CISSP Security Training

Objetivo

Los objetivos del presente entrenamiento son:

- Brindar una comprensión integral de los principios y prácticas de seguridad de la información, alineados con los contenidos requeridos por ISC2 para su certificación CISSP, la cual permita a los participantes desarrollar una visión estratégica y operativa sobre la protección de los activos de información.

- Introducir a los participantes en la identificación, evaluación y gestión de riesgos de seguridad, fomentando la aplicación de controles adecuados según el contexto organizacional y el cumplimiento de regulaciones vigentes.

- Brindar el conocimiento necesario para identificar y definir medidas de protección en sistemas, redes, aplicaciones y datos, incorporando conceptos actualizados sobre criptografía, virtualización, cloud computing, IAM y seguridad en el desarrollo de software.

- Formar profesionales capaces de participar en procesos de detección, respuesta y recuperación ante incidentes de seguridad, con conocimientos sobre forensia digital, gestión de vulnerabilidades, monitoreo continuo y operación de centros de seguridad (SOC).

- Preparar a los participantes para desempeñarse en roles clave dentro de equipos de ciberseguridad, fomentando una cultura de mejora continua, liderazgo en seguridad, cumplimiento normativo y toma de decisiones fundamentadas en indicadores de riesgo y desempeño.

Descripción

Este curso de 40 horas en Seguridad de la Información y Ciberseguridad ofrece una visión integral de los principios, prácticas y controles necesarios para proteger los activos críticos de una organización. A fin de garantizar una formación completa y actualizada según estándares internacionales, este programa de formación se encuentra alineado con los dominios de conocimiento requeridos por ISC2 en el marco de su certificación CISSP (Certified Information Systems Security Professional). De este modo, el entrenamiento busca introducir al alumno en el mundo de la Seguridad de la Información y la Ciberseguridad en temas claves para el desarrollo de su actividad

CISSP Security Training

profesional y entregar contenido de valor para aquellos que además, estén evaluando obtener su certificación internacional.

A lo largo del curso, se abordan temas clave como gestión de riesgos, seguridad de activos, arquitectura y diseño seguro, criptografía, seguridad en redes y comunicaciones, gestión de identidades y accesos, evaluación de vulnerabilidades, respuesta a incidentes y seguridad en el desarrollo de software. La formación incluye además conceptos de seguridad operativa, normativas internacionales, metodologías de desarrollo seguro y técnicas actuales de protección ante amenazas emergentes, con una fuerte orientación profesional.

Habilidades a adquirir

Al finalizar el programa, los participantes habrán adquirido una comprensión sólida de los fundamentos de la seguridad de la información y la ciberseguridad, así como de las mejores prácticas aplicables en entornos corporativos. Estarán capacitados para identificar activos críticos, analizar riesgos, implementar controles técnicos y administrativos, y colaborar en el diseño de soluciones seguras a nivel organizacional.

Además, los alumnos serán capaces de describir marcos normativos reconocidos, interpretar políticas de seguridad, participar en auditorías, comprender el proceso de gestión incidentes, y contribuir activamente en procesos de mejora continua en entornos de seguridad. La formación los prepara para asumir roles clave en equipos de seguridad, responder eficazmente ante amenazas, y desenvolverse con solvencia en proyectos de cumplimiento, protección de activos y gobierno de la seguridad.

Pre-requisitos

Aunque no es un requisito, se recomienda que los asistentes posean conocimientos básicos de controles de Seguridad de la Información y Networking

Duración

40 hs.

Audiencia

El entrenamiento se encuentra dirigido a:

- Oficiales de Seguridad de la Información
- Administradores de sistemas

CISSP Security Training

- Administradores de redes
- Profesionales de tecnología que quieran especializarse en Seguridad de la Información
- Estudiantes y entusiastas que quieran iniciarse en Seguridad de la Información

Perfil del instructor

Para esta capacitación en particular, el instructor es Experto en Ciberdelincuencia y Tecnologías Aplicadas a la Investigación" por la Universidad Austral-Argentina | Universidad Abat Oliba CEU-Barcelona y ha obtenido las principales certificaciones internacionales relacionadas con Ciberseguridad/Seguridad de la Información, tal como, por ejemplo:

- CISSP (Certified Information System Security Professional)
- CISM (Certified Information Security Management)
- CSSLP (Certified Secure Software Lifecycle Professional)
- CEH (Certified Ethical Hacker)
- CNDA (Certified Network Defense Architect for Government Agencies)
- CCSK (Certificate of Cloud Security Knowledge)
- CCISO (Chief Information Security Officer – Associate)

Temario

- Introducción a CISSP
  - ✓ Introducción al Mundo de las Certificaciones
  - ✓ Beneficios de la Obtención de Certificaciones Internacionales
  - ✓ Nuestra Propuesta de Formación & su Alineación con los Requisitos de CISSP y otras Certificaciones Internacionales.

- Seguridad y Gestión del Riesgo
  - ✓ Introducción a la Seguridad de la Información
  - ✓ Gestión de la Seguridad de la Información
  - ✓ Marco Normativo
  - ✓ Gestión del Riesgo
  - ✓ Cumplimiento y Regulación
  - ✓ Seguridad del Personal
  - ✓ BCP / DRP

CISSP Security Training

- Seguridad de Activos
  - ✓ Ciclo de Vida de la Información
  - ✓ Estadios de la Información
  - ✓ Aplicación de Controles
  - ✓ Políticas Relacionadas con la Protección de Datos
  - ✓ Roles & Responsabilidades
  - ✓ Clasificación de la Información
  - ✓ Otros Aspectos de Interés

- Arquitectura e Ingeniería de Seguridad
  - ✓ Arquitectura de Computadoras
  - ✓ Principios de Diseño Seguro
  - ✓ Mecanismos de Protección
  - ✓ Modelos de Seguridad
  - ✓ Guías de Evaluación
  - ✓ Ataques/Vulnerabilidades
  - ✓ Virtualización & Cloud Computing
  - ✓ Introducción a Criptografía
  - ✓ Algoritmos Criptográficos
  - ✓ Modelos de Confianza & PKI
  - ✓ Ataques Criptográficos

- Seguridad de Comunicaciones & Redes
  - ✓ Modelo de Referencia OSI
  - ✓ Métodos de Acceso
  - ✓ TCP/IP
  - ✓ Dispositivos de Red
  - ✓ Firewalls
  - ✓ Sistemas de Detección y Prevención de Intrusiones
  - ✓ Redes Privadas Virtuales (VPN)
  - ✓ Wireless LAN
  - ✓ Ataques Típicos en Red
  - ✓ Recomendaciones y Buenas Prácticas

- Gestión de Identidades & Accesos (IAM)
  - ✓ Introducción al Control de Acceso
  - ✓ Modelos de Control de Acceso
  - ✓ Identidad & Gestión de Acceso
  - ✓ Identificación, autenticación, autorización y auditoría

CISSP Security Training

- ✓ Técnicas de identificación & autenticación
- ✓ Biometría
- ✓ MFA
- ✓ Federación & SSO
- ✓ Kerberos & LDAP

- Evaluación & Pruebas de Seguridad
  - ✓ Ciberamenazas
  - ✓ Estrategias de Evaluación Prueba & Auditoría
  - ✓ Introducción a la Evaluación de Vulnerabilidades
  - ✓ Vulnerability Assessment & Pentest
  - ✓ Clasificación de Vulnerabilidades & Parches
  - ✓ Gestión de Vulnerabilidades
  - ✓ Monitoreo & Evaluación de Aplicaciones
  - ✓ Red, Blue & Purple Team
  - ✓ Gestión de Logs & Monitoreo
  - ✓ Security Operations Center (SOC)
  - ✓ Key Performance & Risk Indicators

- Operaciones de Seguridad
  - ✓ Investigación & Forensia
  - ✓ Gestión de Incidentes
  - ✓ Controles Operativos & Protección de Recursos
  - ✓ Estrategias de Resguardo & Recuperación
  - ✓ Malware
  - ✓ Operación de Medidas Preventivas
  - ✓ Seguridad Física & Ambiental
  - ✓ Gestión administrativa
  - ✓ Controles
  - ✓ Gestión y Respuesta ante Incidentes
  - ✓ Forensia
  - ✓ Prevención de Fuga de Información
  - ✓ Malware
  - ✓ Seguridad Física y Ambiental

- Seguridad en el Desarrollo de Software
  - ✓ Introducción a la Seguridad en el Desarrollo de Software
  - ✓ Lenguajes de Programación
  - ✓ SDLC/SDC
  - ✓ Metodologías de Desarrollo
  - ✓ Bases de Datos

CISSP Security Training

- ✓ DevOps & DevSecOps
- ✓ Amenazas & Ataques
- ✓ Pautas & Estándares de Programación Segura