MCR0002. Prevención y protección en ciberseguridad

MCR0002

Prevención y protección en ciberseguridad

Sistemas informáticos seguros

Duración: 50 horas

Modalidad: 100% online

Requisitos y conocimientos previos: no se requiere nivel académico previo, pero al ser en modalidad online es necesario poseer conocimientos básicos de informática, así como habilidades básicas de comunicación lingüística que permitan el aprendizaje y el seguimiento de la formación.

Objetivos

- Conocer y asimilar los conceptos de seguridad en los sistemas de información en función de la sociedad de la información.
- Estudiar los principales riesgos de seguridad, tipos de vulnerabilidades, errores de programa, programas maliciosos, etc.
- Aplicar los estándares y buenas prácticas principales en materia de seguridad en sistemas de información.
- Conocer los conceptos relacionados con la ciberseguridad.
- Analizar e identificar las amenazas más frecuentes en los sistemas de información.
- Estudiar los principales estándares que rigen la ciberseguridad.
- Identificar las características y ventajas de las redes de radio definidas por software y las redes de radio cognitivas.
- Conocer los mecanismos y sistemas de seguridad de las redes inalámbricas y configurar su seguridad.
- Aplicar políticas de seguridad adecuadas para establecer comunicaciones seguras.

- Comprender los conceptos básicos de la protección de datos y las medidas de protección para el acceso a los recursos y comunicaciones.

- Conocer los conceptos básicos relacionados con la propiedad intelectual y las principales medidas de seguridad contra malware.

- Desarrollar una comprensión integral de los sistemas de gestión ambiental y los riesgos ambientales asociados a las actividades productivas de las organizaciones.

Contenidos

Módulo 1: Fundamentos y políticas de seguridad informática (20 horas)

Unidad 1: Introducción a la seguridad en sistemas de información

1.1. Fundamentos de seguridad

1.2. Riesgos

1.3. Amenazas

Unidad 2: Políticas de seguridad informática

2.1. Gestión de la ciberseguridad

2.2. Políticas de seguridad

2.3. Medidas de protección

Módulo 2: Seguridad física y lógica, acceso remoto, control de acceso a aplicaciones y aspectos legales (30 horas)

Unidad 3: Seguridad física y seguridad lógica

3.1. Dispositivos tamper-proof

3.2. Análisis de canal lateral (Side channel analysis)

3.3. Software Defined Radio y Cognitive Radio Networks

3.4. Control de acceso

3.5. Amenazas y software malicioso

Unidad 4: Seguridad en redes inalámbricas

4.1. Interconexión remota de sedes

4.2. Demostración práctica de diferentes redes privadas virtuales (VPN)

Unidad 5: Control de acceso a aplicaciones

5.1. Autenticación y autorización en servicios web

5.2. OAuth, OAuth2 y tokens

Unidad 6: Aspectos legales y herramientas de seguridad

6.1. Aspectos jurídicos en entornos tecnológicos

6.2. Protección de datos y control de acceso

6.3. Propiedad intelectual y licencias

6.4. Protección contra malware