cybertrust

Gestión del Riesgo para la Continuidad del Negocio:

De la Teoría a la Acción

cybertrust Academy

En un entorno cambiante y expuesto a disrupciones, el gestionar los riesgos que afectan la continuidad operativa es clave para proteger los procesos críticos y fortalecer la resiliencia organizacional.

Este taller entrega herramientas prácticas basadas en la norma ISO 31000, integrando conceptos de la ISO 22301, para aplicar una gestión de riesgos efectiva enfocada en la continuidad del negocio. A través de actividades participativas y casos reales, los participantes aprenderán a identificar, analizar, evaluar, tratar y monitorear los riesgos, contribuyendo activamente a la preparación y respuesta ante eventos disruptivos.

¿A QUIÉN VA DIRIGIDO?

Este taller está dirigido a profesionales que lideran, gestionan o colaboran en procesos vinculados a la continuidad operativa, la gestión de riesgos y la resiliencia organizacional, incluyendo:

- Equipo de Continuidad del Negocio y Crisis.
- Dueños / Líderes de procesos priorizados / críticos.
- Responsables de continuidad del negocio, crisis, cumplimiento normativo, etc.
- Equipos de riesgos, TI, comunicaciones, facilities, soporte, auditoría y seguridad.
- Consultores o asesores en resiliencia, continuidad del negocio y crisis.

El contenido se adapta tanto a organizaciones del sector público como privado, especialmente en industrias reguladas como banca, seguros, salud, servicios críticos e infraestructura.

OBJETIVO GENERAL

Desarrollar en los participantes las competencias necesarias para identificar, analizar, evaluar y tratar los riesgos que puedan afectar la continuidad operativa de una organización, aplicando los lineamientos de la norma ISO 31000 e integrando principios clave de la gestión de continuidad del negocio según la ISO 22301.

OBJETIVOS ESPECÍFICOS

- Comprender los fundamentos de la gestión de riesgos y su vínculo con la continuidad del negocio.
- Analizar el contexto organizacional y los criterios clave para la gestión del riesgo.
- Identificar, analizar y evaluar los riesgos que amenacen la continuidad.
- Diseñar los planes de tratamiento para abordar los riesgos tratables (sobre el apetito al riesgo organizacional).
- Establecer los mecanismos de comunicación, monitoreo y mejora continua en la gestión de riesgos.

CONTENIDO

Módulo 1: Fundamentos y Comprensión del Contexto Organizacional

- Principios, marco y proceso de la ISO 31000.
- Relación entre gestión de riesgos y continuidad del negocio (ISO 22301).
- Términos clave: riesgo, amenaza, vulnerabilidad, impacto, resiliencia.
- Contexto organizacional y partes interesadas.
- Apetito y tolerancia al riesgo.
- Relación con el Análisis de Impacto al Negocio (BIA).

Módulo 2: Identificación Riesgos de Continuidad del Negocio

- Tipologías de amenazas (naturales, tecnológicas, humanas, externas).
- Identificación de eventos disruptivos y fallas críticas.
- Relación con escenarios definidos en el BIA.
- Técnicas de identificación: entrevistas, análisis histórico, revisión de procesos.
- Casos de estudio para realizar la fase de identificación.

Módulo 3: Análisis del Riesgo

- Definición de escalas: impacto y probabilidad.
- Evaluación al riesgo inherente y residual.
- Aplicación de la matriz de riesgo.
- Casos de estudio para realizar la fase de análisis.

Módulo 4: Evaluación del Riesgo

- Alineación con el apetito y tolerancia al riesgo.
- Criterios de decisión y escalas de aceptación.
- Evaluación comparativa (ranking y semáforos).
- Casos de estudio para aplicar la fase de evaluación.

Módulo 5: Tratamiento del Riesgo

- Estrategias de tratamiento: evitar, mitigar, transferir, aceptar.
- Controles actuales vs. controles requeridos.
- Planes de Tratamiento del Riesgo (PTR).
- Casos de estudio para abordar la fase tratamiento.

CONTENIDO

Módulo 6: Comunicación, Consulta y Gestión de Partes Interesadas

- Flujo de comunicación del riesgo.
- Mecanismos de consulta con las partes interesadas.
- Comunicación en contexto de incidentes.
- Cultura del riesgo.

Módulo 7: Monitoreo, Revisión e Integración con el SGCN

- Indicadores clave de riesgo (KRI) y desempeño (KPI).
- Frecuencia de revisión y actualización de riesgos.
- Auditorías internas y lecciones aprendidas.
- Integración con BIA, RIA y PCN.

DURACIÓN Y MODALIDAD

- **Duración:** 8 horas
- **Formato:**
  - 2 Sesiones - 4 Horas.
- **Modalidad:** Presencial.
- **Incluye:**
  - Material Digital del Curso.
  - Material de apoyo.
  - Diploma de Participación.

cybertrust

academiacybertrust@cybertrust.one

Agustinas N°833, Torre B, piso 8