

METODOLOGÍA Y PLANIFICACIÓN DEL RIESGO TECNOLÓGICO

25 DE SEPTIEMBRE

TARIFA*: 775 € · SOCIO: 660 € · SOCIO CORPORATIVO: 540 €

HORAS CPE: 8

INSCRÍBETE



NIVEL: TODOS

La evolución de las tecnologías de la información y la explosión actual de tecnologías y negocios digitales exponen a las organizaciones a una serie de riesgos adicionales que es fundamental controlar.

Desde Auditoría Interna es necesario conocer tanto los sistemas de información tradicionales como los proyectos de transformación digital que afrontan o afrontarán las organizaciones.

Identificados adecuadamente los diferentes elementos tecnológicos (Arquitectura empresarial, tecnológica o digital) podremos empezar a identificar los diferentes riesgos existentes para valorar convenientemente el nivel de control existente.

Este seminario ayudará a definir las diferentes funciones recogidas bajo la conocida como Auditoría de TI y su evolución hacia Auditoría de Riesgos Tecnológicos y/o Digitales.

OBJETIVOS

- Conocer cuáles son los principales riesgos tecnológicos y como planificar de forma adecuada su evaluación en el marco de la auditoría.
- Explicar a auditores no especializados en TI los principales aspectos a tener en cuenta en auditoría de riesgos tecnológicos.
- Ayudar a auditores de TI a sentar las bases para desarrollar la Auditoría de Riesgos Tecnológicos.
- Conocer los *frameworks* y estándares de referencia en el control de riesgos tecnológicos, así como normas de obligado cumplimiento.
- Identificar los conocimientos, experiencia y capacidades para establecer el área.
- Conocer las fuentes de información más apropiadas para el desarrollo y apoyo del área.

TEMARIO

Construyendo la Auditoría de Riesgos Tecnológicos.

- Situación actual de las tecnologías de información y nuevas tecnologías digitales.
- Universo auditable de TI. Creando nuestro mapa de procesos.
- Metodología de planificación de auditorías tecnológicas.
- Auditoría integral.

Frameworks, estándares de referencia y normas.

- Generales de auditoría: COSO.
- Riesgos tecnológicos: COBIT.
- Ciberseguridad: ISO 27001.
- Cumplimiento: GDPR y marcos sectoriales.

Formando al auditor de riesgos tecnológicos.

- Conocimientos técnicos.
- Otras capacidades.

La evolución de Auditoría de Riesgos Tecnológicos.

- El futuro del área.

DESTINATARIOS

- Directores de Auditoría Interna.
- Auditores Internos operativos (sin conocimientos de TI).
- Auditores Internos de TI.
- Profesionales de TI (sin conocimientos de Auditoría Interna).

DIRECCIÓN TÉCNICA

Manuel Mendiola Antona, CIA, CRMA, CISA, CISM, CGEIT, CRISC

Auditor Informático.

Diplomado en Informática de Gestión. Director asociado.

Responsable Riesgos Tecnológicos. PKF ATTEST.

PONENTES

Diego Bueno, Auditor IT, ISO 27001 ISMS Auditor, CISSP

Director Auditoría Riesgos Tecnológicos y Banca Digital en Grupo Bankinter.

Ingeniero Informático.

Máster en Gestión de Empresas MBA.

Colaborador del CSA (Cloud Security Alliance).

Profesor asociado del IE (Instituto de Empresa).

Alberto Arroyo, Auditor IT, ISO 27001 ISMS Auditor, CISA

Auditor Jefe - Auditoría Riesgos Tecnológicos y Banca Digital en Grupo Bankinter.

Ingeniero Superior de Telecomunicaciones.

PCI Compliance - Isec.

HORARIO

De 9,00 h. a 18,00 h.

LUGAR DE CELEBRACIÓN

MADRID · Sede social del IAI (Santa Cruz de Marcenado, 33-1º).