UC0959-262_CAMN
Prevención y protección en ciberseguridad

Descripción:

Idioma del Curso: Español
Próximos inicios:
14/05/2024
Precio: 0 eur. Financiado por la Unión Europea – NextGenerationEU
Modalidad: 100% Online (Sin horarios ni desplazamientos)
Diploma: Sí
Unidad de competencia (UC) relacionada: MRR_IFCT_UC0959_262
Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

Este curso ofrece una comprensión esencial de las amenazas cibernéticas y cómo prevenirlas. Los participantes aprenderán sobre medidas de seguridad informática, cómo proteger los datos personales y empresariales, y cómo evitar ataques de malware y phishing. Con un enfoque práctico, se proporcionan estrategias para mantenerse seguros en el mundo digital actual.

Nº de horas:
60 horas

Objetivos:

El objetivo general del curso es capacitar a los participantes en el diseño de políticas de seguridad informática y en la aplicación práctica de medidas tecnológicas y metodológicas para prevenir accidentes relacionados con el uso de tecnologías informáticas y la gestión de datos en el negocio, empresa o institución.

Requisitos y conocimientos:

Acción formativa subvencionada dirigida a personas ocupadas de Catalunya.

Para realizar este curso no se requiere nivel académico previo, pero se deben tener conocimientos básicos en informática, así como habilidades básicas de comunicación lingüística que permitan el aprendizaje y el seguimiento de la formación.

Contenido UC0959-262_CAMN: Prevención y protección en ciberseguridad

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

Unidad didáctica 1: Introducción a la seguridad en sistemas de información

1.1. Fundamentos de seguridad.
1.2. Riesgos.
1.3. Amenazas.

Unidad didáctica 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. (35 horas)
Unidad didáctica 3: Seguridad física y seguridad lógica
3.1. Dispositivos tamper-proof.
3.2. Side channel análisis.
3.3. Software Defina Radio y Cognitive Radio Networks.
3.4. Control de acceso.
3.5. Amenazas y software nocivo.

Unidad didáctica 4: Seguridad en redes inalámbricas
4.1. Interconexión remota de sedes.
4.2. Demostración práctica de distintas redes privadas virtuales.

Unidad didáctica 5: Control de acceso a aplicaciones
5.1. Autenticación y autorización en servicios WEB.
5.2. OAuth, OAuth2 y tokens.

Unidad didáctica 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. Protección intelectual y licencias.
6.4 Protección frente a malware.

Módulo transversal obligatorio de sostenibilidad medioambiental:

Módulo 3. Gestión Ambiental:
Reducción de Riesgos y Mejora Continua en la Gestión de los Recursos Naturales (5 horas)
Unidad didáctica 7 - Sistemas de gestión ambiental
7.1. Identificar los procesos que conforman los sistemas de gestión ambiental.
Unidad didáctica 8 - Riesgos ambientales