Experto Universitario de Seguridad de la Información

Información General

Fecha de inicio: 24/06/2026

Frecuencia: Semanal

Carga horaria por clase: 90 min

Presentación

La generalización y expansión del uso de las tecnologías, telecomunicaciones e informática en los diferentes contextos empresariales, académicos, personales y públicos, hacen de las TICs una base común para todas nuestras actividades. Esta plataforma además de ser mantenida en su funcionamiento, debe ser protegida con el fin de controlar que los activos informáticos no sean presa de ataques, fraudes o mal uso por los delincuentes informáticos, empleados desleales o terceros mal intencionados. La comprensión de la seguridad de la información desde la función del oficial de seguridad, hace de ésta una posición clave en la gestión y entendimiento de la protección de estos activos. Desde aquí, es preciso entender cómo los elementos informáticos, los activos de información, los procesos y la concientización de las personas, conforman la consolidación de la seguridad en la organización. Y este curso prepara a los participantes para ejecutar con éxito dicha tarea. Área, campo o disciplinas de conocimiento del curso: Telecomunicaciones Administración de Servidores Administración de Redes de Datos Seguridad Informática Computación Seguridad de la Información Seguridad Informática

Objetivos Generales

Aprendan a desarrollar el plan estratégico de seguridad requerido por la organización. Adquieran los conocimientos sobre los elementos tecnológicos, redes y servidores de datos que generan un impacto de valor en la organización. Obtengan los conocimientos necesarios para la obtención de la certificación internacional de seguridad CISSP. Obtengan los conocimientos necesarios para rendir satisfactoriamente los exámenes de las siguientes certificaciones oficiales: Instalación y configuración de Windows Server 2019/2022/2025 ISC2 Certified Information Systems Security Professional.

Objetivos Específicos

- Aprendan las bases informativas conceptuales para la obtención de la certificación internacional de seguridad CISSP.
- Conozcan sobre los sistemas criptográficos y sus aplicaciones prácticas existentes, abordando sus vulnerabilidades más comunes y los potenciales ataques y amenazas.
- Aprendan a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.
- Conozcan las herramientas esenciales y las buenas prácticas necesarias para obtener el nivel máximo de seguridad en una red de servidores de arquitectura Microsoft Windows Server ó Linux Server, protegiéndola de potenciales amenazas.
- Conozcan los conceptos básicos referentes a la implementación, configuración,

mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.

- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.
- Aprendan a armar, configurar y administrar una pequeña red fácilmente.
- Conozcan los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.
- Conozcan todos los niveles y componentes que permitan el aseguramiento y protección de los activos de información, asociando su clasificación, nivel de riesgo y mejores prácticas aplicado a los mismos en términos de la seguridad de la información.
- Conozcan sobre cómo planificar la prevención, monitoreo y continuidad del negocio / operación de una organización.
- Aprendan de los contenidos, conceptos y las metodologías necesarias para entender sobre la protección de activos de información e informáticos en una organización.

Destinatarios

- Administradores de sistemas, técnicos informáticos, administradores de redes, y analistas, consultores, desarrolladores y auditores de seguridad.

Plan de Estudios

Módulo 1: Diseño de Redes Seguras

- Introducción a las redes informáticas. Historia de las redes informáticas. Comunicaciones OSI / TCP-IP. Conceptos generales de redes. Tipos de topologías
- Instalación y Configuración de redes. Modelo TCP/IP. Direccionamiento IP. Seguridad en Redes. Armado de una red (Práctica-Lab)
- Redes informáticas potenciales riesgos. Amenazas y ataques. Servicios de red (Cuáles son, niveles de importancia, alcances de uso). Potenciales ataques (Explicación + Práctica-Lab).
- Redes informáticas seguridad aplicada Dispositivos de seguridad (Funcionalidades y modos de uso). Estructuración de una red segura. Armado de una red segura (Práctica-Lab).

Módulo 2: Administración de Servidores (Windows ó Linux)

- Introducción a los servidores informáticos / Roles y Funciones
- Conociendo Linux (Práctica-Lab)
- Instalando y configurando nuestro servidor (Práctica-Lab).
- Soporte, mantenimiento y solución de problemas (Práctica-Lab).

Módulo 3: Hardening (Windows Servers ó Linux Servers)

- Introducción a implementaciones de seguridad.
- Configuraciones y Servicios (Parte 1) Configuraciones de seguridad de OS (Práctica-Lab). Servicios disponibles para instalar.
- Configuraciones y Servicios (Parte 2). Instalación y configuración básica de servicios (Práctica-Lab).
- Seguridad Aplicada. Potenciales ataques (Lista y explicación + Práctica-Lab). Escaneo de

vulnerabilidades y comparación de resultados Antes-Después (Práctica-Lab).

Módulo 4: Seguridad de la Información

- Introducción sobre Criptografía. El ABC de la Criptografía. Conceptos de sistemas criptográficos. Implementación de sistemas criptográficos (Práctica-Lab).
- Seguridad en los sistemas criptográficos. Vulnerabilidades de sistemas criptográficos (Explicación de potenciales ataques). Quebrando la seguridad de sistemas criptográficos (Práctica-Lab)
- Introducción a la certificación CISSP / Cryptography (Criptografía).
- Access Control (Control de Accesos).
- Application Development Security (Seguridad aplicado al Desarrollo de Aplicaciones).
- Application Development Security (Seguridad aplicado al Desarrollo de Aplicaciones).
- Business Continuity and Disaster Recovery Planning (Continuidad del Negocio y Plan de Recuperación ante Desastres).
- Information Security Governance and Risk Management (Gobierno de la Seguridad de la Información y Gestión del Riesgo).
- Legal, Regulations, Investigations and Compliance (Aspectos Legales, Regulaciones, Investigaciones y Cumplimiento).
- Operations Security (Seguridad de las Operaciones).
- Physical (Environmental) Security (Seguridad Física).
- Security Architecture and Design (Diseño y Arquitectura de Seguridad).
- Telecommunications and Network Security (Seguridad aplicada a la redes y telecomunicaciones).

Bibliografía

- ISO 27001 Controls – A Guide to Implementing and Auditing — Autora: Bridget Kenyon. Editorial: IT Governance Publishing. Edición: 2ª (reeditada 2024 para alinearse con ISO/IEC 27001:2022) Paradigm itgovernanceusa.com ISBN—13: 9781787784314
- ISO 27001 Internal Audits & Data Protection: Strengthening Compliance & Security — Autor: Dr. Mohamed—Ali Ibrahim. Editorial: Independently Published / Ingram International Inc. Publicación: 2025 ThriftBooks ISBN—13: 9798310263697
- Eleventh Hour CISSP: Study Guide, Third Edition — Autor(es): Eric Conrad, Seth Misenar, Joshua Feldman. Editorial: Syngress. Edición: 3ª (publicado en 2016) Iberlibro (ES) ISBN—13: 9780128112489
- CISSP All—In—One Exam Guide, Ninth Edition — Autor(es): Fernando Maymí, Shon Harris. Editorial: McGraw—Hill Education. Edición: 9ª (publicado en 2021 / 2022) ISBN—13: 9781260467376