ISACA Certified in Risk and Information Systems Control (CRISC)

Descrición

Co curso Certified in Risk and Information Systems Control (CRISC®) demostrarás a túa experiencia na xestión de riscos informáticos. Ao adoptar un enfoque proactivo, aprenderás a mellorar a resistencia empresarial da túa organización, ofrecer valor ás partes interesadas e optimizar a xestión de riscos en toda a empresa. Como CRISC, estarás preparado/a para abordar a tecnoloxía emerxente, incluída a avaliación de riscos de IA e as mellores prácticas xerais para a xestión e mitigación de riscos relacionados coa ética e a gobernanza de datos de IA.

Obxectivos

O curso está orientado a que os/as participantes comprendan:

- Gobernanza: Establecer un marco para aliñar riscos con obxectivos empresariais.
- Avaliación: Identificar e analizar os riscos de TI e o seu impacto.
- Resposta: Deseñar estratexias para mitigar e xestionar riscos.
- Controis: Supervisar e optimizar controis de TI continuamente.

Dirixido a

Este curso está dirixido a:

- Xestores/as de riscos: Profesionais que identifican e mitigan riscos empresariais.
- Auditores/as de TI: Expertos/as en avaliar controis e procesos de tecnoloxía.
- Analistas de riscos: Especialistas en análises e implementación de medidas de control.
- Profesionais de seguridade da información: Enfocados/as en protexer activos de información.
- Xerentes de cumprimento: Responsables de cumprir normativas e regulacións.

PRERREQUISITOS PARA OBTER A CERTIFICACIÓN:

- Presentar evidencia verificada de tres (3) anos de experiencia laboral realizando as tarefas dun CRISC tanto en o Dominio 2 (Avaliación de Riscos) como no Dominio 3 (Resposta e Informes de Riscos).
- A experiencia laboral debe obterse dentro dos dez anos anteriores á data da solicitude ou dentro dos cinco (5) anos a partir da data de aprobación inicial do exame.

BENEFICIOS Opción gratuita dun exame de certificación oficial

Diploma de asistencia

Perfil do docente

APMG Accredited Trainer CRISC

PROGRAMA Programación 2026/27

TIPO CURSO

MATRÍCULA Gratuíta

PERIODO INSCRICIÓN 24/10/2026 - 08/11/2026

PROBA DE SELECCIÓN 10/11/2026 (18:30)

CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	16 (Mínimo 10)
METODOLOXÍA	Virtual
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	20 horas
DATA INICIO	23/11/2026
DATA FIN	27/11/2026
HORARIO	De luns a venres de 16:30 a 20:30 horas.
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	Certified in Risk and Information Systems Control (CRISC®)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	ISACA Ciberseguridade/Ciberseguridad
PERIODO DOCENCIA	23/11/2026 - 27/11/2026

Temario

DOMINIO 1- GOBERNANZA
Goberno da organización:

- Estratexia, metas e obxectivos da organización
- Estrutura organizativa, funcións e responsabilidades
- Cultura organizativa
- Políticas e normas
- Procesos empresariais
- Activos da organización

Gobernanza do risco:

- Xestión do risco empresarial e marco de xestión do risco
- Tres liñas de defensa
- Perfil de risco
- Apetito e tolerancia ao risco
- Requisitos legais, regulamentarios e contractuais
- Ética profesional da xestión de riscos

DOMINIO 2- AVALIACIÓN DO RISCO DE IT
Identificación do risco en IT:

- Eventos de risco (por exemplo, condicións contribuíntes, resultado da perda)
- Modelización de ameazas e panorama de ameazas
- Análises de vulnerabilidade e deficiencias de control (p. ex., análise de causa raíz)
- Desenvolvemento de escenarios de risco

Análise e avaliación de riscos en IT:

- Conceptos, normas e marcos de avaliación de riscos
- Rexistro de riscos
- Metodoloxías de análises de riscos
- Análises do impacto na empresa
- Risco inherente e residual

DOMINIO 3- RESPOSTA Aos RISCOS E INFORMES
Resposta ao risco:

- Tratamento do risco / Opcións de resposta ao risco
- Propiedade do risco e do control
- Xestión de riscos por terceiros
- Xestión de problemas, achados e opoñas excepción
- Xestión de riscos emerxentes

Deseño e aplicación de controis:

- Tipos, normas e marcos de control
- Deseño, selección e análise de controis
- Implantación de controis
- Probas de control e avaliación da eficacia

Seguimento e notificación de riscos:

- Plans de tratamento de riscos
- Recollida, agregación, análise e validación de datos
- Técnicas de supervisión de riscos e controis
- Técnicas de presentación de informes sobre riscos e controis (mapas de calor, cadros de mando, taboleiros de control)
- Indicadores clave de rendemento

DOMINIO 4: TECNOLOXÍA E SEGURIDADE DA INFORMACIÓN

Principios das Tecnoloxías da Información:

- Arquitectura empresarial
- Xestión de operacións de TI (por exemplo, xestión de cambios, activos de TI, problemas, incidentes)
- Xestión de proxectos
- Xestión de recuperación de desastres
- Xestión do ciclo de vida dos datos
- Ciclo de vida do desenvolvemento de sistemas
- Tecnoloxías emerxentes

Principios da Seguridade da Información:

- Conceptos, marcos e normas de seguridade da información
- Formación sobre seguridade da información
- Xestión da continuidade das actividades
- Principios de privacidade e protección de datos