

## 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.

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.

- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit versión 2

#### 4. Uso de herramientas para la auditoría de sistemas

- Herramientas del sistema operativo tipo Ping, Traceroute, etc.
- Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
- Herramientas de análisis de vulnerabilidades tipo Nessus
- Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
- Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
- Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

#### 5. Descripción de los aspectos sobre cortafuegos en auditorías de Sistemas Informáticos.

- Principios generales de cortafuegos
- Componentes de un cortafuegos de red
- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Arquitecturas de cortafuegos de red
- Otras arquitecturas de cortafuegos de red

#### 6. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

- Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- Guía para la elaboración del plan de auditoría
- Guía para las pruebas de auditoría
- Guía para la elaboración del informe de auditoría

#### 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 - MF0487_3	90	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 3

**Denominación:** GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

**Código:** MF0488\_3

**Nivel de cualificación profesional:** 3

**Asociado a la Unidad de Competencia:**

UC0488\_3: Detectar y responder ante incidentes de seguridad

**Duración:** 90 horas

## Capacidades y criterios de evaluación

C1: Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.

CE1.1 Describir las técnicas de detección y prevención de intrusos, exponiendo los principales parámetros que pueden emplearse como criterios de detección.

CE1.2 Determinar el número, tipo y ubicación de los sistemas de detección de intrusos, garantizando la monitorización del tráfico indicado en el plan de implantación.

CE1.3 Seleccionar las reglas del sistema de detección de intrusos, en función del sistema informático a monitorizar.

CE1.4 Determinar los umbrales de alarma del sistema, teniendo en cuenta los parámetros de uso del sistema.

CE1.5 Elaborar reglas de detección, partiendo de la caracterización de las técnicas de intrusión.

CE1.6 A partir de un supuesto práctico convenientemente caracterizado en el que se ubican servidores con posibilidad de accesos locales y remotos:

- Instalar y configurar software de recolección de alarmas.
- Configurar diferentes niveles de recolección de alarmas.

CE1.7 En una colección de supuestos prácticos en un entorno controlado de servidores en varias zonas de una red departamental con conexión a Internet:

- Decidir áreas a proteger.
- Instalar un sistema de detección de intrusos.
- Definir y aplicar normas de detección.
- Verificar funcionamiento del sistema atacando áreas protegidas.
- Elaborar un informe detallando conclusiones.

C2: Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.

CE2.1 Analizar la información de los sistemas de detección de intrusos, extrayendo aquellos eventos relevantes para la seguridad.

CE2.2 Analizar los indicios de intrusión, indicando los condicionantes necesarios para que la amenaza pueda materializarse.

CE2.3 Clasificar los elementos de las alertas del sistema de detección de intrusiones, estableciendo las posibles correlaciones existentes entre ellos, distinguiendo las alertas por tiempos y niveles de seguridad.

CE2.4 A partir de un supuesto práctico, en el que realizan intentos de intrusión al sistema informático:

- Recopilar las alertas de los sistemas de detección de intrusiones.
- Relacionar los eventos recogidos por los sistemas de detección de intrusiones.
- Determinar aquellas alertas significativas.
- Elaborar el informe correspondiente indicando las posibles intrusiones y el riesgo asociado para la seguridad del sistema informático de la organización.

CE2.5 Establecer procesos de actualización de las herramientas de detección de intrusos para asegurar su funcionalidad según especificaciones de los fabricantes.

C3: Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

CE3.1 Describir las fases del plan de actuación frente a incidentes de seguridad, describiendo los objetivos de cada fase.

CE3.2 Indicar las fases del análisis forense de equipos informáticos, describiendo los objetivos de cada fase.

CE3.3 Clasificar los tipos de evidencias del análisis forense de sistemas, indicando sus características, métodos de recolección y análisis.

CE3.4 Describir las distintas técnicas para análisis de programas maliciosos, indicando casos de uso.

CE3.5 En un supuesto práctico, en el que se ha producido una intrusión en un sistema informático:

- Realizar la recogida de evidencias volátiles.
- Realizar la recogida de evidencias no volátiles.
- Análisis preliminar de las evidencias.
- Análisis temporal de actividad del sistema de ficheros.
- Elaborar el informe final, recogiendo las evidencias encontradas, las posibles vulnerabilidades utilizadas para la intrusión y la actividad realizada por el intruso que ha sido detectada en el sistema.

CE3.6 Estandarizar métodos de recuperación de desastres de equipos informáticos ante la detección de intrusiones.

## Contenidos

### 1. Sistemas de detección y prevención de intrusiones (IDS/IPS)

- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

### 2. Implantación y puesta en producción de sistemas IDS/IPS

- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

### 3. Control de código malicioso

- Sistemas de detección y contención de código malicioso
- Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
- Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
- Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
- Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

- Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

#### 4. Respuesta ante incidentes de seguridad

- Procedimiento de recolección de información relacionada con incidentes de seguridad
- Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
- Proceso de verificación de la intrusión
- Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

#### 5. Proceso de notificación y gestión de intentos de intrusión

- Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
- Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
- Establecimiento del nivel de intervención requerido en función del impacto previsible
- Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
- Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

#### 6. Análisis forense informático

- Conceptos generales y objetivos del análisis forense
- Exposición del Principio de Lockard
- Guía para la recogida de evidencias electrónicas:
  - o Evidencias volátiles y no volátiles
  - o Etiquetado de evidencias
  - o Cadena de custodia
  - o Ficheros y directorios ocultos
  - o Información oculta del sistema
  - o Recuperación de ficheros borrados
- Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
- Guía para la selección de las herramientas de análisis forense

#### 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 - MF0488_3	90	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 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.