

## GUION DEL CURSO

**ESPECIALIDAD: SEGURIDAD INFORMÁTICA**

**CÓDIGO DE LA ESPECIALIDAD: IFCT0109**

**CÓDIGO DEL CURSO: 22/1232**

**FECHA DE INICIO: 15/03/2023**

**FECHA DE FINAL: 24/07/2023**

**HORARIO: 09:00h – 14:00h**

**CALENDARIO (días no lectivos): 20 de marzo / 3, 4, 5, 6 y 7 de abril / 1, 2, 18 y 29 de mayo**

**DURACIÓN (horas totales): 420 horas + 80 horas (prácticas profesionales no laborales)**

### OBJETIVO GENERAL DEL CURSO:

Al finalizar la formación, el alumno será capaz de:

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.

### RELACIÓN DE MÓDULOS (objetivo, contenido y duración):

RELACIÓN SECUENCIAL DE LOS MÓDULOS DEL CERTIFICADO	Horas
MF0486_3: SEGURIDAD EN EQUIPOS INFORMÁTICOS	90
MF0487_3: AUDITORÍA DE SEGURIDAD INFORMÁTICA	90
MF0488_3: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA	90
MF0489_3: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS	60
MF0490_3: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO	90
MP0175: MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES	80

#### MF0486\_3: SEGURIDAD EN EQUIPOS INFORMÁTICOS (90 Horas)

Objetivo: Asegurar equipos informáticos

Contenidos:

##### **1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos**

- Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
- Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
- Salvaguardas y tecnologías de seguridad más habituales
- La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

##### **2. Análisis de impacto de negocio**

- Identificación de procesos de negocio soportados por sistemas de información
- Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
- Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

##### **3. Gestión de riesgos**

- Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
- Metodologías comúnmente aceptadas de identificación y análisis de riesgos
- Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

#### 4. Plan de implantación de seguridad

- Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
- Guía para la elaboración del **plan de implantación de las salvaguardas seleccionadas**

#### 5. Protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

#### 6. Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas

- Determinación de los perímetros de seguridad física
- Sistemas de control de acceso físico mas frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
- Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
- Exposición de elementos mas frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
- Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
- Elaboración de la normativa de seguridad física e industrial para la organización
- Sistemas de ficheros más frecuentemente utilizados
- Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
- Configuración de políticas y directivas del directorio de usuarios
- Establecimiento de las listas de control de acceso (ACLs) a ficheros
- Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
- Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
- Sistemas de autenticación de usuarios débiles, fuertes y biométricos
- Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
- Elaboración de la normativa de control de accesos a los sistemas informáticos

#### 7. Identificación de servicios

- Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
- Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

#### 8. Robustecimiento de sistemas

- Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
- Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
- Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
- Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
- Actualización de parches de seguridad de los sistemas informáticos
- Protección de los sistemas de información frente a código malicioso
- Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
- Monitorización de la seguridad y el uso adecuado de los sistemas de información

#### 9. Implantación y configuración de cortafuegos

- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
- Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
- Definición de reglas de corte en los cortafuegos
- Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

### MF0487 3: AUDITORÍA DE SEGURIDAD INFORMÁTICA (90 Horas)

Objetivo: Auditar redes de comunicación y sistemas informáticos

Contenidos:

#### **1. Criterios generales comúnmente aceptados sobre auditoría informática**

- Código deontológico de la función de auditoría
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor
- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

#### **2. Aplicación de la normativa de protección de datos de carácter personal**

- Principios generales de protección de datos de carácter personal
- Normativa europea recogida en la directiva 95/46/CE
- Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

#### **3. Análisis de riesgos de los sistemas de información**

- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente
- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- Relación de las distintas alternativas 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

### MF0488 3: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA (90 Horas)

Objetivo: Detectar y responder ante incidentes de seguridad

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

## MF0489\_3: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS (60 Horas)

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

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 pública
- 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



## MF0490 3: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO (90 Horas)

Objetivo: Gestionar servicios en el sistema informático

Contenidos:

### **1. Gestión de la seguridad y normativas**

- Norma ISO 27002 Código de buenas prácticas para la gestión de la seguridad de la información
- Metodología ITIL Librería de infraestructuras de las tecnologías de la información
- Ley orgánica de protección de datos de carácter personal.
- Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

### **2. Análisis de los procesos de sistemas**

- Identificación de procesos de negocio soportados por sistemas de información
- Características fundamentales de los procesos electrónicos
  - o Estados de un proceso,
  - o Manejo de señales, su administración y los cambios en las prioridades
- Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
- Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
- Técnicas utilizadas para la gestión del consumo de recursos

### **3. Demostración de sistemas de almacenamiento**

- Tipos de dispositivos de almacenamiento más frecuentes
- Características de los sistemas de archivo disponibles
- Organización y estructura general de almacenamiento
- Herramientas del sistema para gestión de dispositivos de almacenamiento

### **4. Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**

- Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
- Identificación de los objetos para los cuales es necesario obtener indicadores
- Aspectos a definir para la selección y definición de indicadores
- Establecimiento de los umbrales de rendimiento de los sistemas de información
- Recolección y análisis de los datos aportados por los indicadores
- Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

### **5. Confección del proceso de monitorización de sistemas y comunicaciones**

- Identificación de los dispositivos de comunicaciones
- Análisis de los protocolos y servicios de comunicaciones
- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- Procesos de monitorización y respuesta
- Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

### **6. Selección del sistema de registro de en función de los requerimientos de la organización**

- Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
- Análisis de los requerimientos legales en referencia al registro
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
- Asignación de responsabilidades para la gestión del registro
- Alternativas de almacenamiento para los registros de sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
- Guía para la selección del sistema de almacenamiento y custodia de registros

### **7. Administración del control de accesos adecuados de los sistemas de información**

- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
- Requerimientos legales en referencia al control de accesos y asignación de privilegios
- Perfiles de de acceso en relación con los roles funcionales del personal de la organización
- Herramientas de directorio activo y servidores LDAP en general
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
- Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

## **METODOLOGÍA DIDÁCTICA (máquinas virtuales, conexiones remotas, versiones software, dominios, suscripciones, ...):**

En la primera sesión, el docente valora los conocimientos previos de los alumnos de cara a adecuar los contenidos del programa al nivel del grupo. De esta manera sopesa la necesidad de establecer varios niveles dentro del curso.

Aunque se dé el caso que durante el proceso de selección del alumnado se haya realizado una prueba de nivel, el docente puede proponer la realización de cuestionario/prueba para determinar el nivel inicial de los alumnos, esta tendrá meramente valor informativo.

Además de obtener información real de los conocimientos previos este cuestionario sirve, para que el alumno a final de curso pueda comparar sus conocimientos iniciales con lo aprendido durante el curso.

Como los objetivos señalan diversas acciones que los alumnos han de desempeñar, la enseñanza no puede fundamentarse en un solo método o en una misma forma de impartir la clase.

Por el contrario, se presentarán varias actividades para los alumnos, de tal manera que según sea el tipo de objetivo serán las acciones a realizar por el docente y los alumnos.

### **1. EXPOSICIÓN TEÓRICA**

El docente comienza la unidad formativa exponiendo la parte teórica del módulo, apoyándose en los distintos medios con los que cuenta, presentaciones con diapositivas, manuales, temario propio etc.

Una vez realizada la exposición y tras las resolver las posibles dudas que han surgido, el docente propone a los alumnos una aplicación práctica de lo explicado.

### **2. APLICACIONES PRÁCTICAS**

Relacionados con la explicación teórica el docente va a proponer casos prácticos cuya complejidad irá aumentando según los alumnos los vayan resolviendo.

El número de prácticas realizadas en cada módulo va a depender del ritmo de adquisición de contenidos, ya que estas son medidores de los procesos de aprendizaje, no obstante, es necesario que se lleven a término un mínimo establecido previamente por el docente en función del/los niveles que tengan los alumnos.

Las aplicaciones prácticas de la enseñanza abarcarán distintas fases que se ejecutarán a través de tareas. Dichas tareas serán:

- Tareas de procedimiento o rutina, en las que se pide al alumnado que aplique un procedimiento adquirido durante la fase teórica que le lleve a una determinada respuesta.
- Tareas de opinión, en las que se pide al alumnado que aporte los conocimientos adquiridos durante su vida profesional y que puedan ser de utilidad para el resto del grupo. De esta manera se fomenta el trabajo en equipo y se aumenta la autoestima de los alumnos
- Tareas de comprensión, en las que los conocimientos son redescubiertos por el alumnado

## **MATERIAL DIDÁCTICO DEL ALUMNO (fungible):**

CUADERNO, BOLÍGRAFO, PENDRIVE 16 GB.

## **DOCUMENTACIÓN DIDÁCTICA DEL ALUMNO (denominación, formato e idioma):**

Hacking ético de redes y comunicaciones. LUIS HERRERO PÉREZ

Editorial: Ra-Ma (edición papel en castellano)

ISBN: 978-84-18971-20-4

## **SISTEMA DE EVALUACIÓN (instrumentos, criterios y momentos):**

El alumnado debe ser evaluado de manera equitativa y justa de acuerdo con el nivel de enseñanza impartida.

La evaluación del alumnado es un proceso continuo durante el curso, este método permitirá tomar decisiones respecto a la posibilidad de introducir modificaciones en el proceso de enseñanza-aprendizaje.

Red de Centros Propios de Formación

Durante el proceso de evaluación se valorarán dos aspectos fundamentales:

- Actitud del alumno frente al curso y al aprendizaje: Motivación, relaciones con el resto de los alumnos, asistencia y comportamiento.
- Adquisición de destrezas/aptitudes, en función de los objetivos del curso.

Los criterios de evaluación utilizados, serán conocidos por el alumnado en la primera sesión, de manera que se garantice la objetividad y transparencia del proceso.

En los certificados de profesionalidad, los criterios de evaluación están determinados por el RD que regula el mismo.

Se evaluará por módulo formativo/unidad formativa a los alumnos

#### PROCEDIMIENTO DE LA EVALUACIÓN

- Se realizarán pruebas teórico prácticas durante el desarrollo de las diferentes unidades formativas, estas tendrán una valoración del 30% de la nota final.
- Se realizarán pruebas teórico prácticas al final de cada módulo formativo, estas pruebas aunarán lo aprendido en las diferentes unidades formativas que componen el módulo y tendrán una repercusión del 70% de la nota final.

**ES NECESARIO CUMPLIR CON EL 75% DE ASISTENCIA AL MÓDULO FORMATIVO PARA PODER SER EVALUABLE**

En caso de no superar dichas pruebas el alumnado podrá realizar una prueba de recuperación.

#### **PRÁCTICAS EN CENTROS DE TRABAJO (si procede):**

El presente certificado contempla la ejecución de prácticas no laborales con una duración de 80 horas.

Concepción y finalidad del módulo

Es un bloque de formación específica que se desarrolla en un ámbito productivo real, la empresa, donde los alumnos pueden observar y desempeñar las actividades y funciones propias de los distintos puestos de trabajo del perfil profesional y conocer la organización de los procesos productivos o de servicios y las relaciones laborales.

Este módulo tiene por finalidad:

- Facilitar la identificación con la realidad de un entorno productivo y la posibilidad de la inserción profesional.
- Evidenciar las competencias profesionales adquiridas en el centro formativo y de aquellos aspectos que resultan más difíciles de ser comprobados por requerir situaciones reales de producción.
- Completar aquellas capacidades, que, por motivos normalmente estructurales, no se pudieron concluir en el centro formativo, incluidas las actitudes relacionadas con la profesionalidad.

Para la obtención del certificado de profesionalidad es necesaria la superación del módulo de prácticas no laborales.

Estarán exentos de realizar este módulo los alumnos de los programas de formación en alternancia con el empleo, en el área del correspondiente certificado, así como quienes acrediten una experiencia laboral de al menos tres meses, que se corresponda con las capacidades recogidas en el citado módulo.

#### **VISITAS DIDÁCTICAS:**

Se realizará una visita didáctica adicional a la duración del curso relacionada con la especialidad y que suponga un valor añadido al aprendizaje práctico del alumnado. La asistencia a esta visita didáctica es voluntaria y se suspende el curso ese día, alargándose la finalización de la acción formativa un día más.