PROGRAMACIÓN DIDÁCTICA
SEGURIDAD INFORMÁTICA
2º SISTEMAS MICROINFORMÁTICOS Y REDES

Ciudad
Educativa
Municipal
FUHEM
Hipatia

INDICACIONES DE FORMATO

PORTADA: Como se muestra en el modelo y con encabezado marcada la opción de primera página diferente para que no se muestre ni el año ni el logotipo en la portada.

EPÍGRAFES: Letra "Titillium Web", tamaño 12, justificado a la derecha y subrayado con línea de tabla abajo.

PÁRRAFO: Letra "Titillium Web", tamaño 10, interlineado sencillo, justificado, párrafo anterior 12 ptos.

Introducción

Esta programación se corresponde con el módulo denominado: "Seguridad Informática" que se encuadra en el segundo curso del ciclo formativo de grado medio correspondiente al título de Técnico en Sistemas microinformáticos y redes.

Los objetivos generales (o capacidades terminales) de este módulo profesional que el alumno debe alcanzar/demostrar son consecuencia del desglose de la competencia general y de las capacidades profesionales que se debe adquirir a lo largo del proceso de enseñanza-aprendizaje del ciclo formativo de "Sistemas microinformáticos y redes", así como al dominio profesional propio de la unidad de competencia a la que está ligado, es decir, "Sistemas de comunicaciones y redes", tal como establece el Real Decreto 1691/2007, de 14 de diciembre, que estable el título de Técnico/a en "Sistemas Microinformáticos y Redes" y sus correspondientes enseñanzas comunes.

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.

Este profesional ejerce su actividad principalmente en empresas del sector servicios que se dediquen a la comercialización, montaje y reparación de equipos, redes y servicios microinformáticos en general, como parte del soporte informático de la organización o en entidades de cualquier tamaño y sector productivo que utilizan sistemas microinformáticos y redes de datos para su gestión.

Entorno profesional

Este profesional ejerce su actividad principalmente en empresas del sector servicios que se dediquen a la comercialización, montaje y reparación de equipos, redes y servicios microinformáticos en general, como parte del soporte informático de la organización o en entidades de cualquier tamaño y sector productivo que utilizan sistemas microinformáticos y redes de datos para su gestión.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

- Técnico instalador-reparador de equipos informáticos.
- Técnico de soporte informático.
- Técnico de redes de datos.
- Reparador de periféricos de sistemas microinformáticos.
- Comercial de microinformática.
- Operador de tele-asistencia.
- Operador de sistemas.

Objetivos de área

Los objetivos del área son los que marca el Real Decreto 1691/2007 de 14 de diciembre en su Anexo I, apartado "Módulo profesional: Seguridad Informática". Se corresponden con los objetivos marcados como a), c), d), e), g), k) y l) en el art. 9 del citado RD.

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) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
c) 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.
d) 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.
e) Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
f) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
g) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.

Contribución al desarrollo de las competencias profesionales

Los contenidos son los que marca el Decreto 34/2009, de 2 de abril, del Consejo de Gobierno, por el que se establece para la Comunidad de Madrid el currículo de ciclo formativo de grado medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes, publicado en el BOCM núm. 92 de lunes 20 de abril de 2009. Estos contenidos se detallan en el Anexo I, apartado "Módulo profesional 5: Seguridad Informática (Código 0226)".

Organización y secuenciación de contenidos

UNIDAD 1. Conceptos básicos de seguridad informática

CONTENIDOS

- 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

UNIDAD 2. Seguridad pasiva. Hardware y almacenamiento

CONTENIDOS

- 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
- NAS (Network Attached Storage)
- SAN (Storage Area Network)

UNIDAD 2. Seguridad pasiva. Hardware y almacenamiento

CONTENIDOS

- 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
- NAS (Network Attached Storage)
- SAN (Storage Area Network)

UNIDAD 3. Seguridad pasiva. Recuperación de datos

- 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

UNIDAD 4. Sistemas de identificación. Criptografía

- 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

- Software que vulnera la seguridad del sistema
  - Clasificación de atacantes
  - Tipos de ataques (sniffing, DoS, virus, etcétera)
  - Software malicioso (malware)
  - Técnicas usadas para el fraude y robo (ingeniería social, phising, spoofing, etcétera)
  - Impactos
  - Educación y formación del usuario. Consejos prácticos. Copias de seguridad e imágenes de respaldo.

UNIDAD 5. Seguridad activa en el sistema

- 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.

UNIDAD 6. Seguridad activa en redes

- 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 Si-Fi
  - Seguridad en los protocolos para comunicaciones inalámbricas
  - Tipos de ataques
  - Mecanismos de seguridad

UNIDAD 7. Seguridad de alto nivel en redes: cortafuegos

- 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.

UNIDAD 8. Seguridad de alto nivel en redes: proxy

- 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

Temporalización

TEMPORALIZACIÓN	UNIDAD DIDÁCTICA
1ª EVALUACIÓN	UT 1. Conceptos básicos de la seguridad informática
	UT 2. Seguridad pasiva. Hardware y almacenamiento
	UT 3. Seguridad pasiva. Recuperación de datos
	UT 4. Sistemas de identificación. Criptografía
2ª EVALUACIÓN	UT 5. Seguridad activa en el sistema

	UT 6. Seguridad activa en redes
	UT 7. Seguridad de alto nivel en redes: cortafuegos
	UT 8. Seguridad de alto nivel en redes: proxy

Metodología y estrategias didácticas

La metodología del proceso de enseñanza/aprendizaje del Módulo "Seguridad Informática" está condicionada por las necesidades de formación que requiere el mundo productivo, es decir, es activa y práctica, adecuada en cada momento, tal como se observa en las actividades diseñadas, a la formación necesaria para los posibles cambios que puedan producirse en su entorno productivo. Por lo que, en cuanto a la metodología didáctica cabe decir que es importante que el alumno se considere como la parte activa más importante en su acción formativa.

La forma de actuar vendrá encabezada con una presentación teórico-práctica, pasando a continuación a la realización de los ejercicios necesarios para la asimilación de los contenidos. Estos ejercicios deberán reforzar los contenidos expuestos y deberán invitar al alumno a explorar y buscar soluciones por él mismo.

Las prácticas se realizarán individualmente, por parejas, utilizando en todo momento el trabajo cooperativo.

Creemos que un aspecto básico en la formación del alumno/a es desarrollar capacidades, habilidades y destrezas que le permitan ser capaz de resolver autónomamente los problemas que el proceso de aprendizaje se le puedan presentar, contando siempre con la ayuda y colaboración del profesor/a.

En todas las unidades se realizarán prácticas más sencillas con los contenidos de cada unidad.

Dado que educamos a alumnos que vienen de una formación general, consideramos fundamental conectar tantas veces como sea posible los conceptos explicados en el libro con situaciones prácticas y cercanas a la realidad laboral. Por este motivo, las actividades propuestas en las unidades se han basado en tareas que se realizan habitualmente en el mundo profesional.

Puesto que en el aula encontramos una gran diversidad de alumnado, este libro pretende facilitar la labor docente incluyendo en el material complementario para el profesor actividades de refuerzo, para los alumnos que tengan más dificultad en adquirir las competencias, y actividades de ampliación, para aquellos que completen el proceso de aprendizaje antes de lo planificado.

Las unidades del libro incluyen muchos casos prácticos ya resueltos, para que los alumnos avancen por sí mismos en su propio proceso de aprendizaje.

ACTIVIDADES, PROFUNDIZACIONES Y REFUERZOS

Se realizarán una serie de refuerzos educativos para los alumnos que presenten unas mayores dificultades de aprendizaje. Estos refuerzos serán obligatorios en algunos casos, designados por el profesor, y voluntarios para cualquier otro alumno. Para no fomentar diferencias entre los alumnos, el profesor hablará de forma particular con cada alumno al que se le darán los refuerzos educativos de forma obligatoria. Estos refuerzos educativos se darán, cuando el profesor lo estime oportuno.

Estas clases de refuerzo servirán también para contactar más con los alumnos, y así poder ayudar ante cualquier problema que puedan tener.

No obstante, lo primero que se hará será contar con el Departamento de Orientación. Son ellos los más expertos en estas situaciones y supondrán siempre, una de las mejores referencias a tener.

Criterios de evaluación. Procedimientos e instrumentos

Los criterios de evaluación son los que marca el Real Decreto 1691/2007 de 14 de diciembre en su Anexo I, apartado "Módulo profesional: Seguridad Informática". En él se indican los siguientes resultados de aprendizaje y criterios de evaluación:

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

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. 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.

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

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.

3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

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.

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico.

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.

5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

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.

Criterios de clasificación y de promoción.

La evaluación se adecuará a los criterios de evaluación establecidos en el Real Decreto 1691/2007 de 14 de diciembre, con el fin de comprobar si el alumno ha adquirido los objetivos de cada módulo.

Si durante un periodo de evaluación (trimestre) un alumno acumula en una asignatura un número de faltas sin justificar mayor que el número de horas que semanalmente se cursa en esa asignatura más una, perderá el derecho

a ser evaluado, debiendo presentarse directamente a la prueba de recuperación. En el boletín de notas figurará como "No calificado por faltas de asistencia".

Por la orden 2323/2003, de 30 de abril, por la que se regula la matriculación, si un alumno acumula un número de faltas de asistencia no justificadas equivalentes al 15% de las horas de formación que correspondan al total de los módulos en que el alumno este matriculado, se podrá anular la matrícula por inasistencia. Asimismo, será causa de baja de matrícula la inasistencia no justificada del alumno a las actividades de todos los módulos en que esté matriculado por un periodo de 15 días lectivos consecutivos.

Los procedimientos de evaluación considerados para evaluar y calificar al alumno son los siguientes:

- Examen práctico y/o teórico.
- Practicas individuales o grupales.
- Ejercicios prácticos en clase y/o casa.

La calificación asignada a cada uno de los procedimientos considerados será:

- Prueba escrita y/o teórica: aporta el 50% de la calificación.
- Prácticas y ejercicios realizados en clase: aportan el 40% de la calificación.
- Actitud (respeto a los compañeros, cuidado de material, respeto al docente, cumplimiento de las tareas diarias propuestas, comportamiento en el aula, puntualidad…): aporta el restante 10% de la calificación.

El docente dará a conocer a los alumnos al comienzo de cada evaluación los criterios y los procedimientos de evaluación del módulo, explicando qué criterios serán tenidos en cuenta a la hora de evaluar cada práctica y cómo afectará esto a su nota.

Para poder aplicar los porcentajes, el examen de evaluación debe tener una puntuación por encima de 4 puntos sobre 10.

Cuando un estudiante intente aprobar la asignatura usando medios fraudulentos (copiar, entregar trabajos copiados, usar dispositivos digitales para acceder a información externa, entre otros) con la intención de aprobar la asignatura, módulo, materia o ámbito, en lugar de demostrando sus propios conocimientos, la prueba quedará automáticamente anulada con la calificación de 0

Medidas de recuperación y promoción:

Posteriormente a la celebración de la sesión de evaluación, el docente entregará individualmente las actividades, el examen y proyecto/s corregidos indicando los errores cometidos, los mínimos exigibles no superados y los aspectos a corregir para la recuperación, en el caso de necesitarla.

Se corregirá en clase el examen de la evaluación. Antes de la prueba de recuperación, se hará un seguimiento personalizado de la evolución y el trabajo realizado por el alumno que tenga que realizarla, para poder corregir de manera más eficaz sus fallos.

Si el alumno suspendiera alguna evaluación deberá realizar una prueba de recuperación en la siguiente evaluación, excepto en la tercera, que será en la convocatoria final de junio. Esta prueba de recuperación estará compuesta por una prueba escrita y/o teórica dependiendo de la parte suspensa. Se incluirá en el examen preguntas relacionadas directamente con los trabajos, ejercicios y/o prácticas que se hayan realizado en la evaluación.

Los exámenes de recuperación de evaluación se calificarán de 0 a 10 no pudiendo tener una nota superior a 7.

Si algún alumno suspendiera alguna recuperación tendrá otra oportunidad en la convocatoria de junio, en la que se podrá examinar de las evaluaciones suspensas, debiendo realizar las pruebas que en cada evaluación se han detallado.

La calificación final será la media aritmética de las notas obtenidas en cada evaluación. En la nota final se tendrá en cuenta positivamente la entrega de trabajos, practicas durante el curso. Tanto esta calificación final como la de las evaluaciones serán numéricas, de 1 a 10 puntos, sin decimales. Si al alumno se le comunicara la de evaluación con decimales será sólo a efectos informativos, sirviendo para obtener con mayor precisión la calificación final de curso.

Los alumnos que deseen presentarse a subir nota deben hacerlo en la convocatoria ordinaria de Junio, teniendo en cuenta los siguientes puntos:

- Sólo podrán hacerlo si han superado todas las evaluaciones.
- La repetición de la prueba escrita de evaluación implica una nueva evaluación, lo que supone una subida o bajada de nota. Por ello se les concederá un tiempo de cortesía en el cual decidirán si realmente quieren seguir con la prueba o no.
- Pudiendo subir hasta dos puntos y bajar máximo un punto.
- Un alumno que tenga aprobada la materia y se presente a subir nota nunca podrá suspender.
- El docente del módulo debe conocer con antelación el deseo del alumno de presentarse a esta prueba.

Los alumnos con la asignatura suspensa en la convocatoria de junio tendrán que examinarse de todos los contenidos del curso en septiembre. Se les entregará orientaciones de trabajo desarrollados por el departamento (resúmenes, esquemas, ejercicios, practicas…), que les ayuden a preparar dicha prueba.

En la prueba de junio se tendrán en cuenta los contenidos mínimos indicados en el Real Decreto 1691/2007 de 14 de diciembre, que son los siguientes:

- 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. Orientaciones pedagógicas.

Recuperación de módulos pendientes durante cursos posteriores:

La asignatura pendiente de cursos anteriores se aprobará a través de exámenes que serán realizados en dos convocatorias excluyentes, es decir se examinarán de todo el temario antes de las vacaciones de Navidad y si no superasen esta convocatoria tendrán otra oportunidad el mes de febrero.

Se dará instrucciones al alumnado para que pueda entregar esquemas, ejercicios y prácticas programadas en diferentes momentos antes del examen para facilitar el aprendizaje de los contenidos y se tendrá en cuenta en la nota final (un 20%).

Por lo tanto, la nota será: un 80% la nota del examen y un 20% la entrega correcta y en fecha de los materiales pautados. Teniendo que obtener una media de 5 para superar el módulo.

Criterios de ortografía, acentuación y puntuación:

En todos los ejercicios se ponderará específicamente la capacidad expresiva y la corrección idiomática, y para ello se tendrá en cuenta:

a) La propiedad del vocabulario.
b) La corrección sintáctica.
c) La puntuación apropiada.
d) La adecuada presentación.
e) La corrección ortográfica.

La ortografía será calificada y podrá restar de la prueba escrita hasta 1,50 puntos de la calificación obtenida. Cada error de grafía y cada dos errores de tilde deducirán 0,25 puntos de la nota del ejercicio. Se conceden tres faltas de ortografía de crédito.

Recursos didácticos

Se emplea libro de texto.

Seguridad Informática + Cd. Editorial Mc-Graw Hill. Alfredo Abad Domingo.
Se utilizarán de apoyo otros manuales cómo:

- Seguridad Informática (ciclo formativo de grado medio) editorial Editex. Purificación Aguilera
- Seguridad Informática. Editorial Ra-Ma Costa Santos, Jesús.

Durante las prácticas y controles que se desarrollan a lo largo del curso, los alumnos van creando material relacionado con cada tema. Las correcciones que se efectúan, tanto de modo individual como colectivo, permiten ajustar dicho material a lo pedido, de modo que al acabar cada tema poseen bastantes documentos y ejemplos resueltos.

La asignatura se imparte en tres aulas:

- Aula informática, donde los alumnos tienen a su disposición un ordenador de sobremesa para cada uno con los sistemas operativos Windows 7 y Ubuntu 12.04 instalados. Estos ordenadores están conectado en red con acceso a internet, y tienen instalado todo el software necesario para cursar la asignatura.
- Aula de teoría, que cuenta con pizarra digital y diversos libros sobre distintos aspectos de la informática.
- Taller de prácticas, donde se disponen de varios ordenadores donde se realizarán actividades de clonación, configuración de Raids, instalación de programas para realizar copias de seguridad u otros que ayuden a mejorar el aprendizaje del alumno en los contenidos de la materia.

El Pendrive del alumno, es la herramienta donde los alumnos deben almacenar todos los apuntes entregados por el profesor así como las prácticas realizadas por los alumnos. Se valorará la organización de los archivos en carpetas siguiendo las especificaciones dadas por el profesor así como la concordancia entre lo almacenado y lo escrito en el cuaderno del alumno.
Existen múltiples herramientas que nos facilitan el aprendizaje del alumno:

- Paquete office.
- Programas específicos para la seguridad informática
- Trabajo en máquina virtual
- Analizador de tramas (Sniffer) para estudio de las tramas de comunicaciones.
- Internet

Atención a la diversidad

Se realizarán una serie de refuerzos educativos para el alumnado que presente unas mayores dificultades de aprendizaje. Estos refuerzos serán obligatorios en algunos casos, designados por el profesor, y voluntarios para cualquier otro alumno. Para no fomentar diferencias entre el alumnado, el profesor hablará de forma particular con cada alumno al que se le darán los refuerzos educativos de forma obligatoria.

Necesidades educativas especiales

Este alumnado deberá alcanzar los objetivos generales mínimos definidos por la ley. Para ello, se harán adaptaciones curriculares, para variar la temporalidad que el alumno pueda necesitar, así como, para contar con los materiales necesarios para ello.

Se trabajará en colaboración con el Departamento de Orientación, y se procurará la ayuda y asesoría de los padres del alumno.

Alumnado con altas capacidades

Ante la sospecha de la existencia de un alumno con altas capacidades, se avisará al Departamento de Orientación, para que proceda a la evaluación. Adicionalmente, si existe esta sospecha, será porque este alumno muestra rapidez fuera de lo normal para entender los conceptos explicados. En este sentido, se tendrán ejercicios de dificultad añadida pensados por si este alumno supera con rapidez los propuestos al resto de sus compañeros.

Contribución al Plan de fomento y desarrollo de la lectura

Dado el carácter práctico de los módulos y asignaturas que impartimos, pretendemos continuar promoviendo en todos los módulos y asignaturas la competencia lingüística (habilidades que permiten buscar, recopilar y procesar información y ser competente a la hora de comprender, componer y usar textos diferentes con intenciones comunicativas diversas).

En algunas asignaturas de bachillerato y de la ESO y en los grupos de FP del departamento se podrá recomendará un libro a lo largo del curso relacionado con los contenidos impartidos para fomentar esta competencia, con el que se realizará un trabajo y puesta en común o coloquio.

Además, en los módulos de PCPI y el ciclo formativo de grado medio trabajaremos utilizando internet noticias relacionadas con los contenidos impartidos como la seguridad informática, sistemas operativos, nuevas herramientas web, evolución de los ordenadores, etc. para fomentar la lectura y la compresión lectora durante todo el año.

Contribución al Plan TIC

Como principal objetivo dentro del plan TIC pretendemos seguir utilizando los profesores del departamento la plataforma educativa Moodle, iniciado en cursos anteriores, como herramienta imprescindible en el desarrollo de los contenidos y la metodología de nuestras asignaturas y módulos. Además haremos:

- Uso de la informática y de Internet como herramientas propias de la materia y que son necesarias para la consecución de los objetivos de esta materia.
- Uso de programas de tratamiento de textos.
- Uso de programas de hojas de calculo
- Uso de programas de presentación de proyectos
- Uso de todo tipo de recursos multimedia.
- Uso de programas específicos de las asignaturas o módulos del curso (simuladores de electrónica y electricidad, simuladores de red, creación de planos de red, gestión de recursos, retoque fotográfico, servidores,)
- Uso de software libre cómo el paquete “OpenOffice”.
- Creación y uso de Blogs y gestores de contenido.
- Uso de pizarra digital (PDI) como herramienta imprescindible de trabajo en el aula.
- Uso responsable del móvil como herramienta de trabajo para algunas prácticas en los módulos de formación profesional.

Actividades complementarias y extraescolares

Durante todo el curso realizaremos actividades entre todos los componentes del departamento llevando a cabo un proyecto en común que integren los contenidos impartidos en el departamento y relacionado directamente con el proyecto de centro de este año, "El cine".

Las actividades que proponemos este curso son:

CFGM - Sistemas microinformáticos y redes y PCPI sistemas microinformáticos

- Participar en alguna actividad programada dentro de la Semana de la ciencia - 1º , 2º CFGM y PCPI (1r trimestre)
- Visita al CPD del Instituto Geográfica Nacional. 2º SMR (1r trimestre)
- Realizar alguna visita de las programadas en Ifema - 1º y 2º CFGM (2º trimestre)
- Participar a lo largo del año en unas Jornadas software de libre - 1º y 2º CFGM y PCPI. (3er trimestre)

Cualquier otra actividad que se programe dentro del curso académico.

Procedimientos de evaluación y revisión de los procesos y los resultados de las programaciones didácticas

Para evaluar y revisar los procesos y los resultados de las programaciones se realizará al finalizar cada trimestre unos cuestionarios a los alumnos y al finalizar el curso un cuestionario a los profesores por asignaturas o modulo, que se utilizaran después para la realización de la memoria y para las posibles modificaciones del próximo curso.

Estos cuestionarios son los que a continuación se añaden en los dos anexos: ANEXO 1. ALUMNOS, ANEXOS 2 PROFESORES.

ANEXO 1

Cuestionario de evaluación del alumno

ASIGNATURA/MÓDULO: _____

Indica con valores de 1 (muy negativo) a 5 (muy positivo) el siguiente cuestionario. Asimismo en las preguntas más concretas toda tu aportación ayuda a mejorar la formación impartida.

1. ¿En qué grado te han resultado interesantes los contenidos desarrollados? ¿Cuáles?
2. ¿En qué grado te han resultado difíciles los contenidos desarrollados? ¿Cuáles?
3. ¿Los contenidos han seguido un orden que ha facilitado su comprensión?
4. ¿Cómo valoras la distribución de contenidos teóricos y los prácticos?

METODOLOGÍA

5. ¿Las actividades desarrolladas han favorecido la aplicación práctica de los conocimientos impartidos?
6. Valora en cada caso del 1 (muy negativo) al 5 (muy positivo) y si quieres añadir algo más hazlo debajo de la tabla:

PRACTICA/TRABAJO/ EJERCICIOS/...	**Me ha gustado**	**He aprendido**	**Grado de dificultad**	**Tiempo utilizado en clase para realizarlo**	**…..**

7. ¿Has tenido oportunidad de hacer preguntas para aclarar dudas?
8. ¿Cómo valoras los trabajos en grupo realizados? Explica con detalle.

PROFESOR

9. ¿Ha explicado con claridad y con el suficiente grado de detalle con el fin de facilitar la comprensión del tema?
10. ¿Ha motivado interés por el aprendizaje?
11. ¿Su nivel de conocimientos ha sido adecuado?
12. ¿Se ha preocupado por comprobar que se entendían los contenidos impartidos?

13. ¿Ha proporcionado soluciones ágiles y eficaces ante imprevistos?

RECURSOS MATERIALES

14. La documentación facilitada ha sido útil (libro de texto, apuntes, documentos fotocopiados, documentos mandados por email,…)

15. El aula reunía las condiciones necesarias.

16. Los recursos necesarios para la realización de la asignatura/ módulo han estado disponibles en el momento oportuno

EVALUACIÓN

17. ¿La forma de evaluar el aprendizaje adquirido te ha parecido correcta?

TEMPORALIZACIÓN

18. ¿Cómo valoras el número de horas impartidas en cada unidad o tema, practicas, trabajos,…? Pocas, Suficiente, Demasiadas

ACTIVIDADES EXTRAESCOLARES

19. Valora el grado de satisfacción de las actividades extraescolares realizadas en la asignatura o módulo

SATISFACIÓN

20. ¿Crees que se han alcanzado los objetivos del curso, es decir si crees que has aprendido?

21. ¿Crees que aplicarás a tu vida profesional la formación impartida?

22. ¿Crees que has aprovechado el curso para aprender lo máximo?

COMENTARIOS FINALES

23. Señala los aspectos más positivos de la asignatura o módulo

24. Señala los aspectos que deberían mejorarse de la asignatura o módulo

25. Si quieres comentar algo que esté recogido en el cuestionario….

ANEXO 2

Cuestionario de evaluación del profesor

ASIGNATURA/MÓDULO: _____

1. ¿Has cumplido con los temas o unidades propuestas en la programación de la asignatura?:

   SI

   Temas o unidades de la programación trabajados en clase:

   NO

   Temas o unidades de la programación no trabajados en clase:

3. ¿Has trabajado temas que no están en la programación? ¿en qué momentos? ¿por qué?

4. Has seguido con el contenido de tus programaciones en su totalidad
   - SI
   - NO

4. Cambios que has realizado respecto a la programación durante el curso.
   1. Contenidos
   2. Temporalización
   3. Metodología
   4. Criterios evaluación
   5. Criterios de calificación
   6. Recursos didácticos

4. Actividades extraescolares:
   - Cuales se ha realizado
   - Cuales no se han realizado
   - Valorar la temporalización
   - Valoración contenido

4. Escribe las estadísticas obtenidas la asignatura/módulo:

Nº TOTAL ALUMNOS	**% APROBADOS**	**% SUSPENSOS**

Nº TOTAL ALUMNOS	**10 - 9**	**8-7**	**6-5**	**4-3**	**2-1-0**

4. Cambios que harías en la programación para el curso próximo.

1. Contenidos
2. Temporalización
3. Metodología
4. Criterios evaluación
5. Criterios de calificación
6. Recursos didácticos
7. Actividades extraescolares