CURSO
GESTIÓN AGIL INTEGRAL: RIESGOS DE TI/OPERATIVOS/CONTINUIDAD

La Gestión de Riesgos aplicada a TI de una forma ágil e integrada a las Operaciones

Instructor: Ing. Daniel De Giorgio, ISO 27001_02_32_35, ISO 22301, SSBB, ITIL –

Duración: 16hs

Un enfoque **aplicable y práctico** con: **casos prácticos reales, juegos** originales de **simulación**, **videos**, ejemplos de **entregables, plantillas** y ejercicios basados en **desafíos cotidianos** que las organizaciones de **nuestro contexto regional** deben resolver, con **la teoría al servicio de la acción**.

OBJETIVO DEL CURSO

Este curso le permite desarrollar la experiencia necesaria para ayudar a una organización a establecer, implementar, administrar y mantener un Programa de Gestión de Riesgos de TI basado en las mejores prácticas internacionales. Crear escenarios de riesgos, analizar los riesgos de TI, evaluar controles mitigantes, crear informes para la toma de decisiones, seleccionar la mejor opción para el tratamiento, priorizar planes de acción, actualizar el perfil de riesgo, mejorar y definir KRIs serán algunas de las habilidades que los participantes obtendrán en este curso.

Recorre las mejores prácticas de Gestión de riesgos de TI y Operativos y las etapas necesarias para desarrollar y comprender el proceso, incluyendo los pasos críticos necesarios para lograr una comprensión profunda de la naturaleza y las necesidades de funcionamiento de una Organización, la identificación e implementación de estrategias, cambios en la estructura de la organización y procesos de negocio.

Utilizando casos de estudio basados en escenarios de la vida real, los asistentes adquirirán conocimientos prácticos sobre cómo llevar a cabo una implementación de un programa de Gestión de Riesgos de TI. Permite a los asistentes beneficiarse de un ambiente de aprendizaje dinámico, donde la interacción entre pares fortalece la adquisición de conocimientos a través del intercambio de ideas y experiencias de la vida real.

DESTINATARIOS

Profesionales de las áreas de Seguridad de la Información, Continuidad del Negocio, Riesgos Tecnológicos/Operacionales, Auditoría, Tecnología y Sistemas, Procesos y Cumplimiento. Consultores y Profesionales involucrados en implementar un Programa de Seguridad de la Información en sus Organizaciones.

- Gerentes o consultores involucrados en la Gestión de Riesgos / Seguridad de la Información.
- Asesores expertos que buscan dominar la implementación de un Programa de Riesgos de TI.
- Personas responsables de mantener la conformidad con los requisitos de Riesgos Tecnológicos.
- Miembros del equipo de TI / Riesgos Tecnológicos

TEMARIO

❖ Módulo 1: Enfoque Integral para Gestión Ágil de Riesgos de TI y Operativos

- Introducción
- Estándares Internacionales al servicio de la Gestión Ágil Integral
- Nueva versión del Estándar ISO 31000
- Integrar y Optimizar la Gestión de los Riesgos de TI

❖ Módulo 2: Establecer el Contexto para la Gestión Integral de los Riesgos SI

- Análisis de Contexto Interno/Externo para gestionar Riesgos
- Criterios Metodológicos para Analizar y Aceptar Riesgos
- Inventario de Procesos a Analizar
- Relación entre la Gestión de Riesgos y la Gestión de Continuidad
- Análisis de Impacto al Negocio
- Clasificación de la Información
- Dependencia de Procesos en Activos de TI

❖ Módulo 3: Identificar los Escenarios de Riesgos TI y Operativos a Analizar

- Escenarios de Riesgos - Componentes
- Técnicas de Identificación de Escenarios. Visión General
- Profundizando sobre Técnicas de Identificación de Escenarios de Riesgos de TI
- Identificación de Riesgos de TI y Gestión de Proyectos
- Identificación de Riesgos de Ciberseguridad
- Nivel de Granularidad de los Escenarios de Riesgos
- Registro de Riesgos Ejemplo de Escenarios Confidencialidad
- Otros ejemplos de Escenarios de Riesgos de TI y Operativos

❖ Módulo 4: Análisis de Riesgos de TI y Operacionales

- Análisis de Riesgo de los Activos de TI - Enfoque
- Análisis de Riesgo de TI - Impacto y Criticidad
- Análisis de Riesgo de TI - Probabilidad y Ocurrencia
- Matriz para Análisis de Riesgo de los Activos de TI
- Relacionar Riesgos de los Activos de TI con los Procesos Operativos
- Análisis Cuantitativo de los Riesgos de TI y Operativos. Desafíos
- Análisis Cuantitativo de los Riesgos de TI y Operativos. Pasos
- Integrar Riesgos de TI al Riesgo Operacional
- Resultados Integrados - Criterios para Consolidar

❖ Módulo 5: Evaluación y Tratamiento de los Riesgos de TI y Operativos

- Evaluación de Riesgos: Causas de los Escenarios
- Evaluar Relaciones entre Escenarios de Riesgos
- Comparación Apetito de Riesgos Genéricos o Específicos
- Tratamiento de los Riesgos Inaceptables
- Gestión de la Continuidad y Tratamiento de Riesgos
- Gestionar Proyectos para Tratar Riesgos
- Monitoreo y Control de la Gestión de Riesgos de TI y Operativos
- Mejora Continua de las Capacidades de la Gestión de Riesgos
- De la Gestión de Riesgos Estática a la Dinámica
- Conclusiones y Cierre

DESAFIOS FRECUENTES ABORDADOS POR EL TALLER:

- **Síndrome de la hoja en blanco:** dificultades para empezar a construir y gestionar un Programa de Riesgos Tecnológicos.
- **Alcances desmedidos:** expectativas de querer analizar todos los impactos a todos los activos.
- **El enemigo interior:** silos y solapamientos entre áreas, culturas organizacionales nocivas ("esto no va a pasarnos a nosotros").
- **La obsesión teórica:** metodologías que brillan en el PDF y se apagan al aplicarlas en la realidad.
- **La trampa del pasado:** gestionando el Programa ignorando expectativas, tendencias y necesidades de las partes interesadas.
- **Enfoques estáticos** (para amenazas dinámicas): el peligro de la foto desactualizada y la "falsa sensación de seguridad".
- **Percepción negativa:** la Seguridad de la Información vista como un gasto o solo para cumplir.
- **Des-Integración:** inconsistencias con objetivos, necesidades y prioridades del Negocio.
- **La verdad incómoda:** dificultades para exponer los resultados y necesidades de un Programa de Riesgos Tecnológicos a la Alta Gerencia.

PERFIL DEL INSTRUCTOR: Ing. Daniel De Giorgio, MBCI, ISO LI&LA, SSBB, ITIL:

- Ingeniero Electrónico (UBA).
- Instructor certificado y profesional certificado del Business Continuity Institute UK(BCI).
- Instructor certificado y profesional certificado (Implementador Líder y Auditor Líder) de las normas internacionales ISO-22301, ISO-22317, ISO 22316, ISO 27001, ISO 27002, ISO 27035, ISO-27031 e ISO-27032.
- Asesor Certificado del Modelo de Madurez BCMM © de Virtual Corporation (USA).
- Profesional Certificado Six Sigma Black Belt.
- Profesional Certificado ITIL.
- Profesor universitario invitado en la Maestría de Seguridad de la Información de la Universidad Nacional de Buenos Aires.
- Cuenta con 38 años de experiencia profesional en Tecnologías de la Información y Comunicaciones (TIC) y en la Implementación y Gestión de Programas de Continuidad del Negocio en la industria financiera.

- Disertante en Congresos Internacionales en temas de Continuidad del Negocio.
- Amplia trayectoria en Latinoamérica brindando talleres in-company para distintas industrias.
- Experiencia profesional en Latinoamérica en consultoría sobre las temáticas abordadas en el taller.
- Ha implementado exitosamente Sistemas de Gestión de Seguridad de la Información y Continuidad del Negocio en entidades financieras de la República Argentina y asesora empresas en implementaciones de BCM.
- Director del BCI Regional Forum Argentina.
- Miembro del Comité Editorial del Disaster Recovery Journal en español.
- Miembro de la Junta Directiva de ALCONT (Asociación Latinoamericana de Continuidad de Negocio).
- Miembro del Comité Académico de Usuaria (Asociación Argentina de Usuarios de la Informática y las Telecomunicaciones).
- Miembro #17762 del Business Continuity Institute UK).