CURSO CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL – CISSP

Certificación:
-Certificado de Asistencia EUD y (ISC)²

Duración:
40 Horas

Tipo de Curso:
Presencial o en Línea

Idioma:
Español.

Contacto:
Fundación de Egresados de la Universidad Distrital
www.egresadosudistrital.edu.co
Cr. 20 # 32 A - 45
Bogotá D.C. / Colombia

CONTENIDO

Resumen del curso:
Este curso está diseñado para profesionales de la seguridad de la información con profundos conocimientos y experiencia técnica y gerencial para diseñar, diseñar y administrar de manera efectiva la postura general de seguridad de una organización. Esta capacitación proporciona una revisión integral de los conceptos de seguridad de los sistemas de información y las mejores prácticas de la industria, que cubre los siguientes ocho dominios del Cuerpo común de conocimientos (CBK ®) de CISSP:

- Dominio 1: Seguridad y Gestión de Riesgos
- Dominio 2: Seguridad de activos
- Dominio 3: Arquitectura e ingeniería de seguridad
- Dominio 4: Comunicación y Seguridad de la Red
- Dominio 5: Gestión de acceso e identidad (IAM)
- Dominio 6: Pruebas de evaluación de seguridad
- Dominio 7: Operaciones de seguridad
- Dominio 8: Seguridad en el desarrollo de software

Los objetivos de aprendizaje de los capítulos orientados al temario se proporcionan a continuación:

Capítulo 1: El entorno de seguridad de la información
Objetivos de aprendizaje:
- Código de ética organizacional.
- Relacionar la confidencialidad, integridad, disponibilidad, no repudio, autenticidad, privacidad y seguridad con el debido cuidado y diligencia.
- Relacionar el gobierno de la seguridad de la información con las estrategias, metas, misiones y objetivos comerciales de la organización.
- Aplicar los conceptos de ciberdelincuencia a las violaciones de datos y otros compromisos de seguridad de la información.
- Relacionar los requisitos legales, contractuales y reglamentarios de privacidad y protección de datos con los 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.

Capítulo 2: Seguridad de los activos de información
Objetivos de aprendizaje:
- Relacionar los modelos de ciclo de vida de gestión de activos de 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 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 de la organización.

Capítulo 3: Gestión de acceso e identidad (IAM)
Objetivos de aprendizaje:
• Explicar el ciclo de vida de la identidad tal como 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, la autorización y la contabilidad para lograr las 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.

Capítulo 4: Arquitectura e ingeniería de seguridad
Objetivos de aprendizaje:
• Describir los principales componentes 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 los principios de seguridad a las 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 de la organización.
• Gestionar el uso de certificados y firmas digitales para satisfacer las necesidades de seguridad de la información de la organización.
• Descubrir las implicaciones de no utilizar técnicas criptográficas para proteger la cadena de suministro.
• Aplicar diferentes soluciones de gestión criptográfica para satisfacer las necesidades de seguridad de la información de la organización.
• Verificar que las soluciones criptográficas funcionen y cumplan con las amenazas cambiantes 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.

Capítulo 5: Comunicación y seguridad de la red
Objetivos de aprendizaje:
• 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.

CURSO CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL – CISSP

Certificación:
-Certificado de Asistencia EUD y (ISC)²

Duración:
40 Horas

Tipo de Curso:
Presencial o en Línea

Idioma:
Español.

Contacto:
Fundación de Egresados de la Universidad Distrital
www.egresadosudistrital.edu.co
Cr. 20 # 32 A - 45
Bogotá D.C. / Colombia

• Describir la evolución de los métodos para proteger los protocolos de comunicaciones IP.
• Explicar las implicaciones de seguridad de los entornos de red enlazados (cable y fibra) y no enlazados (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.

Capítulo 6: Seguridad en el desarrollo de software
Objetivos de aprendizaje:
• Reconocer los muchos 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 bases de datos y sistemas de almacenamiento de datos.
• Explicar la aplicabilidad del marco OWASP a varias arquitecturas web.
• Seleccionar estrategias de mitigación de malware adecuadas a las necesidades de seguridad de la información de la organización.
• Contrastar las formas en que las diferentes metodologías, marcos y pautas 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 entornos de sistemas y aplicaciones.

Capítulo 7: Evaluación y pruebas de seguridad
Objetivos de aprendizaje:
• 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 prueba de seguridad.
• Explicar la evaluación y las pruebas internas, externas y de terceros.
• Explicar los problemas de gestión y gobierno relacionados con la planificación y realización de evaluaciones de seguridad.
• Explicar el papel de la evaluación en la toma de decisiones de seguridad basada en datos.

Capítulo 8: Operaciones de seguridad
Objetivos de aprendizaje:
• Mostrar cómo recopilar y evaluar de manera eficiente y efectiva los datos de seguridad.
• Explicar los beneficios de seguridad de la gestión y el control de cambios efectivos.

CURSO CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL – CISSP

Certificación:
-Certificado de Asistencia EUD y (ISC)²

Duración:
40 Horas

Tipo de Curso:
Presencial o en Línea

Idioma:
Español.

Contacto:
Fundación de Egresados de la Universidad Distrital
www.egresadosudistrital.edu.co
Cr. 20 # 32 A - 45
Bogotá D.C. / Colombia

• 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 varias instalaciones, sistemas y características de infraestructura.

Capítulo 9: Combinando todo

Objetivos de aprendizaje:
• Explicar cómo se relacionan los marcos y procesos de gobierno 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 forma de fortalecer y hacer cumplir los procesos de seguridad de la información.
• Mostrar cómo hacer operativos los sistemas de información y la gestión de riesgos de la cadena de suministro de TI.

CURSO CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL – CISSP

Certificación:
-Certificado de Asistencia EUD y (ISC)²

Duración:
40 Horas

Tipo de Curso:
Presencial o en Línea

Idioma:
Español.

Contacto:
Fundación de Egresados de la Universidad Distrital
www.egresadosudistrital.edu.co
Cr. 20 # 32 A - 45
Bogotá D.C. / Colombia