Descriptor oferta formativa

Procedimientos de ciberseguridad para la protección de la información

Resumen

Modalidad de Enseñanza:
Elearning asincrónico

Horas disponibles:
60 Hrs.

Código Sence:
1238054406

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

www.caphome.cl

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: Introducción a la Ciberseguridad
- ¿Qué es la Ciberseguridad?: Definición, importancia y alcance.
- Amenazas y vulnerabilidades cibernéticas: Comprensión de amenazas comunes.
- Consideraciones legales y éticas: Leyes y regulaciones cibernéticas.

Objetivos módulo 1

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

Módulo 2: Aspectos Técnicos de la Ciberseguridad
- Manejo y análisis de artefactos: Construcción de entorno, procesamiento, almacenamiento y análisis de artefactos.
- Análisis Forense: Análisis Local, de red y de servidor web.
- Desarrollo de Contramedidas: Marco para el análisis, uso de indicadores, forense digital.
- Manejo de incidentes de amenazas móviles.
- Automatización y orquestación: Manejo de Incidentes, análisis forense de red, Honeypots, manejo de vulnerabilidades.

Objetivos módulo 2
- Identificar vulnerabilidades cibernéticas a través del análisis técnico y automatización.

Módulo 3: Aspectos Operativos de la Ciberseguridad.
- Manejo de Incidentes: Durante ataques a infraestructura crítica, amenazas persistentes avanzadas, redes sociales como vectores de ataque.
- Costo de Incidente de TIC: Comprensión del impacto financiero.
- Manejo de Incidentes en la nube y a gran escala: estrategias y mejores prácticas.
- Configuración de un CSIRT: Gestión, reclutamiento, desarrollo de Infraestructura.

Objetivos módulo 3
- Analizar las estrategias operativas considerando la gestión de incidentes críticos en infraestructura, TIC y entornos en la nube.

Procedimientos de ciberseguridad para la protección de la información

Módulo 4: Aspectos Legales y de Cooperación en Ciberseguridad.

- Contactos externos y cooperación con las fuerzas del orden: Evaluación de canales de comunicación, identificación de rastros de cibercrimen.
- Manejo de incidentes y cooperación: Durante campañas de phishing, cooperación en el área de cibercrimen.
- Participación de CERT: En el manejo de incidentes relacionados con varias obligaciones.

Objetivos módulo 4

Analizar la cooperación en ciberseguridad, relacionando el manejo de incidentes y contactos externos.

Módulo 5: Formación Avanzada y Soluciones Digitales en Ciberseguridad

- Entrenamiento Inteligente en Ciberseguridad: Definición, Aplicaciones y Beneficios.
- Soluciones digitales en ciberseguridad: Herramientas, tecnologías y plataformas.

Objetivos módulo 5

Aplicar soluciones digitales en ciberseguridad, considerando diversas tecnologías y plataformas.