Seminario Taller
GESTION DE CONTINUIDAD DEL NEGOCIO (BCM)- ALINEADO CON LA NORMA ISO 22301/2012- IMPLANTACION Y AUDITORIA

Contenido:	Pág

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 y el impacto que pueden causar en los procesos del negocio y proporciona el marco para la construcción de la resiliencia con la capacidad para una respuesta defectiva que salvaguarde los intereses, la reputación, la marca y el valor de las actividades".

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

La norma ISO 22301:2012 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 22301:2012.

POR QUÉ ASISTIR A ESTE SEMINARIO?.

Este seminario permitirá a los asistentes conocer los procesos para la creación, implementación, operación y evaluación de un Sistema de Gestión de continuidad del Negocio (BCMS) basado en la norma ISO 22301: 2012.

Durante 3 días, los conferencistas compartirán experiencias y vivencias sobre teoría y la práctica de la implementación de un BCMS en empresas de diferentes tamaños y grados de sofisticación, y darán res-

puesta a las inquietudes de los participantes respecto a los problemas y desafíos que se presentan en la ejecución del proyecto.

Algunos interrogantes que podrán resolver los participantes en este seminario son:

- Como establecer la necesidad de implementar un BCMS en las organizaciones.
- Como establecer, implementar, operar y evaluar un BCMS según lo define la norma ISO 22301:2012.
- Cómo soportar, presentar y obtener el apoyo de la alta gerencia para implementar un BCMS.
- Cómo identificar los requerimientos presupuestales para el BCMS
- Como identificar, medir, controlar y monitorear los riesgos que puedan afectar la continuidad de los procesos críticos.
- Cómo desarrollar un análisis de impacto al negocio.
- Cómo definir las estrategias de continuidad y documentar los procedimientos de recuperación y continuidad necesarios.
- Como evaluar la efectividad del BCMS.
- Como aplicar la norma ISO 19011:2011 para realizar una auditoría al BCM?.
-

1. OBJETIVOS DEL SEMINARIO

- Presentar la metodología para desarrollar el plan de gestión de continuidad del negocio (BCMS) dentro de la organización, en concordancia con la las norma ISO 22301:2012
- 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 mejora continua del 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 de Sistemas, responsables de la continuidad del negocio, Organizaciones en proceso de implementación sistemas de gestión de continuidad del negocio o planes de continuidad del negocio.

3. TEMAS DEL SEMINARIO

DIA 1.

1. **INICIO Y ADMINISTRACION DEL BCMS – 3 horas**.
   - La norma ISO 22301:2012.
   - 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 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 MTD.
   - Identificar RPO y RTO.

   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.
   - Auditoria del BCMS.

5. **AUDITORIA AL BCMS UTILIZANDO LA NORMA ISO 19011: 2011.**
6. **El PROCESO DE CERTIFICACION INTERNACIONAL (2 horas).**

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

Presentación de los temas por parte de los instructores utilizando diapositivas, 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

AUDISIS entregará certificación de asistencia a los participantes que asistan al 80% en adelante de las horas programadas.

8. INSTRUCTORES

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, 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. – 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 27001:2013.
- 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 talle 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 seguridad realizados para FUNDACION DE LA MUJER, FINAGRO, COMFENALCO TOLIMA, FIDUCIARIA BOGOTA, SEGUROS GENERALI, LAFAYETTE, PROENFAR, INIF, HOSPITAL SAN IGNACIO, BOLSA MERCANTIL DE COLOMBIA, TERMINAL DE TRANSPORTES, UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA Y EL ICFES. También ha sido instructor en cursos y seminarios organizados por AUDISIS.

9. FECHAS, DURACIÓN Y HORARIO DEL SEMINARIO

LUGAR: Bogotá, D.C. - GHL Hotel Capital.
FECHAS: Junio 5, 6 y 7 de 2019.
Noviembre 5, 6 y 7 de 2019.
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 **075 11792-9** del Banco de Bogotá, Sucursal Galerías.

10. VALOR INVERSIÓN POR PARTICIPANTE

Pagos antes del Seminario	Pagos después del Seminario
COL $ 1.450.000 + IVA	$ 1.515.000 + IVA

Descuentos por Participantes de la misma Empresa	
3 Participantes	3 %
4 y 5 Participantes	5 %
Más de 6 Participantes	7.5 %

Miembros de ISACA y del IIA : Descuento del 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

Se acepta anulación de inscripciones por escrito, hasta 4 días hábiles antes de la realización del seminario Después de esta fecha, únicamente se aceptará el cambio de participantes.

13. PLAZO PARA CANCELAR LA REALIZACIÓN DEL SEMINARIO

AUDISIS se reserva el derecho de cancelar el seminario en caso de no completarse el número mínimo de participantes requeridos.

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 y el mejoramiento continuo de la calidad.

1. **CONSULTORÍA EN GESTION DE RIESGOS, SEGURIDAD Y CONTROL INTERNO EN PROCESOS DE NEGOCIO Y TECNOLOGIA DE INFORMACION.**

   - Implantación de Sistemas de Control Interno (COBIT, MECI, COSO).
   - Implantación de Gestión de Seguridad de la Información (ISO 27001).
   - Implantación de Gestión de Riesgos empresariales con base en ISO 31000:2009 (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. Desarrollo de programas Antifraude.

2. **AUDITORÍAS DE SISTEMAS Y DE PROCESOS DEL NEGOCIO.**

   - Auditorías de Sistemas de Información "Basada en Riesgos Críticos".
   - Pruebas de Hacking Ético.
   - Auditoría Forense.
   - Auditoría Basada en Riesgos críticos a procesos de Negocio.

3. **OUTSOURCING DE AUDITORÍAS INTERNAS DE SISTEMAS DE INFORMACIÓN.**

4. **AUTOMATIZACIÓN DE PRUEBAS DE AUDITORÍA A LA MEDIDA DE LAS NECESIDADES DE LA EMPRESA (Desarrollo de CAATTs).**

5. **INTERVENTORIA EN PROYECTOS DE SISTEMAS, SEGURIDAD Y AUDITORÍA DE SISTEMAS.**

   - Interventoría al diseño y/o estrategias de tecnología.
   - Interventoría a la implantación de soluciones de tecnología.
   - Interventoría al desarrollo de soluciones de tecnología.
   - Interventoría a la gerencia de proyectos de tecnología.

6. **PERITAZGOS EN LITIGIOS DE CONTRATOS DE SERVICIOS PROFESIONALES EN TECNOLOGÍA DE INFORMACIÓN.**

7. **EDUCACIÓN Y DESARROLLO PROFESIONAL EN CONTROL INTERNO, ADMINISTRACIÓN DE RIESGOS, SEGURIDAD DE TI Y AUDITORÍA DE SISTEMAS.**

   - Seminarios abiertos virtuales para para participantes de diferentes empresas.
   - Seminarios cerrados presenciales o virtuales, dentro de las empresas.

NUESTROS PRODUCTOS

- **AUDIRISK:** Software de Auditoría Basada en Riesgos críticos para Procesos de Negocio, Sistemas y Tecnología de Información. (*)

- **CONTROLRISK:** Software de Gestión de Riesgos y Diseño de Controles para Procesos de Negocio, Sistemas y Tecnología de Información**.** (*)

- **IDEA**: Software para Análisis, Extracción, Auditoría de Datos y Desarrollo de CAATTs.

- **WORKING PAPERS:** Software de Papeles de Trabajo de Auditoria Financiera.

- **MONITOR:** Software de Monitoreo Continuo y Auditoría Continua de Riesgos y Controles.

(*) La integración de **AUDIRISK** con **CONTROLRISK** permite a los auditores y administradores de riesgos compartir la **base de conocimientos o metadata de la empresa** que contiene la definición de categorías de riesgo, amenazas, activos impactados, vulnerabilidades, agentes generadores de riesgo, controles, objetivos de control y escenarios riesgo.