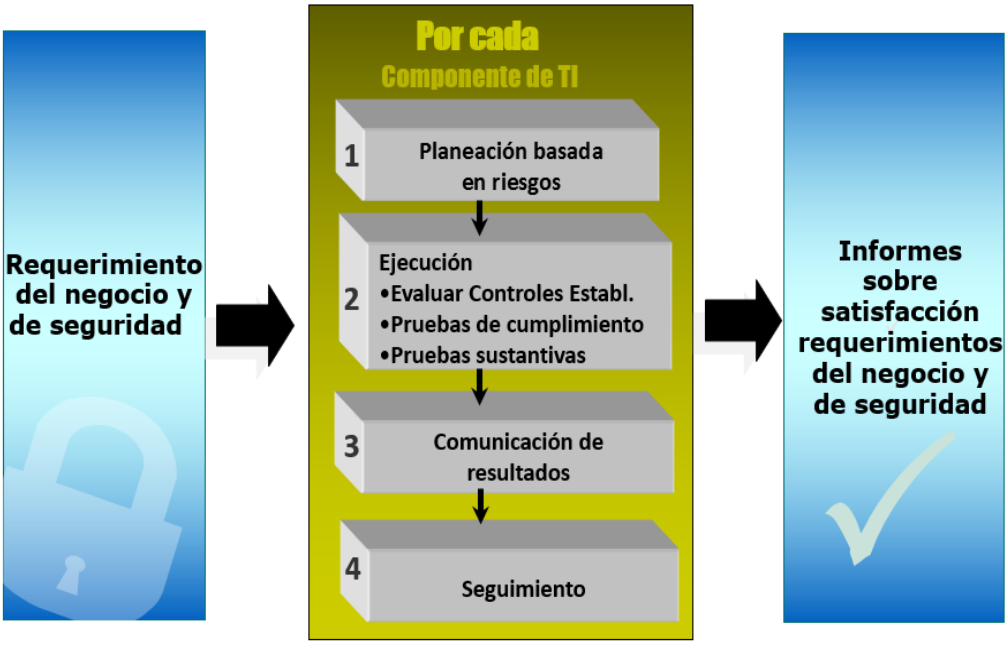
Seminario – Taller Virtual
AUDITORÍA DE TECNOLOGIA DE INFORMACIÓN, BASADA EN RIESGOS CRITICOS.

Contenido:	Pág

PRESENTACIÓN

La Auditoría de Sistemas, interna o externa, *"es una especialidad de la auditoría que realiza una evaluación independiente y objetiva de los Servicios de Sistemas (infraestructura de Tecnología de Información, Data Center, Aplicaciones de Computador que soportan el desarrollo de las operaciones de negocio y de apoyo administrativo en las Empresas y otras actividades técnicas y administrativas relacionadas con Tecnología de Informacion), con la finalidad de proveer razonable confianza a la Gerencia de la Empresa y a otras partes interesadas, respecto a que los controles internos establecidos proveen seguridad razonable, eficiencia, eficacia y el cumplimiento con las normas legales y regulatorias, reducen los riesgos inherentes del negocio a niveles tolerables y aseguran la satisfacción de los objetivos y necesidades de la organización".*

Auditoría de Sistemas Basada en Riesgos Críticos.



Como apoyo a la AUDITORIA INTERNA, en el contexto de la tercera línea de defensa de la organización, la auditoría de sistemas tiene como objetivos evaluar y verificar que los controles internos establecidos en los servicios de sistemas de la Empresa sean apropiados para reducir los riesgos inherentes a niveles aceptables de riesgo residual (en aspectos de seguridad de la información, efectividad, confiabilidad y cumplimiento con las normas regulatorias) y para asegurar la satisfacción de los objetivos y necesidades de la organización .

Basándose en los resultados de Auditorías de Sistemas de Información profesionalmente desarrolladas, la Junta Directiva, la Gerencia de la Empresa, la Gerencia de Tecnología, la Auditoría Interna y los responsables de las operaciones pueden tomar decisiones para asegurar su confianza en la efectividad de los controles establecidos y que los servicios de sistemas satisfagan los requerimientos legales, técnicos y funcionales de la organización.

Las Auditorías de Sistemas de Información, internas o externas, realizan un examen objetivo e independiente de los procesos y operaciones de tecnología de información, con el fin de evaluar, verificar e informar a la Gerencia y otras partes interesadas, sobre la eficiencia de las operaciones de TI, el diseño y efectividad de los Control Interno en los servicios de Sistemas y la seguridad y confiabilidad de la información que generan los sistemas de información.

Este seminario presentará la metodología para realizar auditorías de sistemas, alineadas con las normas de auditoria de aceptación general (NAGAs) y las normas de auditoría de TI promulgadas por el IIA e ISACA y las buenas y mejores prácticas de gestión y seguridad de TI vigentes en el mundo (COBIT, ITIL, ISO 27001:2013, ISO 20000, ISO 22301 e ISO 38500).

PROPUESTA DE VALOR

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

a. Elaborar el **plan anual de la auditoría de sistemas "basado en valoración de riesgos"**, para los procesos de la infraestructura de servicios de TI y las aplicaciones de computador que soportan los procesos las operaciones de negocio y administrativas de la empresa.

b. Planear y desarrollar **auditorías de sistemas a la infraestructura de TI y las aplicaciones de computador en producción, basadas en riesgos críticos**, de acuerdo con estándares internacionales de auditoria generalmente aceptados y las normas de auditoria promulgadas por IIA e ISACA.

c. Identificar, analizar y evaluar los eventos de riesgo negativos que pueden presentarse en la infraestructura de TI y las Aplicaciones de Computador, evaluar el diseño y efectividad de los control establecidos y ejecutar las pruebas de auditoría (de cumplimiento y sustantivas).

d. Elaborar y organizar papeles de trabajo de la Auditoría de Sistemas.

e. Elaborar informes eficaces de Auditoría de Sistemas, con los resultados de la Auditoria Basada en Riesgos Críticos.

1. OBJETIVOS DEL SEMINARIO

a) Presentar la metodología para realizar Auditorías de Tecnología de Información (TI), "basada en riesgos críticos", de acuerdo con las normas de auditoría generalmente aceptadas, las normas de Audito ría Interna del IIA, las normas de auditoría de sistemas emitidas por ISACA y normas locales expedidas por los organismos de supervisión y control del Estado.

b) Desarrollar habilidades en los participantes para planear y desarrollar auditorías **de sistemas basadas en riesgos críticos**, en los Servicios de tecnología de Información y las aplicaciones de computador que soportan el desarrollo de las operaciones de las empresas.

C) Presentar y analizar las técnicas y herramientas de auditoria asistidas por computador para apoyar la planeación y desarrollo de las **auditorías de tecnología de información basadas en riesgos críticos**.

2. A QUIÉN VA DIRIGIDO.

El seminario está dirigido a Auditores de Sistemas, Auditores Internos y Externos, Revisores Fiscales, Contralores, Funcionarios de Oficinas de Control Interno y consultores en auditoría que deseen actualizar o profundizar sus conocimientos sobre auditoría de sistemas de información.

3. TEMAS DEL SEMINARIO

DIA 1.

1) **INTRODUCCION.**

- Objetivos y alcance de la Auditoría de Sistemas de Información.
- Normas de Auditoria de Aceptación General y su aplicabilidad en Auditoria de Sistemas.
- Normas de Auditoría de Sistemas promulgadas por ISACA.
- La Auditoria de Sistemas dentro de las Auditorias Internas, Revisorías Fiscales y Auditorias Financieras.
- Los Enfoques de Auditoría proactivo y reactivo.

2) PLANEACION ANUAL DE AUDITORIA DE SISTEMAS, BASADA EN VALORACION DE LA EXPOSICION A RIESGOS de los procesos de TI y las aplicaciones de computador.

- Definición del Universo de Servicios de TI Auditables en la Empresa.
- Definición del Universo de Clases de Riesgos que podrían afectar negativamente las operaciones de Negocio y Servicios de la Empresa a través de la tecnología de información.
- Elaboración y procesamiento de cuestionarios con factores de riesgo para evaluar exposición a riesgos de los procesos de TI y las aplicaciones de computador en producción.
- Taller 1: Planeación de la Auditoría a los procesos de Control General de TI.
- Taller 2: Planeación de la Auditoría de Aplicaciones de Computador en producción.

3. TEMAS DEL SEMINARIO

3) MARCO DE REFERENCIA PARA EL DESARROLLO DE AUDITORIAS DE SISTEMAS "BASADAS EN RIESGOS CRITICOS".

- Fases y Etapas de la metodología de Auditoría de Sistemas basada en Riesgos Críticos.
- Productos entregables de cada etapa de la metodología.

DIA 2.

4) AUDITORIA A LA INFRAESTRUTURA DE TI – PARTE 1: PLANEACIÓN BASADA EN RIESGOS.

- Memorando de planeación, comprensión del proceso o sistema objeto de la Auditoría, identificación y análisis de la muestra de riesgos inherentes para los cuales se evaluará el control interno y se ejecutaran pruebas de auditoría.
- Taller 3: Identificación de muestra de Riesgos Inherentes para procesos de la infraestructura de TI (Controles Generales de TI).
- Taller 4: Análisis y Evaluación de la muestra de riesgos inherentes para procesos de la infraestructura de TI (Controles Generales de TI).

5) AUDITORIA A LA INFRAESTRUCTURA DE TI – PARTE 2: EVALUACIÓN DEL DISEÑO Y EFECTIVIDAD DE LOS CONTROLES ESTABLECIDOS.

- Conceptos sobre controles, tipos de controles y alternativas utilizadas por los Auditores para evaluar la efectividad del sistema de control interno.
- El Enfoque Proactivo / preventivo de los controles.
- Cómo Identificar y documentar los controles establecidos en la organización para reducir la severidad de los riesgos inherentes.
- Criterios para evaluar la el diseño y la efectividad de los controles establecidos.
- Taller 4: Evaluación de controles por eventos de riesgo críticos, para LA infraestructura de TI (Controles Generales de TI)**.**

6) **AUDITORIA A LA INFRAESTRUCTUA DE TI – PARTE 3: DISEÑO Y EJECUCIÓN DE PRUEBAS DE AUDITORIA.**

- Diseño, planeación y ejecución de Pruebas de Cumplimiento y sustantivas con base en los resultados de la evaluación del control interno por eventos de riesgo.
- Técnicas y procedimientos de Auditoría a utilizar en las pruebas de auditoria
- Taller 5: Diseño de Pruebas de cumplimiento y sustantivas a la infraestructura de TI (Controles Generales de TI), por sitios de prueba.

DIA 3.

7) AUDITORIA A LAS APLICACIONES DE COMPUTADOR EN FUNCIONAMIENTO, BASADA EN RIESGOS CRITICOS.

- Planeación detallada de la Auditoría (objetivos, alcance, puntos de interés, asignación de recursos).
- Comprensión (Caracterización) del ambiente técnico, administrativo y operativo de la Aplicación sujeta a auditoría.
- Taller 6: Identificación, análisis y Evaluación de Riesgos inherentes (eventos de riesgo negativos) a considerar por la auditoria.
- Técnicas y procedimientos de Auditoría a utilizar en las pruebas de auditoría.
- Taller 7: Evaluación del diseño y Efectividad del control interno existente para los eventos de riesgo negativos.
- Taller 8: elaboración del informe de la Auditoría con los resultados de la evaluación de controles.
- Diseño, planeación y ejecución de Pruebas de Cumplimiento y sustantivas con base en los resultados de la evaluación de control interno por eventos de riesgo negativos (amenazas).

8) PAPELES DE TRABAJO DE LA AUDITORÍA DE SISTEMAS.

- Criterios y procedimientos para elaboración y conservación de los papeles de trabajo.
- Archivos permanentes (forma y contenido).
- Archivos Corrientes (Forma y Contenido).

9) ***INFORMES DE AUDITORIA DE SISTEMAS****.*

- *Importancia de las comunicaciones eficaces en Auditoria.*
- *Criterios y procedimientos para redactar informes de auditoría eficaces.*
- *Taller 9: Redacción de Informes de Auditoria de Sistemas.*

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores y desarrollo progresivo de talleres preparados para ejecutar las etapas de la metodología de auditoría de Tecnología de información basada en riesgos.

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

- **Obligatorios**: Conocimientos básicos de Sistemas de Información y metodologías de gestión de riesgos.
-
- **Deseables:** Llevar un computador portátil (Windows,32 MB en RAM, 60MB en disco duro y unidad de entrada para acceder a los materiales de trabajo, 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.

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 Y DURACIÓN

FECHA: Agosto 23, 24 y 25 de 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	$ 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

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.

(*) Requiere tener instalado el Software IDEA.