

# **PROGRAMACIÓN DIDÁCTICA**

**CURSO: 2011/2012**

## **CUALIFICACIÓN PROFESIONAL**

**Técnico de Sistemas Microinformáticos y  
Redes**

## **MÓDULO PROFESIONAL**

**Seguridad Informática**

**Código: 0226**

## **FAMILIA PROFESIONAL**

**Informática y Comunicaciones**

**NIVEL**

**DURACIÓN HORAS**

**Formación Profesional  
de Grado Medio**

**110**

**PROFESORES:** Juan Carlos Fuentes Miralles  
M<sup>a</sup> Consuelo Rubio Sánchez

## INDICE DE CONTENIDOS:

### 1.INTRODUCCIÓN

#### 1.1.Marco legal

#### 1.2.Descripción del entorno

#### 1.3.Características del alumnado

### 2.OBJETIVOS

#### 2.1.Objetivos generales del ciclo formativo

#### 2.2.Objetivos del módulo

#### 2.3.Objetivos relacionados con temas transversales.

### 3.CONTENIDOS

#### 3.1.Conceptos básicos de la seguridad informática

#### 3.2.Seguridad pasiva. Hardware y almacenamiento

#### 3.3.Seguridad pasiva. Recuperación de datos

#### 3.4.Sistemas de identificación. Criptografía

#### 3.5.Seguridad activa en el sistema

#### 3.6.Seguridad activa en redes

#### 3.7.Seguridad de alto nivel en redes: cortafuegos

#### 3.8.Seguridad de alto nivel en redes: proxy

### 4.METODOLOGÍA: ORIENTACIONES DIDÁCTICAS

### 5.CRITERIOS DE EVALUACIÓN

#### 5.1.Procedimientos de evaluación

#### 5.2.Plan de recuperación

### 6.ATENCIÓN A ALUMNOS CON NECESIDADES EDUCATIVAS ESPECÍFICAS

### 7.MATERIALES Y RECURSOS DIDÁCTICOS

## 1. INTRODUCCIÓN

El presente documento es la programación didáctica del módulo de **Seguridad informática**, que se imparte en el segundo curso del Ciclo Formativo de Grado Medio, correspondiente al título de **Técnico en Sistemas Microinformáticos y Redes (SMR)**.

La duración del módulo es de 110 horas lectivas y se desarrolla a lo largo de los tres trimestres del primer curso, impartándose cinco horas semanales.

### 1.1 Marco legal

La elaboración de la Programación Didáctica del módulo profesional Aplicaciones informáticas perteneciente al Ciclo Formativo de Grado Medio – Sistemas Microinformáticos y Redes, se fundamenta en la normativa que se detalla a continuación:

- Ley Orgánica 1/1990 de Ordenación del Sistema Educativo.
- Real Decreto 676/1993, de 7 de mayo, por el que se establecen las directrices generales sobre los títulos y las correspondientes enseñanzas mínimas de Formación Profesional.
  - Real Decreto 1691/2007, de 14 de diciembre, por el que se establece el título de técnico en Sistemas Microinformáticos y Redes, y se fijan sus enseñanzas mínimas.
- Orden de 29 de julio 2009, de la Conselleria de Educación, por la que se establece para la Comunitat Valenciana el currículo del ciclo formativo de Grado Medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes. [2009/9808]
- Real Decreto 1744/1998, de 31 de julio, sobre uso y supervisión de libros de texto y demás material curricular correspondiente a las enseñanzas de régimen general.
- Orden de 20 de diciembre de 94, de la Consellería de Educación y Ciencia, por la que se dictan instrucciones para el desarrollo de la educación en valores en las actividades educativas de los centros docentes (DOGV de 3 de marzo).
- Orden de 14 de marzo de 2005, de la Consellería de Cultura, Educación y Deporte, por la que se regula la atención al alumnado con necesidades educativas especiales.

### 1.2 Descripción del entorno

Para la preparación de esta programación didáctica la vamos a situar en el I.E.S. San Vicente del Raspeig. Este instituto es de construcción recientemente contando con un profesorado joven y dinámico y con unas instalaciones inmejorables.

Además existe un tejido de servicios que demanda cada vez más, profesionales de la informática para el mantenimiento de sus equipos e infraestructuras.

Es muy importante conocer las posibilidades de la inserción laboral de nuestros estudiantes, ya que ayuda a determinar los aprendizajes prioritarios y útiles de cara a su futuro laboral. Con todo esto, lo más probable es que nuestros alumnos acaben ocupando puestos en empresas no dedicadas a la informática, pero con la necesidad de tener algún profesional de la informática que pueda administrar y mantener sus sistemas informáticos.

Otro aspecto a destacar es la existencia de dos lenguas oficiales en la Comunidad Valenciana, que son el valenciano y el castellano. Por tanto, es importante formar adecuadamente a los alumnos en las dos lenguas, facilitando su futura integración e inserción socio-laboral.

### **1.3 Características del alumnado**

En la mayoría de casos, nos vamos a encontrar con alumnos cuya mayor motivación es conseguir una rápida inserción laboral.

Los criterios de acceso al ciclo son:

El requisito académico que da acceso directo para cursar Ciclos Formativos de Grado Medio es estar en posesión del **título de Graduado en Educación Secundaria Obligatoria**.

#### **Otros accesos directos:**

Quienes posean alguna de las titulaciones o acreditaciones académicas siguientes:

- **Técnico Auxiliar.**
- **Técnico.**
- Haber superado el segundo curso de **Bachillerato Unificado y Polivalente.**
- Haber superado el **segundo curso del primer ciclo experimental** de la reforma de las enseñanzas medias.

- Haber superado, de las **enseñanzas de Artes Aplicadas y Oficios Artísticos, el tercer curso del Plan de 1963 o segundo de comunes experimental.**
- Haber superado **otros estudios declarados equivalentes** a efectos académicos con alguno de los anteriores.

**Acceso mediante prueba,** El acceso mediante prueba a los Ciclos Formativos de Grado Medio se efectuará con arreglo a lo dispuesto en el artículo 6 del Real Decreto 676/1993, de 7 de mayo.

Con todo esto nos da un perfil de alumnos cuya edad superior a los 15 años, con una clara predisposición por aprender y trabajar, que buscan una rápida incorporación al mundo laboral.

También conviene mencionar que, dada la zona en la que se encuentra San Vicente del Raspeig, los alumnos de este centro provienen de diversas nacionalidades y también de diferentes poblaciones vecinas. Lo que incrementa la pluralidad del alumnado en base a características sociales, económicas, etc.

## **2 OBJETIVOS**

### **2.1 Objetivos generales del ciclo formativo**

Se establecen en el Real Decreto 1691/2007, de 14 de diciembre, por el que se establece el título de técnico en Sistemas Microinformáticos y Redes, y se fijan sus enseñanzas mínimas.

- a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
- b) Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.
- c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
- d) Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y

características del despliegue, para replantear el cableado y la electrónica de la red.

- e) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
- f) Interconectar equipos informáticos, dispositivos de red local y de conexión con redes de área extensa, ejecutando los procedimientos para instalar y configurar redes locales.
- g) Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- h) Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- i) Interpretar y seleccionar información para elaborar documentación técnica y administrativa.
- j) Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.
- k) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
- l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
- m) Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.
- n) Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.
- o) Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción.
- p) Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.
- q) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.

- r) Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.

## **2.2 Objetivos del módulo**

- Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades.
- Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información.
- Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.
- Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico.
- Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento.

## **2.3 Objetivos relacionados con temas transversales**

En el currículo de la nueva Formación profesional Específica aparece un nuevo concepto general que se denomina Temas Transversales, los cuales deben impregnar la práctica educativa y estar presentes explícitamente en los diferentes módulos profesionales.

Los temas que se consideran transversales en el currículo son:

- Educación moral y cívica
- Educación para la paz
- Educación para la igualdad de ambos sexos
- Educación ambiental
- Educación para la salud y educación sexual
- La educación del consumidor
- La educación vial

Dadas las características de este módulo profesional los temas transversales que principalmente abordaremos serán la educación salud, educación ambiental, educación

cívica, y para la igualdad de ambos sexos. Podemos establecer unos objetivos básicos a cumplir:

- Comprender las normas básicas de seguridad a la hora de trabajar en el mantenimiento de equipos informáticos.
- Conocer y respetar las principales normas de ergonomía en el puesto de trabajo.
- Resolver los conflictos mediante el diálogo, siendo tolerantes y aceptando las ideas de los demás como bases de una convivencia en paz, así como respetar y aceptar a todas las personas sea cual sea su condición social, sexual o religiosa.

### 3. CONTENIDO

#### 3.1 Contenidos relacionados con los bloques temáticos del currículo.

A la hora de especificar los contenidos, distinguimos tres tipos.

- Conceptuales: representan el saber. Son los conocimientos necesarios.
- Procedimentales: representan el saber hacer. Son las habilidades y destrezas necesarias para desempeñar el puesto de trabajo.
- Actitudinales: representan el saber estar y actuar. Son las actitudes y características favorables para desempeñar el puesto de trabajo.

La mayor parte de los contenidos debe ser de tipo procedimental, ya que la formación profesional tiene un claro referente ocupacional y práctico. Los contenidos se programan de cara a que el alumno adquiera las capacidades terminales.

Orden de 29 de julio 2009, de la Conselleria de Educación, por la que se establece para la Comunitat Valenciana el currículo del ciclo formativo de Grado Medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes. En dicha Orden se regula los **contenidos mínimos** del módulo de **Seguridad informática**

#### •Aplicación de medidas de seguridad pasiva:

- Ubicación y protección física de los equipos y servidores.
- Sistemas de alimentación ininterrumpida.

#### •Gestión de dispositivos de almacenamiento:

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.

- Almacenamiento remoto y extraíble.
- Criptografía.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.

•**Aplicación de mecanismos de seguridad activa:**

- Identificación digital. Firma electrónica y certificado digital.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Utilización de cortafuegos en un sistema o servidor.
- Listas de control de acceso.
- Política de contraseñas.
- Recuperación de datos.
- Software malicioso. Clasificación. Herramientas de protección y desinfección.

•**Aseguramiento de la privacidad:**

- Métodos para asegurar la privacidad de la información transmitida.
- Fraudes informáticos y robos de información.
- Control de la monitorización en redes cableadas.
- Seguridad en redes inalámbricas.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos en equipos y servidores.

•**Cumplimiento de la legislación y de las normas sobre seguridad:**

- Legislación sobre protección de datos.

•**Legislación sobre los servicios de la sociedad de la información y correo electrónico.**

Con esta descripción de los bloques de contenidos se conseguirá que el alumno vaya adquiriendo de forma progresiva los conocimientos, habilidades y actitudes necesarias.

A los Reales Decretos se pueden añadir otros contenidos siempre que sean adecuados para la formación y futura inserción laboral del alumnado. El Real Decreto de título también establece los criterios de evaluación para cada uno de los resultados de aprendizaje de cada módulo.

Vamos a exponer en detalle cada una de las unidades los contenidos establecidos

en el el currículo de SMR.

## **Unidad 1. Conceptos básicos de la seguridad informática**

1. Seguridad informática ¿por qué?
2. Objetivos de la seguridad informática
3. Clasificación de seguridad
  - 3.1. Seguridad física y lógica
  - 3.2. Seguridad activa y pasiva
4. Amenazas y fraudes en los sistemas de la información
  - 4.1. Actuaciones para mejorar la seguridad
  - 4.2. Vulnerabilidades
  - 4.3. Tipos de amenazas
  - 4.4. Pautas de protección para nuestro sistema
5. Leyes relacionadas con la seguridad de la información
  - 5.1. Normativa que protege los datos personales
  - 5.2. Normativa de los sistemas de información y comercio electrónico

## **Unidad 2. Seguridad pasiva. Hardware y almacenamiento**

1. Ubicación y protección física
  - 1.1. Factores para elegir la ubicación
  - 1.2. Control de acceso
  - 1.3. Sistemas de climatización y protección en el CPD
  - 1.4. Recuperación en caso de desastre
2. Sistemas de alimentación ininterrumpida
  - 2.1. Definición de SAI
  - 2.2. Tipos de SAI
  - 2.3. Modo de funcionamiento
3. Almacenamiento de la información
4. Almacenamiento redundante y distribuido
  - 4.1. RAID en Windows
  - 4.2. RAID en Windows Vista
  - 4.3. RAID en Windows 2008 Server
5. Clusters de servidores

5.1. Clasificación de los clusters

5.2. Componentes de los clusters

6. Almacenamiento externo

6.1. Network Attached Storage

6.2. Storage Area Network

### **Unidad 3. Seguridad Pasiva. Recuperación de datos**

1. Introducción

2. Tipos de copias de seguridad

3. Copias de seguridad de los datos

3.1. Copia de seguridad de datos en Windows

3.2. Copia de seguridad de datos en Linux

4. Modos de recuperación frente a pérdidas en el sistema operativo

5. Creación de imágenes del sistema

6. Copia de seguridad del registro

7. Políticas de copias de seguridad

### **Unidad 4. Sistemas de identificación. Criptografía**

1. ¿Cómo aseguramos la privacidad de la información?

2. Un poco de historia de la criptografía

3. Criptografía simétrica y asimétrica

3.1. Criptografía simétrica

3.2. Criptografía asimétrica

3.3. Criptografía híbrida

4. Algoritmos

5. Función Resumen

6. Firma digital

7. Certificados digitales

8. PKI

### **Unidad 5. Seguridad activa en el sistema**

1. Introducción a la seguridad del sistema

2. Seguridad en el acceso al ordenador
  - 2.1. ¿Cómo evitamos que personas ajenas modifiquen la BIOS?
  - 2.2. ¿Cómo proteger el GRUB con contraseña?
  - 2.3. Cifrado de particiones
- 2.4. Cuotas de disco
- 2.5. Activación y uso de cuotas de disco en Windows
- 2.6. Cuotas de usuario en UBUNTU
3. Autenticación de los usuarios
  - 3.1. Políticas de contraseñas
  - 3.2. Sistemas biométricos
  - 3.3. Listas de control de acceso
4. Vulnerabilidades del sistema
  - 4.1. Evitar vulnerabilidades en Windows
5. Monitorización del sistema
  - 5.1. Monitorización en Windows
  - 5.2. Monitorización en Linux
6. Software que vulnera la seguridad del sistema
  - 6.1. Clasificación de los atacantes
  - 6.2. Tipos de ataques

## **Unidad 6. Seguridad activa en redes**

1. Seguridad en la conexión a redes no fiables
    - 1.1. Spyware en tu ordenador
  2. Protocolos seguros
    - 2.1. Protocolo HTTPS
    - 2.2. Protocolo SSH
  3. Seguridad en redes cableadas
    - 3.1. Red privada virtual (VPN) ¿Qué es una VPN? ¿Cómo funciona una VPN?
- Instalación y configuración de una VPN
- 3.2. Detección de intrusos
  - 3.3. Arranque de servicios Servicios en Windows Vista Servicios en Ubuntu
4. Seguridad en redes inalámbricas

- 4.1. Tecnologías Wi-fi
- 4.2. Conceptos de redes Wi-fi
- 4.3. Seguridad Wi-fi

5. Seguridad WEP

6. Seguridad WPA

- 6.1. Seguridad WPA personal

6.2. Seguridad WPA empresarial

**Unidad 7. Seguridad de alto nivel en redes: cortafuegos**

1. Seguridad de alto nivel

2. Cortafuegos: qué son y para qué sirven

3. Tipos de cortafuegos

- 3.1. Según su ubicación

- Cortafuegos personales

- Cortafuegos de subredes

- 3.2. Según su tecnología

4. Filtrado de paquetes

- 4.1. Parámetros utilizados para filtrar paquetes

- 4.2. Reglas de filtrado

5. Uso de cortafuegos

- 5.1. Criterios para elegir un cortafuegos

- 5.2. Instalación y configuración de un cortafuegos comercial

6. Arquitecturas de red con cortafuegos

- 6.1. Dual-Homed Host

- 6.2. Screened Host

- 6.3. Screened subnet

7. Monitorización y logs

- 7.1. Registro de actividad de los sistemas operativos

7.2. Registros de actividad del cortafuegos

**Unidad 8. Seguridad de alto nivel en redes: proxy**

1. Introducción

2. Características del proxy
3. Funcionamiento del proxy
4. WinGate
  - 4.1. Instalación
  - 4.2. Configuración inicial
  - 4.3. Servicios de WinGate
    - Parada y arranque de los servicios
    - Configuración de los servicios
  - 4.4. Tipos de proxy
  - 4.5. Creación de usuarios
5. PureSight
6. Control de log en WinGate
7. Squid
  - 7.1. Instalación de Squid
  - 7.2. Configuración inicial
  - 7.3. Control de acceso en Squid
  - 7.4. Autenticación
  - 7.5. Clasificación de sitios en Squid
  - 7.6. Gestión del proxy con Webmin.
    - Control de log
    - Instalar y configurar Webmin para Squid
    - Utilización de Webmin
    - Análisis del log de Squid con Webmin

## **TEMPORIZACIÓN DE LOS CONTENIDOS**

1ª Evaluación : Unidades 1,2,3,4

2ª Evaluación: Unidades 5,6,7,8

A continuación estableceremos la distribución de conceptos, procedimientos y actitudes

de las diferentes unidades.

## **Unidad 1. Conceptos básicos de seguridad informática**

### **Conceptos**

- Visión global de la seguridad informática. Conceptos
- Servicios de seguridad
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - No repudio
- Clasificación de seguridad
  - Seguridad física y seguridad lógica
  - Seguridad activa y seguridad pasiva
  - Modelo de seguridad
- Amenazas y fraudes
  - Activos
  - Impactos
  - Riesgos
  - Vulnerabilidades
  - Tipos de amenazas
- Legislación
  - Protección de datos
  - Servicios de la sociedad de la información y correo electrónico

### **Procedimientos**

- Determinar los problemas que pueden surgir por no tener un acceso a Internet correctamente protegido.
- Valorar los problemas que pueden surgir por no tener protegidos los sistemas.
- Reconocer los certificados digitales.
- Verificar la integridad de los ficheros.
- Reconocer los activos, daños e impactos que pueden sufrir las empresas que no

están bien protegidas.

- Determinar las pautas de protección de los sistemas.
- Identificar los ataques recibidos.
- Conocer el proceso legal para almacenar información personal de clientes.

### **Actitudes**

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a posibles amenazas, tanto físicas como lógicas.
- Valorar la necesidad de utilizar todas las medidas de seguridad necesarias para proteger la información.
- Mostrar interés en la adquisición de conocimientos.
- Darse cuenta de lo importante que es saber proteger correctamente los equipos de las posibles amenazas, tanto físicas como lógicas.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

### **Objetivos mínimos**

- La importancia de mantener la información segura.
- Las diferencias entre seguridad física y lógica.
- La necesidad de proteger físicamente los sistemas informáticos.
- La importancia de establecer una política de contraseñas.
- Las ventajas que supone la utilización de sistemas biométricos.
- La clasificación de los principales tipos de software malicioso.
- La incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
- La necesidad de controlar el acceso a la información personal almacenada.
- El conocimiento de la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Qué figuras legales intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- La obligación de poner a disposición de las personas los datos personales que les conciernen.

- La legislación sobre protección de datos de carácter personal.
- Las normas sobre gestión de seguridad de la información.

## **Unidad 2.Seguridad pasiva. Hardware y almacenamiento**

### **Conceptos**

- Ubicación y protección física de los equipos y servidores
  - Condiciones ambientales
  - Plan de seguridad física
  - Protección del hardware
  - Control de accesos
  - Plan recuperación en caso de desastres
- Sistemas de alimentación ininterrumpida (SAI)
  - Definición
  - Tipos
  - Modo de funcionamiento
- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad
- Almacenamiento redundante: RAID (Redundant Array of Independent Disk)
  - Tipos
  - Ventajas y niveles
- Cluster de servidores
  - Servicios y ventajas
  - Tipos
  - Componentes
- NAS (Network Attached Storage)
  - Características
  - Dispositivos
- SAN (Storage Area Network)
  - Características
  - Tecnologías

**Procedimientos**

- Determinar los problemas que pueden surgir por no escoger correctamente la ubicación de un CPD.
- Valorar los problemas que pueden surgir por no considerar la seguridad necesaria en los centros de procesamiento de datos.
- Determinar la necesidad de los planes de recuperación en caso de desastre.
- Conocer las ventajas del uso de equipos SAI y seleccionarlos correctamente para satisfacer las necesidades concretas del sistema.
- Valorar la necesidad de utilizar sistemas de almacenamiento redundante o distribuido para proteger los datos de los equipos.
- Determinar qué tipo de sistema de almacenamiento redundante o distribuido es más adecuado para nuestros equipos.

**Actitudes**

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a amenazas físicas.
- Valorar la necesidad de utilizar todas las medidas necesarias para proteger nuestros sistemas.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

**Objetivos mínimos**

- Las características de la ubicación física y condiciones ambientales de los equipos y servidores.
- El funcionamiento de los sistemas de alimentación.
- La selección de puntos de aplicación de los sistemas de alimentación ininterrumpida.
- La interpretación de la documentación técnica relativa a la política de almacenamiento.
- Los factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
- La clasificación y enumeración de los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
- Las tecnologías de almacenamiento redundante y distribuido.

- Las características y el uso de medios de almacenamiento remotos y extraíbles.
- Los protocolos de actuación ante incidencias y alarmas detectadas en el subsistema físico.

### **Unidad 3.Seguridad pasiva. Recuperación de datos**

#### **Conceptos**

- Copias de seguridad e imágenes de respaldo
  - Tipos de copias de seguridad
  - Copias de seguridad encriptadas
  - Compresión en copias de seguridad
- Medios de almacenamiento en copias de seguridad
  - Discos duros
  - Discos ópticos
  - Cintas magnéticas
  - Dispositivos de memoria flash
- Políticas de copias de seguridad
  - Medios a utilizar
  - Planificación, frecuencia y rotaciones
  - Información a copiar
  - Costes
  - Estrategias
  - Documentación técnica
- Software de copias de seguridad
  - Configuración de copias de seguridad en sistemas libres y propietarios
- Recuperación de datos

#### **Procedimientos**

- Determinar el tipo de copia a realizar.
- Realizar copias de seguridad.
- Hacer imágenes de los sistemas.

- Recuperar imágenes.
- Realizar copias de seguridad comprimidas.
- Determinar el tipo de almacenamiento más apropiado para la copia de seguridad.
- Definir la política de copias de seguridad.
- Planificar las rotaciones y las frecuencias de las copias de seguridad.
- Realizar la recuperación de datos borrados o perdidos.
- Restaurar las copias de seguridad.

### **Actitudes**

- Valorar la necesidad de realizar copias de respaldo para recuperar la información en caso de perderla.
- Apreciar la importancia que tiene la realización de imágenes de sistema.
- Valorar la necesidad de conocer software específico para recuperar información borrada.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

### **Objetivos mínimos**

- Seleccionar estrategias para la realización de copias de seguridad.
- Valorar la frecuencia y el esquema de rotación.
- Realizar copias de seguridad con distintas estrategias.
- Crear y restaurar imágenes de restauración de sistemas en funcionamiento.
- Aplicar técnicas de recuperación de datos.
- Definir las políticas de copias de seguridad adecuadas a una situación determinada.
- Valorar la importancia de mantener la información segura.
- Identificar las características de los medios de almacenamiento remotos y extraíbles.
- Utilizar medios remotos y extraíbles.

## **Unidad 4. Sistemas de identificación. Criptografía**

### **Conceptos**

- Métodos para asegurar la privacidad de la información transmitida
- Criptografía
  - Cifrado de clave secreta (simétrica)
  - Cifrado de clave pública (asimétrica)
  - Funciones de mezcla o resumen (hash)
- Sistemas de identificación
  - Firma digital
  - Certificados digitales
  - Distribución de claves. PKI
  - Tarjetas inteligentes
- Seguridad del sistema
  - Amenazas y ataques
  - Seguridad en el arranque
  - Particiones del disco y seguridad
  - Actualizaciones y parches de seguridad en el sistema y en las aplicaciones
  - Autenticación de usuarios
    - Listas de control de acceso
    - Sistemas biométricos
    - Política de contraseñas
    - Cuotas de disco
  - Monitorización y logs del sistema
- Software que vulnera la seguridad del sistema
  - Clasificación de atacantes
  - Tipos de ataques (sniffing, DoS, virus, etcetera)
  - Software malicioso (malware)
  - Técnicas usadas para el fraude y robo (ingeniería social, phishing, spoofing, etcétera)
  - Impactos

–Educación y formación del usuario. Consejos prácticos. Copias de seguridad e imágenes de respaldo

### **Procedimientos**

- Cifrar textos mediante diversos algoritmos.
- Generar parejas de claves para el cifrado asimétrico.
- Exportar e importar certificados.
- Intercambiar claves o certificados.
- Revocar un certificado.
- Instalar una entidad emisora de certificados.
- Realizar peticiones de certificados a una entidad emisora.
- Retirar certificados.
- Firmar mensajes.
- Obtener certificados digitales.
- Enviar correos electrónicos haciendo uso del certificado digital.

### **Actitudes**

- Apreciar la necesidad de cifrar la información para mantener la confidencialidad.
- Valorar la importancia del uso de los certificados y firmas digitales.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

### **Objetivos mínimos**

- Instalar, probar y actualizar aplicaciones específicas para la detección y eliminación de software malicioso.
- Describir y utilizar sistemas lógicos de identificación como la firma electrónica, el certificado digital, etcétera.
- Valorar las ventajas que supone la utilización de sistemas biométricos.
- Clasificar y detectar las principales incidencias y amenazas lógicas de un subsistema lógico.
- Aplicar técnicas de monitorización de accesos y actividad e identificar situaciones anómalas.

## **Unidad 5. Seguridad activa en el sistema**

### **Conceptos**

- Seguridad en el arranque y en particiones.
- Actualizaciones y parches de seguridad en el sistema y en las aplicaciones.
- Autenticación de usuarios.
- Listas de control de acceso.
- Monitorización del sistema.
- Software que vulnera la seguridad del sistema.

### **Procedimientos**

- Proteger el arranque del sistema frente a intrusos.
- Cifrar particiones para que no sean accesibles a personal ajeno.
- Crear cuotas de disco.
- Definir políticas de contraseñas.
- Crear contraseñas seguras.
- Definir listas de control de acceso.
- Monitorizar el sistema.
- Hacer ARP spoofing y DNS spoofing.
- Comprometer una sesión telnet.
- Configurar un análisis con antivirus.
- Detectar las amenazas del sistema.

### **Actitudes**

- Apreciar la necesidad de proteger al sistema frente a los atacantes.
- Valorar la importancia de definir cuotas de disco.
- Valorar la importancia de monitorizar el sistema.
- Valorar la repercusión del uso de antivirus para evitar la entrada de troyanos, gusanos y virus.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

**Objetivos mínimos**

- Instalar, probar y actualizar aplicaciones específicas para detectar y eliminar software malicioso.
- Clasificar y detectar las principales incidencias y amenazas lógicas de un subsistema lógico.
- Aplicar técnicas de monitorización de accesos y actividad e identificar situaciones anómalas.
- Valorar las ventajas que supone la utilización de sistemas biométricos.

**Unidad 6. Seguridad activa en redes****Conceptos**

- Seguridad en la conexión a redes no fiables
- Introducción a protocolos seguros
- Seguridad en redes cableadas
  - Intrusiones externas vs. intrusiones internas
  - Redes privadas virtuales (VPN)
  - Detección de intrusos
  - Seguridad en los accesos de red: Arranque de servicios y monitorización
- Seguridad en redes inalámbricas
  - Tecnologías Wi-Fi
  - Seguridad en los protocolos para comunicaciones inalámbricas
  - Tipos de ataques
  - Mecanismos de seguridad

**Procedimientos**

- Conocer los riesgos que implica conectarse a redes no seguras como Internet.
- Reconocer los protocolos seguros y las ventajas de utilizarlos.
- Conocer las alternativas de conexión segura a través de redes inseguras.
- Valorar la necesidad de utilizar herramientas de detección de spyware, malware e intrusos.
- Determinar la necesidad de iniciar automáticamente o no determinados servicios del sistema operativo.

- Valorar los riesgos de seguridad de las conexiones inalámbricas.
- Conocer los distintos estándares IEEE 802.11.
- Conocer las alternativas de seguridad para redes inalámbricas.

### **Actitudes**

- Valorar la importancia de proteger nuestros sistemas cuando se utilizan redes no seguras, ya sean cableadas o inalámbricas.
- Mostrar iniciativa para proteger la red doméstica.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

### **Objetivos mínimos**

- Identificar la necesidad de inventariar y controlar los servicios de red.
- La importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
- Aplicar medidas para evitar la monitorización de redes cableadas.
- Clasificar y valorar las propiedades de seguridad de los protocolos usados en redes inalámbricas.
- Actualizar periódicamente los sistemas para corregir posibles vulnerabilidades.

## **Unidad 7. Seguridad de alto nivel en redes: cortafuegos**

### **Conceptos**

- Seguridad de alto nivel
- Cortafuegos
  - Características
  - Ventajas de uso
  - Tipos
- Filtrado de paquetes
- Reglas de filtrado
  - Uso de cortafuegos
    - Criterios de elección

- Instalación y configuración
- Arquitecturas de red con cortafuegos
- Monitorización y logs

### **Procedimientos**

- Conocer las ventajas del uso de cortafuegos.
- Elegir el cortafuegos idóneo para el sistema que se vaya a proteger.
- Establecer las reglas de filtrado adecuadas para la red.
- Instalar y configurar un cortafuegos.
- Identificar distintas arquitecturas de red, así como sus ventajas e inconvenientes.
- Reconocer la información recogida en los archivos de monitorización.

### **Actitudes**

- Valorar la importancia de proteger nuestros equipos de accesos desde el exterior y el interior de nuestra red.
- Utilizar la lógica para establecer las reglas de filtrado más adecuadas en cada situación.
- Mostrar iniciativa para proteger la red doméstica.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

### **Objetivos mínimos**

- Identificar la necesidad de inventariar y controlar los servicios de red.
- Instalar y configurar un cortafuegos en un equipo o servidor.
- Configurar las reglas de seguridad que hay que aplicar en un cortafuegos.
- Utilizar medidas para evitar la monitorización.

## Unidad 8. Seguridad de alto nivel en redes: proxy

### Conceptos

- Características del proxy
- Funcionamiento del proxy
- WinGate
  - Configuración inicial
  - Servicios de WinGate
  - Tipos de proxy
  - Creación de usuarios
- PureSight
- Control de log en WinGate
- Squid
  - Instalación de Squid
  - Configuración inicial
  - Control de acceso en Squid
  - Autenticación
  - Clasificación de sitios en Squid
  - Gestión del proxy con Webmin. Control de log

### Procedimientos

- Identificar las funciones de un proxy y aplicarlas en una situación concreta y definida.
- Conocer y manejar los principales proxys que hay en el mercado (WinGate y Squid).
- Configurar adecuadamente las reglas de acceso de un proxy WinGate y de un Squid.
- Utilizar clasificaciones de sitios de Internet para restringir el acceso a un determinado tipo de contenidos.
- Comprender y controlar los ficheros de log generados por los proxys.

### Actitudes

- Organizar y analizar el trabajo, antes de realizarlo y durante su desarrollo.

- Tener una actitud crítica pero respetuosa con los compañeros, lo que favorece unas mejores relaciones laborales en un futuro puesto de trabajo.
- Resolver problemas y tomar decisiones siguiendo las normas y procedimientos establecidos.
- Participar de forma activa en la vida económica, social y cultural con una actitud crítica y responsable.
- Reconocer los derechos y deberes.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

### **Objetivos mínimos**

- Identificar la necesidad de inventariar y controlar los servicios de red.
- Instalado un proxy.
- Configurar un proxy ajustándose a unas necesidades concretas.
- Identificar y analizar el software disponible en el mercado, y describir sus principales características.

#### 4.- METODOLOGÍA: ORIENTACIONES DIDÁCTICAS

El R.D. 362/2004, de 5 de marzo, por el que se establece la ordenación general de la formación profesional específica, establece en su artículo 13 punto 4: *“La metodología didáctica de las enseñanzas de formación profesional integrará los aspectos científicos tecnológicos y organizativos que en cada caso correspondan, con el fin de que el alumnado adquiera una visión global de los procesos productivos propios de la actividad profesional correspondiente”*.

En función de las capacidades terminales y sus correspondientes criterios de evaluación de éste módulo, así como de las capacidades profesionales descritas en la Orden de 29 de julio 2009, de la Conselleria de Educación, se deduce que el proceso de enseñanza-aprendizaje lo basaremos en todo momento en el “saber hacer”.

Se concibe la educación como un proceso constructivo en el que la cooperación entre el profesor y el alumno/a obtiene como resultado una experiencia de aprendizaje útil y significativo. El profesor actúa como guía, ayudando al alumno/a a conseguir los objetivos del módulo.

Este concepto de educación asegura que los alumnos/as podrán utilizarlo aprendido tanto en circunstancias reales de trabajo como en la incorporación de nuevos conocimientos.

Como consecuencia las estrategias metodológicas a seguir por los profesores de la asignatura son:

- Método expositivo e interrogativo: consiste en el sistema clásico de enseñanza en que se imparten nuevos conocimientos.
  - Para la explicación de cada Unidad de Trabajo se realizará una exposición teórica de los contenidos de la unidad por parte del profesor.
  - Posteriormente se realizarán una serie de ejercicios propuestos por el profesor y resueltos y corregidos por él en clase. El objetivo de estos ejercicios es llevar a la práctica los conceptos teóricos que se asimilaron en la exposición teórica anterior.
  - El profesor resolverá todas las dudas que puedan tener los alumnos, tanto teóricos como prácticos. Si se considera necesario se realizarán

ejercicios específicos que aclaren los conceptos que más cueste comprender a los alumnos.

□El profesor propondrá un conjunto de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser resueltos por los alumnos, bien en horas de clase o bien en casa.

•Método de aprendizaje por descubrimiento: consiste en proponer un problema a los alumnos, y que a través de unas indicaciones básicas sean capaces de encontrar la solución.

•Método de aprendizaje por proyectos: consiste en asignar proyectos de trabajo individuales o en grupo, en que los alumnos deben alcanzar unos objetivos.

Con todo ello, planteamos los siguientes grupos de actividades que se concretarán en cada unidad de trabajo.

•Actividades de introducción y motivación: para presentar un tema nuevo y captar el interés de los alumnos.

•Actividades de desarrollo: para profundizar en los contenidos de un tema.

•Actividades de refuerzo: para ayudar a los alumnos con un ritmo más lento de lo normal a alcanzar los mínimos exigibles.

•Actividades de ampliación: para que los alumnos con un ritmo más rápido de lo normal puedan profundizar en su aprendizaje, manteniendo el interés en clase.

A lo largo del módulo también se pueden desarrollar algunas de las siguientes actividades adicionales:

•Actividades complementarias: charlas o debates impartidas por empresas o profesionales, para compartir su experiencia con los alumnos.

Las prácticas se resolverán de forma individual, ya que habrá un alumno por ordenador, no es aconsejable que haya más de dos alumnos por cada equipo informático teniendo que realizar una memoria o trabajo práctico a su finalización.

## 5 CRITERIOS DE EVALUACIÓN

### 5.1 Procedimientos de evaluación

La evaluación educativa se entiende como una actividad sistemática y continuada, integrada en el proceso educativo, cuya finalidad consiste en obtener la máxima información sobre el alumno, el proceso educativo y todos los factores que en él intervienen, para tomar decisiones con el fin de orientar y ayudar al alumno y mejorar el proceso educativo, reajustando objetivos, pensando programas, métodos y recursos.

El seguimiento del proceso de enseñanza-aprendizaje se lleva a cabo a través de la evaluación. Ésta ha de cumplir las siguientes características:

- **Continua** a lo largo de todo el proceso de aprendizaje. Se tendrá en cuenta la evaluación inicial, la evaluación formativa y la evaluación sumativa.
- **Integradora**: no sólo se han de evaluar los contenidos, sino también el resto de componentes que forman parte de la formación del alumnado, como actitudes, destrezas, comportamientos, capacidad de investigación y de iniciativa, etc.
- **Individualizadora**: ha de ajustarse a las características personales de cada alumno/a.
- **Orientadora**: debe informar al alumnado del grado de evolución conseguido respecto a los objetivos del módulo y la mejor forma de alcanzarlos.

La Orden de 14 de noviembre de 1994 por la que se regula el proceso de evaluación del alumnado en la Formación Profesional Específica, establece que “la evaluación de los aprendizajes se realizará tomando como referencia las capacidades y criterios de evaluación establecidos para cada módulo profesional”. En cuanto a los criterios de evaluación dice: “los criterios de evaluación establecen los resultados mínimos que deben ser alcanzados en el proceso enseñanza-aprendizaje”.

Dado que el enfoque de la metodología didáctica a emplear es fundamentalmente procedimental, la evaluación dará mucha importancia a la realización de prácticas en el aula de informática y a la presentación de trabajos y ejercicios resueltos por parte de los alumnos. No obstante también se realizarán una serie de pruebas escritas al término de cada uno de los bloques temáticos, cuyo objetivo es comprobar el grado de asimilación de los contenidos conceptuales

- Para poder superar el nivel mínimo que requiere los objetivos de formación, y por lo tanto, poder aprobar el Módulo Profesional, los alumnos deberán:
- Superar todos los exámenes y controles escritos o en ordenador realizados a lo largo del curso.
- Realizar, entregar y superar todos los ejercicios prácticos, trabajos, supuestos teórico-prácticos, etc. y cualquier otro elemento evaluador de tipo procedimental, individual o en grupo, que sean establecidos por el profesor.

Los alumnos serán evaluados al finalizar cada unidad de trabajo mediante la corrección de las prácticas de taller asociadas y de las actividades realizadas en el aula, y de una prueba escrita sobre los contenidos vistos en la unidad de trabajo.

La nota de cada alumno se compone de cuatro componentes:

• **Sesiones de prácticas (40 %):**

- Observación del trabajo diario de los alumnos.
- Corrección del cuaderno de clase de los alumnos.
- Sesiones de prácticas en grupo.
  - Calificación de los informes de autoevaluación del alumno. Se calificará la correcta evaluación del propio trabajo y la correcta justificación de dicha calificación.
  - Calificación de la práctica asignada por el profesor.
- Sesiones de prácticas individuales.
  - Calificación de los informes de autoevaluación del alumno. Se calificará la correcta evaluación del propio trabajo y la correcta justificación de dicha calificación.
  - Calificación de la práctica asignada por el profesor.

• **Pruebas escritas y pruebas prácticas (50 %):**

- Preguntas tipo test.
- Preguntas objetivas de respuestas cortas.
- Problemas.

- Ejercicios delante del ordenador.

• **Actitud y asistencia a clase (10 %):**

- Respeta los equipos y el material de clase.
- Respeta a los compañeros.
- Es puntual en la entrega de trabajos y en la asistencia a clase.
- Limpieza y orden del cuaderno de clase.
- Participa en el desarrollo de la clase con aportaciones inteligentes.
- Asiste diariamente a clase.

Se debe obtener al menos un 5 en todas las partes para superar la asignatura.

## **5.2 Plan de recuperación**

Se realizará una recuperación al final de cada evaluación con aquellas unidades que no han sido superadas en la primera convocatoria del examen.

Además de una recuperación de toda la asignatura en la convocatoria extraordinaria de Junio. Será requisito para hacer este examen presentar los ejercicios o trabajos propuestos por el profesor en la fecha indicada por el mismo.

## **6 ATENCIÓN A ALUMNOS CON NECESIDADES EDUCATIVAS ESPECÍFICAS**

Resulta muy complicado que todos los alumnos de una misma clase tenga en mismo nivel, unos pocos tardarán muy poco en asimilar los conceptos y otros tardarán un poco más que los demás en asimilarlos. Por eso la La **Ley Orgánica 10/2002** (LOCE) hace mención en su capítulo VII a la atención a los alumnos con necesidades educativas específicas, desarrollando para:

- Alumnos extranjeros (artículo 42)
- Alumnos superdotados intelectualmente (artículo 43)
- Alumnos con necesidades educativas especiales (artículo 44)

Se entiende por adaptación curricular (AC) a la acomodación o ajuste de la oferta educativa común, a las posibilidades y necesidades de cada alumno, o más concretamente, al conjunto de acciones dirigidas a adecuar el currículo a las necesidades de un alumno o grupo determinado.

Las adaptaciones curriculares (AC) las preparará el departamento didáctico de la familia profesional correspondiente en colaboración con el departamento de orientación. En ningún caso, las adaptaciones curriculares supondrán la supresión o modificación de objetivos (capacidades terminales) relacionados con la competencia profesional básica característica de cada título. Por lo tanto estas solo afectarán al metodología, actividades y a la temporización necesaria para la obtención de los objetivos. También sería conveniente preparar materiales adicionales a utilizar por el alumnado.

### **Alumnos superdotados intelectualmente**

A los alumnos que posean características de sobredotación y a aquellos que por su capacidad o experiencia tengan un nivel claramente superior al resto de la clase, se les propondrán actividades específicas que permitan desarrollar su intelecto de la forma más adecuada. Se les recomendará y propondrá la realización de actividades de mayor complejidad que al resto de la clase que amplíen los conceptos bien sea con la lectura de artículos o bibliografía avanzados o la realización de actividades de mayor complejidad.

### **Alumnos con dificultad de aprendizaje**

A los alumnos que presenten dificultades de aprendizaje se les tratará de orientar

hacia la realización de las actividades más básicas que cumplan los objetivos marcados para el módulo. Se les proporcionará información de apoyo adecuada a su nivel.

### **Alumnos con discapacidad física**

Con respecto a los alumnos que presenten alguna discapacidad física según sea ésta temporal o permanente se actuará de diferente forma. Para las discapacidades físicas permanentes se realizarán las adaptaciones curriculares que sean oportunas, basadas en la adaptación de los espacios, aspectos físicos, equipamiento y recursos. En el caso de discapacidades físicas temporales se realizará la adaptación que se considere más adecuada para cada caso particular durante el tiempo que dure la discapacidad.

### **Alumnos extranjeros**

En el caso de alumnos extranjeros con problemas de comunicación asociados al lenguaje sería conveniente que se les dedicase alguna hora a la semana para su más rápida comprensión de la lengua. Esto podría ser llevado a cabo por profesorado del centro que disponga en su horario de alguna hora para poder normalizar en la lengua a este tipo de alumnado ayudado en la medida de lo posible por los profesores de las materias impartidas para que adapten sus materiales a la lengua nativa del alumno.

### **Alumnos con necesidades educativas especiales**

Para los alumnos con necesidades educativas especiales se realizarán adaptaciones curriculares, éstas podrán ser significativas o no significativas. Cualquier adaptación curricular que hagamos a alumnos con necesidades educativas especiales la haremos siempre en colaboración con el Departamento de Orientación, el cual nos indicará los grados y formas de aprender del alumno con el fin de determinar que objetivos de la programación conviene modificar o adaptar. Todo esto intentando siempre integrar al alumno con el resto de compañeros.

## **7 MATERIALES Y RECURSOS DIDÁCTICOS**

- Aula de informática:
- PC's conectados en red. El aula deberá disponer de al menos del suficiente número de ordenadores para que no haya más de dos alumnos por puesto de trabajo, aunque es recomendable que cada alumno tenga su ordenador.

- Pizarra
- Presentaciones en PowerPoint o similar
- Cañón para mostrar la salida del ordenador del profesor a los alumnos.
- Ordenador-servidor conectado al cañón.
- Conexión a Internet.

Bibliografía:

Apuntes de clase elaborados por el profesor.

Libro base: Seguridad informática. Ed. McGraw-Hill. ISBN: 978-84-481-7137-7