DATOS IDENTIFICATIVOS DEL MÓDULO FORMATIVO

MÓDULO FORMATIVO	SISTEMAS SEGUROS DE ACCESO Y TRATAMIENTO DE DATOS	Duración	60
Código	MF0489_3		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área profesional	Sistemas y telemática		
Certificado de profesionalidad	Seguridad informática	Nivel	3
Resto de formación para completar el certificado de profesionalidad	Seguridad en equipos informáticos	Duración	90
	Auditoría de seguridad informática		90
	Gestión de incidentes de seguridad informática		90
	Gestión de servicios en el sistema informático (Transversal)		90
	Prácticas profesionales no laborales en seguridad informática		80

Apartado A: **REFERENTE DE COMPETENCIA**

Este módulo formativo se corresponde con la unidad de competencia UC0489_3: DISEÑAR E IMPLEMENTAR SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

Capacidades y criterios de evaluación

C1: Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.

CE1.1 Describir las diferencias entre los algoritmos de cifrado de clave privada y los de clave pública, indicando sus diferentes usos.

CE1.2 Identificar los diferentes modos de cifrado, describiendo las características principales.

CE1.3 Clasificar los diferentes algoritmos de clave privada, describiendo sus fases de ejecución.

CE1.4 Clasificar los diferentes algoritmos de clave pública, describiendo sus fases de ejecución.

CE1.5 Identificar los diferentes protocolos de intercambio de claves, describiendo su funcionamiento.

C2: Implantar servicios y técnicas criptográficas en aquellos servicios que lo requieran según especificaciones de seguridad informática.

CE2.1 Justificar la necesidad de utilizar técnicas criptográficas en las comunicaciones entre sistemas informáticos en función de los canales utilizados.

CE2.2 Definir las técnicas de cifrado para conectar de forma segura dos redes describiendo las funcionalidades y requisitos necesarios.

CE2.3 Definir las técnicas empleadas para conectar de forma segura dos equipos (túneles SSL y SSH), describiendo las funcionalidades y requisitos necesarios.

CE2.4 En un caso práctico, en el que se desea establecer una comunicación segura entre dos sistemas informáticos:

- Analizar los requisitos de seguridad de la arquitectura de comunicaciones propuesta.
- Indicar la solución más indicada, justificando la selección.
- Instalar los servicios de VPN e IPSec para conectar redes.
- Instalar los servicios de túneles SSL o SSH para conectar equipos distantes.

C3: Utilizar sistemas de certificados digitales en aquellas comunicaciones que requieran integridad y confidencialidad según especificaciones de seguridad.

CE3.1 Identificar los atributos empleados en los certificados digitales para servidor, describiendo sus valores y función.

CE3.2 Describir los modos de utilización de los certificados digitales, asociándolos a las especificaciones de seguridad: confidencialidad, integridad y accesibilidad.

CE3.3 Describir la estructura de un sistema de sellado digital, indicando las funciones de los elementos que la integran.

C4: Diseñar e implantar servicios de certificación digital según necesidades de explotación y de seguridad informática.

CE4.1 Describir la estructura de la infraestructura de clave pública, indicando las funciones de los elementos que la integran.

CE4.2 Describir los servicios y obligaciones de la autoridad de certificación, relacionándolos con la política de certificado y la declaración de prácticas de certificación.

CE4.3 Identificar los atributos obligatorios y opcionales de un certificado digital, describiendo el uso habitual de dichos atributos.

CE4.4 Describir la estructura de una infraestructura de gestión de privilegios, indicando las funciones de los elementos que la integran.

CE4.5 Determinar los campos de los certificados de atributos, describiendo su uso habitual y la relación existente con los certificados digitales.

CE4.6 En un caso práctico, en el que se desea establecer un sistema de certificación para un sistema informático:

- Diseñar una infraestructura de clave pública, en función de las especificaciones.
- Justificar la jerarquía de autoridades de certificación diseñada.

- Emitir los certificados siguiendo los procedimientos indicados en la Declaración de Prácticas de Certificación.

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 más 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.

Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

– Estar en posesión del título de Bachiller
– Estar en posesión de algún certificado de profesionalidad de nivel 3.
– Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional
– Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior
– Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años
– Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad: Seguridad informática.