CISSP, seguridad de la SI, preparación para la certificación

Curso práctico de 5 días - 35h
Ref.: CIS - Precio 2025: 2 770€ sin IVA

Este curso detalla los conceptos de seguridad necesarios para obtener la certificación CISSP. Le preparará para el examen cubriendo todo el Common Body of Knowledge (CBK), el núcleo de conocimientos de seguridad definido por el International Information Systems Security Certification Consortium (ISC)².

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Conocer el lenguaje común de conocimientos sobre seguridad informática

Desarrollar una visión global de los problemas de seguridad informática

Profundizar en el conocimiento de los ocho dominios CISSP

Preparación para el examen de certificación CISSP

CERTIFICACIÓN

Para obtener la certificación, debe registrarse en el sitio web del ISC2 y presentar una solicitud de elegibilidad.

PROGRAMA

última actualización: 02/2024

1) La seguridad de la SI y el CBK (ISC)²

- Seguridad de los sistemas de información.
- ¿Por qué la certificación CISSP?
- Presentación del ámbito cubierto por el CBK.

2) Gestión de la seguridad y seguridad operativa

- Prácticas de gestión de la seguridad. Redacción de políticas, directivas, procedimientos y normas de seguridad.
- El programa de concienciación sobre seguridad, las prácticas de gestión, la gestión de riesgos, etc.
- Seguridad operativa: medidas preventivas, de detección y correctivas, funciones y responsabilidades de todos los implicados.
- Buenas prácticas, seguridad a la hora de contratar personal, etc.

3) Arquitectura, modelos de seguridad y control de acceso

- Arquitectura y modelos de seguridad: arquitectura de sistemas, modelos teóricos de seguridad de la información.
- Métodos de evaluación de sistemas, modos de seguridad operativa, etc.
- Sistemas y metodologías de control de acceso. Categorías y tipos de control de acceso.
- Acceso a datos y sistemas, sistemas de prevención de intrusiones (IPS) y sistemas de detección de intrusiones (IDS).
- Registros de auditoría, amenazas y ataques relacionados con el control de acceso, etc.

4) Criptografía y seguridad en el desarrollo

- Criptografía. Conceptos, criptografía simétrica y asimétrica.
- Funciones hash, infraestructura de clave pública, etc.

PARTICIPANTES

Responsables de seguridad de los SI o cualquier otra persona con un papel en la política de seguridad de los SI.

REQUISITOS PREVIOS

Conocimientos básicos de redes y sistemas operativos, así como de seguridad de la información.
Conocimientos básicos de normas de auditoría y continuidad de las actividades.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- Seguridad en el desarrollo de aplicaciones y sistemas. Bases de datos y almacenes de datos.
- Ciclo de desarrollo, programación orientada a objetos, sistemas expertos, inteligencia artificial, etc.

5) Telecomunicaciones y seguridad de las redes

- Seguridad en redes y telecomunicaciones. Conceptos básicos, modelo TCP/IP, equipos de red y seguridad.
- Protocolos de seguridad, ataques a redes, copias de seguridad de datos, tecnologías inalámbricas, VPN...

6) Continuidad de las actividades, legislación, ética y seguridad física

- Continuidad de la actividad y planificación de la recuperación en caso de catástrofe.
- Plan de continuidad de la actividad, plan de recuperación en caso de catástrofe.
- Medidas de emergencia, programa de formación y sensibilización, comunicación de crisis, ejercicios y pruebas.
- Derecho, investigación y ética: derecho civil, penal y administrativo, propiedad intelectual.
- El marco jurídico de las investigaciones, las normas que rigen la admisibilidad de las pruebas, etc.
- Seguridad física. Amenazas y vulnerabilidades vinculadas al entorno de un lugar, perímetro de seguridad.
- Requisitos de disposición, vigilancia de los locales, protección del personal, etc.

FECHAS

Contacto