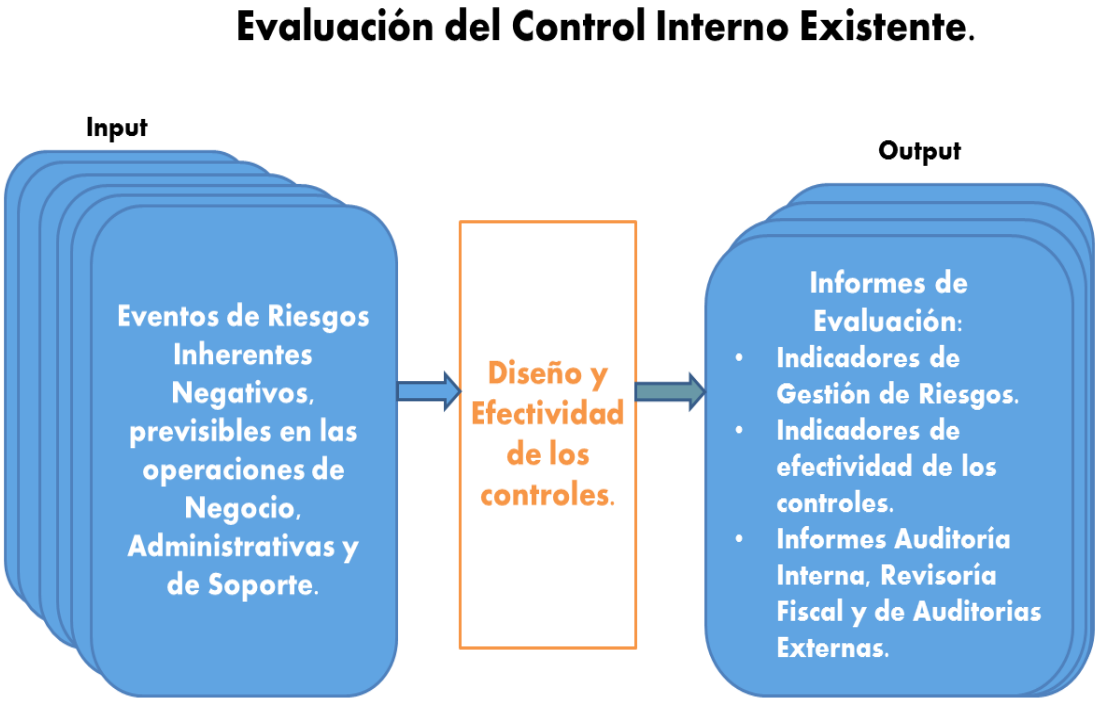
Seminario – Taller Virtual
EVALUACIÓN DE CONTROLES INTERNOS, PARA AUDITORES

Contenido:	Pág

PRESENTACIÓN

Evaluar el diseño y la Efectividad del Control de Riesgos por los auditores internos y externos, Revisores Fiscales y los administradores de riesgos, es una *actividad indispensable* para el aseguramiento de la *adecuada gestión de riesgos y de control interno* en 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).



Los resultados de la evaluación y aseguramiento por parte de los auditores deberían revelar ***los niveles reales de protección ofrecida por los controles establecidos y del 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. Estos resultados servirán como retroalimentación para que *la Gerencia y los responsables de los procesos auditados, realicen ajustes necesarios en el control de riesgos para proteger los activos de la organización y asegurar que los procesos y sistemas satisfacen sus necesidades de manera segura y confiable.*

Los resultados de estas evaluaciones también se divulgan en informes periódicos de las Gerencias de Riesgos, los cuales 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.

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

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) Aplicar los *estándares y buenas prácticas de análisis de riesgos* para identificar vulnerabilidades y agentes generadores del riesgo que deben eliminarse y neutralizarse con los controles.

b) 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.

c) 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*

d) 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 monitores periódicos que deben efectuarse en los diferentes sistemas de gestión de riesgos de la organización.

e) *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 VA 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 *estándares y buenas prácticas q*ue se utilizan 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) 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.

3) 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 o 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. 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

FECHAS: Mayo 4, 5 y 6 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	COL $ 1.500.000 + IVA

Descuentos por Inscripción.	
Clientes de servicios y productos de AUDISIS	10%
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.