Seminario Taller Virtual
IMPLANTACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO - ALINEADO CON LA NORMA ISO 22301:2019.

PRESENTACIÓN

La Gestión de Continuidad del Negocio (BCM por sus siglas en inglés – Business Continuity Management), está definida como *"el proceso integral de gestión que identifica las amenazas potenciales que pueden poner en riesgo la continuidad de la organización, el impacto que éstas pueden causar en los procesos del negocio y provee el marco para la construcción de la resiliencia con capacidad de respuesta efectiva para salvaguardar los intereses, la reputación, la marca y el valor de las actividades de la Empresa".*

Para todas las organizaciones, administrar adecuadamente la continuidad de sus operaciones y contar con los procedimientos que garanticen salvaguardar la vida de sus empleados y visitantes, así como la reanudación oportuna y ordenada de sus procesos y funciones críticas después de una interrupción, es de vital importancia y es definitivamente la diferencia entre el éxito y el fracaso.

La norma ISO 22301:2019 establece los controles que cubren el ciclo de vida de un BCM alineado con las mejores prácticas del mercado; este curso está enfocado en entender las actividades de establecimiento, implementación, operación, evaluación y mejora de un BCM de acuerdo a la norma ISO 22301:2019.

POR QUÉ ASISTIR A ESTE SEMINARIO?.

Durante 3 días, los conferencistas compartirán experiencias y vivencias teóricas y prácticas de la implementación y Auditoria de un Sistema de Gestión de Continuidad del Negocio (BCMS) 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.

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

a) Justificar la necesidad de implementar un BCMS en las organizaciones.

b) Establecer, implementar, operar y evaluar un BCMS según lo define la norma ISO 22301:2019

c) Soportar, presentar y obtener el apoyo de la alta gerencia para implementar un BCMS.
d) Identificar las partes interesadas en el BCMS
e) Diseñar, documentar e implantar la política del BCMS, que incluya el alcance, los objetivos y los requisitos legales, normativos y comerciales aplicables a las organizaciones.
f) Identificar los requerimientos presupuestales para el BCMS
g) Identificar, medir, controlar y monitorear los riesgos que puedan afectar la continuidad de los procesos críticos.
h) Desarrollar el análisis de impacto del negocio (BIA)
i) Definir las estrategias de continuidad y documentar los procedimientos de recuperación y continuidad necesarios.
j) Definir un plan general de manejo de crisis y el plan de comunicaciones en crisis.
k) Evaluar la efectividad del BCMS
l) Aplicar la norma ISO 19011:2018 para auditor el BCM.

1. OBJETIVOS DEL SEMINARIO

- Presentar la metodología para desarrollar el sistema de gestión de continuidad del negocio (BCMS) dentro de la organización, en concordancia con la las norma ISO 22301:2019.
- Desarrollar habilidades en los participantes para realizar una adecuada administración de riesgos de continuidad y la elección de los controles más eficaces y eficientes para mitigarlos.
- Desarrollar habilidades para desarrollar un análisis de impacto al negocio BIA.
- Desarrollar habilidades para identificar y documentar las estrategias de continuidad.
- Desarrollar habilidades para realizar pruebas y mejorar continuamente el BCMS

2. A QUIENES ESTÁ DIRIGIDO

Gerentes de Tecnología de Información y Comunicaciones, Gerentes de Riesgos, Jefes de Planeación, Administradores de Seguridad Informática, Oficiales de Seguridad, Auditores Internos, Revisores Fiscales, Auditores de Sistemas, responsables de la continuidad del negocio, Organizaciones en proceso de implementación sistemas de gestión de continuidad del negocio o del BCP.

3. TEMAS DEL SEMINARIO

DIA 1.

1. **INICIO Y ADMINISTRACION DEL BCMS – 3 horas**.
   - **La norma ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements**
   - Definición y conceptos generales del continuidad del negocio.
   - Establecer la necesidad y alcance del BCMS en la Organización.
   - Obtener el apoyo de la alta gerencia para el desarrollo y mantenimiento del BCM.
   - Identificar la organización y responsabilidades del BCM (implementación y operación)
   - Política del BCMS.

2. **METODOLOGIA PARA IMPLANTACION DEL BCMS – Parte 1 (5 Horas).**

   Análisis de impacto al negocio..
   - Identificar procesos y recursos críticos.
   - identificar los impactos financieros, operativos, comerciales, de SST, reputacionales y legales generados por la pérdida de disponibilidad de los procesos
   - Identificar MTD, RPO, RTO y WRT.

   Evaluación y control de riesgos.
   - Identificar amenazas.
   - Identificar vulnerabilidades.
   - Identificar controles necesarios.

DIA 2.

3. **METODOLOGIA PARA IMPLANTACION DEL BCMS – Parte 2 (8 horas).**

   Desarrollo de estrategias de continuidad.
   - Identificación de requerimientos.
   - Opciones de estrategia de continuidad.
   - Implementando las estrategias de continuidad – Costos.

   Desarrollar y documentar procedimientos de
   - Recuperación y continuidad
   - Preparación y respuesta de emergencias.

DIA 3.

4. **METODOLOGIA PARA IMPLANTACION DEL BCMS – Parte 3. (6 horas)**

   - Programas de concienciación y capacitación del BCMS
   - Pruebas del BCMS
   - Mantenimiento del BCMS.
   - Comunicación de crisis.

5. **AUDITORIA AL BCMS UTILIZANDO LA NORMA ISO 19011: 2018 (2 horas).**
6. **El PROCESO DE CERTIFICACION INTERNACIONAL (2 horas).**

DURACION: 24 Horas

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores utilizando filminas, desarrollo de ejercicios de aplicación 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 y los talleres y casos de estudio.

6. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

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

7. CERTIFICACIÓN DE ASISTENCIA

A los participantes que participen en el 80% o más de las sesiones del seminario se entregará certificación de asistencia.

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 Auditoria / Consultoria de AUDISIS**. Ingeniero de Sistemas. MBA, Magister en Dirección y Administración de Empresas. Título de Posgrado en Auditoría de Sistemas. CISA (Certified Information Systems Auditor). Experto en Seguridad y Auditoría de sistemas. 32 años de experiencia. Expresidente de la Asociación Colombiana de Auditores de Sistemas (ACDAS) y fundador y expresidente 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, Central de Bogotá, Antonio Nariño, El Rosario, Santo Tomás de Aquino (Bucaramanga), Universidad Militar, UNAB, FUNDEMA (Manizales), Santiago de Cali, Libre de Colombia (Bogota 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 capítulos de Bogotá y Medellín y al LATINCACS de México.

Alvaro Mauricio Romero. – Consultor Seguridad Informática y análisis forense., de AUDISIS.

Experto en Tecnología y Seguridad Informática con certificaciones como auditor líder BS ISO/IEC 27001:2005 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 y CISSP. Auditor interno norma ISO 9001 versión 2000. Cuenta con más de 18 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 del sistema, y auditorias basadas en riesgos en Organizaciones nacionales e internacionales del sector servicios y financiero.

Se ha desempeñado por más de 10 años como docente en Seminarios, diplomados y especializaciones de Seguridad Informática y Análisis Forenses 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. Entre otros, los seminarios dictados son:

- Seminario taller Implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2005.
- Seminario para auditores internos del SGSI.
- Seminario taller de implementación del plan de continuidad del Negocio BCP.
- Seminario taller de control interno y diseño de controles con énfasis en el cumplimiento de la CE038 SFC y CE023 SSF.
- Seminario taller de auditoria basada en riesgos.
- Seminario taller de Ethical hacking y análisis forense informático.

Actualmente es docente en la ESCUELA DE COMUNICACIONES DEL EJERCITO NACIONAL en la especialización de seguridad física y de la información dictando las cátedras de seguridad en sistemas operativos, plan de continuidad del negocio, ethical hacking y análisis forense informático.

Como consultor de AUDISIS ha participado en proyectos de implantación del BCP en DINISSAN y SCARE y en proyectos de seguridad y auditoría al BCP en 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. FECHAS, DURACIÓN Y HORARIO DEL SEMINARIO

FECHAS: Octubre 12, 13 y 14 del 2022.

DURACIÓN: 24 Horas

HORARIO: De 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm

FORMA DE PAGO

- En cheque a nombre de AUDISIS o transferencia de fondos a la cuenta corriente de AUDISIS.
- Transferencia de fondos a la cuenta corriente Numero **07511792-9** del Banco de Bogotá, Sucursal Galerías.

10. 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%

11. 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**.

12. 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.

13. 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.

14. SEMINARIO IN-HOUSE

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.

15. 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. Softwa-

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.