a consecuencias desastrosas para la organización

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 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.

PROPUESTA DE VALOR

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

Durante 3 días, los instructores compartirán experiencias y vivencias sobre teoría y la práctica de la implantación 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 de implantación y mantenimiento.

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

- Preparar el plan de implantación del SGSI, definir la estructura del proyecto y obtener la aprobación de la Gerencia.
- Soportar y documentar las actividades críticas del proyecto de implantación del SGSI.
- Identificar, evaluar severidad, controlar y monitorear los riesgos inherentes a los activos de información para asegurar que estos activos se mantienen protegidos dentro de límites aceptables de seguridad de la información.
- Definir las políticas y procedimientos del SGSI.
- Administrar el cambio de cultura organizacional en la empresa con respecto a la Seguridad de la Información.
- Realizar las auditorías internas del SGSI y promover el mejoramiento continuo del SGSI.
- Tramitar las actividades necesarias para obtener la certificación del SGSI .

1. OBJETIVOS DEL SEMINARIO

- Presentar la metodología para implantar el 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 gestionar adecuadamente los riesgos inherentes a la seguridad de los activos de información y la elección de los controles eficaces y eficientes para mitigarlos.
- Desarrollar habilidades para definir y documentar políticas y procedimientos del SGSI.
- Conocer herramientas de software para apoyar la implantación y mantenimiento del SGSI.

2. A QUIENES ESTA DIRIGIDO?

Gerentes de Tecnología de Información y Comunicaciones, Gerentes de Riesgos, Gerentes de Seguridad de la información, Jefes de Planeación, Administradores de Seguridad Informática, Oficiales de Seguridad, Auditores Internos, Revisores Fiscales y Auditores de Sistemas.

3. TEMAS DEL SEMINARIO

DIA 1.

1. INTRODUCCION AL 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 implantar 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 IMPLANTAR EL SGSI – Parte 2 (8 horas).

- Análisis de Requerimientos de Seguridad de la Información.
- Evaluación de Riesgos y Planeación del Tratamiento de Riesgos – Normas ISO 27005 e ISO 31000:2018.
- Selección de Objetivos de Control y Controles requeridos – Norma ISO 27001: 2013
- Determinar Efectividad de los controles y las métricas.

3. TEMAS DEL SEMINARIO

DIA 3.

4. METODOLOGIA PARA IMPLANTAR EL 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).

6. AUDITORIA INTERNA AL SGSI
DURACION: 24 horas

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores utilizando filminas, desarrollo de ejercicios y talleres de aplicación de conceptos claves 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, 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

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

8. DIRECTOR E 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, 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. Consultor Seguridad Informática y análisis forense, AUDISIS.

Profesional experto en Tecnología y Seguridad Informática. Estudios en Ingeniería Electrónica con certificaciones como Auditor líder BS ISO/IEC 27001 Information Security Management System otorgada por el BSI British Standards Management System, CEH (Certified Ethical Hacker & Countermeasures), Cerificado en Ciberseguriad y la plataforma de seguridad de checkpoint, auditor interno ISO 9001 versión 2001.

Amplia experiencia en el sector financiero como Director de Informática, diseño e implementación de sistemas de gestión de seguridad informática y planes de continuidad. Antes de vincularse a AUDISIS, trabajó como Director Nacional de Tecnología e Infraestructura en Liberty Seguros S. A. (agosto 2003 – Octubre 2007); Jefe de Comunicaciones Red Metropolitana en el Banco Colpatria Red Multibanca (octubre 2009 – Julio 2003), Porvenir en instalación y soporte en redes (Febrero 2002 – Agosto 1-995). Experiencia en el diseño, implementación y administración de sistemas de Gestión de Seguridad de la Información y del Plan de Continuidad del Negocio y Recuperación del sistema en multinacionales del sector servicios con sucursales a nivel nacional. Ha participado como docente en Diplomados de Seguridad informática y Análisis forense en las universidades Javeriana, Manuela Beltrán, Autónoma y CIDE

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

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, HORARIO Y DURACIÓN

FECHAS: Octubre 25, 26 y 27 del 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	COL $ 1.651.400 + IVA

Descuentos por Inscripción.	
Clientes de servicios y productos de AUDISIS	5%
Tres o más inscritos de la misma empresa	7.5%
Miembros de ISACA e IIA	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 SEMINARIO

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 (571) 3099764
Celular: 3173638828

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, 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 COMPU-TADOR (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.