PROGRAMACIÓN DIDÁCTICA DEL MÓDULO PROFESIONAL

SEGURIDAD INFORMÁTICA

C.F.G.M. Sistemas Microinformáticos y Redes

Curso 2023/2024

Sandra Rodríguez Moreno
IES Aguadulce – Presencial
Aguadulce (Almería)

Contenido

1. Introducción....3
2. Objetivos generales del ciclo....4
2.1. Objetivos generales del ciclo formativo....4
2.2. Competencia general....5
2.3. Competencias profesionales, personales y sociales....5
2.4. Entorno profesional....6
3. Currículo del módulo profesional....6
3.1. Resultados de aprendizaje....7
3.2. Criterios de evaluación....7
4. Contenidos y temporalización....9
4.1. Contenidos....9
4.2. Unidades didácticas....10
4.3. Temporalización....14
5. Materiales didácticos y recursos....14
6. Metodología....14
6.1. Utilización del aula virtual como apoyo a la docencia reglada....15
7. Evaluación....16
7.1. Criterios, estrategias y procedimientos de evaluación....16
7.2. Instrumentos de evaluación....19
7.3. Superación del módulo....19
8. Atención al alumnado con necesidades específicas de atención educativa (NEAE)....20
9. Conexión con los temas transversales....21
10. Planes y programas....21
10.1. Plan de igualdad entre hombres y mujeres....21
10.2. Plan lector....21
10.3. Otros planes....22
11. Actividades extraescolares y complementarias....22
12. Bibliografía de aula y departamento....22
Anexo I. Tabla de RA y CE ponderados....24

1. Introducción

En la redacción de esta programación se han tenido en cuenta normativa diferente que puede agruparse en diferentes ámbitos de más general a más específico.

- **Relacionado con el "Sistema educativo":**
  - **Ley Orgánica 2/2006,** de 3 de mayo, de Educación (LOE).
  - **Ley 17/2007,** de 10 de diciembre, de Educación de Andalucía (LEA).
  - **Ley 3/2020**, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación.
- **Relacionado con la "Formación Profesional":**
  - **Real Decreto 659/2023**, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional que está en vigor pero no detalla las enseñanzas mínimas.
  - **Real Decreto 1147/2011**, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.
  - **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.
  - **Decreto 436/2008,** de 2 de septiembre, por el que se establecen la ordenación y las enseñanzas de la Formación Profesional Inicial que forma parte del Sistema Educativo en la Comunidad Autónoma de Andalucía.
- **Relacionado con "El Ciclo Formativo":**
  - **Real Decreto 1691/2007,** de 14 de diciembre (BOE nº. 15 de 17 enero de 2008) se establece el título de Técnico en Sistemas Microinformáticos y Redes.
  - **Orden EDU/2187/2009,** de 3 de julio, por la que se establece el currículo del ciclo formativo de Grado Medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes.
  - **Orden de 7 de julio de 2009,** por la que se desarrolla el currículo correspondiente al título de Técnico en Sistemas Microinformáticos y Redes en la Comunidad Autónoma de Andalucía.

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

- Denominación: Sistemas Microinformáticos y Redes.
- Nivel: Formación Profesional de Grado Medio.
- Duración: 2.000 horas.
- Familia Profesional: Informática y Comunicaciones.
- Referente europeo: CINE3 (Clasificación Internacional Normalizada de la Educación).

Este módulo se impartirá en el segundo curso del Ciclo Formativo con una carga lectiva de 5 horas semanales, con un total de horas a lo largo del curso de 105.

2. Objetivos generales del ciclo.

2.1. Objetivos generales del ciclo formativo.

Los objetivos generales de este ciclo formativo, especificados en el BOE nº 15 del 17 de enero de 2008, son los siguientes:

1. **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.**
2. 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.
3. **Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.**
4. **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.**
5. **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.**
6. Interconectar equipos informáticos, dispositivos de red local y de conexión con redes de área extensa, ejecutando los procedimientos para instalar y configurar redes locales.
7. **Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.**
8. Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
9. Interpretar y seleccionar información para elaborar documentación técnica y administrativa.
10. **Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.**
11. **Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.**
12. **Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.**
13. **Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.**
14. 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.
15. Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción.

16. Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.
17. Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
18. 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.

El módulo profesional de Seguridad informática contribuya a alcanzar los objetivos generales marcados en negrita.

2.2. Competencia general.

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

2.3. Competencias profesionales, personales y sociales.

Las competencias profesionales, personales y sociales de este título son las 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.
b) Montar y configurar ordenadores y periféricos, asegurando su funcionamiento en condiciones de calidad y seguridad.
c) Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
d) Replantear el cableado y la electrónica de redes locales en pequeños entornos y su conexión con redes de área extensa canalizando a un nivel superior los supuestos que así lo requieran.
e) Instalar y configurar redes locales cableadas, inalámbricas o mixtas y su conexión a redes públicas, 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.
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.
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.
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.
q) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales originados por cambios tecnológicos y organizativos en los procesos productivos.
r) Resolver problemas y tomar decisiones individuales siguiendo las normas y procedimientos establecidos definidos dentro del ámbito de su competencia.
s) Ejercer sus derechos y cumplir con las obligaciones derivadas de las relaciones laborales, de acuerdo con lo establecido en la legislación vigente.
t) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y aprendizaje.
u) Crear y gestionar una pequeña empresa, realizando un estudio de viabilidad de productos, planificación de la producción y comercialización.
v) Participar de forma activa en la vida económica, social y cultural, con una actitud crítica y responsable.

2.4. Entorno profesional.

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

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

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

3. Currículo del módulo profesional.

El Currículo del módulo profesional estará constituido por los resultados de aprendizaje y criterios de evaluación que a continuación se citan:

3.1. Resultados de aprendizaje.

RA1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades.

RA2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información.

RA3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.

RA4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico.

RA5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento.

3.2. Criterios de evaluación.

A continuación, se detallan los criterios de evaluación para cada uno de los resultados de aprendizaje:

RA1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades:

- Se ha valorado la importancia de mantener la información segura.
- Se han descrito las diferencias entre seguridad física y lógica.
- Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.
- Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
- Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
- Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
- Se han indicado las características de una política de seguridad basada en listas de control de acceso.
- Se ha valorado la importancia de establecer una política de contraseñas.
- Se han valorado las ventajas que supone la utilización de sistemas biométricos.

RA2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información:

- Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
- Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad entre otros).
- Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
- Se han descrito las tecnologías de almacenamiento redundante y distribuido.
- Se han seleccionado estrategias para la realización de copias de seguridad.

- Se ha tenido en cuenta la frecuencia y el esquema de rotación.
- Se han realizado copias de seguridad con distintas estrategias.
- Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
- Se han utilizado medios de almacenamiento remotos y extraíbles.
- Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

RA3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático:

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

RA4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico:

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

RA5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento:

- Se ha descrito la legislación sobre protección de datos de carácter personal.
- Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
- Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.

- Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Se han contrastado las normas sobre gestión de seguridad de la información.

4. Contenidos y temporalización.

4.1. Contenidos

A continuación, se detallan los contenidos mínimos, establecidos en la legislación vigente, que los alumnos deberán adquirir para poder superar este módulo.

1. 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.
2. 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.
3. 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.
   - Auditorías de seguridad.
   - Actualización de sistemas y aplicaciones.
4. 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.
5. 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.

4.2. Unidades didácticas.

Dados los contenidos expuestos anteriormente, se propone un desglose de los mismos en las siguientes unidades de trabajo:

UD1. Introducción a la Seguridad Informática.
UD2. Seguridad Física.
UD3. Seguridad Lógica.
UD4. Seguridad del Almacenamiento.
UD5. Criptografía y sus aplicaciones.
UD6. Software Malicioso y medidas de protección contra el Malware.
UD7. Seguridad en Redes.
UD8. Normativa sobre seguridad y Protección de Datos.

A continuación, se detallan para cada unidad de trabajo, los contenidos a impartir en cada una de ellas.

UD1	Introducción a la Seguridad Informática		Nº horas dedicadas	10h
CP	**OG**	**RA**	**Contenidos propuestos y ordenados**	
J,L,O	10,11,12	1	1. Conceptos de seguridad: ▪ Activos, vulnerabilidades, riesgos, amenazas, impactos. ▪ Identificación y tipos de amenazas. ▪ Seguridad física y seguridad lógica. ▪ Seguridad activa y seguridad pasiva. 2. Principios de la seguridad informática: ▪ Confidencialidad, integridad y disponibilidad. ▪ Autenticación/Identificación, no repudio. 3. Políticas de seguridad y planes de contingencia. ▪ Auditoría, mantenimiento.	
CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje				

UD2	Seguridad Física		Nº horas dedicadas	13h
CP	**OG**	**RA**	**Contenidos propuestos y ordenados**	
A,I,J, O	5,10,11,12	1	1. Conceptos de seguridad física ▪ Fenómenos naturales y riesgos humanos 2. Protección física de los equipos. ▪ Protección, aislamiento, ventilación. 3. Sistemas de alimentación ininterrumpida. ▪ SAI/UPS: Tipos, monitorización, PDUs 4. Controles de presencial y acceso. 5. Centros de proceso de datos	

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

UD3	Seguridad Lógica	Nº horas dedicadas	10h

CP	OG	RA	Contenidos propuestos y ordenados
I,J,L, O	5,7,10	1	1. Concepto de seguridad lógica. 2. Acceso a sistemas operativos y aplicaciones. ▪ Contraseñas, Listas de control de acceso 3. Acceso a aplicaciones por Internet. 4. Alternativas de gestión de identidades. ▪ Autenticación y autorización. ▪ Contraseñas de un solo uso, security tokens, identificación biométrica. ▪ Single Sign-On, Identidad federada, OpenId.

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

UD4	Seguridad del Almacenamiento	Nº horas dedicadas	17h

CP	OG	RA	Contenidos propuestos y ordenados
A,C	1,3	2	1. Gestión y Políticas de almacenamiento. ▪ Medidas de seguridad física y seguridad lógica 2. Dispositivos de almacenamiento. ▪ Medios: magnéticos, ópticos, híbridos, electrónicos, otros ▪ Ubicación: locales, externos, remotos. ▪ Almacenamiento redundante y distribuido 3. Tecnologías de almacenamiento redundante y distribuido ▪ RAID 4. Copias de seguridad. ▪ Completas, diferenciales, incrementales. ▪ Frecuencia, recuperación y política de retención. 5. Gestión de imágenes del sistema ▪ Clonación: disco/disco, partición/partición, archivo de imagen 6. Recuperación de datos eliminados

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

UD5	Criptografía y sus aplicaciones	Nº horas dedicadas	10h

CP	OG	RA	Contenidos propuestos y ordenados
A,C,I,J, P	3,11,12	4	1. Introducción a la criptografía. ▪ Criptología, criptografía, criptoanálisis, criptosistema. ▪ Texto plano, mensajes cifrados, conjuntos de claves, transformaciones, de cifrado y descifrado. ▪ Criptosistemas simétricos y asimétricos. Clave secreta y clave pública. 2. Cifrado de clave simétrica

			▪ Cifradores de flujo y de bloque. ▪ Ataque por criptoanálisis, método de fuerza bruta. ▪ Algoritmos: DES, AES, RC5, IDEA 3. Cifrado de clave asimétrica ▪ Autenticación y confidencialidad ▪ Algoritmos: RSA, DSA, ElGamal 4. Algoritmo de cifrado HASH. 5. Sistemas híbridos. ▪ PGP, GnuPG, OpenPGP. 6. Aplicaciones prácticas de la criptografía. 7. Firma digital ▪ Ordinaria, con árbitro ▪ Firma electrónica, firma electrónica avanzada/reconocida. 8. Certificados digitales ▪ Conceptos, autoridades de certificación, solicitud y uso ▪ Clases de certificados 9. DNI electrónico 10. SSL y TLS 11. Cifrado de la información
CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje			

UD6	Software malicioso y medidas de protección contra el malware		Nº horas dedicadas	18h
CP	**OG**	**RA**	**Contenidos propuestos y ordenados**	
A,C,I,J,N,P	**1,3,12,13**	**3**	1. Concepto de software malicioso ▪ Malware. Vulnerabilidades del software. ▪ Vulnerabilidades asociadas a las personas. 2. Clasificación del Malware. ▪ Gusanos, troyanos, virus, adwares, dialers, backdoors, keyloggers, spywares, otros. ▪ Bulos/Hoax, Jokes/bromas ▪ Ramsomware, rogueware, bombas lógicas, password stealers, 3. Denegación de servicio. ▪ Ataques internos/externos 4. Publicidad y correo no deseado ▪ Spam, LSSICE 5. Ingeniería social y fraudes informáticos ▪ Suplantación de identidad. Phising. ▪ Cadenas de correos/mensajes. Correos millonarios 6. Medidas preventivas ▪ Antivirus, antispyware, antirootkit, antimalware. ▪ Suites de seguridad. ▪ Protección, detección, eliminación. ▪ Cortafuegos. Políticas. Clasificación. ▪ Correos electrónicos. 7. Medidas paliativas. ▪ Copias de seguridad, software congelador. 8. Centros de protección y respuesta frente a amenazas ▪ CERT/CSIRT 9. Buenas prácticas ▪ Actualizaciones, antimalware, cuentas, contraseñas, correo, aplicaciones, copias de seguridad, otras medidas.	

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

UD7	Seguridad en redes		Nº horas dedicadas	15h
CP	**OG**	**RA**	**Contenidos propuestos y ordenados**	
C,I,J,L, O	1,3,4,5,7,13	4	1. Vulnerabilidad de los servicios en red ▪ Nivel físico, de enlace, de red, de transporte, de sesión, de presentación y de aplicación. ▪ Ataques de denegación de servicio en redes. 2. Monitorización ▪ Mirroring y networktap. ▪ Herramientas: Wireshark, Ettercap, Ntop, Nagios, PandoraFMS, otras 3. Técnicas de protección ▪ Cortafuegos, DMZ, Detección de intrusos, proxies, UTM, 4. Protección en redes inalámbricas. ▪ Mecanismos de seguridad: WEP, WPA, WPA2 ▪ Filtrado MAC, ocultación SSID 5. Auditoría de seguridad en redes. ▪ Auditoría de red interna, perimetral y de DMZ ▪ Test de intrusión ▪ Auditoría de aplicaciones, análisis forense ▪ Herramientas: enumeración, rastreo, barrido, fingerprinting, análisis de vulnerabilidades, test de penetración	

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

UD8	Normativa sobre seguridad y protección de datos.		Nº horas dedicadas	12h
CP	**OG**	**RA**	**Contenidos propuestos y ordenados**	
J,L,O	11,12	5	1. Protección de datos de carácter personal: ▪ Ley Orgánica de Protección de Datos de Carácter Personal (LOPD). ▪ Reglamento de Medidas de Seguridad (RMS). ▪ Ley de Datos de Carácter Personal. 2. Legislación sobre los servicios de la sociedad de la información y correo electrónico: ▪ Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE). ▪ Ley sobre normas reguladoras de firma electrónica. ▪ Ley sobre el DNI electrónico. 3. Sistemas de gestión de seguridad de la información ▪ Contenido de un SGSI ▪ Implantación de un SGSI	

CP = Competencias profesionales. OG = Objetivos generales. RA = Resultados de aprendizaje

4.3. Temporalización

La duración total del módulo es de 105 horas, a impartir en dos trimestres, y con una carga semanal de 5 horas. La temporalización estimada en cada uno de los trimestres, y la ponderación de las unidades de trabajo es la siguiente:

Unidad de Trabajo	Duración estimada	Temporalización
UD1. Conceptos básicos sobre seguridad informática.	**10 horas**	**1º Trimestre (14 Semanas)**
UD2. Seguridad Física	**13 horas**	
UD3. Seguridad Lógica	**10 horas**	
UD4. Seguridad del Almacenamiento	**17 horas**	
UD5. Criptografía y sus aplicaciones	**10 horas**	
UD6. Software Malicioso y medidas de protección frente al Malware	**18 horas**	**2º Trimestre (10 semanas)**
UD7. Seguridad en redes	**15 horas**	
UD8. Normativa sobre seguridad y protección de datos.	**12 horas**	

5. Materiales didácticos y recursos.

El equipamiento informático con el que se cuenta para este módulo es el siguiente:

- Un aula con 16 ordenadores.
- Ordenador del profesorado.
- Un proyector multimedia.
- Red con acceso a Internet.
- Plataforma Moodle Centros de la Consejería de Educación y Deporte.

Se utilizará también el proyector multimedia para que el alumnado pueda ver directamente en una pantalla grande las instrucciones que hay que realizar con el ordenador para llevar a cabo una tarea determinada.

En la plataforma Moodle como apoyo a la docencia, se pondrá a disposición del alumnado los apuntes y materiales necesarios para el desarrollo de la clase. Además, el alumnado subirá a la misma las tareas y ejercicios propuestos.

En cuanto al material didáctico empleado para el diseño de las actividades a realizar en el aula y de esta programación, se utilizan los apuntes que el profesorado facilita al alumnado.

6. Metodología.

La metodología a seguir deberá ser flexible y dinámica, adaptada en todo momento a objetivos y contenidos, y orientada de manera constante por un proceso de evaluación formativa. Dicha metodología deberá adecuarse en todo momento al tipo de alumnado que se nos presente.

A priori no se descarta ninguno de los recursos metodológicos comúnmente admitidos: charla, ejercicio práctico, debate, conferencia, medios audiovisuales, formulación de problemas, exposición, orientación, trabajos individuales y de grupo, investigación en el medio, visitas técnicas, etc.

En términos generales cabe establecer el siguiente esquema:

- En las cuestiones de contextualización y fundamentos se recurrirá a la exposición, trabajo individual y de grupo, investigación y debate.
- En las más auténticamente procedimentales, la exposición (inicialmente necesaria) se reducirá al mínimo, dando paso de manera inmediata a los ejemplos, ejercicios prácticos, resolución de problemas, realización de trabajos y crítica de los mismos, práctica en ordenador con las herramientas de desarrollo, etc.
- En las de profundización la exposición tomará un papel más relevante, pero sin descuidar en ningún caso los aspectos de aplicación.

De una u otra forma, la metodología tenderá a conseguir progresivamente hábitos de autonomía y autosuficiencia en el alumnado, a través de la resolución de las dificultades que paulatinamente vayan surgiendo, dando especial relevancia a la iniciativa, la lógica, el método, la acumulación de experiencia y la capacidad de reacción; en suma, el desarrollo de habilidades, destrezas y criterios propios que producirán un gradual aumento de la independencia del alumnado respecto del profesor.

La organización del espacio físico tenderá a optimizarlo y adecuarlo a los fines perseguidos.

Se fomentará la lectura realizando lecturas sobre unidades o artículos relacionados con los temas que se traten en cada momento.

Por último, a modo de síntesis y sin perjuicio del necesario rigor conceptual, se tendrá siempre presente la consideración de que lo importante es desarrollar las capacidades para abordar realizaciones prácticas similares a aquellas que se va a tener que afrontar en la vida profesional, una vez concluida la etapa formativa.

6.1. Utilización del aula virtual como apoyo a la docencia reglada.

A lo largo del curso se utilizará el Aula Virtual como apoyo a la docencia reglada. Se fomentará un mayor uso conforme el alumnado vaya promocionando de curso. En general, su utilización responderá a las siguientes pautas:

- Se definirá la estructura del curso en unidades, temas, secciones, etc.
- Se procurará que el desarrollo de los contenidos del curso esté disponible en el Aula Virtual, sobre todo en los niveles en los que no se disponga de un libro de texto o materiales de referencia.
- Se proporcionarán recursos educativos para el tratamiento de los contenidos programados (documentos explicativos, materiales audiovisuales, cuestionarios, actividades resueltas, recursos de refuerzo y de ampliación, modelos de pruebas, etc.).
- Se podrán establecer tareas y otras actividades de evaluación cuya entrega quede registrada en el Aula Virtual.

7. Evaluación

7.1. Criterios, estrategias y procedimientos de evaluación.

La evaluación, en sus diversas vertientes, constituye un análisis de los factores y elementos que intervienen en el proceso educativo, valorando su adecuación y eficacia. En función del momento en que se realice, se puede distinguir:

a) **Evaluación inicial**. Se realiza antes de comenzar el proceso de enseñanza-aprendizaje y su finalidad será obtener un diagnóstico previo sobre ideas y conocimientos previos del alumnado, su nivel inicial y posibles dificultades de aprendizaje.
   El módulo de Seguridad informática está formado por 12 alumnos. Partiendo de los resultados obtenidos en la evaluación inicial, podemos afirmar que el nivel de conocimientos relacionados directamente con el módulo del grupo es medio-bajo. No se distinguen diferencias significativas entre el alumnado, conformando un grupo más o menos homogéneo.
   Referente al ritmo de aprendizaje y/o capacidades intelectuales, la mayoría del alumnado estaría en un nivel normal, existiendo un conjunto pequeño de alumnos con un nivel de aprendizaje más bajo.
   La motivación del alumnado y el interés por el aprendizaje puede ser considerada como media. La mayoría del alumnado tiene como motivación para finalizar sus estudios, el continuarlos con un ciclo formativo de grado superior.
   Se puede concluir diciendo que el grupo es homogéneo, está cohesionado, es colaborativo, tiene una actitud un poco distraída y deben prestar más atención.
b) **Evaluación formativa**. Esta evaluación será continua, realizándose un seguimiento constante de los progresos del alumnado, teniendo en cuenta sus capacidades, el interés manifestado, el esfuerzo realizado y los criterios de evaluación que marca la legislación.
c) **Evaluación sumativa**. Tiene por objeto medir el resultado al finalizar el proceso de enseñanza-aprendizaje.

Los resultados de aprendizaje expresan en forma de resultados, que deben ser alcanzados por el alumnado, los aspectos básicos de la competencia profesional y del nivel de formación que acredita el título. Caracterizan y establecen la validez del título en todo el territorio del Estado, y determinan la cualificación mínima del mismo que debe ser alcanzada por todas las administraciones educativas, a fin de conseguir la preparación profesional básica y su necesario grado de homogeneidad. Cabría pues plantearse su adaptación al entorno circundante, con objeto de reflejar su realidad y mejorar las expectativas del alumnado. La evaluación será continua, realizándose un seguimiento constante de los progresos del alumnado. Además, se tendrán en cuenta sus capacidades, el interés manifestado, el esfuerzo realizado y los criterios de evaluación que marca la legislación.

Referencia normativa:

La Orden de 29 de septiembre de 2010, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía, establece en su Artículo 2, Apartado 5, que el departamento de

familia profesional, a través del equipo educativo de cada uno de los ciclos formativos, desarrollará el currículo mediante la elaboración de las correspondientes programaciones didácticas de los módulos profesionales. Su elaboración se realizará siguiendo las directrices marcadas en el proyecto educativo del centro, especialmente en lo referente a Los procedimientos y criterios de evaluación comunes para las enseñanzas de formación profesional inicial.

El Departamento de Informática, a través del equipo educativo del ciclo SMR, propone lo siguiente en relación a la evaluación del ciclo formativo para su inclusión en el Proyecto Educativo del centro como ítems generales de partida en el proceso de evaluación que serán concretados en el apartado de criterios de evaluación e instrumentos de evaluación de cada módulo:

LA EVALUACIÓN DEL CICLO FORMATIVO.

Procedimientos y criterios de evaluación comunes para las enseñanzas de formación profesional inicial.

La aprobación del módulo requerirá la superación de todos los resultados de aprendizaje del mismo. La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación. Los pesos de los criterios de evaluación se repartirán en función de su importancia dentro el criterio de evaluación. Además, cada criterio de evaluación podrá participar en distintos instrumentos, repartiéndose su peso de forma proporcional o ponderada entre dichos instrumentos.

En el anexo I se adjunta la tabla con todos los resultados de aprendizaje relacionados con sus correspondientes criterios de evaluación y sus ponderaciones. También se indica en qué instrumentos participarán dichos criterios de evaluación.

Instrumentos de evaluación.

- Se evaluarán los siguientes ítems:
  - Tareas y actividades.
  - Tareas de ampliación (voluntarias).
  - Competencias personales y sociales. Se evaluarán las establecidas para cada módulo en la orden que desarrolla el currículo, así como la participación en clase.
  - Pruebas teóricas y/o prácticas.

Calificaciones

- Para aprobar el módulo la nota media ponderada final debe ser superior o igual a 5 (sobre 10).
- La ponderación de los ítems se establecerá en la programación de cada módulo.
- A efectos de cómputo de la nota final de cada módulo, la calificación mínima de cada ítem evaluable será establecida dentro de la programación de cada módulo. Si no se alcanzara la calificación mínima establecida dentro de la programación para uno o más de los ítems, la calificación máxima alcanzable será de 4.
- La información sobre objetivos, contenidos y criterios de evaluación y calificación será facilitada por el profesorado de cada módulo profesional al alumnado durante el primer trimestre del curso académico.

Criterios de calificación - Redondeo

Cuando el alumnado tenga una nota superior a cinco, las calificaciones finales que arrojen números decimales se redondearán a la unidad, eliminando la parte decimal y aproximando la unidad a la más cercana. De este modo, si la parte decimal fuera inferior a 0,500 se aproximará a la unidad inferior. Si esta fuera igual o superior a 0,500, se aproximará a la unidad superior.

Para el cálculo de la calificación final se tomará la nota real obtenida en cada evaluación, y no su expresión en el número entero consignado en la aplicación Séneca al término de cada uno de los trimestres.

Período final de recuperación / mejora de calificaciones.

El período final de recuperación o mejora de calificaciones, se utilizará para que el alumnado alcance los resultados de aprendizaje no superados o los mejore en su caso. La nota final se obtendrá teniendo en cuenta todo el trabajo hecho durante el curso, pero considerando las notas "recuperadas" en lugar de las notas suspensas originales.

Por tanto, no hay que establecer criterios de evaluación diferentes para ese período, sino que durante el mismo el alumnado podrá:

- Volver a ser evaluado de los resultados de aprendizaje no superados, a través de los ítems evaluables anteriormente descritos.
- Realizar las tareas que estén suspensas o no entregadas, o realizar otras tareas donde se evalúen los resultados de aprendizaje no superados.
- Obtener notas de mejora de sus competencias personales y sociales o participación en clase, que permita mejorar la nota en ese apartado.

De acuerdo con la Orden de 29 de septiembre de 2010, el carácter de la evaluación será continua por tanto la asistencia del alumnado durante todo este periodo de recuperación es obligatoria.

"En caso de comprobarse que el alumno no ha realizado su trabajo (cuestionario, tarea, etc.) de manera legítima (copia de otro compañero, falsificación de resultados, plagio de otras fuentes, etc.), tendrá una puntuación de un 0 en dicho trabajo. Para asegurarse de esto, el profesorado podrá hacer las comprobaciones y preguntas que considere convenientes pudiendo exigir si fuera necesario una defensa de su trabajo. Este tipo de comportamientos no estarán exentos de otras medidas disciplinarias que se puedan acometer en función de la gravedad del acto realizado".

Criterios de corrección en la expresión escrita.

Tal y como se establece en el Proyecto Educativo del Instituto, los aspectos formales de la expresión escrita serán objeto de valoración por parte de todos los departamentos didácticos en las diferentes pruebas que realice el alumnado.

En los Ciclos Formativos se podrá restar hasta 1 punto de la nota, atendiendo a los errores cometidos en los parámetros siguientes:

- Presentación digital o manuscrita: márgenes, numeración de páginas, letra clara y legible, limpieza, ausencia de tachones, uso del bolígrafo o herramienta adecuada.

- Redacción: falta de coherencia y cohesión, estructuración mediante párrafos, conectores, oraciones completas, puntuación (comas y puntos), concordancia.
- Ortografía: faltas ortográficas, tildes, subrayado de títulos de libros, mayúsculas.
- Extensión: cuando el texto no se ajuste significativamente a la extensión solicitada.

7.2. Instrumentos de evaluación.

Los instrumentos de evaluación del alumnado serán la observación sistemática, la observación directa, exposición y la realización de trabajos. El seguimiento individual del alumno o alumna se llevará a cabo a través del trabajo diario de clase, la realización de ejercicios individuales, las preguntas individualizadas y la realización de supuestos prácticos. El seguimiento del alumno o alumna como miembro de un grupo se hará con el trabajo diario, ejercicios del grupo, preguntas y supuestos.

Se recurrirá básicamente al trabajo práctico con y sin herramientas de desarrollo (tanto individual como por parejas, con o sin la posterior defensa), resolución de problemas y ejercicios sobre aspectos parciales. Se realizarán pruebas escritas a fin de valorar el grado de adquisición de los contenidos por parte del alumnado. Además, el alumnado recogerá la teoría y problemas expuestos en clase, y esta podrá ser revisada puntualmente por el profesor y las puntuaciones obtenidas formarían parte de la nota final.

Se valorará la iniciativa, originalidad y participación del alumnado, la exactitud y precisión en el desarrollo de los ejercicios y prácticas realizadas.

7.3. Superación del módulo.

Para conseguir la superación del módulo de Seguridad Informática, se tendrán en cuenta los criterios de evaluación antes mencionados, que se traducirán en actividades específicas, con su correspondiente componente práctico. Cada R.A. tendrá un peso en el módulo y a la vez cada uno de los R.A. se conseguirá superando los criterios de evaluación asociados, cada uno de los cuales tiene un peso en el cómputo total de la nota final del módulo.

El peso de cada uno de los R.A. es el siguiente:

- **R.A. 1: 22%**
- **R.A. 2: 23%**
- **R.A. 3: 20%**
- **R.A. 4: 29%**
- **R.A. 5: 6%**

En el anexo I se muestra la tabla donde se relacionan resultados de aprendizaje y criterios de evaluación indicando peso para cada resultado de aprendizaje y criterio de evaluación.

Dado el carácter abierto y flexible de esta programación, los instrumentos de evaluación podrán variar en función del ritmo y/o necesidades del grupo de clase, pudiendo si fuera preciso evaluar un mismo criterio con un instrumento sólo 100%, dos instrumentos de evaluación en cuyo caso ponderará cada instrumento al 50%, y si fueran tres al 33% cada uno de ellos. Todos los porcentajes aplicables sobre el peso total atribuible a dicho CE.

La tabla mostrada en el anexo I es una aproximación de la planificación inicial del curso que puede verse alterada en función del desarrollo del mismo y de las necesidades del proceso enseñanza-aprendizaje del alumnado, principalmente en los instrumentos evaluación a utilizar.

Para aprobar una evaluación será necesario obtener una nota igual o superior a 5, se podrá hacer media de los diferentes R.A. si estos tienen una nota mínima de 4. En caso de no llegar al 4 en alguno de los R.A. la nota máxima obtenible será de 4.

La expresión de cada una de las evaluaciones se realizará en forma de calificaciones numéricas comprendidas entre 1 y 10 sin decimales, considerándose positivas las calificaciones iguales o superiores a 5 y negativas las restantes.

Si se obtiene una calificación igual o superior a 5, el módulo se considerará apto y en caso contrario no apto.

La nota de cada Resultado de Aprendizaje (R.A.), se obtendrán en función de la ponderación de los criterios de evaluación asociados al mismo.

Si el alumnado no supera algún R.A. deberá presentarse a las pruebas de recuperación que se podrán realizar en los próximos trimestres. Quedando la nota del trimestre suspensa hasta que no recupere los R.A. asociados a dicho trimestre.

Además, deberá entregar las prácticas pendientes.

La nota de cada evaluación se obtendrá de la ponderación de los criterios de evaluación (C.E.) vistos en cada trimestre.

La nota de la evaluación final se obtendrá de la ponderación de todos los C.E. asociados a cada R.A.

8. Atención al alumnado con necesidades específicas de atención educativa (NEAE).

Se debe regular la atención a los alumnos y alumnas con necesidades específicas de atención educativas. Por este motivo en este módulo se tendrán en cuenta, en caso de necesidad, la utilización del material adecuado para los alumnos y alumnas con deficiencias auditivas, visuales o motoras.

- Para los alumnos o alumnas con deficiencia visual se adaptarán el hardware y el software a sus necesidades.
- Los alumnos o alumnas con deficiencia motora estarán ubicados en las mesas y sillas que pertinentemente se soliciten a tal efecto.

- Para los alumnos/as con TDAH se remite al documento que se encuentra en el departamento de orientación de este centro.
- Para las posibles adaptaciones NO SIGNIFICATIVAS se cambiará la metodología adaptándola a las necesidades del alumnado.

9. Conexión con los temas transversales.

Durante el desarrollo de este módulo profesional se intentará fomentar en los alumnos y alumnas actitudes relacionadas con:

- La educación para la igualdad entre los sexos, mediante trabajos con grupos mixtos.
- La educación para el cuidado del medio ambiente, mediante reciclado de papel y tóner.
- La educación moral y cívica, mediante una actitud de respeto en clase.
- La educación para la salud, mediante ergonomía y hábitos posturales.

10. Planes y programas.

10.1. Plan de igualdad entre hombres y mujeres.

Teniendo en cuenta el alumnado al que se le imparte este módulo, y la presencia mínima de alumnas en el mismo, es complicado llevar a cabo este punto, no obstante, se trabaja ponderando la labor y la figura de la mujer en la sociedad. Las medidas que se tomarán serán las siguientes:

- Visibilizar el papel de la mujer: se destacarán las figuras femeninas que han contribuido en el desarrollo de la materia, en nuestro caso en Informática.
- Utilizar el lenguaje igualitario, inclusivo, y no sexista: se utilizará la lengua tanto oral como escrita para nombrar una realidad que no excluya a las mujeres, en concreto, haciendo hincapié en las exposiciones diarias del alumnado.
- Evitar estereotipos: se evitarán los estereotipos asociados al sexo, en concreto, explicando todas aquellas situaciones que se planteen a lo largo del curso.
- Participación en las actividades del plan de Igualdad: se instará a participar en talleres, charlas, presentaciones, etc., que se realicen en el centro para la consecución de la plena igualdad entre hombres y mujeres.

10.2. Plan lector.

Desde el módulo de Seguridad Informática fomentamos la lectura de las siguientes formas:

- Realización de prácticas sobre texto de actualidad (periódicos digitales, prensa escrita, manuales de informática).

Como lecturas recomendadas:

- Prensa escrita y digital.
- Manuales digitales de Seguridad Informática, vídeos sobre seguridad, foros de actualidad, etc.

10.3. Otros planes.

Como se ha venido realizando en cursos anteriores, este año se realizarán talleres orientados a mejorar la empleabilidad del alumnado, como son el programa INNICIA.

11. Actividades extraescolares y complementarias.

En el presente curso está previsto realizar visitas a empresas relacionadas con las TIC y el desarrollo de aplicaciones, la participación en las Jornadas Oriéntate 2024 así como la posibilidad de asistir a seminarios en la Universidad de Almería.

Durante el primer trimestre también se planifica una actividad consistente en la asistencia a AndaluciaSkills.

12. Bibliografía de aula y departamento.

- Seguridad Informática. Costas Santos, Jesús. 2010. Editorial Ra-Ma.
- Seguridad en Sistemas Operativos Windows y Linux. Gómez López, Julio y otros. 2011. Editorial Ra-Ma
- Seguridad Informática. Triviño, Ignacio. 2019. Editorial Síntesis.
- Material aportado por el profesorado.

Anexo I. Tabla de RA y CE ponderados

RA	CE	Peso CE	TR/PR	EX
RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades. **[22%]**	a) Se ha valorado la importancia de mantener la información segura.	**2%**	X	X
	b) Se han descrito las diferencias entre seguridad física y lógica.	**2%**	X	X
	c) Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.	**3%**	X	X
	d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	**2%**	-	X
	e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	**3%**	X	-
	f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	**2%**	X	-
	g) Se han indicado las características de una política de seguridad basada en listas de control de acceso.	**3%**	X	X
	h) Se ha valorado la importancia de establecer una política de contraseñas.	**3%**	X	X
	i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	**2%**	X	X
RA	**CE**	**Peso CE**	**TR/PR**	**EX**
RA2. Gestiona dispositivos de almacenamiento, describiendo los procedimientos efectuados y aplica técnicas para asegurar la integridad de la información. [23%]	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	**1%**	-	X
	b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad entre otros).	**1%**	-	X
	c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.	**2%**	-	X
	d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	**3%**	-	X
	e) Se han seleccionado estrategias para la realización de copias de seguridad.	**2%**	X	X
	f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.	**1%**	X	X
	g) Se han realizado copias de seguridad con distintas estrategias.	**4%**	X	-
	h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.	**2%**	X	X
	i) Se han utilizado medios de almacenamiento remotos y extraíbles.	**3%**	X	-
	j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	**4%**	X	-

RA	CE	Peso CE	TR/PR	EX
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático. [20%]	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.	**1%**	-	X
	b) Se han clasificado los principales tipos de software malicioso.	**2%**	-	X
	c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.	**3%**	X	X
	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.	**3%**	X	X
	e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	**6%**	X	X
	f) Se han aplicado técnicas de recuperación de datos.	**5%**	X	-
RA	**CE**	**Peso CE**	**TR/PR**	**EX**
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico. [29%]	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.	**3%**	-	X
	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.	**3%**	X	X
	c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	**3%**	-	X
	d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	**3%**	X	X
	e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	**4%**	-	X
	f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	**3%**	-	X
	g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	**3%**	X	X
	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	**7%**	X	X

RA	CE	Peso CE	TR/PR	EX
RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento. [6%]	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	**1%**	X	X
	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	**1%**	X	X
	c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	**1%**	X	X
	d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	**1%**	X	X
	e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	**1%**	X	X
	f) Se han contrastado las normas sobre gestión de seguridad de la información.	**1%**	X	X
RA	**CE**	**Peso CE**	**TR/PR**	**EX**