

Las tecnologías de la información se encuentran presentes en cualquier entorno de negocio. Las organizaciones hacen frente a diversas maneras de tratar la información que utilizan, en las que la tecnología juega un papel cada vez más relevante. Además, el entorno regulatorio es cada vez más exigente, lo que obliga a entidades y profesionales a ser conscientes, no únicamente, del tipo de tecnología que utilizan, sino del cómo y para qué la utilizan.

Disponer de los conocimientos, habilidades y capacidades necesarias para evaluar los riesgos de la tecnología actual y cómo se gestionan, adquiere una importancia crítica para varios perfiles profesionales, especialmente los vinculados a las actividades de Auditoría Interna.

Itinerario formativo en Auditoría Interna de TI

Ponemos a tu disposición un itinerario integral de formación de contenidos teórico-prácticos, que comprende diferentes enfoques de auditoría en el marco de las tecnologías y los sistemas de información.

Esta formación se clasifica en **bloques de conocimiento**, cada uno de ellos con diferentes niveles de profundización en función del grado de especialización que pretendas adquirirse, donde se conocerán en detalle las problemáticas de cada uno de los ámbitos evaluados, permitiendo a los alumnos disponer de conocimientos específicos, en función del itinerario seleccionado.

1 · GENERAL

Metodología y planificación del Riesgo Tecnológico.

2 · PROCESOS DE NEGOCIO

Auditoría interna del sistema de gestión de continuidad del negocio.

3 · APLICACIONES

Auditoría interna de aplicaciones.

4 · DATOS

Auditoría interna de la calidad del dato.

Seguridad de la información y ciberseguridad.

5 · INFRAESTRUCTURA

Introducción a la auditoría interna de seguridad en las comunicaciones.

ESPECIALIZACIÓN

Taller práctico: auditoría continua.

Analytics – Automatización y monitorización continua de controles en la empresa.

ESPECIALIZACIÓN

Auditoría interna de canales digitales.

Auditoría interna de las inversiones en tecnologías emergentes.

ESPECIALIZACIÓN

Riesgos del outsourcing: modelos cloud y on premise.

ESPECIALIZACIÓN

Introducción a la auditoría interna de protección de datos.

Auditoría interna del cumplimiento del RGPD.

Data Science.

ESPECIALIZACIÓN (FORENSE)

Análisis forense.

Algunos cursos complementarios (no tecnológicos)

- Iniciación a la Auditoría Interna.
- Análisis de procesos.
- Prevención, detección e investigación de fraude.
- Auditorías internas integrales.
- Ágile en Auditoría Interna.
- Auditoría Interna de departamentos de pequeña dimensión
- Taller: Auditoría Interna de procesos externalizados.

ESPECIALIZACIÓN (CIBERSEGURIDAD)

Auditoría interna de ciberseguridad.

ESPECIALIZACIÓN (CIBERSEGURIDAD)

Auditoría interna de seguridad física.

Auditoría interna de seguridad en dispositivos móviles.

Auditorías avanzadas de Ciberseguridad. Red Teaming.

BLOQUE 1 GENERAL

Formación base: Adquirir los conocimientos fundamentales sobre el riesgo tecnológico al que se exponen las organizaciones y los marcos de actuación y diferentes metodologías para afrontar los trabajos de revisión de riesgos tecnológicos.

- *Metodología y planificación del Riesgo Tecnológico.*

Formación especializada: Conocer la metodología y beneficios de la auditoría continua y la automatización de controles mediante talleres eminentemente prácticos y herramientas específicas.

- *Taller práctico: auditoría continua.*
- *Analytics – Automatización y monitorización continua de controles en la empresa.*

BLOQUE 4 DATOS

Formación base: adquirir los conocimientos básicos sobre la información como un activo básico para alcanzar los objetivos de una organización. Conocer cómo Auditoría Interna puede ayudar en la consecución de los objetivos de la organización, evaluando si la información necesaria estará siempre disponible de forma íntegra y veraz, y si se dispone de controles adecuados para garantizar su confidencialidad.

- *Auditoría interna de la calidad del dato.*
- *Seguridad de la información y ciberseguridad.*

Formación especializada: conocer los trabajos a desarrollar por Auditoría Interna para evaluar el cumplimiento de los Principios, Derechos y Obligaciones recogidos en el Reglamento Europeo de Protección de Datos. Capacitar a los asistentes sobre qué se entiende por ciencia de datos, estudiando en particular el machine learning y sus potenciales aplicaciones.

- *Introducción a la auditoría interna de protección de datos.*
- *Auditoría interna del cumplimiento del RGPD.*
- *Data Science.*

Formación especializada en ciberseguridad: conocer los elementos clave para definir la estrategia de ciberseguridad de la compañía. Evaluar las capacidades y el grado de protección de la compañía frente a los ciberriesgos.

- *Auditoría interna de ciberseguridad.*

BLOQUE 2 PROCESOS DE NEGOCIO

Formación base: Conocer los elementos principales para la evaluación de un Plan de Continuidad del Negocio (PCN) y planes asociados como los de contingencia y los de recuperación de desastres.

Presentar un posible programa de Auditoría Interna de aseguramiento relacionado con el PCN.

- *Auditoría interna del sistema de gestión de continuidad del negocio.*

Formación especializada: Proporcionar la base necesaria para la realización de revisiones del grado de innovación de las organizaciones, en ámbitos relacionados con las nuevas tecnologías y la transformación digital, así como de los canales online utilizados por la compañía.

- *Auditoría interna de canales digitales.*
- *Auditoría interna de las inversiones en tecnologías emergentes.*

BLOQUE 3 APLICACIONES

Formación base: presentar un posible enfoque detallado de evaluación del correcto funcionamiento, control y seguridad de las aplicaciones utilizadas por la compañía, así como su adecuación a las necesidades del negocio y a los requerimientos legales y regulatorios existentes.

- *Auditoría interna de aplicaciones.*

Formación especializada: conocer los principales tipos de servicios tecnológicos que se suelen externalizar, los principales riesgos asociados a estas subcontrataciones –incluidos aquellos relacionados con servicios en la nube– y la perspectiva a adoptar durante los trabajos de auditoría interna en este ámbito.

- *Riesgos del outsourcing: modelos cloud y on premise.*

BLOQUE 5 INFRAESTRUCTURA

Formación base: formar a los asistentes para evaluar las medidas de control adoptadas para garantizar comunicaciones seguras.

- *Introducción a la auditoría interna de seguridad en las comunicaciones.*

Formación especializada forense: conocer las cuestiones legales más importantes a tener en cuenta durante el desarrollo de investigaciones forenses y los aspectos prácticos-metodológicos de estas investigaciones, así como la aplicación de herramientas informáticas para la captura y análisis de evidencias digitales.

- *Análisis forense.*

Formación especializada en ciberseguridad: profundizar sobre la metodología para la realización de revisiones sobre la protección de las personas de la organización y la seguridad física de activos, incluidos los dispositivos móviles. Conocer qué son y cómo se llevan a cabo las auditorías Red Teaming.

- *Auditoría interna de seguridad física.*
- *Auditoría interna de seguridad en dispositivos móviles.*
- *Auditorías avanzadas de Ciberseguridad. Red Teaming.*