JUNTA DE ANDALUCIA

CONSEJERIA DE EDUCACION
IES Gonzalo Nazareno

Ciclo Formativo de Grado Superior de Sistemas Microinformáticos y Redes

Programación del módulo Seguridad Informática

Curso 2018/2019

Profesor: José Domingo Muñoz Rodríguez

Índice

1. Introducción

En este documento se presenta la programación didáctica para el módulo profesional Seguridad Informática, y se basa en la siguiente legislación:

- **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 EDU/2187/2009**, de 3 de julio, por la que se establece el currículo del ciclo formativo de Grado Medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes
- **ORDEN de 7 de julio de 2009**, por la que se desarrolla el currículo correspondiente al título de Técnico en Sistemas Microinformáticos y Redes (BOJA Nº 165 de 25 de agosto de 2009).
- **ORDEN de 29 de septiembre de 2010**, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad autónoma de Andalucía. (BOJA 15-10-2010)

Este módulo profesional se imparte durante el segundo curso y tiene asignadas un total de 105 horas, a razón de 5 horas semanales.

2. Competencias, objetivos generales y resultados de aprendizaje

2.1. Competencia General

La competencia general de este título consiste en instalar, configurar y mantener sistemas microinformáticos, aislados o en red, así como redes locales en pequeños entornos, asegurando su funcionalidad y aplicando los protocolos de calidad, seguridad y respeto al medio ambiente establecidos.

2.2. Competencias profesionales, personales y sociales

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

- a) Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos, interpretando la documentación

técnica asociada y organizando los recursos necesarios.
- c) Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
- i) Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información.
- j) Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
- l) Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
- n) Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
- o) Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.
- p) Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
- t) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y aprendizaje.

2.3. Unidades de competencia asociada al módulo

La superación de este módulo aportará los conocimientos necesarios para que el alumno pueda obtener y acreditarse en las siguientes Unidades de Competencia:

- **UC0958_2**: Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes.
- **UC0957_2**: Mantener y regular el subsistema físico en sistemas informáticos.

2.4. Objetivos generales

La formación del módulo contribuye a alcanzar los objetivos generales de este ciclo formativo que se relacionan a continuación:

- 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.
- 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.
- g) Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- 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

2.5. Resultados de aprendizajes

- **RA1**: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
- **RA2**: Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.
- **RA3**: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
- **RA4**: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.
- **RA5**: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

2.6 Relación entre competencias, objetivos generales y resultados de aprendizaje

- CPPS = Competencias profesionales, personales y sociales.
- OG = Objetivos generales.

CPPS	OG	Resultados de aprendizaje
a, c, j, l, n, o, p, t	a, c, e, g, k, l, m	**RA1**: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
i, o p, t	a, k, l, m	**RA2**: Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

a, c, n, o p, t	c, l, m	**RA3**: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
a, c, j, n, o p, t	d, e, g, l	**RA4**: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.
j, n, o p, t	a	**RA5**: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

3. Contenidos y temporalización

Hemos estructurado el contenido en 5 bloques de unidades didácticas:

BLOQUE 1. SEGURIDAD FÍSICA Y AMBIENTAL

- UD1. Introducción a la Seguridad Informática.
- UD2. Seguridad Física.

BLOQUE 2. ALMACENAMIENTO DE LA INFORMACIÓN

- UD 3. Gestión del Almacenamiento de la información.
- UD 4 . Copias de Seguridad e imágenes de respaldo.

BLOQUE 3. LEGISLACIÓN

- UD 5. Normativa sobre seguridad y protección de datos.

BLOQUE 4. SEGURIDAD LÓGICA

- UD 6. Seguridad Lógica.
- UD 7. Criptografía.
- UD 8. Fraudes y Software Malicioso.
- UD 9. Medidas de protección contra el Malware.

BLOQUE 5. SEGURIDAD EN REDES

- UD 10. Seguridad en redes.
- UD11. Ataques y contramedidas.
- UD 12. Auditorías de Seguridad.

3.1 Temporalización de unidades didácticas

A continuación, mostramos las unidades de trabajo, las horas asignadas, así como la relación con los Resultados de Aprendizaje.
El número totales de este módulo es: 105 h (5 horas/semana)

Unidad	Trimestre	Nº Horas
BLOQUE 1. SEGURIDAD FÍSICA Y AMBIENTAL		
UD1. Introducción a la Seguridad Informática	1	10
UD2. Seguridad Física	1	10
BLOQUE 2. ALMACENAMIENTO DE LA INFORMACIÓN		
UD 3. Gestión del Almacenamiento de la información	1	10
UD 4 . Copias de Seguridad e imágenes de respaldo.	1	10
BLOQUE 3. LEGISLACIÓN		
UD 5. Normativa sobre seguridad y protección de datos	1	5
BLOQUE 4. SEGURIDAD LÓGICA		
UD 6. Seguridad Lógica	1	10
UD 7. Criptografía	1	15
UD 8. Fraudes y Software Malicioso	2	5
UD 9. Medidas de protección contra el Malware	2	5
BLOQUE 5. SEGURIDAD EN REDES		
UD 10. Seguridad en redes	2	10
UD11. Ataques y contramedidas	2	10
UD 12. Auditorías de Seguridad	2	5

3.2. Relación de unidades didácticas con resultados de aprendizajes

A continuación mostramos los resultados de aprendizajes que se van a alcanzar en cada unidad didáctica:

Unidad	RA relacionados
BLOQUE 1. SEGURIDAD FÍSICA Y AMBIENTAL	
UD1. Introducción a la Seguridad Informática	RA1
UD2. Seguridad Física	RA1
BLOQUE 2. ALMACENAMIENTO DE LA INFORMACIÓN	
UD 3. Gestión del Almacenamiento de la información	RA2
UD 4 . Copias de Seguridad e imágenes de respaldo.	RA2
BLOQUE 3. LEGISLACIÓN	
UD 5. Normativa sobre seguridad y protección de datos	RA5
BLOQUE 4. SEGURIDAD LÓGICA	
UD 6. Seguridad Lógica	RA1,RA3
UD 7. Criptografía	RA1,RA3
UD 8. Fraudes y Software Malicioso	RA1,RA3

UD 9. Medidas de protección contra el Malware	RA1,RA3
BLOQUE 5. SEGURIDAD EN REDES	
UD 10. Seguridad en redes	RA4
UD11. Ataques y contramedidas	RA4
UD 12. Auditorías de Seguridad	RA4

3.3. Relación secuenciada de unidades didácticas

3.3.1. Introducción a la Seguridad Informática

R.A.	Trimestre	Horas	CPPS	OG
RA1	1	10	a, c, j, l, n, o, p, t	a, c, e, g, k, l, m

Objetivos Didácticos

- Valorar la importancia de mantener la información segura
- Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
- Describir los principios básicos de la seguridad.
- Identificar cada tipo de amenaza.
- Conocer qué son y qué utilidad tienen las políticas de seguridad
- Aprender en qué consisten los planes de contingencias.
- Contenidos conceptuales
- Contenidos procedimentales

Contenidos

- Importancia de la Seguridad Informática.
- Elementos vulnerables en el Sistema Informático
- Principios de la Seguridad Informática: Confidencialidad, Disponibilidad, Integridad y no repudio.
- Seguridad activa y Seguridad pasiva. Seguridad física y lógica
- Mecanismos de seguridad: Preventivos, Detectivos, Correctivos
- Amenazas. Interrupción, Integración, Interceptación y Modificación
- Políticas de seguridad informática
- Planes de contingencias

Actividades de enseñanza-aprendizaje

- **Presentación del módulo**
  - Se realizará una breve descripción de los contenidos del módulo, de la metodología a seguir y de los criterios de calificación, justificando la importancia del mismo y mostrando su aplicación práctica en el mundo

laboral.

- **Evaluación inicial**
  - Se entregará al alumnado un cuestionario inicial con cuestiones relacionadas, entre otros aspectos, con sus conocimientos acerca la materia del módulo.
- **De motivación y presentación del tema**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**
  - Se iniciará un debate a partir de las preguntas planteadas en la presentación de la unidad.
- **De desarrollo de contenidos**
  - Práctica 1: Mitos de la seguridad. Por grupos tendrán que responder una serie de cuestiones relativas a los conceptos aprendidos.
- **De consolidación**
  - Práctica 2: Shodan, el buscador terrorífico. Utilizando el motor de búsqueda Shodan averiguar qué tipo de información proporciona y si todas las conexiones tienen implementadas medidas de seguridad.
  - Práctica 3: Uso del analizador de protocolos Wireshark. Utilizando el analizador de protocolos Wireshark responder a las cuestiones planteadas en la tarea.
- **De síntesis**
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no ha superado y porqué.

3.3.2. Seguridad Física

R.A.	Trimestre	Horas	CPPS	OG
RA1	1	10	a, c, j, l, n, o, p, t	a, c, e, g, k, l, m

Objetivos Didácticos

- Definir características de la ubicación física y condiciones ambientales de equipos y servidores
- Aplicar medidas de seguridad física preventivas
- Verificar el funcionamientos de los Sistemas de Alimentación Ininterrumpida (SAI) y conocer las ventajas de su uso
- Seleccionar correctamente los SAI para satisfacer las necesidades requeridas
- Valorar la importancia de los Centros de Respaldo

Contenidos

- Importancia de la Seguridad Física
- Seguridad en Centros de Proceso de Datos (CPD)

    - Control de acceso y presencia
    - Sistemas contra incendios
    - Ubicación y condiciones ambientales
- SAI
    - Problemas en la red eléctrica. Causas y efectos
    - Tipos de SAI
    - Potencia necesaria
    - Monitorización
- Centros de Respaldo

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema**
    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**
    - Se indicarán una serie de fenómenos naturales y riesgos humanos que pueden poner en peligro la seguridad física de los equipos de una empresa y se pedirá a los alumnos que reflexionen sobre si se podrían evitar y cómo.
- **De desarrollo de contenidos**
    - Práctica : Incendios, control de acceso y de presencia: Proyecto para dotar a un CPD de las medidas de seguridad físicas necesarias en cuanto a control de acceso y presencia así como prevención y extinción de incendios.
    - Práctica (Por grupo): Videovigilancia IP: Configuración por grupos de las IPCam's disponibles en el Departamento.
- **De consolidación**
    - Práctica : Selección SAIs: Se diseñarán presupuestos de SAI's que cubran las necesidades requeridas.
    - Práctica (Por grupo): Gestión SAIs: Monitorización de SAI y cálculo de potencias requeridas.
- **De síntesis**
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad.

3.3.3. Gestión del Almacenamiento de la información

R.A.	Trimestre	Horas	CPPS	OG
RA2	1	10	i, o	a, k, l, m

Objetivos Didácticos

- Conocer las características de la gestión del almacenamiento
- Diseñar políticas de almacenamiento

- Utilizar los medios de almacenamiento y saber cómo protegerlos
- Reconocer las tecnologías de almacenamiento más utilizadas.
- Recuperar ficheros eliminados

Contenidos

- Gestión de la información y políticas de almacenamiento.
- Dispositivos de almacenamiento. Clasificación.
- Almacenamiento remoto y externo
- Recuperación de ficheros.
- Almacenamiento Redundante y Distribuido
    - RAID 0
    - RAID 1
    - RAID 5

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema**
    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**
    - Se iniciará un debate dirigido sobre las medidas adoptadas por los alumnos para almacenar de forma segura su información y conocer los dispositivos de almacenamiento que habitualmente utilizan.
- **De desarrollo de contenidos**
    - Estudio sobre los últimos dispositivos de almacenamiento que hay en el mercado determinando el precio/GB. Se analizarán pros y contras del uso de las diferentes posibilidades de almacenamiento remoto.
- **De consolidación**
    - Práctica: Congelación del sistema. Descargar, instalar y configurar una herramienta para congelar el sistema tanto en Windows como Debian.
    - Práctica: RAID. Creación por software en Debian y Windows de RAID0, 1 y 5, simulando fallos en discos, sustituyendolos por otros y comprobando la sincronización.
    - Práctica (Por grupos): Almacenamiento en la nube. Trabajo de investigación sobre distintos proveedores de almacenamiento en la nube, eligiendo el más adecuado a sus necesidades.
- **De síntesis**.
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no ha superado y porqué.

3.3.4. Copias de Seguridad e imágenes de respaldo

R.A.	Trimestre	Horas	CPPS	OG
RA2	1	10	i	l, m

Objetivos Didácticos

- Conocer las estrategias para la realización de copias de seguridad.
- Establecer una planificación para la realización de copias de seguridad.
- Realizar y restaurar copias de seguridad
- Crear y recuperar imágenes de respaldo

Contenidos

- Concepto de copia de seguridad. Tipos
- Diseño de una planificación de copias de seguridad
- Realización y restauración de copias de seguridad
- Gestión de imágenes
    - Tipos de imágenes
    - Creación y recuperación de imágenes

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema**
    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica de la unidad.
- **De valoración de conocimientos previos.**
    - Se hará una puesta en común en la que se indicarán errores humanos típicos que ponen en peligro la seguridad de nuestros datos.
- **De desarrollo de contenidos.**
    - Realizar una tabla comparativa indicando ventajas e inconvenientes de los distintos tipos de copias de seguridad.
    - Determinar la política de copias de seguridad a llevar a cabo en una empresa.
    - Indicar en qué situaciones es interesante realizar imágenes del sistema.
    - Realizar copias de seguridad de carpetas en Debian con tar y en Windows
- **De consolidación.**
    - Práctica: Recuperación de ficheros borrados. Se utilizarán diversas herramientas libres que permiten la recuperación de ficheros eliminados de distintos dispositivos (Foremost, TestDisk, Recuva...)
    - Práctica: Realización y restauración de copias de seguridad. Realizar copias de seguridad con una herramienta de terceros y elaborar un pequeño manual de usuario en el que se indicarán las características de la aplicación y las ventajas que ofrece sobre Windows o tar (Cobian).
    - Realizar distintos tipos de imágenes del sistema con herramientas libres como Clonezilla
- **De síntesis.**
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.5. Normativa sobre seguridad y protección de datos

R.A.	Trimestre	Horas	CPPS	OG
RA5	1	5	j, n, o	a

Objetivos Didácticos

- Conocer la normativa que rige los datos de carácter personal, el comercio electrónico y la propiedad intelectual
- Conocer distintos tipos de delitos informáticos y la normativa española que los regula y sanciona
- Comprender la necesidad de conocer y respetar la normativa legal aplicable

Contenidos

- Protección de datos de carácter personal
- Comercio electrónico
- Normas ISO sobre gestión de seguridad de la información
- Propiedad intelectual y delitos informáticos

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos.**
  - Se lanzarán una serie de preguntas como: ¿Sabes en qué consiste la protección de datos?, ¿Qué es la LOPD?, ¿Qué entendemos por delito informático?.
- **De desarrollo de contenidos.**
  - Buscar en Internet hechos que vulneren el derecho a la intimidad de personas relacionadas con el uso de las nuevas tecnologías.
  - Buscar ejemplos de empresas españolas que han sido sancionadas en materia de protección de datos, así como la cuantía con la que han sido penalizadas.
  - Explicar las medidas que debe adoptar una empresa que vende sus productos por Internet para estar dentro de la legalidad y enumerar las leyes que deben respetarse.
- **De consolidación.**
  - Se plantean una serie de casos en los que los alumnos (en grupos de 4) deberán determinar si se produce o no algún delito o hecho sancionable. En caso afirmativo indicar el culpable, rango de penas a los que se enfrenta, y qué artículos concretos se le aplicarían.
  - Realizar un pequeño resumen del objetivo de las leyes estudiadas en la unidad y de los casos en lo que se aplican.
- **De síntesis**
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.6. Seguridad Lógica

R.A.	Trimestre	Horas	CPPS	OG
RA1, RA3	1	10	c, n	c

Objetivos Didácticos

- Comprender aspectos básicos de la seguridad lógica
- Valorar el uso de contraseñas seguras
- Analizar las ventajas de tener el sistema y aplicaciones actualizadas
- Garantizar el acceso restringido de los usuarios a datos y aplicaciones mediante políticas de seguridad

Contenidos

- Principios de la seguridad lógica
    - Políticas de seguridad corporativa
- Control de acceso lógico
    - Configuración de contraseñas seguras en Windows y Linux
    - Control de acceso en el gestor de arranque y en la BIOS
    - Control de acceso en el Sistema Operativo y aplicaciones
- Acceso a aplicaciones por internet

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema**.
    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**
    - Mediante una serie de preguntas se iniciará un pequeño debate: ¿Crees que tus contraseñas son seguras? ¿Qué entendemos por contraseña segura?. ¿Sería conveniente utilizar la misma contraseña para todas las aplicaciones?. ¿Por qué?
- **De desarrollo de contenidos**
    - En parejas deberán concretar el conjunto de normas que formarían la política de seguridad corporativa de una empresa de seguros y determinar si afectarían a todos sus departamentos.
    - Establecer y gestionar contraseñas usando directivas de seguridad en Windows y el servicio PAM en Linux.
    - Poner contraseñas de administrador y usuario a la BIOS.
    - Configurar el Boot Manager de Linux para protegerlo.
- **De consolidación**
    - Utilizando una herramienta para auditar contraseñas como John the Ripper comprobar la robusted de las contraseñas de los usuarios del sistema.
    - Comprobarlo también utilizando una herramienta alternativa en Windows

(Ophcrack).
    - Elaboración de un diccionario de herramientas mencionadas en la unidad indicando, entre otros aspectos, su descripción, web de descarga, web de su manual de uso y ejemplos de aplicación
- **De síntesis.**
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.7. Criptografía

R.A.	Trimestre	Horas	CPPS	OG
RA1, RA3	1	15	o	c, l

Objetivos Didácticos

- Entender lo que es la criptografía y sus usos
- Distinguir los distintos tipos de sistemas de cifrado con sus ventajas e inconvenientes
- Comprender el proceso de la firma digital.
- Conocer el funcionamiento los certificados digitales
- Utilizar adecuadamente herramientas de cifrado y firmado

Contenidos

- ¿Qué es la criptografía?
- Cifrando con clave simétrica
- Cifrando con clave asimétrica
- Funciones Hash.
- Firma digital
- Certificados digitales

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica de la unidad.
- **De valoración de conocimientos previos.**
    - Se lanzarán una serie de preguntas, tales como si saben qué es la escítala, cómo enviar un fichero top secret... y se les pedirá que en parejas elaboren un mensaje que sólo entiendan ellos y que posteriormente expliquen a sus compañeros el algoritmo utilizado.
- **De desarrollo de contenidos.**
    - Cifrado de ficheros con algoritmos simétricos en Windows (IZArc) y Linux (GPG).

    - Cifrar, firmar/verificar ficheros con algoritmos asimétricos en Linux (GPG).
    - Cifrar particiones y discos duros en Linux y Windows.
    - Envío seguro de documentos a través del correo electrónico utilizando criptografía de clave pública para el cifrado/firmado (GPG4Win).
    - Comprobación de que la navegación es segura. Instalación de certificados digitales en distintos navegadores.
- **De consolidación.**
    - Se propondrá que cada alumno envíe al profesor un mensaje (solo para él) y firmado por ellos. El mensaje contendrá, al menos, un archivo cifrado, un archivo firmado y un archivo explicando el proceso. .
- **De síntesis.**
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.8. Fraudes y Software Malicioso

R.A.	Trimestre	Horas	CPPS	OG
RA1, RA3	2	5	a, c, o	c, l, m

Objetivos Didácticos

- Reconocer el software malicioso, sus posibles fuentes y los distintos tipos que existen.
- Distinguir entre publicidad y correo no deseado
- Conocer en qué consiste la ingeniería social
- Identificar las nuevas posibilidades y riesgos que poseen Internet y las Redes Sociales

Contenidos

- Malware. Clasificación del Software malicioso.
    - Impacto producido
    - Forma de propagarse
    - Acciones que realiza
- Ingeniería social. Fraudes informáticos
    - Suplantación de identidad
    - Cadenas de correos
    - Correos millonarios
- Publicidad y correo no deseado

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**

    - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**.
    - Se lanzarán preguntas, con el fin de iniciar un debate, como "¿Alguno ha tenido un virus en su ordenador? ¿Qué problemas os ocasionó? ¿Cómo llegó el virus a vuestro ordenador? ¿Lo podrías haber evitado?
- **De desarrollo de contenidos**.
    - De una lista de malwares, deberán indicar de qué tipo son, cuál es su método de propagación y cuál es su nivel de peligrosidad.
    - Descargar un Keylogger y configurarlo para que envíe los registros vía web.
    - Realizar en parejas una búsqueda por internet de noticias sobre malware reales y actuales en la que aparezca una breve descripción, una explicación del por qué de su nombre, su método de propagación y mecanismo de reparación manual.
- **De consolidación**.
    - Se les hará entrega de cuatro supuestos prácticos (mail recibido del banco que pide contraseña, compra con enlace a empresa transportes, venta y datos paypal, punto de acceso que no funciona correctamente). Deberán leerlos, e indicar cómo actuar en cada caso, respondiendo a las preguntas planteadas
- **De síntesis**.
    - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.9. Medidas de protección contra el Malware

R.A.	Trimestre	Horas	CPPS	OG
RA1, RA3	2	5	a, c, o	c, l, m

Objetivos Didácticos

- Conocer cómo se puede proteger un equipo para evitar infecciones de malware
- Aprender a actuar ante una infección por malware
- Diferenciar entre antivirus personales y corporativos
- Aprender a evitar infecciones en correos corporativos
- Analizar las distintas herramientas antimalware existentes

Contenidos

- Protección y desinfección
- Herramientas antimalware
    - Antivirus personales y corporativos
    - Antispyware
    - Otras herramientas

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica de la unidad.
- **De valoración de conocimientos previos**.
  - Se lanzarán una serie de preguntas, tales como ¿Creéis que estáis protegidos de los virus? ¿Qué medidas de seguridad implementáis en vuestros equipos? ¿Con un antimalware ya no os entrarán virus?
- **De desarrollo de contenidos**.
  - Elegir tres herramientas antimalware y comparar el resultado analizando una serie de características dadas (tiempo y tamaño de la actualización, porcentaje de CPU ocupada, opciones de escaneo...)
  - Instalar un antivirus en Debian e investigar sobre su funcionamiento.
  - Instalar una herramienta para actualizar automáticamente aplicaciones en un entorno Windows (techtracker-free)
- **De consolidación**.
  - A partir de la información encontrada en esta URL: http://www.av-test.org/en/home en la que se muestra un estudio de distintas herramientas antimalware sobre el consumo de recursos, opciones de escaneo, cantidad de malware encontrado, realizar por parejas una síntesis de dicho informe incluyendo una conclusión final
- **De síntesis**.
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.10. Seguridad en redes

R.A.	Trimestre	Horas	CPPS	OG
RA4	2	10	n, o	d, e, g

Objetivos Didácticos

- Identificar las vulnerabilidades existentes en la comunicación de equipos.
- Conocer qué es una herramienta de monitorización y cómo puede ayudarnos a mejorar la seguridad de la red.
- Aprender cómo funcionan herramientas de protección como cortafuegos, proxies o detectores de intrusos.
- Conocer los mecanismos de seguridad en redes inalámbricas y sus vulnerabilidades
- Asegurar la privacidad de la información transmitida en redes instalando el software específico

Contenidos

- Vulnerabilidades de los servicios de red
- Monitorización
- Técnicas de protección: Cortafuegos, DNZ, IDS, Proxies
- Seguridad en redes inalámbricas

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos.**
  - Se discutirán cuestiones como ¿qué medidas de seguridad implementáis en la wifi de vuestra casa? ¿Soléis conectaros a redes wifi abiertas? ¿Tenéis configurado algún cortafuegos en vuestro equipo? ¿Lo creéis necesario?.
- **De desarrollo de contenidos.**
  - Realizar una presentación en parejas en la que se expliquen los distintos tipos de vulnerabilidades de servicios de red apoyándose en hechos reales y recientes.
  - Monitorizar la red mediante el uso de la herramienta libre NAGIOS.
  - Desarrollar un script que se ejecute al arrancar el servidor y que aplique, mediante con las iptables una serie de reglas establecidas
  - Configurar un IDS (sistema de detección de intrusos) como Snort para sistemas Linux
- **De consolidación.**
  - Probar la fortaleza de los distintos tipos de autenticación en redes inalámbricas con herramientas como aircrack
- **De síntesis.**
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.11. Ataques y contramedidas

R.A.	Trimestre	Horas	CPPS	OG
RA4	2	4	c, n, o	d, e, l

Objetivos Didácticos

- Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolos con las necesidades del uso informático.
- Valorar la importancia de mantener la información segura
- Aplicar medidas para evitar la monitorización de redes cableadas
- Saber asegurar la privacidad de la información transmitida instalando software específico

Contenidos

- Anatomía de un ataque.

- Técnicas de ataque
- Debilidades de seguridad comúnmente explotadas
- Ataques TCP/IP: Man in the Middle. Contramedidas
- Ataques Proxy: Ultrasurf. Contramedidas

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**.
  - Tras visualizar un vídeo sobre el ataque que sufrió Sony en su plataforma playstation se iniciará un debate dirigido con el objetivo de recopilar información de las ideas previas de los alumnos sobre la temática de la unidad.
- **De desarrollo de contenidos**.
  - Se deberá realizar, en pequeños grupos, un trabajo de investigación sobre el uso de distintas técnicas de anonimato para realizar un ataque informático.
  - Desarrollar una guía sobre cómo usar TOR para navegar de forma anónima Reproducir un ataque MITM (man in the middle) con herramientas como arpspoof o ettercap y posteriormente instalar alguna herramienta que lo detecte.
  - Utilizando UltraSurf saltarse las reglas establecidas en el proxy de la clase.
  - Investigar cómo se puede combatir UltraSurf
- **De consolidación**.
  - En parejas deberán elegir 2 tipos de ataques de una lista que se les proporcionará (ARP Spoofing, Phissing, Sniffing..), explicar en qué consisten y describir las medidas de seguridad que se pueden tomar para evitarlos.
  - Realizar una presentación sobre un ataque realizado en móviles o redes sociales que deberán buscar los alumnos, explicando en qué consiste y las medidas de seguridad a tomar para poder evitarlo.
- **De síntesis**.
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

3.3.12. Auditorías de Seguridad

R.A.	Trimestre	Horas	CPPS	OG
RA4	2	5	a, c, j, n, o	d, e

Objetivos Didácticos

- Aprender qué es una auditoría de seguridad y para qué se utiliza
- Identificar los distintos tipos de auditorías que se pueden realizar

- Conocer técnicas y herramientas que utilizan los auditores para realizar auditorías

Contenidos

- ¿Qué son las auditorías de seguridad en redes?
- Tipos de auditorías de red
- Test de intrusión
- Análisis forense
- Herramientas para auditorías

Actividades de enseñanza-aprendizaje

- **De motivación y presentación del tema.**
  - Se hará una presentación de cuáles son los objetivos que se han de alcanzar, así como de la utilidad práctica.
- **De valoración de conocimientos previos**.
  - Se debatirá la respuestas a las preguntas: ¿Dónde creéis que está el enemigo cuando se realiza un ataque a una organización? ¿Podríamos saber qué vulnerabilidades explotó y que hizo el intruso dentro? ¿Cómo?
- **De desarrollo de contenidos**.
  - En pequeños grupos deberán realizar una presentación sobre los distintos tipos de auditorías. La presentación incluirá, al menos, una empresa que las realice (datos de contacto y servicios que ofrece).
  - Tras el visionado de un vídeo ilustrativo sobre FOCA, se familiarizan con la herramienta extrayendo los metadatos de distintos archivos e interpretando la información recopilada.
  - Búsqueda, lo más detallada posible, de la información de un dominio mediante Whois o Netcraft.
  - Utilizando Nmap o Zenmap contestar las preguntas incluidas en la práctica como qué puertos tiene abiertos una determinada máquina, los servicios que hay disponibles en la red, cuántas máquinas hay en la red ...
- **De consolidación**.
  - Desde la web de secunia, en grupos deberán elaborar un breve informe sobre las vulnerabilidades encontradas en el año 2018 indicando qué tipos de programas tienen más vulnerabilidades, cuánto tiempo tardan en aparecer los parches, desde dónde se ataca.... para posteriormente hacer una puesta en común con los datos obtenidos.
- **De síntesis**.
  - Se realizará un test de repaso (autoevaluación) en el que se recapitularán los contenidos y objetivos fundamentales de la unidad para que el alumno posteriormente reflexione sobre los que no superado y porqué.

4. Temas transversales

Temas transversales que se relacionan más directamente con nuestro módulo y que por tanto pueden tratarse de forma natural serán los siguientes:

- **Trabajo colaborativo**: El alumnado debe aprender a trabajar de forma colaborativo con otros compañeros. El perfil profesional en el que se está

formando exige que en muchos puestos de trabajo desempeñe laborales dentro de un equipo y por la tanto debe aprender en la toma de decisiones, trabajo y presentación de resultados de forma conjunta con otros compañeros.

- **Educación para la salud**: Trabajaremos **educación postural**, los alumnos deben ser consciente de que una mala postura frente al ordenador de forma continuada puede crear muchos problemas de salud, por ejemplo: contracturas musculares cérvico dorsales; **educación visual**, pasar excesivas horas frente al ordenador sin la protección adecuada (protector de pantalla, una pantalla de baja radiación, etc) pueden provocar problemas de visión: picor, enrojecimiento, etc.
- **Educación ambiental**, el medio ambiente en general y nuestro entorno en particular contribuye a que tengamos una vida mejor. Fomentaremos el uso de los puntos verdes, distribuidos por la localidad.
- **Educación para el consumidor**, trabajaremos el Software legal. Problemática del software ilegal. Software libre. Saber comprar adecuadamente cualquier producto hardware y software en función de las necesidades y prestaciones que vamos buscando.

5. Metodología

Como orientación metodológica vamos a seguir principalmente un modelo constructivista de aprendizaje, que podemos resumir en las siguientes ideas principales:

- El alumno es el protagonista de su propio aprendizaje, ya que es él quien construye sus conocimientos, habilidades y destrezas.
- Fomentaremos el autoaprendizaje consistente en la búsqueda, recopilación y tratamiento de la información auxiliado por la orientación del profesor.
- Los conocimientos previos de los alumnos son tenidos en cuenta en cada una de las unidades de trabajo.
- Han de considerarse a los compañeros del alumno como un factor de aprendizaje a contemplar y potenciar, resultando de vital importancia los trabajos en grupo, debates, diseño de experiencias, evaluación de resultados, etc.
- Construcción de aprendizajes significativos, mediante la selección de contenidos que estén relacionados entre sí y tengan carácter funcional en la consecución de los resultados de aprendizaje.

Por lo tanto las estrategias metodologías que se va a seguir tendrá como objetivo conseguir progresivamente desarrollar la autonomía y autosuficiencia de los alumnos y alumnas, mediante la superación de las dificultades que irán surgiendo, concediendo especial relevancia a potenciar la iniciativa, la aplicación de la técnica apropiada y la capacidad de reacción ante nuevas situaciones.

Jugamos con ventaja; dado que esta Enseñanza no es obligatoria, los alumnos vienen con buena disposición por aprender. Nos vamos a valer de esa motivación inicial para aumentarla y para conseguir nuestras metas.

Desarrollaremos las clases de la siguiente forma:

- Al empezar la unidad utilizaremos con frecuencia la técnica del “interrogatorio dirigido”; es decir, se plantearán unas series de cuestiones que tienen como objetivos incentivar y crear una serie de inquietudes en el alumnado. Las

soluciones a esas cuestiones se resolverán en grupo. De esta forma se facilitará la comunicación en grupo y la participación activa del alumno/a.
- A continuación, se presentará la unidad didáctica. Daremos a conocer a los alumnos los contenidos y objetivos que pretendemos con la unidad.
- Los temas se expondrán en un lenguaje sencillo, a la vez que técnico, para que el alumno, futuro profesional, vaya conociendo la terminología y el argot que se utiliza en el campo de la programación.
- Emplearemos esquemas y diagramas que hagan más fácil y ameno el proceso de enseñanza y aprendizaje.
- Las clases serán eminentemente prácticas, complementadas con contenidos de soporte necesarios para llevar a cabo los procedimientos planteados.
- Emplearemos los primeros minutos de cada clase para realizar un pequeño resumen de la clase anterior.
- Resolveremos las dudas que se han podido plantear de las clases anteriores, repitiendo si es necesario algo que no ha quedado claro.
- Al final de cada unidad, realizaremos un resumen, que sirva para afianzar los contenidos.
- Intentaremos que las clases sean participativas y activas, y no sean puramente expositivas.
- Diseñaremos algunas actividades que implique trabajo en equipo, para fomentar el trabajo colaborativo.
- Diseñaremos actividades de refuerzo y de ampliación.

En resumen, las actividades de nuestras unidades se organizarán en:

1. Actividades de motivación y presentación del tema.
2. Actividades de valoración de conocimientos previos.
3. Actividades de desarrollo de contenidos.
4. Actividades de consolidación.
5. Actividades de síntesis.
6. Actividades de evaluación.

6. Materiales y recursos didácticos

Los Materiales y recursos didácticos a utilizar son los siguientes:

- Dos pizarras blancas para rotuladores.
- Equipamiento informático: Red Gigabit Ethernet de 15 ordenadores x86_64 con 4 GiB de RAM.
- Acceso a Internet de banda ancha a través de ADSL
- Un vídeo-proyector (cañón) y una pantalla de 2x2 metros para proyectar la salida RGB de un PC.
- Curso en la plataforma educativa moodle: https://dit.gonzalonazareno.org/moodle/course/view.php?id=6
- Software

    - Sistema Operativo Debian GNU/Linux
    - Sistema Operativo Ms. Windows Server
    - Sistema Operativo Ms. Windows.
    - Aplicaciones incluidas en los repositorios de las distribuciones utilizadas.
- Documentación
    - Apuntes elaborados por el profesor.
    - Presentaciones elaboradas por el profesor.
    - Documentación elaborada de forma colaborativa por el alumnado.
    - Documentación publicada en los sitios web de los fabricantes de los dispositivos utilizados.
    - Consultas a la comunidad de usuarios: listas de correo, foros, etc.
    - Tutoriales, libros electrónicos, cursos y cualquier tipo de recurso educativo útil de Internet.

7. Evaluación y recuperación

Las calificaciones del módulo están sujetas a la **orden de 29 de septiembre de 2010**, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía. (Boja 202, de 15 de octubre de 2010).

La evaluación del alumnado será realizada por el profesorado que imparta cada módulo profesional del ciclo formativo, de acuerdo con los r**esultados de aprendizaje**, los criterios de evaluación y contenidos de cada módulo profesional, así como las competencias y objetivos generales del ciclo formativo asociados a los mismos.

7.1. Criterios de evaluación

- **RA1**: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

  Criterios de evaluación

    - a) Se ha valorado la importancia de mantener la información segura.
    - b) Se han descrito las diferencias entre seguridad física y lógica.
    - c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
    - d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
    - e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
    - f) Se han seleccionado los puntos de aplicación de los sistemas de

alimentación ininterrumpida.

- g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
- h) Se ha valorado la importancia de establecer una política de contraseñas.
- i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

- **RA2**: Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

  Criterios de evaluación

  - a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
  - b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
  - c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
  - d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.
  - e) Se han seleccionado estrategias para la realización de copias de seguridad.
  - f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
  - g) Se han realizado copias de seguridad con distintas estrategias.
  - h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
  - i) Se han utilizado medios de almacenamiento remotos y extraíbles.
  - j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

- **RA3**: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

  Criterios de evaluación

- a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
- b) Se han clasificado los principales tipos de software malicioso.
- c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
- d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
- e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.
- f) Se han aplicado técnicas de recuperación de datos.

- **RA4**: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

  Criterios de evaluación

  - a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.
  - b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
  - c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
  - d) Se han aplicado medidas para evitar la monitorización de redes cableadas.
  - e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
  - f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
  - g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
  - h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

- **RA5**: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

  Criterios de evaluación

  - a) Se ha descrito la legislación sobre protección de datos de carácter personal.
  - b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
  - c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
  - d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.
  - e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
  - f) Se han contrastado las normas sobre gestión de seguridad de la información.

7.2. Criterios de calificación

La evaluación del alumnado se hace a partir de los resultados de aprendizajes, los criterios de evaluación y los contenidos, es por ello que vamos a ponderar la consecución de cada resultado de aprendizaje según la importancia y el tiempo que se va dedicar en las unidades didácticas para alcanzarlo. De esta forma podemos considerar los siguientes porcentajes de la calificación final del alumno según los resultados de aprendizajes:

Resultados de aprendizaje	Unidades Didácticas	% Nota final
RA1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	UD1, UD2, UD6, UD7, UD8, UD9	**15%**
RA2: Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	UD3, UD4	**25%**
RA3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	UD6, UD7, UD8, UD9	**25%**
RA4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	UD10, UD11, UD12	**25%**
RA5: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	UD5	**10%**

A partir de estos porcentajes podemos calcular el porcentaje de lo que aporta cada bloque de unidades didácticas a la nota final del alumno.

Bloque	R.A.	Porcentaje
Bloque 1: Seguridad Física	RA1	**20 %**
Bloque 2: Almacenamiento de Información	RA2	**25 %**
Bloque 3: Legislación	RA1, RA3	**5 %**
Bloque 4: Seguridad Lógica	R4	**25 %**
Bloque 5: Seguridad en Redes	R5	**25 %**

- Todos los instrumentos de evaluación (actividades de enseñanza-aprendizajes evaluadas) que se realicen en un bloque serán calificadas con una nota del 1 al 10.
- La nota media de los instrumentos de evaluación realizados en un bloque deberán estar aprobados (así aseguramos que se ha conseguido los resultados de aprendizajes con los que están relacionados).
- La nota media obtenida en un bloque aportará proporcionalmente a la nota final obtenida por el alumno según el porcentaje que hemos indicado anteriormente.

7.2.1. Nota trimestral

La nota trimestral tendrá un carácter informativo acerca del resultado de enseñanza-aprendizaje. Se aplicará un porcentaje en función de los contenidos impartidos.

7.2.2. Nota final del módulo

Como hemos indicado anteriormente la nota final se calculará aplicando la fórmula:

NF = 20% * not.B1 + 25% * not.B2 + 5% * not.B3 + 25% * not.B4 + 25% * not.B5

Para aplicar la fórmula anterior, el alumno ha tenido que sacar una nota igual o superior a 5 en cada uno de los bloques.

Al alumno se le proporcionará la nota por bloque y su resultado de aprendizaje asociado.

7.2.3. Recuperación

- Durante los diferentes trimestres el alumno tendrá posibilidad de realizar actividades para recuperar los bloques realizados en trimestres anteriores.
- Para los alumnos que en la segunda evaluación no superen todos los bloques de unidades didácticas o su calificación no sea superior a 5, se establecerá un periodo recuperación posibilitando la realización de actividades no superada.
- Durante el tercer trimestre del curso tendremos el periodo de recuperación. La asistencia es obligatoria. El alumno sólo deberá recuperar aquel bloque de

contenidos que tenga pendiente. Se guardan las partes aprobadas dentro de cada bloque. Por parte del profesor se realiza una atención individualizada y se repetirán aquellas prácticas y ejercicios que se consideran fundamentales para obtener los resultados de aprendizajes esperados.

- Una vez finalizado este periodo de recuperación, se realizará la denominada evaluación final en el que se computará la calificación de acuerdo al criterio seguido para las evaluaciones parciales.
- Aquellos estudiantes que, habiendo superado el módulo por convocatorias parciales, quieran subir nota, pueden acudir a las clases de recuperación y presentarse a la convocatoria final.

7.3.4. Evaluación del profesor

El profesorado debe evaluar los procesos de enseñanza y su propia práctica docente en relación con el currículo, así como presente programación didáctica, en virtud de su desarrollo real y de su adecuación a las características específicas y a las necesidades educativas de sus alumnos.

Así, el proceso de enseñanza-aprendizaje debe ser objeto de una profunda reflexión por parte del profesorado, no exenta de autocrítica, que ha de servir para modificar aquellos aspectos de la práctica docente que se hayan revelado como poco adecuados a las características de los alumnos y al contexto del Centro con el fin de ir mejorando paulatinamente la calidad de la intervención educativa.

En este módulo, la evaluación de la práctica docente se contemplará de forma interna y de forma externa.

Evaluación interna

Vamos a utilizar la técnica de observación. Debemos darnos cuenta si nuestra contribución al proceso de enseñanza aprendizaje es la correcta.

Nos fijaremos, principalmente en los siguientes aspectos:

1. ¿Los resultados de aprendizaje de los alumnos son los correctos?
2. ¿La metodología utilizada en cada unidad es la más apropiada y es flexible a las necesidades del grupo?
3. ¿El tiempo que le estamos dedicando a cada unidad es el adecuado?

Evaluación externa

En cuanto a la evaluación externa, los alumnos evaluarán el proceso de enseñanza-

aprendizaje mediante un cuestionario en dos momentos: al final de la primera evaluación y al final del curso, evaluando los siguientes aspectos:

1. Práctica docente en las explicaciones teóricas.
2. Práctica docente durante los trabajos prácticos.
3. Contenidos teóricos de la asignatura.
4. Contenidos prácticos de la asignatura.
5. Organización de la asignatura.
6. Criterios de evaluación utilizados.
7. Materiales.
8. Ambiente de Centro.

8. Actividades complementarias y extraescolares

Objetivos Generales

- Conocer un entorno real de trabajo donde se utilicen los sistemas informáticos como herramienta de producción y se vea las diferencias en el modo de trabajar de distintas instituciones o empresas.
- Conocer el hardware de los ordenadores que se utilizan en los distintos centros de trabajo visitados.
- Estudiar el software (sistemas operativos, lenguajes de programación, ...) que se utilizan en la actualidad en entornos de trabajo reales, y estudiar las diferencias con el software estudiado en clase.
- Conocer la figura del administrador de sistemas informáticos en un entorno de trabajo real.
- Hacer un estudio de las tecnologías de comunicación empleada en la actualidad en grandes sistemas informáticos.
- Completar la formación de los alumnos y hacerles ver la realidad y la estrecha conexión entre lo estudiado en el aula y su aplicación en el mundo laboral.
- Fomentar el trabajo en equipo, buscando la integración de funciones y actividades desarrolladas por diferentes alumnos de forma coordinada, así como la consecución de objetivos comunes y la gestión del tiempo desarrollando valores como la comunicación, la confianza y el compromiso y anteponiendo los intereses del grupo a los personales.
- Fomentar el desarrollo de habilidades sociales, especialmente el establecimiento de relaciones interpersonales, eliminando las barreras comunicacionales.
- Fomentar valores relacionados con la convivencia, como la tolerancia, la empatía, el respeto y la confianza, necesarios en la vida en sociedad en general y en la vida laboral en particular.

Relación de actividades complementarias y extraescolares programadas