CICLO FORMATIVO DE GRADO MEDIO

SISTEMAS MICROINFORMÁTICOS Y REDES

IES PINO MONTANO

SEVILLA

SEGURIDAD INFORMÁTICA

Año académico 2022/2023

Antonio José García Cruz

Índice

1. Legislación

Real Decreto 1691/2007, de 14 de diciembre (BOE del 17 de enero de 2008), 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 (BOJA 25 de agosto 2009), por la que se desarrolla el currículo correspondiente al título de Técnico en sistemas Microinformáticos y Redes.

Orden de 29 de septiembre de 2010, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

El título de Técnico en Sistemas Microinformáticos y Redes, queda identificado por los elementos siguientes:

Denominación:	**Sistemas Microinformáticos y Redes.**
Nivel:	**Formación Profesional de Grado Medio.**
Duración:	**2000 horas.**
Familia Profesional:	**Informática y Comunicaciones.**
Referente europeo:	**CINE-3 (Clasificación Internacional Normalizada de la Educación)**

2. Objetivos generales del título

Los objetivos generales de este ciclo formativo son los siguientes:

a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.

b) Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos

de calidad y seguridad, para montar y configurar ordenadores y periféricos.

c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.

d) Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de red.

e) Ubicar y fijar equipos, líneas, canalizaciones y más elementos de una red local cableada, inalámbrica mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.

f) Interconectar equipos informáticos, dispositivos red local y de conexión con redes de área extensa, ejecutando los procedimientos para instalar y configurar redes locales.

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

h) Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.

i) Interpretar y seleccionar información para elaborar documentación técnica y administrativa.

j) Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.

k) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.

l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.

m) Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.

n) Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.

o) Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción.

p) Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.

q) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.

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

3. 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.

4. Resultados de aprendizaje y criterios de evaluación

Resultado de aprendizaje 1
Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades
Criterios de evaluación
a) Se ha valorado la importancia de mantener la información segura. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han definido las características de la ubicación física y las 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 indicado 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.

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

Resultado de aprendizaje 3
Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.
Criterios de evaluación
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad. b) Se han clasificado los principales tipos de software malicioso. c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades. d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas. e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso. f) Se han aplicado técnicas de recuperación de datos.

Resultado de aprendizaje 4
Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico
Criterios de evaluación
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.

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

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

5. Contenidos básicos

- Aplicación de medidas de seguridad pasiva:
  — Seguridad informática. Clasificación, técnicas, 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. Herramientas de 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.

6. Criterios de calificación

6.1. Calificación

El curso se divide en tres evaluaciones. La calificación final de cada una será la media de la calificación de cada una de las unidades didácticas que la componen (salvo en el 3º trimestre):

- **1º trimestre:** de Septiembre a Diciembre.
- **2º trimestre:** de Enero a mediados de Marzo. Donde los alumnas/os que han aprobado los módulos van a la FCT.

- **3º trimestre:** de Marzo a Junio, para aquellos alumnas/os que no han aprobado algún módulo del curso.

Se calificará al alumno mediante notación numérica de 0 a 10. Una calificación por debajo de 5 indicará que no ha superado las pruebas de esa/s unidad/es didácticas.

La evaluación será continua, teniendo en cuenta la asistencia y actitud en clase, valorándose la participación en las clases que se impartan en el aula, el nivel de destreza demostrado en la realización de los ejercicios y trabajos, las aportaciones que realice y el trabajo en casa.

Para mayor información se realizarán trabajos individuales o en pequeños grupos, exposiciones, controles o pruebas individuales durante el trimestre. Estos controles o pruebas podrán realizarse sin previo aviso, para ver el nivel de trabajo diario, y serán tanto de carácter práctico como pruebas objetivas para evaluación de conceptos. El número de controles o pruebas y sus contenidos serán determinados por el profesorado. Al final de cada trimestre, se realizará un examen trimestral que abarcará todos los contenidos del mismo si no se realizan pruebas parciales.

El alumno o alumna que quede demostrado que ha copiado en algún control o examen, obtendrá una nota de 0 en el examen que haya copiado y el profesorado puede poner un examen especial para ese alumno o alumna en la siguiente convocatoria. Además, si hay sospecha de que el alumnado ha copiado en un control o examen, el profesorado puede realizar otro examen sin previo aviso, a parte o a todo el grupo, para determinar cuáles son los conocimientos reales del alumnado.

La materia de la asignatura es acumulativa, es decir, cada conocimiento nuevo que se introduce se apoya o complementa a los anteriores, lo que implica que es necesario repasar continuamente conceptos ya aprendidos, lo que hace que el alumno o alumna los tenga siempre frescos y los llegue a dominar realmente. Por tanto, aunque un alumno tenga superada la materia de una parte necesitará aplicar dichos conocimientos para superar los siguientes.

La nota final del trimestre se obtendrá de las siguientes ponderaciones:

- 10% Comportamiento, actitud, participación
- 20 % Entrega de Boletines (actividades y tareas sobre conceptos, de tipo practico)
- 70% Nota Media de los exámenes (controles sobre conceptos y pruebas prácticas).

Nota trimestre = 0,2*Boletines + 0,7*Exámenes + 0,1*Actitud

La ponderación solo se realizará cuando:

- El alumnado haya superado todos los RA.
- La nota media de los exámenes teóricos haya superado el 5.
- Todas las actividades, boletines y exámenes prácticos sean APTOS.

Los diferentes apartados que intervienen en la evaluación se puntuarán siempre de 0 a 10 puntos.

6.2. Calificación final

La nota final de la asignatura se obtendrá de la media ponderada de todas y cada una de las unidades didácticas que la componen.

Para aplicar esta fórmula cada unidad didáctica ha de estar aprobada por separado.

Observaciones

1. La asistencia a clase es obligatoria, aconsejable y necesaria para la superación del módulo
2. Para superar todos los resultados de aprendizaje será necesario entregar todas las actividades y realizar todos los exámenes relativos al mismo.
3. Para aprobar el módulo es necesario superar todos los resultados de aprendizaje descritos anteriormente.

6.3. Plan de refuerzo y criterios de recuperación

Con carácter excepcional se podrán realizar, de cada unidad pruebas de recuperación que consistirán en pruebas sobre conceptos, pruebas con supuestos prácticos y pruebas prácticas de la unidad. Superar dichas pruebas no supone “aprobar la unidad”. La superación de los contenidos mínimos estará condicionada a la realización de todas las actividades que incluye el módulo para cada unidad de trabajo.

Si un alumno no puede asistir a un examen, tendrá que hacerlo en el siguiente trimestre, si ha presentado justificante.

El alumnado de segundo curso que tenga el módulo de Seguridad Informática no superado mediante evaluación parcial, y por tanto, no pueda cursar el módulo de

FCT, continuará con las actividades lectivas hasta la fecha de finalización del régimen ordinario de clase que no será anterior al día 22 de junio de cada año.

De esta manera, se realizará una serie de actividades que cubrirán los contenidos de conocimiento y práctica en el periodo Marzo-Junio. Para la recuperación y posterior calificación en la convocatoria final, se elaborará un plan personalizado para cada alumnado en el cual se incluirán las actividades de refuerzo y las pruebas escritas o prácticas que deben realizarse en función de los requisitos mínimos no superados en cada caso.

La dinámica diaria será la siguiente:

- Se volverán a explicar los conceptos principales de cada resultado de aprendizaje.
- Se realizarán actividades prácticas para reforzar los contenidos teóricos.
- Se resolverán todas las dudas que puedan surgir.

Al final de dicho periodo, se realizará una evaluación final en Junio: todos aquellos alumnos/as que no hayan superado el módulo en las evaluaciones parciales y sus correspondientes resultados de aprendizaje tendrán derecho a presentarse a una evaluación final, que constará de una prueba sobre el contenido del curso donde se incluirán los resultados de aprendizaje no alcanzados por el alumno/a.

6.4. Instrumentos de evaluación

Los instrumentos de evaluación del alumnado serán:

- Observación sistemática
- Observación directa
- Exposición
- Realización de trabajos

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

- Trabajo diario en clase
- Realización de ejercicios individuales
- Realización de supuestos prácticos.
- Realización de pruebas teórico-prácticas.

Se valorará:

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

6.5. Horas de Libre Configuración adscritas al módulo de Seguridad Informática

Las horas de Libre Configuración, a efectos de evaluación, quedan adscritas al módulo de Seguridad Informática. Esto quiere decir que las horas de Libre Configuración y Seguridad Informática se evaluarán de forma independiente, como si fueran bloques independientes que forman parte de un único módulo, pero con una única nota. Para alcanzar la calificación positiva se habrá de superar cada uno de ellos de forma independiente. La calificación final en el módulo de Seguridad Informática será una media ponderada de ambos bloques:

- Seguridad Informática, 60%.
- Las horas de libre configuración 40%.

Instrumentos de Evaluación

Los instrumentos de evaluación del alumnado serán:

a) Observación sistemática
b) Observación directa
c) Exposición
d) Realización de trabajos

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

a) Trabajo diario en clase
b) Realización de ejercicios individuales
c) Realización de supuestos prácticos.
d) Realización de pruebas teórico-prácticas.

Se valorará:

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

7. Evaluación Inicial

En esta evaluación se ha valorado el grado de los conocimientos previos que tiene el alumnado sobre los esquemas de conocimiento pertinentes para seguridad informática, lo cual permitirá conseguir de cada alumno/a el máximo rendimiento posible. Esta evaluación en ningún caso conlleva calificación para el alumnado.

Los resultados se han puesto en común en la reunión del equipo docente, reflejando en un acta la información obtenida de cada alumno (puede consultarse en la jefatura de estudios).

- **Grupo A:** Este curso 2022/23 tenemos 19 alumnos. Forman un grupo homogéneo tanto en cuanto a conocimientos previos como en edad. La mayoría tiene un nivel medio-bajo en relación con los contenidos de la asignatura. Ninguno tiene experiencia laboral en informática pero sí tienen inquietudes informáticas. No hay en este grupo alumnos repetidores. Hay un alumno absentista.

- **Grupo B:** Este curso 2022/23 tenemos 15 alumnos. Forman un grupo homogéneo tanto en cuanto a conocimientos previos como en edad. La mayoría tiene un nivel medio-bajo en relación con los contenidos de la asignatura. Ninguno tiene experiencia laboral en informática pero sí tienen inquietudes informáticas. En este grupo hay 2 alumnos repetidores de la asignatura más 5 repetidores del módulo. Hay un alumno absentista.

8. Contenidos y secuenciación temporal

La Orden de 7 de julio de 2009 establece que el módulo profesional de Seguridad Informática tendrá una duración de 105 horas. Se impartirá a razón de 5 horas por semana.

Los diferentes contenidos de este módulo, los agrupamos en las siguientes Unidades Didácticas:

Unidad 1.- Introducción a la seguridad informática.
Unidad 2.- Seguridad en el entorno físico.
Unidad 3.- Seguridad en el hardware. Almacenamiento y recuperación de los datos.
Unidad 4.- Sistemas de identificación. Criptografía.
Unidad 5.- Amenazas y seguridad del software.
Unidad 6.- Redes seguras.

La distribución de las distintas unidades en las evaluaciones queda de la siguiente manera:

UNIDAD	Primera Evaluación	Segunda Evaluación
Unidad 1	X	
Unidad 2	X	
Unidad 3	X	
Unidad 4		X
Unidad 5		X
Unidad 6		X

Unidad Didáctica 1			
Título:	Introducción a la seguridad informática	**Duración:**	15 horas

Contenidos

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 la 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
6. Legislación: LOPD
   6.1 Ámbito de aplicación
   6.2 Agencia española de protección de datos
   6.3 Derechos ARCO
   6.4 Niveles de seguridad y medidas asociadas
   6.5 Infracciones y sanciones
7. Legislación: LSSI
   7.1 Ámbito de aplicación
   7.2 Obligación de las empresas
8. Legislación: Derechos de autor
   8.1 Ley de propiedad intelectual
   8.2 Copyright y Copyleft
   8.3 Licencia Creative Commons

Resultados de aprendizaje	Criterios de evaluación
RA1	a) Se ha valorado la importancia de mantener la información segura. b) Se han descrito las diferencias entre seguridad física y lógica.
RA3	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad. b) Se han clasificado los principales tipos de software malicioso.
RA4	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
RA5	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.

Unidad Didáctica 2			
Título:	Seguridad en el entorno físico	**Duración:**	18 horas

Contenidos

1. Seguridad en el entorno físico
    - 1.1 Acceso de personas al recinto
    - 1.2 Alarma contra intrusos
    - 1.3 Instalación eléctrica
    - 1.4 Seguridad de materiales eléctricos y protección de personas frente a la electricidad
    - 1.5 Condiciones ambientales: Humedad y temperatura
    - 1.6 Enemigos de los ordenadores: Partículas de polvo, agua y fuego
2. Centro de proceso de datos y su entorno físico
    - 2.1 Infraestructura
    - 2.2 Acceso
    - 2.3 Redundancia
3. Sistemas de control de acceso
    - 3.1 Personal de vigilancia y control
    - 3.2 Dispositivos de control de acceso en un datacenter
    - 3.3 iButton, Touch memories o llaves electrónicas de contacto
    - 3.4 Sistemas de reconocimiento de personas
    - 3.5 Sistemas biométricos e identificación personal
        - 3.5.1 Propiedades (ideales) de los rasgos biométricos
        - 3.5.2 Sistemas biométricos más utilizados
        - 3.5.3 Comparación de métodos biométricos
4. Políticas, planes y procedimientos de seguridad
    - 4.1 Elementos de las políticas de seguridad
    - 4.2 Características deseables de las políticas de seguridad
    - 4.3 Definición e implantación de las políticas de seguridad
    - 4.4 Inventario y auditoría

Resultados de aprendizaje	Criterios de evaluación
RA1	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 Didáctica 3			
Título:	Seguridad en el hardware. Almacenamiento y recuperación de los datos	**Duración:**	18 horas

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 y Linux
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 y Linux
7. Recuperación de datos
   7.1 Software de recuperación de datos
   7.2 Creación de imágenes del sistema
   7.3 Restauración del sistema

Resultados de aprendizaje	Criterios de evaluación
RA2	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento. b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros). c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red. d) Se han descrito las tecnologías de almacenamiento redundante y distribuido. e) Se han seleccionado estrategias para la realización de copias de seguridad. f) Se ha tenido en cuenta la frecuencia y el esquema de rotación. g) Se han realizado copias de seguridad con distintas estrategias.

	h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles. i) Se han utilizado medios de almacenamiento remotos y extraíbles. j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.
RA3	f) Se han aplicado técnicas de recuperación de datos.

Unidad Didáctica 4			
Título:	Sistemas de identificación. Criptografía	**Duración:**	18 horas

Contenidos

1. Introducción a la criptografía
    1.1 Aspectos de seguridad
    1.2 Concepto de criptografía
    1.3 Historia
    1.4 Primeros sistemas de criptografía
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)

Resultados de aprendizaje	Criterios de evaluación
RA4	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.

Unidad Didáctica 5			
Título:	Amenazas y seguridad del software	**Duración:**	18 horas

Contenidos

1. Fraudes informáticos y robos de información
    1.1 Introducción
    1.2 Software que vulnera la seguridad
    1.3 Vulnerabilidad del software
    1.4 Tipos de ataques
    1.5 Atacantes
    1.6 fraudes en Internet
2. Control de acceso a la información
    2.1 En el sistema operativo
    2.2 Control de acceso a la información
    2.3 Monitorización del sistema
    2.4 Recursos de seguridad en el sistema operativo
3. Seguridad en redes
    3.1 Protocolos seguros
    3.2 Seguridad en redes cableadas
    3.3 Seguridad en redes inalámbricas
4. Seguridad activa
    4.1 Antivirus
    4.2 Antimalware
    4.3 Congelación
    4.4 Correo
    4.5 Cómo crear una contraseña segura
    4.6 Firewall o cortafuegos en equipos

Resultados de aprendizaje	Criterios de evaluación
RA3	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.
RA4	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

Unidad Didáctica 6			
Título:	Redes seguras	**Duración:**	18 horas

Contenidos

1. Redes seguras
    1.1 Niveles OSI
        1.1.1 Seguridad en las capas
    1.2 Redes Privadas virtuales
        1.2.1 Introducción a las Redes Privadas Virtuales
        1.2.2 Analogía: Cada LAN es una isla
        1.2.3 ¿Qué hace una VPN?
        1.2.4 VPN de acceso remoto y VPN punto a punto
        1.2.5 Mantener el tráfico en el túnel VPN
        1.2.6 Encriptación y protocolos de seguridad en una red privada virtual
2. Cortafuegos o Firewall
    2.1 Tipos de Cortafuegos
    2.2 Arquitecturas de firewall
3. Proxy
    3.1 Funcionamiento y características
    3.2 Proxy web y Proxy Caché
    3.3 Proxy en Windows
    3.4 Proxy en Linux
4. IDS Sistemas detectores de intrusos
    4.1 Sistemas detectores de intrusos
    4.2 Clasificación de sistemas IDS
    4.3 Arquitectura de sistemas IDS

Resultados de aprendizaje	Criterios de evaluación
RA4	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red. 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. h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

9. Orientaciones pedagógicas

Se pretende garantizar la consecución de los objetivos propuestos en el Módulo “Seguridad Informática” del ciclo formativo de grado medio de técnico en sistemas microinformáticos y redes, que pertenece a la familia profesional de informática y comunicaciones.

Dado que nuestros alumnos vienen de una formación general, es fundamental conectar tantas veces como sea posible los conceptos explicados 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.

Se realizarán 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.

Uno de los objetivos de la enseñanza en formación profesional es capacitar a los alumnos para que sepan trabajar de manera independiente. Por este motivo se realizarán muchos casos prácticos ya resueltos, para que los alumnos avancen por sí mismos en su propio proceso de aprendizaje.

10. Atención a la diversidad. Alumnos con necesidades específicas

Los conocimientos iniciales del alumnado son diferentes y, por tanto, la situación de partida es también diferente para todos ellos. Por otro lado, los conceptos y destrezas que debe adquirir el alumno/a suponen para algunos de ellos cierto grado de complejidad en este módulo. Por tanto, se planifican varios recursos que se pueden emplear para atender esta diversidad mediante una atención individualizada de los alumnos/as que lo necesiten, mediante propuestas del tipo:

- Como norma general para todo el grupo, las actividades que se desarrollen como aplicación práctica de los conocimientos adquiridos por el alumnado tendrán el nivel equilibrado y necesario para la superación del módulo. No obstante, dichas actividades se irán realizando partiendo de un nivel básico hasta llegar al mínimo exigible para dicho objetivo.

- Para aquellos alumnos/as con alguna dificultad de asimilación de conceptos en alguno de los contenidos del módulo se propondrá la

realización de actividades complementarias para que adquieran el nivel necesario y puedan seguir el ritmo marcado por el profesor.

- Por otro lado, aquellos alumnos/as que adquieran los contenidos de una manera más rápida y efectiva también recibirán una propuesta de actividades de profundización o bien la realización de algún trabajo de campo que pueda ser presentado en clase y forme parte de los archivos del departamento para sucesivos cursos.

- Se potenciarán los trabajos en grupo porque fomentan la colaboración entre los miembros y enriquecen el aprendizaje de los distintos miembros.

- Para aquellos alumnos que presentan alguna necesidad educativa especial se tomarán medidas especiales, tales como sentarlo en un sitio central, de frente a la pizarra y cercano al profesor. Además, se intenta interactuar frecuentemente con él para captar su atención y asegurarse de que están adquiriendo los conocimientos y entendiendo las explicaciones.

11. Actividades Complementarias y Extraescolares

Durante los cursos anteriores anteriores a la pandemia se han venido realizando las siguientes actividades complementarias (todas ellas de carácter no obligatorio y en función de la disponibilidad económica y temporal del grupo):

- Visitas al CICA o en su defecto CPD del SAS
- Visitas al DATACENTER de la Universidad Pablo de Olavide o en su defecto al Datacenter de la Universidad de Sevilla.
- Obtención del CERTIFICADO DIGITAL en una oficina de registro de Hacienda.
- Participación en las CiberOlimpiadas de CyberCamp (Incibe)

Además, todos los años se han venido realizando unas jornadas sobre seguridad informática, con un tema central diferente. Dichas jornadas incluyen:

- Ponencias del alumnado.
- Ponencias de personal ajeno al centro, expertos en seguridad informática.
- Proyección de videos.
- Colaboración con el ciclo de Animación Sociocultural y Turística.

Durante la presumiblemente finalizada situación pandémica, no se pudieron realizar ninguna de las anteriores actividades, quedando emplazadas a su vuelta a la normalidad en la medida en que las circunstancias mejorasen. Siendo así en el momento actual, se procederá en el presente curso a retomar algunas de esas actividades como, por ejemplo, y de momento, la concertada visita al

DATACENTER de la Universidad de Sevilla para el 11 de Noviembre y la obtención del CERTIFICADO DIGITAL en la oficina de registro de la Consejería de Agricultura y Pesca en la citada fecha.

12. Plan de Lectura y Plan de motivación

Toda la información relativa al plan de lectura y de motivación se encuentra expuesta en la programación de departamento, ya que son contenidos puestos en común por el departamento.

13. Contenidos Transversales

Al tratarse de un módulo perteneciente a un tipo de formación específica puede parecer que la relación con este tipo de temas es un poco tangencial. Sin embargo, si se procede a un análisis detenido, se puede observar que algunos de estos temas transversales se desarrollan así:

- **Educación ambiental:** la utilización de la informática, en general, y sobre todo en los negocios, hace que grandes volúmenes de información puedan ser almacenados en soportes informáticos, discos, CD... y enviados de unos lugares a otros a través de las redes informáticas, evitándose de esta manera el consumo de grandes cantidades de papel y, por consiguiente, la destrucción de bosques, contribuyendo de alguna manera a la preservación de los medios naturales y medio-ambientales.

- **Educación del consumidor:** el análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumnado para decidir sobre los productos informáticos que debe adquirir y utilizar de manera ventajosa.

- **Educación para la salud:** cuando se utilizan equipos informáticos se procura que el alumnado conozca una serie de normas de higiene y seguridad en el trabajo, así como sobre las precauciones necesarias en el empleo de los equipos. De esta manera, se intenta que el alumnado sepa los principios de la ergonomía del puesto de trabajo, para que cualquier trabajo frente al ordenador resulte lo más agradable posible y no le cause ningún problema.

- **Educación para la igualdad de oportunidades entre ambos sexos.** Desde este módulo contamos con elementos para concienciar al alumnado sobre la igualdad de oportunidades para alumnos y alumnas:
    - Formando grupos mixtos de trabajo.

- Distribuyendo las tareas a realizar en la misma medida entre el alumnado de ambos sexos.
- Haciendo que todos utilicen los mismos o equivalentes equipos.
- Fomentando la participación de todos, sin distinciones de sexo.

- **Educación para el trabajo.** Respecto a este módulo encontramos los siguientes elementos:
  - Técnicas de trabajo en grupo: sujeción a unas reglas corporativas.
  - Colaboración de varias personas para la realización de un único trabajo.

- **Educación para la paz y la convivencia.** Se trabajan los elementos siguientes:
  - Acuerdos para la utilización de los mismos estándares en toda la comunidad internacional.
  - Trabajo en armoniosa colaboración.
  - Respeto por las opiniones de los demás.
  - Aprender a escuchar.

14. Recursos y Bibliografía

a. Recursos Materiales
   i. Equipamiento audiovisual.
      1. Proyector.
   ii. Equipamiento Informático.
      1. PC conectados en red.
      2. 2 Swicth.
      3. 1 Router.
      4. Conexión Inalámbrica.
      5. Servidor.
      6. Impresora láser.
   iii. Materiales escritos.
      1. Apuntes de clase.
      2. Bibliografía relacionada.
      3. Revistas informáticas.

b. Recursos Lógicos
   i. Plataforma educativa Moodle.
   ii. Sistemas Operativos cliente y servidor.

c. Bibliografía
   i. Apuntes del módulo Seguridad Informática de la plataforma Aula Virtual de la Consejería de Educación y Deporte de la Junta de Andalucía
   ii. Seguridad Informática. Editorial MC Graw-Hill.

Autor: Jose Fabián Roa Buendía.
iii. Seguridad Informática. Editorial McMillan.
Autor: Gema Escrivá Gascó, Rosa Mª Romero Serrano, David Jorge Ramada, Ramón Onrubia Pérez.
iv. Prácticas de Seguridad Informática. Dentro del Profesorado de Castilleja de la Cuesta.
Autor: José Luis Núñez Montes.