I.E.S. "MIGUEL SÁNCHEZ LÓPEZ"
CICLO FORMATIVO DE GRADO MEDIO
"SISTEMAS MICROINFORMÁTICOS Y REDES"

MÓDULO PROFESIONAL:

"SEGURIDAD INFORMÁTICA"

CURSO ACADÉMICO:

2023/2024

PROFESOR:

JACINTO OCHANDO FRESNEDA

1. IDENTIFICACIÓN DEL MÓDULO.

- **Denominación del módulo**: Seguridad Informática
- **Duración del módulo**: 105 h.
- **Denominación del ciclo donde se ubica**: Técnico en Sistemas Microinformáticos y Redes.
- **Ubicación temporal dentro del ciclo**: El módulo se imparte en 2º ciclo.
- **Normativa que regula el ciclo formativo**: REAL DECRETO 1691/2007, de 14 de diciembre, por el que se establece el título de Técnico en Sistemas Microinformáticos y Redes y se fijan sus enseñanzas mínimas, ORDEN de 7 de julio de 2009, por la que se desarrolla el currículo correspondiente al título de Técnico en Sistemas Microinformáticos y Redes. enseñanzas que en virtud de la disposición final tercera.2 de la Ley Orgánica 10/ 2002, de 23 de diciembre, de Calidad de la Educación, quedan sustituidas por el término “enseñanzas comunes”.

2. OBJETIVOS GENERALES

Esta Programación se ha realizado de acuerdo al ***Real Decreto 1691/2007****,* donde se fijan sus enseñanzas mínimas para todo el territorio nacional, ***Decreto 436/2008*** *que regula aspectos generales y la* ***Orden de 7 de Julio de 2009*** *que desarrolla el currículo del* ***Ciclo de Grado Medio de Técnico de Sistemas Microinformáticos y Redes*** para Andalucía***.*** Dicha programación contribuirá a la adquisición y desarrollo de las ***Competencias Profesionales.***

Los ***objetivos generales*** del módulo son los siguientes:

- Instalar y actualizar aplicaciones ofimáticas, interpretando especificaciones y describiendo los pasos a seguir en el proceso.
- Elaborar documentos y plantillas, describiendo y aplicando las opciones avanzadas de procesadores de texto.
- Elaborar documentos y plantillas de hojas de cálculo, describiendo y aplicando opciones avanzadas de hojas de cálculo.
- Elaborar documentos con bases de datos ofimáticas, describiendo y aplicando operaciones de manipulación de datos.
- Manipular imágenes digitales analizando las posibilidades de distintos programas y aplicando técnicas de captura y edición básicas.
- Manipular secuencias de vídeo analizando las posibilidades de distintos programas y aplicando técnicas de captura y edición básicas.
- Elaborar presentaciones multimedia describiendo y aplicando normas básicas de composición y diseño.
- Realizar operaciones de gestión del correo y la agenda electrónica, relacionando necesidades de uso con su configuración.
- Aplicar técnicas de soporte en el uso de aplicaciones, identificando y resolviendo incidencias.

3. COMPETENCIAS PROFESIONALES GENERALES

Según la ORDEN 7 DE JULIO DE 2009, por la que se desarrolla el currículum correspondiente al título de técnico en Sistemas Microinformáticos y Redes en Andalucía (BOJA 25-8-2009, página 12), la formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales 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.
f) Instalar, configurar y mantener servicios multiusuario, aplicaciones y dispositivos compartidos en un entorno de red local, atendiendo a las necesidades y requerimientos especificados.
g) Realizar las pruebas funcionales en sistemas microinformáticos y redes locales, localizando y diagnosticando disfunciones, para comprobar y ajustar su funcionamiento.
h) Mantener sistemas microinformáticos y redes locales, sustituyendo, actualizando y ajustando sus componentes, para asegurar el rendimiento del sistema en condiciones de calidad y seguridad.
j) 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.
k) Elaborar presupuestos de sistemas a medida cumpliendo los requerimientos del 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.
m) Organizar y desarrollar el trabajo asignado manteniendo unas relaciones profesionales adecuadas en el entorno de trabajo.
n) Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
ñ) Utilizar los medios de consulta disponibles, seleccionando el más adecuado en cada caso, para resolver en tiempo razonable supuestos no conocidos y dudas profesionales.
p) Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
r) Resolver problemas y tomar decisiones individuales siguiendo las normas y procedimientos establecidos definidos dentro del ámbito de su competencia.

Estas competencias se corresponden con el REAL DECRETO 1691/2007, de 14 de diciembre, página 3456, por el que se establece el título de técnico en sistemas microinformáticos y redes, las competencias profesionales, personales y sociales asociadas al título son:

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.
f) Instalar, configurar y mantener servicios multiusuario, aplicaciones y dispositivos compartidos en un entorno de red local, atendiendo a las necesidades y requerimientos especificados.
g) Realizar las pruebas funcionales en sistemas microinformáticos y redes locales, localizando y diagnosticando disfunciones, para comprobar y ajustar su funcionamiento.

h) Mantener sistemas microinformáticos y redes locales, sustituyendo, actualizando y ajustando sus componentes, para asegurar el rendimiento del sistema en condiciones de calidad y seguridad.
j) Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
k) Elaborar presupuestos de sistemas a medida cumpliendo los requerimientos del 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 este.
m) Organizar y desarrollar el trabajo asignado manteniendo unas relaciones profesionales adecuadas en el entorno de trabajo.
n) Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
n) Utilizar los medios de consulta disponibles, seleccionando el más adecuado en cada caso, para resolver en tiempo razonable supuestos no conocidos y dudas profesionales.
p) Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
r) Resolver problemas y tomar decisiones individuales siguiendo las normas y procedimientos establecidos definidos dentro del ámbito de su competencia.

4. METODOLOGÍA.

La metodología básica a utilizar será el aprendizaje significativo, el lenguaje utilizado en clase debe ser comprensible por los alumnos, para ello habrá que determinar el dominio del vocabulario informático y el conocimiento de conceptos básicos de informática, que, aunque se supone conocidos en este nivel, permita fijar el punto de partida de la asignatura.

El esquema de trabajo que se seguirá en cada clase será el siguiente:

- Explicaciones teórico-prácticas por parte del profesor con ayuda del proyector.
- Entrega a los alumnos de apuntes y enlaces. Se utilizará Moodle Centros para este fin.
- Entrega de enunciados de ejercicios prácticos a desarrollar sobre los ordenadores para aplicar los conceptos explicados.
- Ejecución práctica de dichos ejercicios
- Pruebas de evaluación y seguimiento para detectar deficiencias y retrasos.

Las actividades prácticas escritas de evaluación se realizarán de manera individual.

Se usará la plataforma on-line (Moodle Centros) como método de comunicación entre alumnado y profesorado. A través de dicha plataforma se realizará el envío de material por parte del profesor al alumnado y el envío de ejercicios resueltos por parte alumnado. El profesor revisará estos ejercicios o prácticas previamente en clase para poder preguntar y ver si el alumno comprende lo que hace. También servirá como lugar en el que el profesor irá colgando información relevante para el grupo: fechas de exámenes, fechas de entrega de ejercicios, etc.

5. ATENCIÓN A LA DIVERSIDAD.

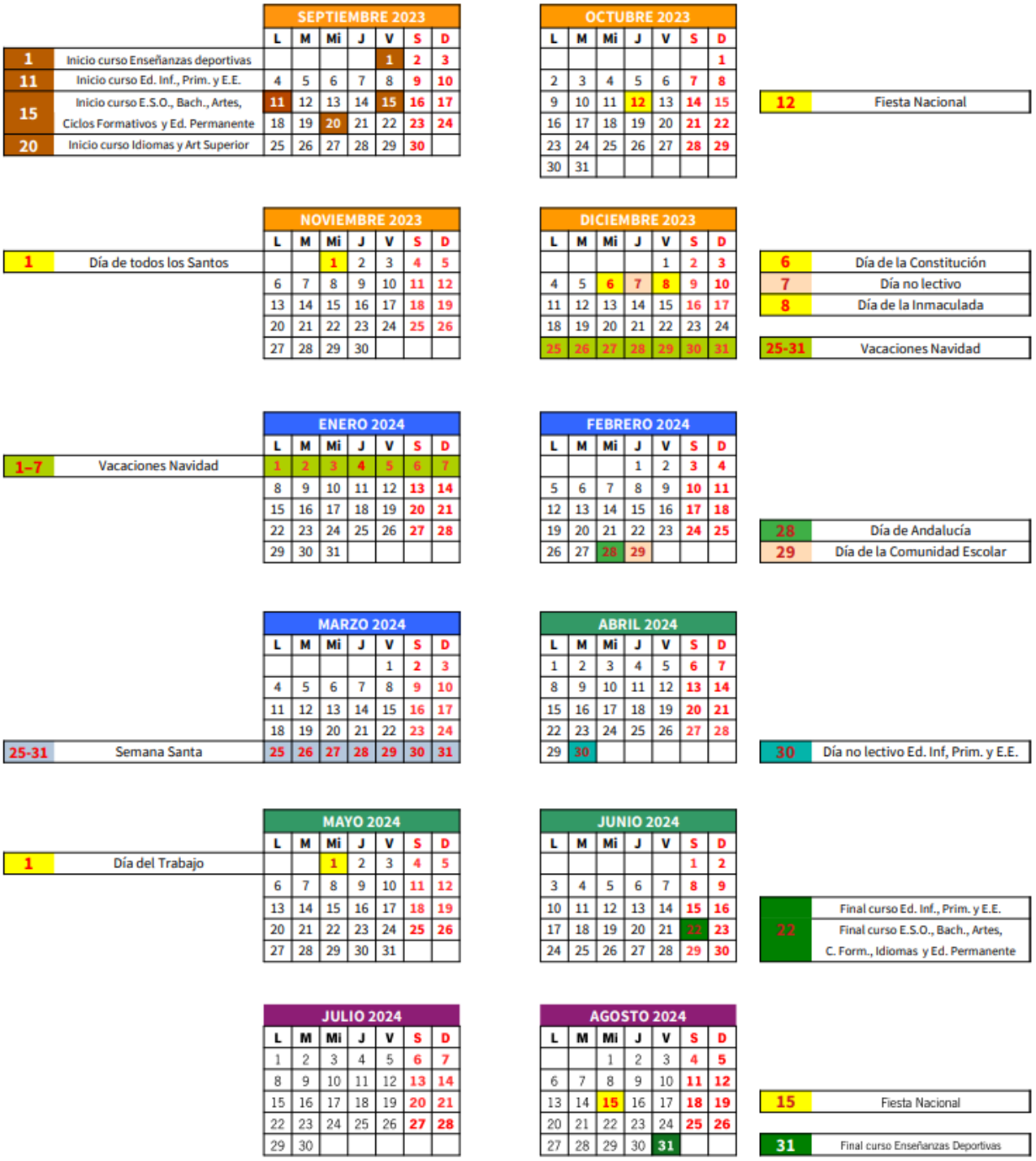
El Ciclo Formativo de Grado Medio en el que se engloba este módulo, es una enseñanza post obligatoria La legislación vigente no contempla la elaboración adaptaciones, sin embargo, se incluyen en esta programación una serie de adaptaciones no significativas en el ámbito metodológico que facilitarán al alumnado la consecución de los objetivos propuestos.

Alumnado con ritmo de aprendizaje más lento: Habrá que ayudarles en la resolución de problemas, dándoles más tiempo para la realización de ejercicios, prácticas, trabajos y proponiéndoles actividades que le permitan la comprensión de los contenidos.

Alumnado repetidor**:** Hay que considerar las distintas posibilidades, es decir, averiguar cuál es el motivo de la repetición y de esta forma determinar si los alumnos y las alumnas pueden estar dentro del grupo de alumnas y alumnos de aprendizaje rápido por aquello de que ya estudiaron la materia anteriormente, o si por el contrario, esta materia no la entienden y hay que buscar la forma de que les llegue, por lo que estarían encuadrados dentro del grupo de los lentos. La otra posibilidad sería que, simplemente, no estudiaron y por lo cual no necesitan otra cosa que seguir el ritmo normal de trabajo del grupo en el que se encuentran.

6. CONTENIDOS.

A continuación, se detallan las diferentes unidades didácticas con sus correspondientes criterios de evaluación.



- 1º evaluación: 15 septiembre de 2023 al 22 de diciembre de 2024
- 2º evaluación: 8 enero de 2024 al 22 de marzo de 2024
- 3º evaluación: 1 de abril de 2024 al 31 de mayo de 2024

6.1 Secuenciación de contenidos

Unidad didáctica 1: Introducción a la seguridad informática

Unidad 1. Introducción a la seguridad informática	%RA	Evaluación	Nº Horas
	20	**1ª**	**15**

Resultados de aprendizaje

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

Objetivos Didácticos

- Comprender el significado de seguridad informática, conocer las propiedades de un sistema seguro y distinguir diversos conceptos y terminología de seguridad.

Contenidos Conceptuales

1. Introducción a la seguridad informática.
2. Clasificación de seguridad.
   2.1. Seguridad activa y pasiva.
   2.2. Seguridad física y lógica.
3. Objetivos de la seguridad informática.
   3.1. Principales aspectos de seguridad.
4. Amenazas y fraudes en los sistemas de información.
   4.1. Vulnerabilidades, amenazas y ataques.
   4.2. Tipos de ataques.
   4.3. Mecanismos de seguridad.
5. Gestión de riesgos.
   5.1. Proceso de estimación de riesgos.
   5.2. Políticas de seguridad.
   5.3. Auditorías.
   5.4. Plan de contingencias.

Criterios de Evaluación

1.a) Se ha valorado la importancia de mantener la información segura.
1.b) Se han descrito las diferencias entre seguridad física y lógica..
1.g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
1.h) Se ha valorado la importancia de establecer una política de contraseñas.

Unidad didáctica 2: Seguridad en el entorno físico

Unidad 2. Seguridad en el entorno físico	%RA	Evaluación	Nº Horas
	20		15

Resultados de aprendizaje

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

Objetivos Didácticos

- Aplicar los mecanismos de seguridad activa en el entorno físico describiendo sus características y relacionándolas con las necesidades de uso de dicho entorno físico.
- Comprender la importancia de la seguridad en el entorno físico (estancias, plantas y edificios) de un sistema de información.
- Conocer algunos sistemas de control de acceso a personas al recinto.
- Saber cuál es la temperatura y la humedad idóneas para las distintas áreas de equipamiento informático.
- Observar el riesgo del agua y del fuego y detectar si se han aplicado las medidas de seguridad activas y pasivas necesarias en el entorno físico.
- Discernir qué es importante que un técnico o técnica en informática conozca el estado en que se encuentra el recinto que aloja un sistema de información en cuanto a seguridad de los espacios físicos.

Contenidos

1. Seguridad en el entorno físico.
    1. Acceso de personas al recinto.
    2. Alarma contra intrusos.
    3. Instalación eléctrica.
    4. Seguridad de materiales eléctricos y protección de personas frente a la electricidad.
    5. Condiciones ambientales: Humedad y temperatura.
    6. Enemigos de los ordenadores: Partículas de polvo, agua y fuego.
2. Centro de proceso de datos y su entorno físico.
    1. Infraestructura.
    2. Acceso.
    3. Redundancia.
3. Sistemas de control de acceso.
    1. Personal de vigilancia y control.
    2. Dispositivos de control de acceso en un datacenter.
    3. iButton, Touch memories o llaves electrónicas de contacto.
    4. Sistemas de reconocimiento de personas.
    5. Sistemas biométricos e identificación personal.
        1. Propiedades (ideales) de los rasgos biométricos.
        2. Sistemas biométricos más utilizados.
        3. Comparación de métodos biométricos.

Criterios de Evaluación

1.c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
1.d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
1.e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
1.f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida
1.i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

Unidad didáctica 3: Seguridad en el hardware. Almacenamiento y recuperación de la información.

Unidad 3. Seguridad en el hardware. Almacenamiento y recuperación de la información.	%RA	Evaluación	Nº Horas
	20	1º	15

Resultados de aprendizaje

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

Objetivos Didácticos

- Gestionar dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información. (Resultado de aprendizaje 3).
- Ser consciente de las consecuencias que puede ocasionar un problema en el hardware de los equipos, conociendo y sabiendo poner en práctica medidas para evitarlos.
- Comprender las diferentes opciones de almacenamiento que proporcionan mayor seguridad ante la pérdida de datos.
- Conocer y saber realizar las diferentes modalidades de copias de seguridad y respaldo que se pueden llevar a cabo para prevenir y recuperarse ante una pérdida de información.

Contenidos

1. Introducción a la seguridad en el hardware.
   1.1. Monitorización del hardware.
2. Sistemas de alimentación ininterrumpida.
   2.1. ¿Qué es un SAI?
   2.2. Tipos de SAI.
3. Almacenamiento redundante.
   3.1. Sistemas de tolerancia a fallos y seguridad física redundante.
   3.2. Sistemas RAID.
   3.3. Configuraciones o niveles RAID básicos.
   3.4. Configuraciones o niveles RAID avanzados.
   3.5. RAID en Windows.
4. Clusters de servidores.
   4.1. Clasificación de los clusters.
   4.2. Componentes de un cluster.
5. Almacenamiento externo.
   5.1. Cloud Computing.
   5.2. NAS.
   5.3. SAN.
6. Copias de seguridad.
   6.1. Políticas de copias de seguridad.
   6.2. Clasificación.
   6.3. Copia de seguridad del registro.
   6.4. Copia de seguridad de datos en Windows.
   6.5. Copia de seguridad de datos en Linux.
7. Recuperación de datos.
   7.1. Software de recuperación de datos.
   7.2. Creación de imágenes del sistema.
   7.3. Restauración del sistema.

Criterios de Evaluación
2.a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento. 2.b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros). 2.c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red. 2.d) Se han descrito las tecnologías de almacenamiento redundante y distribuido. 2.e) Se han seleccionado estrategias para la realización de copias de seguridad. 2.f) Se ha tenido en cuenta la frecuencia y el esquema de rotación. 2.g) Se han realizado copias de seguridad con distintas estrategias. 2.h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles. 2.i) Se han utilizado medios de almacenamiento remotos y extraíbles. 2.j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento

Unidad didáctica 4: Legislación de seguridad

Unidad 4. Legislación de seguridad	%RA	Evaluación	Nº Horas
	10	**1ª**	**15**

Resultados de aprendizaje

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

Objetivos Didácticos

- Conocer las directrices de las principales leyes relacionadas con seguridad, Internet, protección de los datos de carácter personal y propiedad intelectual.

Contenidos

1. Legislación: LOPD.
   1.1. Ámbito de aplicación.
   1.2. Agencia española de protección de datos.
   1.3. Derechos ARCO.
   1.4. Niveles de seguridad y medidas asociadas.
   1.5. Infracciones y sanciones.
2. Legislación: LSSI.
   2.1. Ámbito de aplicación.
   2.2. Obligaciones de las empresas.
3. Legislación: Derechos de autor.
   3.1. Ley de Propiedad Intelectual.
   3.2. Copyright y copyleft.
   3.3. Licencias Creative Commons.

Criterios de Evaluación

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

Unidad didáctica 5: Sistemas de identificación. Criptografía

Unidad 5. Sistemas de identificación. Criptografía	%RA	Evaluación	Nº Horas
	10	**2ª**	**15**

Resultados de aprendizaje

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

Objetivos Didácticos

- Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.
- Conocer el concepto de criptografía y comprender el funcionamiento de sus diferentes técnicas.
- Saber obtener y utilizar certificados digitales, así como conocer su funcionamiento y relacionarlo con las técnicas criptográficas vistas.
- Comprender y saber utilizar las principales instrucciones de la herramienta GnuPG en un entorno Linux.

Contenidos

1. Introducción a la criptografía.
   1.1. Aspectos de seguridad.
   1.2. Concepto de criptografía.
   1.3. Historia.
   1.4. Primeros métodos de cifrado.
2. Técnicas criptográficas
   2.1. Criptografía simétrica.
   2.2. Inconvenientes de la criptografía simétrica.
   2.3. Criptografía de clave pública.
   2.4. Firmas digitales.
   2.5. Funciones 'hash'.
   2.6. Sobres digitales.
3. Certificados digitales.
   3.1. Autoridades de certificación.
   3.2. Obtener un certificado digital en España.
   3.3. PKI.
4. Herramienta GPG en Linux.
   4.1. Comandos para el cifrado simétrico.
   4.2. Comandos para el cifrado asimétrico (de clave pública).

Criterios de Evaluación

4.f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
4.g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.

Unidad didáctica 6: Amenazas y seguridad del software

Unidad 6. Amenazas y seguridad del software	%RA	Evaluación	Nº Horas
	20,10	**2ª**	**15**

Resultados de aprendizaje

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.

Objetivos Didácticos

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

Contenidos

1. Fraudes informáticos y robos de información.
    1. Introducción.
    2. Software que vulnera la seguridad.
    3. Vulnerabilidad del software.
    4. Tipos de ataques.
    5. Atacantes.
    6. Fraude en Internet.
2. Control de acceso a la información.
    1. En el sistema operativo.
    2. Control de acceso a la información.
    3. Monitorización del sistema.
    4. Recursos de seguridad en el sistema operativo.
3. Seguridad en redes.
    1. Protocolos seguros.
    2. Seguridad en redes cableadas.
    3. Seguridad en redes inalámbricas.
4. Seguridad activa.
    1. Antivirus.
    2. Antimalware.
    3. Congelación.
    4. Correo.
    5. Cómo crear una contraseña segura.
    6. Firewall o cortafuegos en equipos.

Criterios de Evaluación

3.a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.

3.b) Se han clasificado los principales tipos de software malicioso.

3.c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.

3.d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.

3.e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

3.f) Se han aplicado técnicas de recuperación de datos.

Unidad didáctica 7: Redes seguras

Unidad 6. Amenazas y seguridad del software	%RA	Evaluación	Nº Horas
	10	2ª	15

Resultados de aprendizaje

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

Objetivos Didácticos

- Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- Interpretar y seleccionar información para elaborar documentación técnica y administrativa.
- Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.
- Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
- Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
- Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.

Contenidos

1. Seguridad en redes.
    a. Protocolos seguros.
    b. Seguridad en redes cableadas.
    c. Seguridad en redes inalámbricas.
2. Cortafuegos o Firewall.
    a. Tipos de Cortafuegos.
    b. Arquitecturas de firewall.
3. Proxy.
    a. Funcionamiento y características.
    b. Proxy web y Proxy Caché.
    c. Proxy en Windows.
        i. Proxy en Windows. Wingate.
        ii. Proxy en Windows. Free proxy.
    d. Proxy en Linux.
        i. Proxy en Linux. Listas de Control de acceso.
        ii. Proxy en Linux. Opciones avanzadas.
4. IDS Sistemas detectores de intrusos.
    a. Sistemas detectores de intrusos.
    b. Clasificación de sistemas IDS.
    c. Arquitectura de sistemas IDS.

Criterios de Evaluación

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

7. VINCULACIÓN CON OTRAS ÁREAS Y CON TEMAS TRANSVERSALES.

Los temas transversales son aquellos que engloban múltiples contenidos que difícilmente pueden asociarse específicamente a ninguna de las áreas, pero estarán impregnados en el currículo. Hay que tener en cuenta que un profesor no sólo es un docente sino también un educador. Algunos de estos temas transversales son:

Educación para la paz (tolerancia, respeto hacia otras ideas diferentes a las propias, etc.).

Coeducación (igualdad de sexos en el trabajo o la educación contra la violencia de género, por ejemplo).

Educación para la salud (corregir las malas posturas de trabajo, educar en contra del tabaco...).

Educación ambiental (crear conciencia sobre el ahorro de papel, fomentando el uso del soporte electrónico).

Fomento de la lectura (utilización de manuales, textos, documentos digitales…).

8. FALTAS DE ASISTENCIA.

Los alumnos tienen la **obligación de asistir a clase**. La falta de asistencia a clase tiene como consecuencia la imposibilidad de poder evaluar de forma continuada al alumno, impidiendo que la evaluación sea continua.

Para el alumnado que no asista con normalidad a clase se le aplicará lo establecido en la Programación del Departamento (Apartado Programaciones Didácticas)

9. EVALUACIÓN Y RECUPERACIÓN

1.1. *Criterios de calificación*

Tal y como establece la legislación vigente, la evaluación del proceso de aprendizaje del alumnado será continua y diferenciada según los módulos, tendrá un carácter formativo y será un instrumento para la mejora tanto de los procesos de enseñanza como de los procesos de aprendizaje.
Los referentes para la comprobación del grado de logro de los objetivos del módulo en las evaluaciones continua y final son los resultados de aprendizaje y sus criterios de evaluación. Así, cada resultado de aprendizaje y sus criterios de evaluación asociados serán evaluados con una o varias actividades de evaluación: pruebas objetivas, supuestos prácticos, actividades, etc.

La calificación del alumnado en cada evaluación y final se obtendrá como resultado de calcular la media de las tareas de evaluación realizadas para cada una de las unidades didácticas hasta el momento de la evaluación y que han sido diseñadas teniendo en cuenta la naturaleza de los resultados de aprendizaje y criterios de evaluación que pretenden valorar.

La falta injustificada a la realización/entrega de estas actividades de evaluación supondrá la obtención de una calificación de 0 en la actividad, así como en los resultados y criterios de evaluación que tiene asociados. En caso de falta justificada, el alumno deberá aportar el consiguiente justificante de algún organismo oficial, para poder realizar dicha prueba fuera de la fecha prevista inicialmente; además, siempre que sea posible, el alumno notificará dicha circunstancia lo antes posible al profesor.

La utilización o intento de utilización de cualquier método de fraude en una prueba escrita supondrá automáticamente la anulación de la prueba y la obtención de una calificación de 0 en la misma, así como en los resultados y criterios de evaluación que tiene asociados.

Ponderación de cada tema:

- Exámenes (teóricos o prácticos): 35%
- Prácticas (actividades de mayor duración y complejidad): 35%
- Actividades: 30%

Procedimientos de Evaluación

- ***Evaluación inicial***: al comienzo del curso se realizará una evaluación inicial mediante un cuestionario con preguntas tipo test y/o cuestiones breves. Se trata de conocer qué punto de partida tiene el grupo respecto a los aprendizajes y experiencias previas del alumnado con respecto a los objetivos que este módulo persigue y los contenidos del mismo.

- ***Evaluación continua***: la superación de este módulo mediante evaluación continua requiere la asistencia regular a clase y el desarrollo de las actividades programadas para el mismo.

A continuación, se exponen los métodos a utilizar para la evaluación continua del alumnado:

- Asistencia y aprovechamiento de las clases teóricas y prácticas.

- Al ser este módulo, eminentemente práctico se evaluarán los conocimientos y las destrezas operativas adquiridas. Los alumnos deben realizar todas las prácticas propuestas por el profesor, y deben entregarlas o explicarlas *in situ* cuando sean solicitadas por el mismo.

- Realización de pruebas o exámenes prácticos ante el ordenador. Ejecución individual de ejercicios de carácter práctico de similar dificultad a los realizados en clase.

- Se considerará evaluación positiva, la consecución de las capacidades finales exigidas al finalizar cada unidad didáctica.

- Mejorará el contenido de la calificación final, la realización de prácticas adicionales que están propuestas para este fin.

- Para cada resultado de aprendizaje se propondrán una serie de ejercicios. La realización correcta de estos, así como la adecuada presentación, se valorará a la hora de la calificación del alumno.

- La buena predisposición para realizar las prácticas y el grado de participación del alumno en clase también tendrá incidencia en la calificación.

MEDIDAS DE RECUPERACIÓN O SUBIDA DE NOTA

Si en la tercera evaluación el alumno no obtiene una calificación positiva, deberá asistir a clase durante el mes de junio para la preparación de las pruebas de la evaluación final. En estas pruebas el alumno deberá enfrentarse a todos aquellos **Resultados de Aprendizaje que no ha superado** durante el curso. La evaluación se hará teniendo en cuenta los objetivos didácticos y los criterios de evaluación fijados en cada una de las unidades didácticas implicadas.

Si en la tercera evaluación el alumno obtiene una calificación positiva, pero quiere mejorar la nota obtenida deberá asistir a clase durante el mes de junio para la preparación de las pruebas de la evaluación final. En estas pruebas el alumno deberá enfrentarse a todos los Resultados de Aprendizaje.

1.2. *Evaluación de Competencias Profesionales*

La evaluación de las competencias profesionales asociadas a cada módulo va asociada con la evaluación de las actitudes y procedimientos de cada tema. En cada unidad didáctica se detalla que competencias serán evaluadas.

Para superar el módulo, todas las competencias profesionales deben estar superadas.

1.3. *Instrumentos de evaluación*

- Registro de tareas en Moodle.
- Participación activa.
- Cuestiones orales en clase.
- Resúmenes, esquemas, mapas conceptuales, ejercicios, actividades, tareas, fichas de trabajo y pruebas objetivas.
- Exámenes (extensos, de respuesta múltiple, pruebas teóricas y/o prácticas).
- Presentaciones orales de trabajos/investigaciones solos o en grupo.

10. SEGUIMIENTO DE LA PROGRAMACIÓN.

A la finalización de cada UNIDAD DIDÁCTICA se deberá hacer un estudio de los objetivos cumplidos y el estado de la temporalización para, en su caso, reajustarla a las nuevas circunstancias. Así mismo se prestará especial atención a la evolución de los alumnos y las alumnas en general, y a los alumnos y las alumnas con necesidades educativas específicas en particular, con la finalidad de reajustar las actividades a realizar por cada uno del alumnado.

Al finalizar cada trimestre los alumnos realizarán un cuestionario que se encuentra en la Plataforma Educativa Moodle Centros para evaluar el proceso de enseñanza.