Introducción

IT Risk Manager se define y se basa en una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en Enterprise Risk Management (ERM), que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados.

El marco de IT Risk Manager se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI:

- Alinear siempre con los objetivos organizacionales.
- Alinear la gestión de las TI con el riesgo organizacional relacionado con el total de ERM.
- Balance de los costes y los beneficios de la gestión de los riesgos de TI.
- Promover la comunicación abierta y equitativa de los riesgos de TI.
- Establecer el tono correcto desde un enfoque de arriba abajo, definiendo y haciendo cumplir la responsabilidad del personal con los niveles de tolerancia aceptables y bien definidos.
- Son un proceso continuo y parte de las actividades diarias.

El modelo se divide en tres ámbitos: gobernanza del riesgo, evaluación de riesgos y el riesgo de respuesta, cada uno con tres procesos:

Gobierno de los riesgos (GR)
- RG1 Establecer y mantener una vista de riesgo común.
- RG2 Integrar con ERM.
- RG3 Tomar decisiones conscientes de los riesgos del negocio.

Evaluación de riesgos (RE)
- RE1 Recoger datos.
- RE2 Analizar los riesgos.
- RE3 Mantener perfil de riesgo.

Respuesta de riesgos
- RR1 Riesgo articulado
- RR2 Manejar riesgos
- RR3 Reaccionar a acontecimientos

La aplicación de mejores prácticas para la gestión de los riesgos de TI, como se describe en RISK IT, proporcionará beneficios tangibles de negocios, por ejemplo, un menor número de eventos inesperados y fracasos, el aumento de la calidad de la información, una mayor confianza de las partes interesadas, menos preocupaciones de carácter regulatorio y nuevas iniciativas para el negocio apoyadas por aplicaciones innovadoras.

Objetivos del Taller

Proporcionar a los participantes los conocimientos y herramientas necesarias para identificar, evaluar y gestionar los riesgos de TI, integrando principios de gobernanza, evaluación y respuesta al riesgo.

A través del uso de marcos de referencia como COBIT y VAL IT, los participantes aprenderán a aplicar estrategias efectivas de mitigación, alineando la gestión del riesgo con los objetivos organizacionales y la toma de decisiones basada en riesgos.

Contenidos

Metodología

Este curso combina teoría y práctica, incorporando ejemplos y el desarrollo de casos para una comprensión aplicada de los conceptos.

Requisitos

Conocimientos básicos de TI; Experiencia en Gestión de Riesgos o Seguridad de la información: Idealmente, experiencia previa en áreas como Gobernanza de TI, Auditoría, Cumplimiento o Ciberseguridad.

Conocimientos básicos de marcos y estándares de gestión de riesgos: Conocer metodologías como COBIT, ISO 27001, NIST, ITIL o ERM, es una ventaja, aunque no es obligatorio.

Habilidades analíticas y toma de decisiones: La capacidad de evaluar amenazas, analizar escenarios de riesgo y proponer estrategias de mitigación es clave.

Dirigido a:

Este curso está dirigido a profesionales responsables de la Gestión de Riesgos en tecnología de la información, incluyendo:

Gerentes y directores de TI, Oficiales de Seguridad de la Información (CISO); Equipos de Ciberseguridad; Auditores de TI y Consultores de Riesgos; Profesionales de Gobernanza y Cumplimiento (GRC); Administradores de Infraestructura y Operaciones de TI; Analistas y Gestores de Riesgos empresariales.

Generalidades

- Duración 24 horas cronológicas.
- Taller cerrado.