ANEXO III

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Seguridad informática

Código: IFCT0109

Familia Profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC153_3 Seguridad informática (RD 1087/05 de 16 de septiembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0486_3: Asegurar equipos informáticos.
UC0487_3: Auditar redes de comunicación y sistemas informáticos.
UC0488_3: Detectar y responder ante incidentes de seguridad.
UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

Entorno Profesional:

Ámbito Profesional:

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

Sectores Productivos:

Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. También está presente en los siguientes tipos de empresas:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (outsourcing) de servicios.

cve: BOE-A-2011-10055

Ocupaciones o puestos de trabajo relacionados:

3820.1017 Programador de Aplicaciones Informáticas
3812.1014 Técnico en Informática de Gestión
Técnico en seguridad informática.
Técnico en auditoría informática.

Duración de la formación asociada: 500 horas

Relación de módulos formativos y de unidades formativas:

MF0486_3: Seguridad en equipos informáticos. (90 horas)
MF0487_3: Auditoría de seguridad informática. (90 horas)
MF0488_3: Gestión de incidentes de seguridad informática. (90 horas)
MF0489_3: Sistemas seguros de acceso y transmisión de datos. (60 horas)
MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MP0175: Modulo de prácticas profesionales no laborales de Seguridad informática. (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: 3

Código: UC0486_3

Realizaciones profesionales y criterios de realización

RP1: Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.

CR1.1 El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados.

CR1.2 Los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema son determinados por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.

CR1.3 EL acceso a los servidores se realiza garantizando la confidencialidad e integridad de la conexión según las normas de seguridad de la organización.

CR1.4 Las políticas de usuario se analizan verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

CR1.5 La política de seguridad es transmitida a los usuarios, asegurándose de su correcta y completa comprensión.

CR1.6 Las tareas realizadas se documentan convenientemente según los procedimientos de la organización.

CR1.7 Las informaciones afectadas por la legislación de protección de datos se tratan verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

cve: BOE-A-2011-10055

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 4

Denominación: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Código: MF0489_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos

Duración: 60 horas

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.

cve: BOE-A-2011-10055

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 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

cve: BOE-A-2011-10055

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 practicas 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

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0489_3	60	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 5

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y

cve: BOE-A-2011-10055