MF0489_3: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Certificado de Profesionalidad IFCT0109
SEGURIDAD INFORMÁTICA

Lugar de impartición: Aemta, C/ Roa de la Vega 14, ent.dcha, León
Dirigido prioritariamente a trabajadores (por cuenta ajena y autónomos) y desempleados

Acción gratuita financiada por el Servicio Público de Empleo Estatal

Objetivo: Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.

Duración: 60 horas presenciales.
Nivel del Certificado: 3

Si estás interesad@ en participar debes cumplimentar la solicitud que se adjunta y enviarla a cursos@aemta.es , junto a la siguiente documentación:

TRABAJADORES y DEMANDANTES DE EMPLEO
○ Solicitud de participación (ANEXO III) ○ Fotocopia DNI ○ Fotocopia Tarjeta de la seguridad Social ○ Fotocopia Cabecera de la última Nomina o último recibo de autónomo o tarjeta de demandante de empleo ○ CV actualizado ○ Fotocopia de titulación académica

*Debes cumplir alguno de los **requisitos de acceso** según artículo 20 del RD 189/2013, de 15 de marzo, que modifica el RD 34/2008, de 18 de enero:*

a) Graduado en ESO para el nivel 2 o título de Bachiller para nivel 3.
b) Certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que desea acceder.
c) Certificado de profesionalidad de nivel 1 de la misma familia y área profesional para el nivel 2 o de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
d) Cumplir el requisito académico de acceso a los ciclos formativos de grado medio para el nivel 2 o de grado superior para el nivel 3, o bien haber superado las correspondientes pruebas de acceso reguladas por las administraciones educativas.
e) Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
f) Tener las competencias clave necesarias, de acuerdo con lo recogido en el anexo IV de este real decreto, para cursar con aprovechamiento la formación correspondiente al certificado de profesionalidad.

Contenidos

1. Criptografía

- Perspectiva histórica y objetivos de la criptografía
- Teoría de la información
- Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
- Elementos fundamentales de la criptografía de clave privada y de clave publica
- Características y atributos de los certificados digitales
- Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
- Algoritmos criptográficos mas frecuentemente utilizados
- Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
- Elementos fundamentales de las funciones resumen y los criterios para su utilización
- Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
- Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
- Criterios para la utilización de técnicas de cifrado de flujo y de bloque
- Protocolos de intercambio de claves
- Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop.

2. Aplicación de una infraestructura de clave pública (PKI)

- Identificación de los componentes de una PKI y su modelo de relaciones
- Autoridad de certificación y sus elementos
- Política de certificado y declaración de prácticas de certificación (CPS)
- Lista de certificados revocados (CRL)
- Funcionamiento de las solicitudes de firma de certificados (CSR)
- Infraestructura de gestión de privilegios (PMI)
- Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
- Aplicaciones que se apoyan en la existencia de una PKI

3. Comunicaciones seguras

- Definición, finalidad y funcionalidad de redes privadas virtuales
- Protocolo IPSec
- Protocolos SSL y SSH
- Sistemas SSL VPN
- Túneles cifrados
- Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN