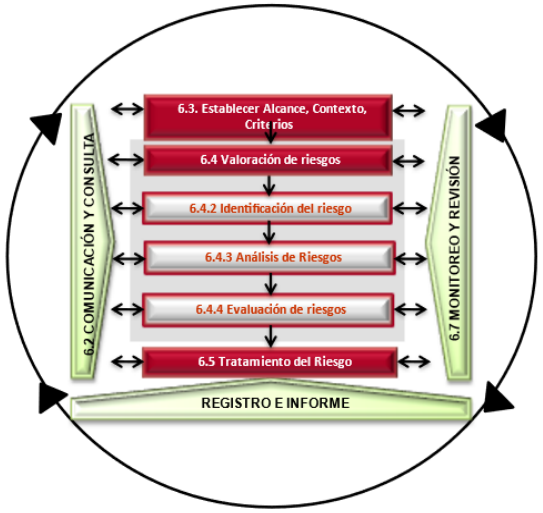
Seminario – Taller Virtual
GESTION DE RIESGOS OPERACIONALES (SARO): IMPLANTACIÓN Y MEJORAMIENTO CONTINUO.

PRESENTACIÓN

El seminario presentará la metodología para implantar el Sistema de Administración del Riesgo Operativo (SARO), de acuerdo con marcos de referencia internacionales de Gestión de Riesgos y las normas establecidas por las Superintendencias Financiera y de Economía Solidaria y el DAFP *para identificar, analizar, valorar, controlar y monitorear los riesgos operativos de los procesos y la tecnología de información de las organizaciones.*

ISO 31000: 2018 - Elementos del Proceso de Gestión del Riesgo



ControlRisk: Software de Administración de Riesgos Empresariales

El Riesgo Operativo se define así*:*

"La posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos". Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

El Sistema de Administración de Riesgo Operativo (SARO) se define así:

"*Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo".*

Los temas del seminario se desarrollarán en concordancia con la **Norma ISO 31000:2018, gestión de riesgos - principios y directrices**, el modelo de Administración de Riesgos Empresariales (ERM, por sus siglas en inglés), el COSO 2013 y las Normas expedidas sobre el SARO por la Superintendencia Financiera de Colombia (SFC) y Superintendencia de Economía Solidarias de Colombia.

PROPUESTA DE VALOR

Al finalizar el seminario los participantes estarán en capacidad de:

a) Elaborar el framework o marco de referencia del sistema de administración del Riesgo Operativo (SARO de la Empresa, armonizado con el Sistema de Gestión de la Calidad (ISO 9001), el sistema de Gestión de Seguridad de la Información (ISO 27001) y el Sistema de Control Interno de la Organización.

b) Identificar los eventos de riesgo inherentes de cada proceso de la Empresa, por cada una de las *clases o categorías de eventos de riesgo operativo (Fraude Interno, fraude externo, relaciones laborales incompatibles, daños a activos físicos, fallas con los asociados o clientes, fallas tecnológicas y errores en la ejecución y administración de procesos)*.

c) Analizar los seis (6) elementos del riesgo aplicando métodos cualitativos y cuantitativos, como base para determinar la gravedad o severidad de los eventos de riesgo y diseñar los controles para mitigarlos.

d) Establecer y aplicar criterios para medir la **efectividad** (eficacia y eficiencia) individual y colectiva de los controles que se establezcan para reducir la severidad de cada uno de los riesgos inherentes a niveles aceptables de riesgo residual.

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

f) Diseñar e Implantar el Registro de Eventos de Riesgo Operativo Ocurridos en la organización.

g) Discernir sobre la importancia y la metodología de implantación y mantenimiento del Plan de Continuidad del Negocio (BCP).

1. OBJETIVOS DEL SEMINARIO

- Transferir conocimientos, experiencia y la metodología *para implantar el sistema de Administración de Riesgo Operativo (SARO) en las empresas.*

- Proveer la metodología para *identificar, analizar, valorar la severidad, controlar y monitorear los eventos de riesgo operativo, inherentes a cada proceso de la organización*.

- Proveer estrategias para proyectar a mediano y largo plazos, la evolución, *perdurabilidad y mejoramiento continuo* del SARO en la Empresa.

2. A QUIÉN VA DIRIGIDO.

El seminario está dirigido a Gerentes y Analistas de Riesgos Operativos de Entidades Financieras, del Sector Solidario y de Entidades Públicas interesadas en el riesgo operativo. También a Auditores Internos, Revisores Fiscales y profesionales de Seguridad de la Información.

3. TEMAS DEL SEMINARIO

DIA 1.

1. MARCOS DE REFERENCIA PARA IMPLANTAR EL SISTEMA DE ADMINISTRACION DEL RIESGO OPERATIVO (SARO).

- Generalidades de la Gestión de Riesgos bajo las norma ISO 31000:2018 y el modelo ERM 2017
- Marco normativo de la SFC para el SARO (Circular 025 de 2020).
- Marco normativo de la Supersolidaria para el SARO (Titulo IV, capitulo IV Circular Básica Contable y Financiera año 2020).
- Marco Normativo para implantar la Gestión de Riesgo Operativo en las entidades del Sector Publico.

2. **METODOLOGIA PARA IMPLANTAR EL SARO EN LOS PROCESOS DE LA ORGANIZACIÓN – Parte 1: El Framework de la Gestión de Riesgos Operativos.**

- Contenido sugerido para el Framework o marco de Trabajo de la Gestión del Riesgo Operativo en la Empresa.
- Diseño de la Política de Gestión de Riesgos Operativos.
- El Universo de Riesgos Operativos de la Empresa.
- Taller 1: Cómo priorizar las clases o categorías de riesgo operativo para la cada proceso.
- El Ciclo PHVA de la Administración de Riesgos por cada proceso o sistema de la Empresa.
- Etapas de la METODOLOGÍA de implantación del sistema de gestión de riesgos operativos, por proceso.
- Estructura de organización y soporte tecnológico requerido para la Gestión de Riesgos Operativos.

3. TEMAS DEL SEMINARIO

DÍA 2.

3. METODOLOGIA PARA IMPLANTAR EL SARO EN LA ORGNIZACION – PARTE 2: IDENTIFICACIÓN Y ANALISIS DE RIESGOS POR PROCESO.

- Definición de Contexto interno y externo del Proceso
- Caracterización del proceso.
- Identificación y priorización de clases de riesgo aplicables por proceso.
- Taller 2: Priorización de categorías del Universo de Riesgos de la Empresa, aplicables al proceso – Aplicación del principio de Pareto y del Poder del 3.
- Taller 3: Identificación de los Eventos de Riesgo Inherentes que pueden presentarse en el proceso
- Los seis (6) elementos del Riesgo
- Métodos de análisis de riesgos (cualitativa y cuantitativa)
- Taller 4: Análisis de los eventos de por cada evento de riesgo inherentes
- Matrices / Mapas de Riesgos Inherentes por proceso.
- Matices / mapas de Riesgo Consolidado de la Organización.
- Taller 5: Definición de objetivos de Control para el proceso.
- Definición de Acciones de Respuesta a Riesgos.

4. METODOLOGIA PARA IMPLANTAR EL SARO EN LA ORGANIZACIÓN – PARTE 3: CONTROL Y TRATAMIETO DE RIESGOS –.

- Conceptos fundamentales sobre controles y metodología de deseño e implantación de controles por riesgo.
- Taller 6: Diseño de controles por evento de riesgo
- Cómo identificar los controles establecidos en el proceso.
- Criterios para determinar la efectividad (Eficacia + Eficiencia) individual y colectiva de los Controles establecidos por evento de riesgo.
- Taller 7: Evaluar efectividad de los Controles por Evento de Riesgo Inherente)
- Elaboración del Mapa de Riesgos Residuales – antes de tratamientos.
- Taller 8: Diseño, implantación y seguimiento del Plan de Tratamiento de Riesgos.
- Elaboración del Mapa de Riesgos Residuales – Después de tratamientos.

DIA 3.

5. METODOLOGIA PARA IMPLANTAR EL SARO EN LA ORGANIZACION – PARTE 4: MONITOREAR LOS RIESGOS Y CONTROLES ESTABLECIDOS.

- Conceptos y metodología para Monitoreo de los Riesgos y Controles
- Elaboración de Guías de Monitoreo / Auto-aseguramiento de Controles (Control Self Assessment)
- Generación de Indicadores de gestión de riesgos por proceso.
- Elaboración del Plan de Acciones de Mejoramiento como resultado de cada monitoreo.

6. METODOLOGIA PARA IMPLANTAR EL SARO EN LA ORGANIZACION – PARTE 5: OTROS COMPONENTES DEL SARO.

- El perfil de riesgos consolidado de la Organización.
- Implantación y mantenimiento del Registro de Eventos de Riesgo Ocurridos (RERO).
- Implantación y Mantenimiento del Plan de Continuidad del Negocio – BCP (El estándar ISO 22301:

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

El seminario está estructurado en la modalidad de Taller y se desarrollará de manera interactiva entre facilitador y participantes, con el apoyo de ayudas audiovisuales, casos y experiencias del mundo real).

Durante el seminario se desarrollará un caso práctico para implantar el SARO para un proceso de la cadena de valor

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

FORMA DE EVALUACION

Al inicio del seminario se aplicará un cuestionario para evaluar el nivel de conocimientos de los participantes.

Cada participante deberá acreditar el diligenciamiento de los formatos en los que se registrará la información del caso práctico que se desarrollará durante el seminario.

Adicionalmente, al final del seminario se aplicará un cuestionario para medir el conocimiento obtenido y comparar con la evaluación del cuestionario inicial.

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: Septiembre 6, 7 y 8 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. PERI-TAZGOS 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.