Descriptor oferta formativa

Procedimientos de ciberseguridad para la protección de la información

Resumen

Modalidad de Enseñanza:
Elearning sincrónico

Horas disponibles:
16 Hrs.

Código Sence:
1238050136

Dirigido a:
- Administradores de sistemas
- Administradores de redes
- Desarrolladores de software
- Analistas de seguridad de la información
- Ingenieros de seguridad
- Consultores de seguridad

Objetivos Generales:
Aplicar procedimientos de ciberseguridad para la protección de la información empresarial

Descripción

A lo largo de las sesiones, los participantes adquirirán habilidades y conocimientos prácticos para identificar y mitigar amenazas cibernéticas, implementando medidas de seguridad y protocolos adecuados. Los temas abordados incluyen la gestión de contraseñas, protección de datos sensibles, prevención de ataques de phishing y malware, así como la respuesta adecuada ante incidentes de seguridad. A través de ejercicios interactivos y casos de estudio, los participantes aprenderán las mejores prácticas en ciberseguridad y estarán preparados para salvaguardar la información crítica de sus organizaciones.

Contenidos

Módulo 1: Fundamentos de Seguridad de la Información
- Conceptos básicos de Seguridad de la Información
- Principios de Seguridad de la Información: Confidencialidad, Integridad, Disponibilidad (CIA)
- Clasificación y control de los activos de información
- Amenazas y riesgos a la seguridad de la información
- Medidas de seguridad: Físicas, Técnicas y Administrativas

Objetivos módulo 1

Identificar los conceptos básicos de acuerdo a los principios de la seguridad de la información

Módulo 2: Seguridad en las Redes y Sistemas
- Conceptos básicos de redes: TCP/IP, protocolos, servicios y aplicaciones
- Seguridad de los sistemas operativos y bases de datos
- Seguridad en redes: Firewalls, IDS/IPS, VPN
- Seguridad en la nube: conceptos y desafíos
- Protección contra malware: Virus, gusanos, trojanos, ransomware

Objetivos módulo 2

Identificar características sobre seguridad en redes y sistemas de la empresa

Módulo 3: Ciberseguridad y Ciberdefensa
- Conceptos básicos de Ciberseguridad y Ciberdefensa
- Amenazas y ataques cibernéticos: Phishing, DoS, DDoS, APT
- Ciberinteligencia: Técnicas y herramientas
- Respuesta a incidentes y gestión de crisis en ciberseguridad
- Marco legal y ético de la Ciberseguridad

Objetivos módulo 3

Aplicar procedimientos de ciberseguridad y ciberdefensa respetando los aspectos legales

Módulo 4: Gestión de la Seguridad de la Información
- Políticas de seguridad: Creación, implementación y auditoría
- Estándares y frameworks de seguridad: ISO 27001, NIST, CIS 4.3
- Gestión de riesgos en seguridad de la información
- Planificación de la continuidad del negocio y recuperación ante desastres
- Formación y concienciación en seguridad de la información

Objetivos módulo 4

Aplicar estándares y frameworks de seguridad considerando ISO 27001, NIST y CIS