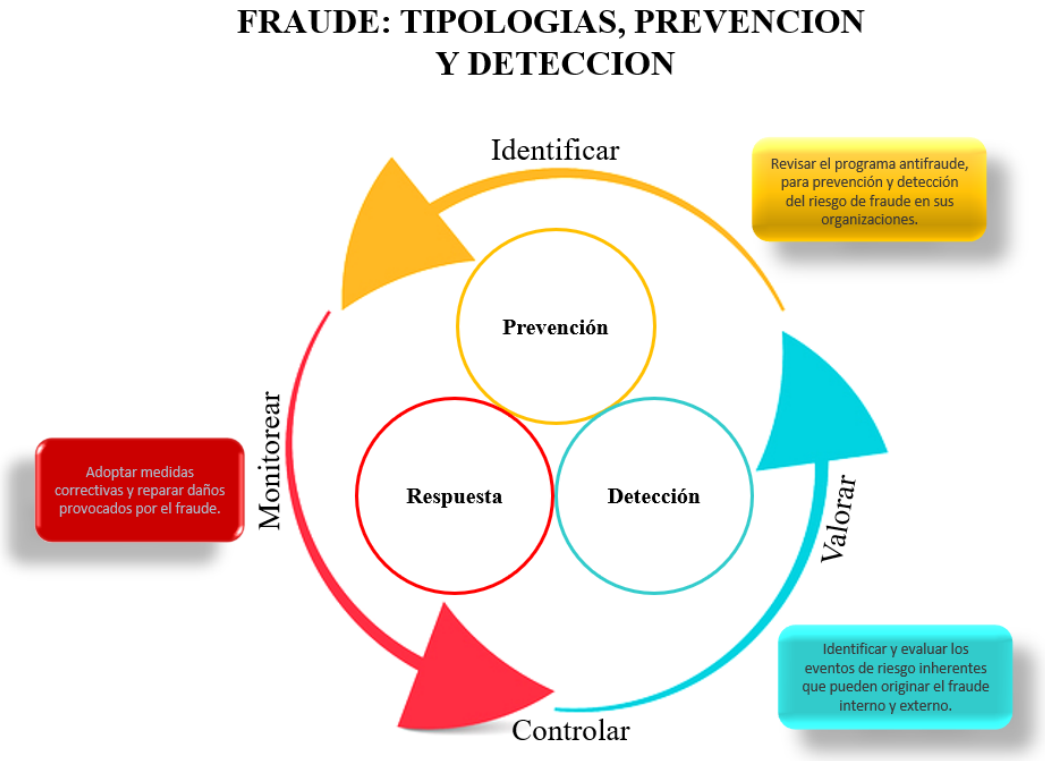
Seminario – Taller Virtual
FRAUDE: TIPOLOGIAS, PREVENCION Y DETECCION

PRESENTACIÓN

Ciberataques, Fraude y riesgos de incumplimiento constituyen la triada de riesgos de seguridad que acechan a las Empresas durante la pandemia. Con este titular el periódico El TIEMPO recientemente resaltó los resultados de la encuesta realizada por KPMG a 642 directivos de igual número de empresas de siete industrias de los sectores manufacturero, productos de consumo y retail, energía, servicios financieros, seguros, farmacéutica y telecomunicaciones de América Latina, Estados Unidos y Canadá.

Contenido: **Pá**



Según la encuesta, un 83 por ciento de los encuestados admite haber sido afectado por algún tipo de ciberataque en los últimos 12 meses. Entre las modalidades de ciberataques reportados se encuentran el phishing (con el 44 por ciento), la estafa o *scamming* (33 por ciento) y el *spydware o malware* (22 por ciento). Los expertos calculan que las pérdidas son millonarias tanto para los que acceden a pagar el rescate como para los que se resisten a caer en las redes de estos delincuentes y pierden datos por meses e incluso de manera definitiva.

Después de los ciberataques, el **fraude interno y externo** es la segunda gran amenaza. El 71 por ciento de los encuestados ha tenido que afrontar este tipo de ataques y la mitad afirma que trabajar desde casa ha impactado negativamente la capacidad de las empresas para responder al fraude.

Y la triada de riesgos críticos de seguridad la completan las **pérdidas derivadas de multas regulatorias o fallas de cumplimiento.** Este punto tiene igual gravedad que el fraude; los directivos encuestados reportaron que sus empresas tienen una perdida combinada promedio por fraudes, incumplimientos y multas regulatorias equivalente al 1 por ciento de sus utilidades**.**

Los expertos de KPMG y recientes hechos demuestran que Colombia también ha sido víctima de esta triada de riesgos de seguridad . En Colombia el caso más reciente fue el de Empresas Municipales de Cali (Emcali), que en octubre 16 de 2021 fue afectada por un ataque de *ransomware* que secuestró (encriptó) la información comercial y a cambio de liberarla los criminales solicitaron entre 50.000 y 100.00 dólares. Otros casos recientes son los ciberataques a la Aeronáutica Civil en horas de la noche del 31 de Agosto del 2021 y a la Pontificia Universidad Javeriana en sus sedes de Bogotá y Cali

Entre los casos más cuantiosos e impactantes de ciberataques a nivel mundial está el de Colonial Pipeline, la empresa que opera una red de oleoductos. Pagó un rescate de cinco millones de dólares a los piratas informáticos que la atacaron en Mayo de 2021.

Los hechos mencionados en los párrafos anteriores son un indicador de la severidad de los tres riesgos de mayor impacto en la actualidad. En este seminario, el énfasis se dará a los riesgos de fraude interno y externo.

PROPUESTA DE VALOR

Al finalizar el seminario los participantes estarán en capacidad de:

a) Revisar el programa antifraude, para prevención y detección del riesgo de fraude en sus organizaciones.

b) Construir matrices de riesgo de fraude interno y externo para los procesos de la cadena de valor y los servicios de Sistemas de la Empresa.

c) Aplicar estándares para identificar, analizar, valorar, controlar y monitorear los eventos de riesgo inherentes que pueden originar fraude interno y externo.

d) Aplicar criterios para evaluar el diseño y la efectividad de los controles sobre los riesgos de fraude interno y externo, en función de las vulnerabilidades y los agentes generadores del fraude identificadas en el análisis de los riesgos.

e) Definir la estructura de organización y de soporte tecnológico requeridos para la gestión eficaz del riesgo de fraude en la empresa.

1. A QUIENES VA DIRIGIDO?

El seminario está dirigido a funcionarios responsables de implementar el Sistema de Administración del Riesgo Operativo (SARO), en entidades del vigiladas por la Superintendencia de Entidades Financiera (Superfinanciera) y la Superintendencia de Entidades Solidarias (Supersolidaria), Superintendencia Nacional de Salud, Auditores Internos, Revisores Fiscales y personal interesado en el SARO.

2. OBJETIVOS DEL SEMINARIO

- Presentar conceptos sobre los riesgos de fraude interno y externo y los patrones de modalidades de fraude de mayor ocurrencia.
- Sensibilizar a los participantes sobre procedimientos para prevenir y detectar fraudes en las operaciones de la Empresa.
- Desarrollar habilidades para evaluar la exposición a riesgos de fraude interno y externo en los procesos de la cadena de valor y en el ambiente de TI.

3. TEMAS DEL SEMINARIO

DIA 1.

- Conceptos de Fraude.
- El triángulo del Fraude.
- Tipologías del Fraude
- El árbol de Fraude
- Modalidades de fraude más frecuentes.
- Ejemplos de fraudes financieros ocurridos en Colombia.
- Fraude relacionado con la Tecnología de Información.
- Signos de peligro de fraude.
- Perfil de los defraudadores.
- Taller 1: Caso de estudio para identificar vulnerabilidades (causas) que permiten la ocurrencia de fraude y Agentes Generadores del Riesgo

DIA 2

- Uso de cuestionarios para evaluar la exposición a riesgos de fraude interno y fraude externo en los procesos de la cadena de valor.
- Uso de cuestionarios para evaluar la exposición a riesgos de fraude interno y fraude externo en los procesos de la cadena de valor.
- Taller 2: Aplicación de cuestionarios para estimar exposición a riesgos en los procesos de la cadena de valor.
- Metodología de Análisis cuantitativo de eventos de riesgos que pueden generar los riesgos de fraude (los seis elementos del riesgo).
- Taller 3: Análisis de Eventos de Riesgos de Fraude.
- Elementos de Control de Fraude.
- Diseño de Controles Antifraude.

DIA 3.

- Gestión proactiva del riesgo de Fraude.
- Guía antifraude COSO - ACFE
- Programa de Prevención, detección e investigación de fraude.
- Auditoría preventiva y proactiva del Riesgo Fraude.

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

El seminario está estructurado en la modalidad de Taller y se desarrollará de manera interactiva entre el instructor y los participantes, con presentaciones de los temas apoyadas en casos y experiencias del mundo real.

Los talleres del seminario se desarrollarán alrededor de temas de identificación, análisis, control y monitoreo de eventos que pueden originar fraude interno y externo.

Se realizarán también ejercicios para afianzar los conceptos y desarrollar habilidades para aplicarlos utilizando y formatos diseñados para el uso de la metodología.

5. MATERIAL PARA LOS PARTICIPANTES

Se entregará material escrito en medios magnéticos, con las ideas claves del seminario, cuestionarios para evaluar la exposición a riesgos en los procesos de la cadena de valor y en TI, formatos de la metodología de análisis de riesgos y enunciados de los ejercicios y talleres.

6. CERTIFICACIÓN DE ASISTENCIA

A los participantes que asistan al 80% por ciento o más del seminario se entregará certificado de asistencia.

7. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- Deseable: Conocimientos básicos de riesgos, controles y auditoría.
- Disponibilidad de computadores portátiles para instalar los casos de estudio y realizar los talleres.

8. DIRECTOR E INSTRUCTORES.

El seminario será dirigido por Euclides Cubillos Moreno, socio director de AUDISIS y desarrollado por expertos en los temas del seminario.

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.

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 Y DURACIÓN

FECHAS: Abril 20, 21 y 22 de 2022.

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 $ 1.436.000 + IVA	$ 1.500.000 + IVA

Descuentos por inscripción.	
Para clientes de seminarios y productos de AUDISIS.	10%
Miembros de ISACA e IIA	5%
Tres o más inscritos de la misma empresa.	7.5%

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

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 COMPUTADOR (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.