IES PADRE POVEDA

DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo:

SEGURIDAD INFORMÁTICA

Familia profesional:

INFORMÁTICA

Ciclo Formativo de Grado MEDIO:

SISTEMAS MICROINFORMÁTICOS Y REDES

Profesor: Emilio Vílchez Rubia

Curso: 2021/22

ÍNDICE

I. ORGANIZACIÓN DE LA MATERIA. ACUERDOS Y CRITERIOS DEL DEPARTAMENTO.

La materia es impartida a un grupo de unos 17 alumnos.

Carga lectiva: La asignatura se imparte a lo largo de los dos primeros trimestres y tiene una carga lectiva de cinco horas semanales.

Se han tenido en cuenta los resultados de la evaluación inicial para concretar diferentes aspectos de la programación, básicamente la metodología y la atención a la diversidad

1. Objetivos

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) Elaborar presupuestos de sistemas a medida cumpliendo los requerimientos del cliente.

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. Unidades didácticas, resultados de aprendizaje y criterios de evaluación

En la siguiente tabla se recogen los contenidos del módulo dividido en las unidades didácticas en las que se han organizado. Junto a dichos contenidos aparecen los resultados de aprendizaje y criterios de evaluación para cada unidad.

Unidades Didácticas	Contenidos	Resultados de Aprendizaje	Criterios de Evaluación
UNIDAD 1: Conceptos sobre seguridad informática	➢ Visión global d ➢ Planificación de la seguridad ➢ Servicios y mecanismos de seguridad ➢ Seguridad física vs. Seguridad lógica. ➢ Legislación sobre protección de datos. ➢ Legislación sobre los servicios de la sociedad de la información y correo electrónico.	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico. R5: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	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 han esquematizado las características de una política de seguridad basada en listas de control de acceso. f) Se ha valorado la importancia de establecer una política de contraseñas. g) Se han valorado las ventajas que supone la utilización de sistemas biométricos. h) Se ha descrito la legislación sobre protección de datos de carácter personal. i) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. j) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. k) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen. l) Se ha descrito la legislación actual sobre los servicios sociedad de la información y comercio electrónico..

			m) Se han contrastado las normas sobre gestión de seguridad de la información.
UNIDAD 2: Seguridad pasiva: equipos	➢ Seguridad activa vs. Seguridad pasiva. ➢ Ubicación y protección física de los equipos y servidores. ➢ Sistemas de alimentación interrumpida (SAI)	R1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades R2: .Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integración de la información	a) Se ha valorado la importancia de mantener la información segura. b) Se han descrito las diferencias entre seguridad activa y pasiva. 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.
UNIDAD 3: Seguridad pasiva: Almacenamiento	➢ Almacenamiento de la Información: rendimiento, disponibilidad, accesibilidad. ➢ Almacenamiento redundante y distribuido. ➢ Clústers: ➢ Tipos de copias de seguridad ➢ Imágenes de respaldo ➢ Criptografía. Copias de seguridad encriptadas. ➢ Compresión en copias de	R1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades R2: .Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integración de la	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 y accesibilidad, entreotros) 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.

	seguridad. ➢ Políticas de copias de seguridad ➢ Software de copias de seguridad. ➢ Configuración de copias de seguridad en sistemas libres y propietarios. ➢ Medios de almacenamiento en copias de seguridad. ➢ NAS (Network AttachedStorage) ➢ SAN (Storage AreaNetwork).	información	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
UNIDAD 4: Criptografía	➢ Métodos para asegurar la privacidad de la información transmitida. ➢ Criptoanálisis y criptografía. ➢ Criptografía clásica. ➢ Criptografía moderna. ➢ Sistemas de identificación: firma electrónica, certificados digitales y otros.	R3: Aplica mecanismos de seguridad a características R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades específico	a) Se han descrito sistemas de identificación como la firma electrónica y el certificado digital, entre otros. b) Se han utilizado sistemas de identificación como la firma electrónica y el certificado digital, entre otros.
UNIDAD 5: Seguridad activa: sistema operativo y aplicaciones	➢ Seguridad del sistema ➢ Seguridad de red (accesos en red y seguridad perimetral) ➢ Cortafuegos en equipos y servidores ➢ Proxys ➢ Servidores proxy ➢ Listas de control de acceso(ACLs). ➢ Recuperación de datos. ➢ Seguridad en la conexión a Internet.	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático. R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	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

UNIDAD 6: Seguridad activa: acceso a redes	➢ Métodos para asegurar la privacidad de la información transmitida. ➢ Introducción a protocolos seguros. ➢ Control de la monitorización en redes cableadas. ➢ Seguridad en redes inalámbricas	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático. R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red. b) Se han aplicado medidas para evitar la monitorización de redes cableadas. c) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas. d) Se han descrito sistemas de identificación como la firma electrónica y el certificado digital, entreotros. e) Se han utilizado sistemas de identificación como la firma electrónica y el certificado digital, entre otros.
UNIDAD 7: Seguridad activa: control de **redes**	➢ Métodos para asegurar la privacidad de la información transmitida. ➢ Introducción a protocolos seguros. ➢ Control de la monitorización en redes. ➢ Seguridad de red(accesos en red y seguridad perimetral) ➢ Cortafuegos en equipos y servidores ➢ Proxys ➢ Servidores proxy en ➢ Servidores antispam.	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático. R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red. b) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado. c) Se han aplicado medidas para evitar la monitorización de redes cableadas. d) Se ha instalado y configurado un cortafuegos en un equipoo servidor.
UNIDAD 8: Ataques y contramedidas	➢ Métodos para asegurar la privacidad de la información transmitida. ➢ Introducción a protocolos seguros. ➢ Control de la monitorización en redes cableadas. ➢ Seguridad en redes inalámbricas.	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	a) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso. b) Se han aplicado medidas para evitar la monitorización de redes cableadas. c) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas. d) Se ha instalado y configurado un cortafuegos en un equipo servidor.

3. Duración del módulo

Este módulo profesional tiene una duración de 105 horas lectivas distribuidas en 5 horas semanales, durante dos trimestres.

4. Contenidos básicos

Aplicación de medidas de seguridad pasiva:

– Seguridad informática. Clasificación, técnicas y prácticas de tratamiento seguro de la información.

– 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.

– Política de almacenamiento.

– Recuperación de datos.

Aplicación de mecanismos de seguridad activa:

– Identificación digital.

– Sistemas biométricos de identificación.

– 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, protección y desinfección.

– Auditorias de seguridad.

– Actualización de sistemas y aplicaciones.

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.

– Publicidad y correo no deseado.

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.

5. Orientaciones pedagógicas

Este módulo profesional contiene la formación necesaria para desempeñar la función de implantación de medidas de seguridad en sistemas informáticos.

La definición de esta función incluye aspectos como:

- La instalación de equipos y servidores en entornos seguros.

- La incorporación de procedimientos de seguridad en el tratamiento de la información.

- La actualización de los sistemas operativos y el software de aplicación instalado.

- La protección frente a software malicioso.

- La aplicación de la legislación y normativa sobre seguridad y protección de la información.

6. Competencias profesionales, personales y sociales que se adquieren:

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.

7. Líneas de actuación en el proceso de enseñanza-aprendizaje

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo están relacionadas con:

– La protección de equipos y redes informáticas.

– La protección de la información transmitida y almacenada.

– La legislación y normativa vigente en materia de seguridad.

8. Contenidos de carácter transversal.

En nuestro tiempo se dan unas expectativas y demandas de la sociedad, hay una serie de cuestiones que los hombres y mujeres deben estar preparados para abordarlas adecuadamente. La sociedad está clamando por la **paz**, por la **igualdad de derecho y oportunidades entre hombres y mujeres**, por un **respeto al medio ambiente**, por **vivir de una manera más saludable**, por un **desarrollo de la afectividad y de la sexualidad** que permita desarrollar las relaciones interpersonales; una sociedad que necesita forjar personalidades autónomas y cívicas, capaces de respetar la opinión de los demás y, a la vez, defender sus derechos, etc…

Para dar respuesta a esta necesidad de la sociedad actual se tratan, en el marco escolar, los **Temas Transversales**. Hay que considerar, consecuentemente, estos temas como algo necesario para vivir en una sociedad como la nuestra; de ahí la especial relevancia e importancia de estos temas no sólo para el desarrollo personal y la **formación integral de los alumnos**, sino para un proyecto de sociedad más libre y respetuosa, y eso ha de hacerse desde los centros educativos.

Los ejes transversales son grandes temas que engloban múltiples contenidos y difícilmente pueden adscribirse a un Módulo específico, sino que se considera que deben impregnar toda la acción educativa, es decir, **deben estar presentes en todas los Módulos del Ciclo Formativo** (de ahí su nombre de transversales).

Para conseguir que el alumno y la alumna los interiorice y sea capaz de hacerlos operativos en su conducta, extrapolándolos a cualquier situación que se le presente, es necesario desarrollar una serie de estrategias.

Las estrategias previstas para los contenidos de valor no se pueden limitar a aconsejar, recomendar o moralizar, sino que existen otras que parecen particularmente indicadas:

- La habituación por repetición de actos.
- La imitación, propuesta de modelos, el ambiente…
- La experimentación o práctica activa, consciente y libre.
- La confrontación: poner en situaciones que obliguen a reaccionar frente a un determinado valor.

Como ya se indicó anteriormente, **las enseñanzas transversales se deben trabajar entre todos los Módulos del Ciclo Formativo** y, por tanto, los contenidos referidos a estas enseñanzas transversales se deben distribuir entre los distintos Módulos; por eso, dependiendo de los

contenidos propios de este Módulo y de lo que se puede realizar desde el mismo, se le prestan especial atención a algunos de ellos.

A continuación se enuncian los objetivos propuestos para las diferentes enseñanzas del Ciclo Formativo:

- **Educación Moral y Cívica**: Realizar un tratamiento adecuado de la información sensible almacenada en una aplicación, respetando el derecho a la privacidad y a la intimidad de las personas, de acuerdo a lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personal. Trabajar en grupo aceptando las responsabilidades y compromiso que conlleva y respetando las iniciativas de los compañeros y compañeras.
- **Educación Ambiental**: Realizar un uso responsable y moderado de los materiales consumibles propios de la actividad informática, usar correctamente los contenedores de reciclado de papel, usar materiales "digitales" (PDFs, Plataformas Educativas, email, etc.…), ahorrar energía apagando los monitores en aquellos momentos en que no sea necesario el uso del ordenador.
- **Educación para la Salud**: Trabajar en condiciones de seguridad y salud, abordando aspectos de prevención de riesgos laborales como por ejemplo: adoptando una posición corporal correcta al sentarse, donde el ángulo correcto de las rodillas, y el de las piernas en relación con la espalda, así como el formado por los codos, debe ser de 90 grados, colocar la silla a una distancia adecuada, los ojos deben de estar a una distancia de 70-80 centímetros del monitor y quedar a la altura del borde superior de la pantalla, etc. El Real Decreto 488/97 establece las disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.
- **Educación para el consumo:** Mediante el análisis del software libre y de pago, atendiendo a sus ventajas e inconvenientes, se intentará crear una conciencia crítica ante el consumo.

Existen otra serie de temas transversales que en algunos casos serán abordados puntualmente en determinadas unidades didácticas: cultura andaluza, educación del consumidor y del usuario, educación para la igualdad de oportunidades de ambos sexos, educación para la paz, educación sexual, educación vial.

Las enseñanzas transversales van a impregnar el quehacer educativo a través de la

metodología utilizada, promoviendo las **actividades grupales**, pues ayudan a la interiorización y compresión de los comportamientos que rigen la vida de un grupo, las normas básicas que hacen que esa **convivencia** sea posible y también a apreciar la **importancia del trabajo cooperativo para lograr un fin común**.

9. Contenidos. Secuenciación por unidades didácticas.

PRIMER TRIMESTRE

UNIDAD 1: CONCEPTOS SOBRE SEGURIDAD INFORMÁTICA

¿Por qué proteger?

¿Qué proteger?

Definiciones

Tipos de ataques

Buenas prácticas

Legislación

UNIDAD 2. SEGURIDAD PASIVA: EQUIPOS

Ubicación del CPD

Centro de respaldo

SAI/UPS

UNIDAD 3: SEGURIDAD PASIVA: ALMACENAMIENTO

Estrategias de almacenamiento

Backup de datos

Imagen del sistema

UNIDAD 4: CRIPTOGRAFÍA

¿Por qué cifrar?

Criptografía

Criptografía simétrica y asimétrica

Cifrar y firmar

PHI. DNIe

SEGUNDO TRIMESTRE

UNIDAD 5: SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

Carrera de obstáculos

Autenticación en el sistema operativo

Cuotas

Actualizaciones y parches

Antivirus

Monitorización

Aplicaciones web

Cloud computing

UNIDAD 6: SEGURIDAD ACTIVA: ACCESO A REDES

Redes cableadas

Redes inalámbricas

VPN

Servicios de red. Nmap y ntstat

UNIDAD 7: SEGURIDAD ACTIVA: CONTROL DE REDES

Expiar nuestra red

Firewall

Proxy

Spam

UNIDAD 8: ATAQUES Y CONTRAMEDIDAS

Ataques TCP/IP. MITM

Ataques wifi. Aircrack-ng

Ataques web. WebGoat

Ataques proxy. Ultrasurf

10. Metodología

10.1. Actividades del profesor en el aula

La metodología general que se llevará a lo largo del curso se basará en los siguientes aspectos:

- **Exposición:** Presentar la información de manera verbal, instrumental o audiovisual.
- **Mostración:** Se muestra una habilidad o se ejecuta una tarea de manera práctica, como modelo para que el alumno la reproduzca posteriormente. Siempre el aprendizaje será mejor cuando el alumno primero ve lo que tiene que hacer y después lo realiza él de forma autónoma. Hay que tener cuidado con esto ya que el alumno se puede acostumbrar a tener siempre un guía que le muestre lo que tiene que hacer, y en este Módulo, uno de los principales objetivos es fomentar la autonomía en el trabajo de los alumnos.
- **Orientación:** Se dan pautas, instrucciones, pistas, vías, guiones, información escrita, etc., para que el alumno realice una tarea o para que utilice fuentes de información. De esta forma se fomentará la autonomía del alumno en la realización del trabajo y el trabajo en grupo, dependiendo de la situación propuesta.
- **Supervisión:** El profesor corrige, mientras el alumno realiza una tarea para garantizar el éxito del trabajo.

La impartición de la asignatura se fundamentará en los siguientes aspectos:

- Hacer un breve resumen de los conceptos que se van a tratar en las tareas a realizar.
- Dar una guía al alumnado en la que se presenta una descripción de los pasos a seguir con el ordenador para la actividad propuesta.
- Comprobar que los alumnos y alumnas son capaces de llevar a cabo la tarea planteada, ayudando a aquellos que muestren dificultad, y detectando aquellos otros que son capaces de hacerlas por sí mismos. Por tanto, se llevara a cabo una comprobación diaria y personal de las actividades prácticas a realizar.

- Para la explicación de cada Unidad de Trabajo, se realizará una exposición teórica de los contenidos de la misma por parte del profesor.
- Posteriormente, se realizarán una serie de ejercicios propuestos por el profesor y resueltos y corregidos por él en clase. El objetivo de estos ejercicios, es llevar a la práctica los conceptos teóricos que se asimilaron en la exposición anterior.
- El profesor resolverá todas las dudas que puedan tener los alumnos del ciclo, tanto teóricos como prácticos. Incluso si él lo considerase necesario se realizarán ejercicios específicos que aclaren los conceptos que más cueste comprender al alumnado.
- El profesor propondrá una serie de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser realizados por los alumnos, bien en horas de clase o bien en casa.
- Algunos ejercicios prácticos, se realizarán en el aula de ordenadores, utilizando el entorno correspondiente a la Unidad Didáctica en la que estemos trabajando. Las prácticas se resolverán de forma individual o en grupo, depende del número de alumnos que haya por cada ordenador, de todas formas no es aconsejable que haya más de dos alumnos por cada equipo informático.
- Además se podrá proponer algún trabajo que englobe conocimientos de varias unidades didácticas para comprobar que los conocimientos mínimos exigidos en cada una de las unidades han sido satisfactoriamente asimilados. Sería recomendable un trabajo por cada evaluación.

Sería conveniente utilizar la Web del centro, en la sección del departamento de informática, para facilitar al alumnado el material que se va dando en clase (apuntes, practicas, páginas Web relacionadas con el modulo,…) con el fin de evitar el excesivo uso de fotocopias y facilitar que el alumnado almacene el material en formato digital.

10.2. Actividades habituales de los alumnos/as

– Se realizarán en clase/casa una serie de ejercicios teórico-prácticos por cada unidad de acuerdo al contenido que se especifica en cada una de ellas en el apartado anterior.

– El alumnado realizará pequeñas exposiciones ante sus compañeros y compañeras que versarán sobre resolución de ejercicios propuestos en la unidad, trabajos voluntarios propuestos por el profesor relacionados con los contenidos de las unidades y trabajos libres

propuestos por el alumnado relacionados con los contenidos de las unidades.

10.3. Materiales didácticos

Materiales

- Un PC por persona con Windows y un software de Virtualización como podría ser VMWAre, VirtualPC o VirtualBOX. Preferentemente VirtualBOX al ser software libre.
- Un Router o Switch en el aula para conectar todos los PC en red.
- Sistemas operativos servidores: Windows 2003/2008 Server, Linux Ubuntu Server.
- También serán positivos todos aquellos instrumentos que faciliten la tarea de exposición del profesor, por ejemplo, cañones de exposición, televisión, video, etc.

Bibliografía

Para apoyar el proceso de enseñanza-aprendizaje se propone usar alguna de las referencias citadas a continuación, aunque no serán imprescindibles, ya que el profesor elaborará los apuntes y materiales necesarios para el desarrollo del módulo, y serán suministrado al alumnado mediante fotocopias o cualquier otro método que se estime conveniente.

Se intentará tener en todo momento a disposición de los alumnos los siguientes libros para consulta:

– Seguridad informática. Edit. McGraw-Hill. (Libro recomendado)

– Diversos manuales y cursos sobre Seguridad informática.

– Plataforma virtual moodle centros habilitada por la Consejería de Educación de la Junta de Andalucía.

10.4. MEDIDAS DE ATENCIÓN A LA DIVERSIDAD

La ***atención a la diversidad*** debe ser entendida como el conjunto de actuaciones educativas dirigidas a dar respuesta a las diferentes capacidades, ritmos y estilos de aprendizaje, motivaciones e intereses, situaciones sociales, culturales, lingüísticas y de salud del alumnado. Estas medidas han de orientarse a alcanzar los objetivos y las competencias establecidas para bachillerato y se regirán por los principios de calidad, equidad e igualdad de oportunidades, normalización, integración e inclusión escolar, igualdad entre mujeres y hombres, no discriminación, flexibilidad, accesibilidad y diseño universal, y cooperación de la comunidad educativa.

Será necesario pues, la integración de medidas metodologías y componentes que permitan al profesorado abordar con garantías, la diversidad de sus aulas.

- La atención a las diferencias individuales en cuanto a motivaciones, intereses, capacidades y estilos de aprendizaje estará contemplada en la combinación de metodologías durante el desarrollo de las unidades didácticas; en la diversidad de agrupamientos y tareas propuestos; en la combinación de lenguajes y soportes; en la posibilidad de articular distintos itinerarios, etc., elementos todos ellos orientados a satisfacer las exigencias de aprendizaje de cada alumno y a permitir su mejor desarrollo individual.

Atención a la diversidad en la metodología. Desde el punto de vista metodológico, la atención a la diversidad implica que el profesor:

Detecte los conocimientos previos, para proporcionar ayuda cuando se observe una laguna anterior.

Procure que los contenidos nuevos enlacen con los anteriores, y sean los adecuados al nivel cognitivo.

Intente que la comprensión de cada contenido sea suficiente para que el alumno pueda hacer una mínima aplicación del mismo, y enlace con otros contenidos similares.

Insistir en los refuerzos positivos para mejorar la autoestima.

Atención a la diversidad en los materiales utilizados

Otros elementos, como los tutoriales paso a paso, los recursos en La Red relacionados con los contenidos tratados, actividades de refuerzo y profundización, trabajos voluntarios o las propuestas de trabajo en grupo contribuyen al objetivo de no dejar atrás a ningún alumno.

En el grupo no hay ningún alumno con NEE.

11. Procedimientos de evaluación y criterios de calificación

11.1. Estrategia de evaluación

La evaluación es una herramienta que permitirá comprobar el grado de consecución de los objetivos por parte del alumnado. Se lleva a cabo a lo largo del proceso de enseñanza-aprendizaje y en su conjunto debe servir para facilitar el proceso de aprendizaje y mejorar los resultados educativos.

Al comienzo del curso se realizará una evaluación inicial para lo cual se pasara un cuestionario con preguntas, con el fin de conocer los estudios y experiencias del alumnado, así como obligar a hacer un esfuerzo de auto evaluación sobre lo que éste cree que sabe y el nivel que cree poseer sobre los temas que deben ser objeto de aprendizaje durante el curso.

Se efectuarán dos evaluaciones correspondientes a los trimestres naturales del curso. La evaluación será independiente para cada una de las evaluaciones, siendo necesario superar los conocimientos mínimos exigibles de cada una de ellas para superar el módulo completo

Para poder superar los módulos del ciclo es obligatorio la asistencia diaria a clase, ahora bien, dicha obligatoriedad podría estudiarse de forma especial para aquellos alumnos en los que concurran circunstancias especiales como:

- Alumnos que hayan encontrado trabajo y quieran seguir realizando sus estudios.
- Alumnos que por necesidades familiares, o de transporte no puedan asistir con regularidad a todas sus clases.
- Cualquier otra circunstancia que el departamento estime oportuna siempre que sea lo suficientemente justificada.

Alumnos de asistencia regular. (Menos del 20 % de faltas)

Los trimestres serán evaluados mediante una serie de controles teórico y/o prácticos. Para superar dichos controles habrá que obtener una calificación igual o superior a cinco sobre diez en cada uno de ellos. La nota final de cada evaluación, así como la nota final de la convocatoria ordinaria se calculará según se establezca en la programación de cada módulo.

Los alumnos que no aprueben alguna evaluación deberán realizar un control de características similares a cada una de las partes no superadas en su momento. Para recuperar la

evaluación el alumno deberá superar cada una de las partes que la forman. La recuperación de dichas partes se hará en una sola convocatoria por evaluación.

Debido a que las materias dadas en cada trimestre son independientes, las evaluaciones aprobadas durante el curso se guardarán para la evaluación final ordinaria (evaluaciones completas, en ningún caso temas sueltos).

En caso de tener que examinarse en la convocatoria final extraordinaria, los alumnos, además de superar la prueba escrita, deberán presentar y superar aquellas prácticas obligatorias que debieran haber superado durante el desarrollo del curso y que aún no las tengan entregadas y superadas. La nota final será la nota obtenida en la prueba extraordinaria siempre y cuando se hayan entregado y superado las prácticas obligatorias.

Para que el alumno pueda realizar un perfecto seguimiento del módulo, no deberá faltar a clase, se comportará correctamente y participará activamente en todas las cuestiones planteadas. Así, si un alumno no realiza alguna de las indicaciones anteriores, la nota de la evaluación se verá afectada a la baja. Es obligatoria la asistencia a clase siempre que no se tenga un motivo justificado.

Alumnos de asistencia irregular. (más de un 20% de faltas)

Estos alumnos se presentarán obligatoriamente a una recuperación final en la convocatoria ordinaria y deberán superar la prueba con una nota igual o superior a 5 sobre 10. En algunos casos, a criterio del profesor, el alumno deberá defender su examen ante varios profesores del Departamento.

En todo caso, estos alumnos estarán obligados a presentar y superar las prácticas de evaluación exigidas al grupo, calificándose les de la misma forma que se ha especificado en el apartado anterior.

11.2. Procedimientos e instrumentos de evaluación

- **Observación del profesor:** el profesor observará cómo se desenvuelven los alumnos en el aula, es decir, su comportamiento con respecto a sus compañeros y si asimila los contenidos.

- **Prácticas y ejercicios realizados en el aula/casa:** medirán de forma efectiva si el alumno está o no capacitado para el desempeño de una determinada función relacionada con los contenidos.
- **Documentación de las prácticas y realización de guías de usuario**: con esta herramienta los alumnos documentarán paso a paso todo el trabajo realizado de instalación y configuración de los diferentes servicios en red.
- **Pruebas teórico-prácticas:** Se realizarán pruebas escritas o en ordenador para comprobar que los alumnos efectivamente han afianzado correctamente los conceptos principales de las distintas unidades.

Los instrumentos de evaluación del alumnado serán:

- Observación sistemática
- Observación directa
- Exposición y documentación de prácticas.
- Realización de trabajos

El seguimiento individual del alumno o alumna se llevará a cabo a través de:

- Trabajo diario de clase/casa
- Realización de prácticas
- Preguntas individualizadas
- Realización de cuestionarios
- Realización de documentaciones.

Se valorará:

- La iniciativa, originalidad y participación del alumnado
- Exactitud y precisión en el desarrollo de los ejercicios y prácticas realizadas

Normas de evaluación

La nota final del módulo reflejará los conocimientos prácticos y teóricos, así como los ejercicios y actividades realizadas en el aula y en casa. La nota de cada evaluación vendrá dada por la suma ponderada de los siguientes conceptos, donde se incluyen los

resultados de aprendizaje y los criterios de evaluación evaluables con el instrumento del cuaderno del profesor y en las propias pruebas escritas y prácticas, que tendrán una ponderación de un 10% de la nota final de cada evaluación:

- Expresarse con corrección por escrito y oralmente (5% de la calificación de la unidad)
- Realizar trabajos en equipo e individualmente
- Mostrar interés y respeto hacia la asignatura y a los compañeros
- Participa en clase

PRIMERA EVALUACIÓN

Unidad Didáctica	Resultados de aprendizaje	Instrumentos de Evaluación			Ponderación criterio Eval. En el bloque	Ponderación de la unidad en la evaluación	Ponderación de la evaluación en la calificación final
		EXAMEN	PRÁCTICAS/TRABAJOS	CUADERNO DEL PROFESOR			
1. Conceptos sobre seguridad informática	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	70%	10%	0%	*80%*	20%	50%
	R5: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	10%	0%	0%	*10%*		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	83%	13%	5%			
2. Seguridad pasiva: equipos	R1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades	35%	15%	0%	50%	20%	
	R2: .Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integración de la información	25%	15%	0%	40%		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	63%	32%	5%			
3. Seguridad pasiva: Almacenamiento	R1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades	20%	10%	0%	*30%*	30%	
	R2: .Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integración de la información	45%	15%	0%	60%		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	68%	27%	5%			
4:Criptografía	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	20%	10%	0%	*30%*	30%	
	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico	40%	20%	0%	60%		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	63%	32%	5%			

SEGUNDA EVALUACIÓN

Unidad Didáctica	Resultados de aprendizaje	Instrumentos de Evaluación			Ponderación criterio Eval. En el bloque	Ponderación de la unidad en la evaluación	Ponderación de la evaluación en la calificación final
		EXAMEN	PRÁCTICAS/TRABAJOS	CUADERNO DEL PROFESOR			
5. Seguridad activa: sistema operativo y aplicaciones	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	40%	30%	0%	*70%*	30%	50%
	R5: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	20%	0%	0%	*20%*		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	63%	32%	5%			
6. Seguridad activa: acceso a redes	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	30%	10%	0%	*40%*	30%	
	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	30%	20%	0%	50%		
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	63%	32%	5%			
7. Seguridad activa: control de redes	R3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	30%	10%	0%	*40%*	25%	
	R4: Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	30%	20%	0%	*50%*		
	Actitud, asistencia, expresión	63%	32%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	60%	30%	5%			
8. Ataques y contramedida	R4: Asegura la privacidad de la información transmitida en redes	45%	45%	0%	90%	15%	

s	informáticas describiendo vulnerabilidades e instalando software específico.						
	Actitud, asistencia, expresión	3%	2%	5%	*10%*		
	Ponderación cada instrumento en la unidad:	48%	47%	5%			

11.3. Formas de recuperación

Evaluación ordinaria

Durante el desarrollo de las unidades didácticas emplearemos unos mecanismos de recuperación, para reforzar o recuperar la materia aún no asimilada antes de realizar alguna prueba o práctica específica. Al ser la evaluación continua permitirá ajustar el desarrollo de la misma al rendimiento de estos alumnos mediante las técnicas e instrumentos ya expuestos. Los mecanismos que utilizaremos para realizar, en caso necesario, este ajuste (mecanismos de recuperación) son los siguientes: las explicaciones individualizadas (con más y distintos ejemplos, con una guía por nuestra parte,…) y la corrección de las actividades de refuerzo para cada unidad (proporcionando más actividades y con la graduación de dificultad precisa).

Aquellos alumnos y alumnas que una vez realizadas pruebas o prácticas específicas en la que no hayan obtenido evaluación positiva, dispondrán de varias oportunidades de recuperar dicha parte de materia o práctica en la evaluación ordinaria:

En la prueba específica del primer o trimestre, además de la propia materia a evaluar al final del trimestre, los alumnos que no hubiesen superado alguna práctica o prueba específica durante dicho trimestre, podrán entregar esas prácticas y presentarse a dichos contenidos respectivamente (sólo correspondientes al trimestre). En caso de no superar alguna parte trimestral quedará pendiente el trimestre completo para la prueba final de evaluación ordinaria.

En la prueba final de evaluación ordinaria (en el segundo trimestre), además de la propia materia a evaluar correspondiente a dicho trimestre y de la recuperación de alguna práctica o prueba específica durante el mismo, los alumnos que tengan que recuperar el primer trimestre deberán presentarse a esta prueba para examinarse del mismo.

Como apoyo a los alumnos con algún trimestre pendiente durante la evaluación ordinaria, se

mantendrán los contenidos, enlaces y cualquier material existente en el servidor del departamento así como los recursos hardware de clase. Además se atenderán dudas.

Evaluación extraordinaria

En el caso de que el alumno no supere el módulo en la convocatoria ordinaria o aquellos que hayan perdido el derecho a evaluación continua, tendrán derecho a volver a intentarlo en la convocatoria extraordinaria.

Es importante destacar que los alumnos que hayan perdido el derecho a la evaluación continua, no podrán presentarse a la prueba final de evaluación ordinaria y por tanto deben examinarse en esta evaluación extraordinaria de todos los contenidos del curso.

Para superar con éxito dicha convocatoria, será necesaria superar la prueba específica, en la que se evaluarán los contenidos relativos a todo el módulo.

La calificación del módulo seguirá los mismos criterios que lo detallados en el apartado de calificación.

GUÍA DE RECUPERACIÓN

UNIDAD 1: CONCEPTOS SOBRE SEGURIDAD INFORMÁTICA

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

¿Por qué proteger?

¿Qué proteger?

Definiciones

Tipos de ataques

Buenas prácticas

Legislación

UNIDAD 2: SEGURIDAD PASIVA: ALMACENAMIENTO

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la

unidad:

Estrategias de almacenamiento

Backup de datos

Imagen del sistema

UNIDAD 3. SEGURIDAD PASIVA: EQUIPOS

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

Ubicación del CPD

Centro de respaldo

SAI/UPS

UNIDAD 4: CRIPTOGRAFÍA

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

¿Por qué cifrar?

Criptografía

Criptografía simétrica y asimétrica

Cifrar y firmar

PHI. DNIe

SEGUNDO TRIMESTRE

UNIDAD 5: SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

Carrera de obstáculos

Autenticación en el sistema operativo

Cuotas

Actualizaciones y parches

Antivirus

Monitorización

Aplicaciones web

Cloud computing

UNIDAD 6: SEGURIDAD ACTIVA: ACCESO A REDES

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

Redes cableadas

Redes inalámbricas

VPN

Servicios de red. Nmap y ntstat

UNIDAD 7: SEGURIDAD ACTIVA: CONTROL DE REDES

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

Expiar nuestra red

Firewall

Proxy

Spam

UNIDAD 8: ATAQUES Y CONTRAMEDIDAS

El alumnado elaborará un resumen de la unidad y se revisarán las actividades que le hayan resultado de mayor dificultad o no hayan sido correctamente asimiladas sobre los puntos principales de la unidad:

Ataques TCP/IP. MITM

Ataques wifi. Aircrack-ng

Ataques web. WebGoat

Ataques proxy.Ultrasur