TEMARIO DEL CURSO

CISSP – Profesional certificado en seguridad de sistemas de información

28 horas | Intermedio–Avanzado

El curso de preparación para el Certified Information Systems Security Professional (CISSP) está diseñado para formar a profesionales en los principios avanzados de la ciberseguridad.

OBJETIVOS DEL CURSO

- Comprender y aplicar los ocho dominios del CISSP en entornos laborales reales.
- Prepararse exhaustivamente para el examen CISSP mediante materiales y técnicas alineadas con ISC2.
- Adquirir conocimientos técnicos para diseñar e implementar programas de seguridad efectivos.
- Conocer marcos regulatorios y estándares globales de ciberseguridad.
- Mejorar habilidades de evaluación, auditoría y mitigación de riesgos en proyectos de TI.

A QUIÉN VA DIRIGIDO

- Directores y gestores de seguridad en tecnologías de la información.
- Profesionales con experiencia en ciberseguridad interesados en obtener la certificación CISSP.
- Consultores, arquitectos y analistas de seguridad informática.
- Administradores de redes y sistemas que buscan especializarse en seguridad.
- Responsables de cumplimiento y gestión de riesgos en organizaciones.

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.

Seguridad y gestión de riesgos

- Comprender, cumplir y promover la ética profesional
- Comprender y aplicar los conceptos de seguridad
- Evaluar y aplicar los principios de gobierno de la seguridad
- Comprender los aspectos legales, regulatorios y de cumplimiento relativos a la seguridad de la información
- Comprender los requisitos de los tipos de investigación (administrativa, penal, civil, regulatoria, estándares del sector)
- Desarrollar, documentar e implantar políticas, normas, procedimientos y directrices de seguridad
- Identificar, analizar, evaluar, priorizar e implantar los requisitos de continuidad de negocio
- Contribuir a las políticas y procedimientos de seguridad del personal y hacerlos cumplir
- Comprender y aplicar los conceptos de gestión de riesgos
- Comprender y aplicar conceptos y metodologías de modelado de amenazas
- Aplicar conceptos de gestión de riesgos de la cadena de suministro (SCRM)
- Establecer y mantener un programa de concienciación, educación y formación en seguridad

MÓDULO 02.

Seguridad de los activos

- Identificar y clasificar la información y los activos
- Establecer requisitos de manejo de la información y los activos
- Aprovisionar la información y los activos de forma segura
- Gestionar el ciclo de vida de los datos
- Garantizar la retención adecuada de los activos (fin de vida, fin de soporte)
- Determinar los controles de seguridad de los datos y los requisitos de cumplimiento

MÓDULO 03.

Arquitectura e ingeniería de seguridad

- Investigar, implantar y gestionar procesos de ingeniería con principios de diseño seguro
- Comprender los conceptos fundamentales de los modelos de seguridad (Biba, Star Model, Bell-LaPadula)
- Seleccionar controles en función de los requisitos de seguridad de los sistemas
- Comprender las capacidades de seguridad de los sistemas de información (protección de memoria, TPM, cifrado/descifrado)
- Evaluar y mitigar las vulnerabilidades de arquitecturas, diseños y elementos de solución de seguridad
- Seleccionar y determinar soluciones criptográficas
- Comprender los métodos de ataque criptoanalítico
- Aplicar principios de seguridad al diseño de instalaciones
- Diseñar controles de seguridad para instalaciones

- Gestionar el ciclo de vida del sistema de información

MÓDULO 04.

Seguridad de las comunicaciones y redes

- Aplicar principios de diseño seguro en arquitecturas de red
- Proteger los componentes de red
- Implantar canales de comunicación seguros según el diseño

MÓDULO 05.

Gestión de identidades y accesos (IAM)

- Controlar el acceso físico y lógico a los activos
- Diseñar la estrategia de identificación y autenticación (personas, dispositivos y servicios)
- Identidad federada con un servicio de terceros
- Implantar y gestionar mecanismos de autorización
- Gestionar el ciclo de vida del aprovisionamiento de identidades y accesos
- Implantar sistemas de autenticación

MÓDULO 06.

Evaluación y pruebas de seguridad

- Diseñar y validar estrategias de evaluación, pruebas y auditoría
- Realizar pruebas de controles de seguridad
- Recopilar datos de los procesos de seguridad (técnicos y administrativos)
- Analizar los resultados de las pruebas y generar informes
- Realizar o facilitar auditorías de seguridad

MÓDULO 07.

Operaciones de seguridad

- Comprender y cumplir con las investigaciones
- Realizar actividades de registro y monitorización
- Realizar la gestión de la configuración (aprovisionamiento, líneas base, automatización)
- Aplicar los conceptos fundamentales de operaciones de seguridad
- Aplicar la protección de recursos
- Gestionar incidentes
- Operar y mantener medidas de detección y prevención
- Implantar y dar soporte a la gestión de parches y vulnerabilidades
- Comprender y participar en los procesos de gestión de cambios
- Implantar estrategias de recuperación
- Implantar procesos de recuperación ante desastres
- Probar los planes de recuperación ante desastres
- Participar en la planificación y los ejercicios de continuidad de negocio
- Implantar y gestionar la seguridad física
- Abordar aspectos de seguridad y protección del personal

MÓDULO 08.

Seguridad en el desarrollo de software

- Comprender e integrar la seguridad en el ciclo de vida de desarrollo de software (SDLC)
- Identificar y aplicar controles de seguridad en los ecosistemas de desarrollo de software
- Evaluar la eficacia de la seguridad del software
- Evaluar el impacto en la seguridad del software adquirido
- Definir y aplicar directrices y estándares de codificación segura