CISSP – Certified Information Systems Security Professional

Este curso de preparación oficial para la certificación CISSP® **proporciona una revisión integral del conocimiento necesario para diseñar, construir y gestionar de manera efectiva la estrategia de seguridad general de una organización**.

Te ayudará a revisar y actualizar tus conocimientos e identificar áreas que necesitas estudiar para el examen CISSP. **El contenido se alinea y cubre de manera integral los ocho dominios del Cuerpo Común de Conocimientos (CBK®) de ISC2 CISSP**, lo que garantiza la relevancia en todas las disciplinas en el campo de la ciberseguridad.

Como **partners de formación de ISC2 ofrecemos el material educativo oficial desarrollado por ISC2®**, para garantizar que tu capacitación sea relevante y esté actualizada. Nuestros instructores son expertos en seguridad verificados y han completado una capacitación intensiva para enseñar contenido ISC2.

Objetivos Didácticos

Después de completar este curso, el candidato será capaz de:

- Aplicar conceptos y métodos fundamentales relacionados con los campos de la tecnología de la información y seguridad.
- Alinear los objetivos operativos organizacionales generales con las funciones e implementaciones de seguridad.
- Determinar cómo proteger los activos de la organización a medida que pasan por su ciclo de vida.
- Aprovechar los conceptos, principios, estructuras y estándares utilizados para diseñar, implementar, monitorear y proteger los sistemas operativos, equipos, redes, aplicaciones y aquellos controles utilizados para hacer cumplir diversos niveles de confidencialidad, integridad y disponibilidad.
- Aplicar principios de diseño de seguridad para seleccionar mitigaciones apropiadas para las vulnerabilidades presentes en tipos y arquitecturas de sistemas de información comunes.
- Explicar la importancia de la criptografía y los servicios de seguridad que puede proporcionar en la era digital y de la información actual.
- Evaluar los elementos de seguridad física en relación con las necesidades de seguridad de la información.
- Evaluar los elementos que componen la seguridad de las comunicaciones y redes en relación con las necesidades de seguridad de la información.
- Aprovechar los conceptos y la arquitectura que definen la tecnología asociada y sistemas de implementación y protocolos en las capas 1 a 7 del modelo de interconexión de sistemas abiertos (OSI) para satisfacer las necesidades de seguridad de la información.
- Determinar modelos de control de acceso apropiados para cumplir con los requisitos de seguridad empresarial.
- Aplicar controles de acceso físico y lógico para satisfacer las necesidades de seguridad de la información.
- Diferenciar entre métodos primarios para diseñar y validar estrategias de prueba y auditoría. que soportan los requisitos de seguridad de la información.
- Aplicar controles y contramedidas de seguridad adecuados para optimizar el rendimiento de una organización. función y capacidad operativa.

- Evaluar los riesgos de los sistemas de información para los esfuerzos operativos de una organización.
- Determinar controles apropiados para mitigar amenazas y vulnerabilidades específicas.
- Aplicar conceptos de seguridad de sistemas de información para mitigar el riesgo de software y sistemas. vulnerabilidades a lo largo del ciclo de vida de los sistemas.

Audiencia

Este curso de capacitación está destinado a profesionales que tengan al menos cinco años de experiencia laboral acumulada y remunerada en dos o más de los ocho dominios de ISC2 CISSP CBK y estén buscando capacitación y certificación CISSP para adquirir credibilidad y movilidad para avanzar dentro de su actual carrera de seguridad de la información. El curso es ideal para quienes trabajan en puestos tales como, entre otros:

- Consultor de seguridad
- Gerente de seguridad
- Director/ Gerente de TI
- Auditor de Seguridad
- Arquitecto de seguridad
- Analista de seguridad
- Ingeniero en Sistemas de Seguridad
- Director de seguridad de la información

Dominios del curso

- Dominio 1: Seguridad y gestión de riesgos
- Dominio 2: Seguridad de activos
- Dominio 3: Arquitectura e ingeniería de seguridad
- Dominio 4: Seguridad de redes y comunicaciones
- Dominio 5: Gestión de identidad y acceso (IAM)
- Dominio 6: Evaluación y pruebas de seguridad
- Dominio 7: Operaciones de seguridad
- Dominio 8: Seguridad del desarrollo de software

Metodología

Aula virtual en directo.

Duración

5 días (35 horas)

Temario del curso

1. **El entorno de seguridad de la información**

   - Justificar un código de ética organizacional.
   - Relacionar la confidencialidad, integridad, disponibilidad, no repudio, autenticidad, privacidad y seguridad con el debido cuidado y la debida diligencia.
   - Relacionar la gobernanza de la seguridad de la información con las estrategias, metas, misiones y objetivos de la organización.
   - Aplicar los conceptos de cibercrimen a las filtraciones de datos y otros compromisos de seguridad de la información.
   - Relacionar los requisitos legales, contractuales y reglamentarios de privacidad y protección de datos con objetivos de seguridad de la información.
   - Relacionar el movimiento transfronterizo de datos y las cuestiones de importación y exportación con la protección de datos, la privacidad y la protección de la propiedad intelectual

2. **Seguridad de los activos de información**

   - Relacionar los modelos de ciclo de vida de gestión de activos TI y seguridad de datos con la seguridad de la información.
   - Explicar el uso de la clasificación y categorización de la información, como dos procesos separados pero relacionados.
   - Describir los diferentes estados de los datos y sus consideraciones de seguridad de la información.
   - Describir los diferentes roles involucrados en el uso de la información y las consideraciones de seguridad para estos roles.
   - Describir los diferentes tipos y categorías de controles de seguridad de la información y su uso.
   - Seleccionar estándares de seguridad de datos para cumplir con los requisitos de cumplimiento organizacional.

3. **Gestión de identidades y accesos (IAM)**

   - Explicar el ciclo de vida de la identidad según se aplica a usuarios humanos y no humanos.
   - Comparar y contrastar modelos, mecanismos y conceptos de control de acceso.
   - Explicar el papel de la autenticación, autorización y contabilidad en el logro de metas y objetivos de seguridad de la información.
   - Explicar cómo las implementaciones de IAM deben proteger los activos físicos y lógicos.
   - Describir la función de las credenciales y el almacén de identidades en los sistemas IAM.

4. **Arquitectura e ingeniería de seguridad**

   - Describir los componentes principales de los estándares de ingeniería de seguridad.
   - Explicar los principales modelos arquitectónicos para la seguridad de la información.
   - Explicar las capacidades de seguridad implementadas en hardware y firmware.
   - Aplicar principios de seguridad a diferentes arquitecturas de sistemas de información y sus entornos.
   - Determinar la mejor aplicación de enfoques criptográficos para resolver las necesidades de seguridad de la información organizacional.
   - Gestionar el uso de certificados y firmas digitales para satisfacer las necesidades de seguridad de la información de la organización.

- Descubrir las implicaciones del no uso de técnicas criptográficas para proteger la cadena de suministro.
- Aplicar diferentes soluciones de gestión criptográfica para satisfacer las necesidades de seguridad de la información organizacional.
- Verificar que las soluciones criptográficas estén funcionando y enfrentando la amenaza en evolución del mundo real.
- Describir las defensas contra ataques criptográficos comunes.
- Desarrollar una lista de verificación de gestión para determinar el estado criptológico de salud y preparación de la organización.

5. **Seguridad de la red y las comunicaciones**

- Describir las características arquitectónicas, tecnologías relevantes, protocolos y consideraciones de seguridad de cada una de las capas del modelo OSI.
- Explicar la aplicación de prácticas de diseño seguro en el desarrollo de infraestructura de red.
- Describir la evolución de los métodos para proteger los protocolos de comunicaciones IP.
- Explicar las implicaciones de seguridad de los entornos de red vinculados (cable y fibra) y no vinculados (inalámbricos).
- Describir la evolución y las implicaciones de seguridad para los dispositivos de red clave.
- Evaluar y contrastar los problemas de seguridad con las comunicaciones de voz en infraestructuras tradicionales y VoIP.
- Describir y contrastar las consideraciones de seguridad para tecnologías clave de acceso remoto.
- Explicar las implicaciones de seguridad de las redes definidas por software (SDN) y las tecnologías de virtualización de redes.
- Laboratorio: Monitoreo y mantenimiento operacional

6. **Seguridad del desarrollo de software**

- Reconocer los numerosos elementos de software que pueden poner en riesgo la seguridad de los sistemas de información.
- Identificar e ilustrar las principales causas de las debilidades de seguridad en el código fuente.
- Ilustrar las principales causas de las debilidades de seguridad en los sistemas de bases de datos y almacenes de datos.
- Explicar la aplicabilidad del marco OWASP a varias arquitecturas web.
- Seleccionar estrategias de mitigación de malware apropiadas para las necesidades de seguridad de la información de la organización.
- Contrastar las formas en que las diferentes metodologías, marcos y directrices de desarrollo de software contribuyen a la seguridad de los sistemas.
- Explicar la implementación de controles de seguridad para ecosistemas de desarrollo de software.
- Elegir una combinación adecuada de pruebas de seguridad, evaluación, controles y métodos de gestión. para diferentes sistemas y entornos de aplicaciones.Laboratorio: Fundamentos de enrutamiento.

7. **Evaluación y pruebas de seguridad**

- Describir el propósito, el proceso y los objetivos de las evaluaciones y pruebas de seguridad formales e informales.
- Aplicar la ética profesional y organizacional a la evaluación y pruebas de seguridad.
- Explicar las evaluaciones y pruebas internas, externas y de terceros.
- Explicar las cuestiones de gestión y gobernanza relacionadas con la planificación y realización de evaluaciones de seguridad.

8. **Operaciones de seguridad**

- Mostrar cómo recopilar y evaluar datos de seguridad de manera eficiente y efectiva.
- Explicar los beneficios de seguridad de una gestión y control de cambios efectivos.
- Desarrollar políticas y planes de respuesta a incidentes.
- Vincular la respuesta a incidentes con las necesidades de controles de seguridad y su uso operativo.
- Relacionar los controles de seguridad con la mejora y el logro de la disponibilidad requerida de los activos y sistemas de información.
- Comprender las ramificaciones de seguridad y protección de diversas instalaciones, sistemas y características de infraestructura.

9. **Poniéndolo todo junto**

- Explicar cómo los marcos y procesos de gobierno se relacionan con el uso operativo de los controles de seguridad de la información.
- Relacionar el proceso de realización de investigaciones forenses con las operaciones de seguridad de la información.
- Relacionar la continuidad del negocio y la preparación para la recuperación ante desastres con las operaciones de seguridad de la información.
- Explicar cómo utilizar la educación, la capacitación, la concientización y el compromiso con todos los miembros de la organización como una manera de fortalecer y hacer cumplir los procesos de seguridad de la información.
- Mostrar cómo operacionalizar los sistemas de información y la gestión de riesgos de la cadena de suministro de TI.