

Programación Seguridad Informática 2024-25

Seguridad Informática

La **normativa de referencia** a tener en cuenta para la elaboración de la programación didáctica del módulo es la siguiente:

Esta programación se basa también en el RD. 1147/11 por el que se establece la ordenación general de la formación profesional del sistema educativo y en la Ley Orgánica 5/2002, de 19 de junio, de Cualificaciones y Formación Profesional, a través de las cuales se ha producido una reforma de la Formación Profesional. Además, se tendrán en cuenta el Decreto 436/2008, de 2 de septiembre, por el que se establece la ordenación y las enseñanzas de la Formación Profesional inicial que forma parte del sistema educativo, así como 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.

El Ciclo Formativo de Sistemas Microinformáticos y Redes (SMR) queda regulado por:

- [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.
- [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.
- [Orden de 28 de septiembre de 2011](#), por la que se regulan los módulos profesionales de formación en centros de trabajo y de proyecto para el alumnado matriculado en centros docentes de la Comunidad Autónoma de Andalucía.
- [Real Decreto 499/2024, de 21 de mayo](#), por el que se modifican determinados reales

decretos por los que se establecen títulos de Formación Profesional de grado medio y se fijan sus enseñanzas mínimas.

1.- Competencias, objetivos y resultados de aprendizaje

En las siguientes páginas enumeraremos, con relación a este módulo profesional:

- Competencias profesionales, personales y sociales
- Objetivos generales
- Resultados de aprendizaje

1.1.- Competencias profesionales, personales y sociales

Este módulo profesional contribuye a la adquisición de las Competencias Profesionales, Personales y Sociales siguientes:

- Relación de Competencias profesionales, personales y sociales, respetando la letra con la que se relaciona en la Orden que regula el ciclo formativo en Andalucía:
 - 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.

De todas estas, la formación del módulo de Seguridad Informática contribuye a alcanzar las siguientes competencias profesionales, personales y sociales: a), d), e), f), g), j), m), n), r)

1.2.- Objetivos generales

Este módulo profesional contribuye a la adquisición de los **Objetivos Generales** siguientes:

- Relación de Objetivos generales, respetando la letra con la que se relaciona en la Orden que regula el ciclo formativo en Andalucía:
 - 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 la red.
 - e) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
 - f) Interconectar equipos informáticos, dispositivos de 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.

La formación de nuestro módulo contribuye a alcanzar los objetivos generales de este ciclo formativo, tal como se indica en la Orden que regula el título, que se relacionan a continuación:

- a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
- c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
- d) Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de la red.
- f) Interconectar equipos informáticos, dispositivos de 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.
- ñ) Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción

1.3.- Resultados de aprendizaje

Finalmente, pasamos a desglosar los **Resultados de Aprendizaje** (abreviado RA) a los que contribuye este módulo profesional según la Orden que regula este ciclo formativo.

- 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.

2.- Unidades de Trabajo

El módulo profesional lo compone un total de 6 Unidades de Trabajo:

UNIDAD DE TRABAJO	TEMPORALIZACIÓN	PONDERACIÓN (%)	RA
UT01: Introducción a la seguridad informática. Legislación y normativa.	14h.	13,3%	1 5
UT02: Seguridad en el entorno físico.	28h.	26,7%	1
UT03: Seguridad en el hardware. Almacenamiento y recuperación de los datos.	18h.	17,1%	2
UT04: Sistemas de identificación. Criptografía.	18h.	17,1%	4
UT05: Amenazas y seguridad del software.	17h.	16,2%	3
UT06: Redes seguras.	10h.	9,5%	4

UT01: Introducción a la seguridad informática. Legislación y normativa

RA	Criterios de evaluación	Contenidos propuestos
<p>RA1</p> <p>Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.</p> <p>RA5</p> <p>Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.</p>	<p>CRITERIOS DE EVALUACIÓN DEL RA1</p> <p>a. Se ha valorado la importancia de mantener la información segura.</p> <p>b. Se han descrito las diferencias entre seguridad física y lógica.</p> <p>c. Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.</p> <p>d. Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.</p> <p>e. Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.</p> <p>f. Se han seleccionado los puntos de aplicación de los sistemas de alimentación</p>	<p>1.- Introducción a la seguridad informática.</p> <p>2.- Clasificación de seguridad.</p> <p>2.1.- Seguridad activa y pasiva.</p> <p>2.2.- Seguridad física y lógica.</p> <p>3.- Objetivos de la seguridad informática.</p> <p>3.1.- Principales aspectos de seguridad.</p> <p>4.- Amenazas y fraudes en los sistemas de información.</p> <p>4.1.- Vulnerabilidades, amenazas y ataques.</p> <p>4.2.- Tipos de ataques.</p> <p>4.3.- Mecanismos de seguridad.</p> <p>5.- Gestión de riesgos.</p> <p>5.1.- Proceso de estimación de riesgos.</p> <p>5.2.- Políticas de seguridad.</p> <p>5.3.- Auditorías.</p> <p>5.4.- Plan de contingencias.</p> <p>6.- Legislación: LOPD.</p>

	<p>ininterrumpida.</p> <p>g. Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.</p> <p>h. Se ha valorado la importancia de establecer una política de contraseñas.</p> <p>i. Se han valorado las ventajas que supone la utilización de sistemas biométricos</p> <p>CRITERIOS DE EVALUACIÓN DEL RA5</p> <p>a. Se ha descrito la legislación sobre protección de datos de carácter personal.</p> <p>b. Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.</p> <p>c. Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.</p> <p>d. Se ha contrastado la obligación de poner a disposición de las personas los datos</p>	<p>6.1.- Ámbito de aplicación.</p> <p>6.2.- Agencia española de protección de datos.</p> <p>6.3.- Derechos ARCO.</p> <p>6.4.- Niveles de seguridad y medidas asociadas.</p> <p>6.5.- Infracciones y sanciones.</p> <p>7.- Legislación: LSSI.</p> <p>7.1.- Ámbito de aplicación.</p> <p>7.2.- Obligaciones de las empresas.</p> <p>8.- Legislación: Derechos de autor.</p> <p>8.1.- Ley de Propiedad Intelectual.</p> <p>8.2.- Copyright y copyleft.</p> <p>8.3.- Licencias Creative Commons.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>personales que les conciernen.</p> <p>e. Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.</p> <p>f. Se han contrastado las normas sobre gestión de seguridad de la información.</p>	
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

UT02: Seguridad en el entorno físico.

RA 1	Criterios de evaluación	Contenidos propuestos
<p>Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades</p>	<p>a) Se ha valorado la importancia de mantener la información segura.</p> <p>b) Se han descrito las diferencias entre seguridad física y lógica.</p> <p>c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.</p> <p>d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.</p> <p>e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.</p> <p>f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.</p> <p>g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.</p> <p>h) Se ha valorado la importancia de establecer una política de contraseñas.</p> <p>i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.</p>	<p>1.- Seguridad en el entorno físico.</p> <p>1.1.- Acceso de personas al recinto.</p> <p>1.2.- Alarma contra intrusos.</p> <p>1.3.- Instalación eléctrica.</p> <p>1.4.- Seguridad de materiales eléctricos y protección de personas frente a la electricidad.</p> <p>1.5.- Condiciones ambientales: Humedad y temperatura</p> <p>1.6.- Enemigos de los ordenadores: Partículas de polvo, agua y fuego</p> <p>2.- Centro de proceso de datos y su entorno físico.</p> <p>2.1.- Infraestructura.</p> <p>2.2.- Acceso.</p> <p>2.3.- Redundancia.</p> <p>3.- Sistemas de control de acceso.</p> <p>3.1.- Personal de vigilancia y control</p> <p>3.2.- Dispositivos de</p>

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.

4.5.- Elementos de las políticas de seguridad

--	--	--

UT03: Seguridad en el hardware. Almacenamiento y recuperación de datos.

RA2	Criterios de evaluación	Contenidos propuestos
<p>Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.</p>	<p>a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.</p> <p>b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).</p> <p>c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.</p> <p>d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.</p> <p>e) Se han seleccionado estrategias para la realización de copias de seguridad.</p> <p>f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.</p> <p>g) Se han realizado copias de seguridad con distintas estrategias.</p> <p>h) Se han identificado las</p>	<p>1.- Introducción a la seguridad en el hardware.</p> <p>1.1.- Monitorización del hardware.</p> <p>2.- Sistemas de alimentación ininterrumpida.</p> <p>2.1.- ¿Qué es un SAI?</p> <p>2.2.- Tipos de SAI.</p> <p>3.- Almacenamiento redundante.</p> <p>3.1.- Sistemas de tolerancia a fallos y seguridad física redundante.</p> <p>3.2.- Sistemas RAID.</p> <p>3.3.- Configuraciones o niveles RAID básicos.</p> <p>3.4.- Configuraciones o niveles RAID avanzados.</p> <p>3.5.- RAID en Windows.</p> <p>4.- Clusters de servidores.</p>

	<p>características de los medios de almacenamiento remotos y extraíbles.</p> <p>i) Se han utilizado medios de almacenamiento remotos y extraíbles.</p> <p>j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento</p>	<p>4.1.- Clasificación de los clusters.</p> <p>4.2.- Componentes de un cluster.</p> <p>5.- Almacenamiento externo.</p> <p>5.1.- Cloud Computing.</p> <p>5.2.- NAS.</p> <p>5.3.- SAN.</p> <p>6.- Copias de seguridad.</p> <p>6.1.- Políticas de copias de seguridad.</p> <p>6.2.- Clasificación.</p> <p>6.3.- Copia de seguridad del registro.</p> <p>6.4.- Copia de seguridad de datos en Windows.</p> <p>6.5.- Copia de seguridad de datos en Linux.</p> <p>7.- Recuperación de datos.</p> <p>7.1.- Software de recuperación de datos.</p> <p>7.2.- Creación de imágenes del sistema.</p> <p>7.3.- Restauración del sistema.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

UT04: Sistemas de identificación. Criptografía.

RA4	Criterios de evaluación	Contenidos propuestos
Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	<p>a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.</p> <p>b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.</p> <p>c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.</p> <p>d) Se han aplicado medidas para evitar la monitorización de redes cableadas.</p> <p>e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.</p> <p>f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.</p> <p>g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.</p> <p>h) Se ha instalado y configurado un</p>	<p>1.- Introducción a la criptografia</p> <p>1.1.- Aspectos de seguridad.</p> <p>1.2.- Concepto de criptografía.</p> <p>1.3.- Historia</p> <p>2.- Técnicas criptográficas</p> <p>2.1.- Criptografía simétrica.</p> <p>2.2.- Inconvenientes de la criptografía simétrica.</p> <p>2.3.- Criptografía de clave pública.</p> <p>2.4.- Firmas digitales.</p> <p>2.5.- Funciones 'hash'.</p> <p>2.6.- Sobres digitales.</p> <p>3.- Certificados digitales.</p> <p>3.1.- Autoridades de certificación.</p> <p>3.2.- Obtener un certificado digital en España.</p> <p>3.3.- PKI.</p> <p>4.- Herramienta GPG en Linux.</p> <p>4.1.- Comandos para el cifrado simétrico.</p> <p>4.2.- Comandos para el cifrado asimétrico (de</p>

	cortafuegos en un equipo o servidor	clave pública).
--	-------------------------------------	-----------------

UT05: Amenazas y seguridad del software

RA3	Criterios de evaluación	Contenidos propuestos
<p>Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático..</p>	<p>a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.</p> <p>b) Se han clasificado los principales tipos de software malicioso.</p> <p>c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.</p> <p>d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.</p> <p>e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.</p> <p>f) Se han aplicado técnicas de recuperación de datos</p>	<p>1.- Fraudes informáticos y robos de información.</p> <p>1.1.- Introducción.</p> <p>1.2.- Software que vulnera la seguridad.</p> <p>1.3.- Vulnerabilidad del software.</p> <p>1.4.- Tipos de ataques.</p> <p>1.5.- Atacantes.</p> <p>1.6.- Fraude en Internet.</p> <p>2.- Control de acceso a la información.</p> <p>2.1.- En el sistema operativo.</p> <p>2.2.- Control de acceso a la información.</p> <p>2.3.- Monitorización del sistema.</p> <p>2.4.- Recursos de seguridad en el sistema operativo.</p> <p>3.- Seguridad en redes.</p> <p>3.1.- Protocolos seguros.</p> <p>3.2.- Seguridad en redes cableadas.</p> <p>3.3.- Seguridad en redes inalámbricas.</p>

		<ul style="list-style-type: none">4.- Seguridad activa.<ul style="list-style-type: none">4.1.- Antivirus.4.2.- Antimalware.4.3.- Congelación.4.4.- Correo.4.5.- Contraseñas seguras.4.6.- Firewall o cortafuegos en equipos
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

UT06: Redes seguras

RA4	Criterios de evaluación	Contenidos propuestos
Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	<p>a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.</p> <p>b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.</p> <p>c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.</p> <p>d) Se han aplicado medidas para evitar la monitorización de redes cableadas.</p> <p>e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.</p> <p>f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.</p> <p>g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.</p> <p>h) Se ha instalado y configurado</p>	<p>1.- Redes seguras.</p> <p>1.1.- Niveles OSI.</p> <p>1.1.1.- Seguridad en las capas.</p> <p>1.2.- Redes Privadas Virtuales.</p> <p>1.2.1.- Introducción a las Redes Privadas Virtuales.</p> <p>1.2.2.- Analogía: Cada LAN es una isla.</p> <p>1.2.3.- ¿Qué hace una VPN?</p> <p>1.2.4.- VPN de acceso remoto y VPN punto a punto.</p> <p>1.2.5.- Mantener el tráfico en el túnel VPN.</p> <p>1.2.6.- Encriptación y protocolos de seguridad en una red privada virtual</p> <p>2.- Cortafuegos o Firewall.</p> <p>2.1.- Tipos de Cortafuegos.</p> <p>2.2.- Arquitecturas de firewall.</p>

un cortafuegos en un equipo o servidor

2.3.- DMZI sistema operativo Windows.

3.- Proxy.

3.1.- Funcionamiento y características.

3.2.- Proxy web y Proxy Caché.

3.3.- Proxy en Windows.

3.3.1.- Proxy en Windows. Wingate.

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

3.- Secuencias de unidades de trabajo y temporalización

Las fechas previstas para cada unidad son las siguientes:

Unidad de trabajo	Días a emplear para la unidad (recomendación)	Fecha de apertura	Fecha de finalización (recomendación)	Fecha TOPE para entregar la tarea (incluyendo 2º envío si fuera necesario)	
UD01: Introducción a la seguridad informática. Legislación y normativa	14	15/09/25	17/10/25	30/01/26	1'
UD02: Seguridad en el entorno físico.	28	20/10/25	09/12/25	30/01/26	1'
UD03: Seguridad en el hardware. Almacenamiento y recuperación de los datos	18	10/12/25	20/01/26	30/01/26	1'
UD04: Sistemas de identificación. Criptografía.	18	02/02/26	13/03/26	29/05/26	2'
UD05: Amenazas y seguridad del software.	17	16/03/26	30/04/26	29/05/26	2'

UD06: Redes seguras.	10	05/05/26	19/05/26	29/05/26	2'
----------------------	----	----------	----------	----------	----

Aclaraciones:

- **Unidad de trabajo:** Nombre de la unidad que corresponde con un Resultado de Aprendizaje
- **Días a emplear para la unidad:** Son los días estimados para el desarrollo de la unidad didáctica.
- **Fecha de apertura:** Es la fecha en la que estarán disponibles los materiales de la unidad de trabajo. La primera unidad no estará disponible hasta que no se realice el cuestionario de conocimientos previos.
- **Fecha de finalización:** Es la fecha orientativa en la que el alumnado terminará los contenidos de la unidad. Se recomienda entregar la tarea cuando se termina la unidad.
- **Fecha TOPE para entregar la tarea:** Esta fecha indica el límite de entrega de tarea indica el último día que se recogerán las tareas indicadas, incluido el segundo envío en caso de que fuera necesario. Después de esta fecha no se recogerán más tareas. Por tanto, se recomienda su entrega al menos una semana antes de la fecha indicada como límite para tener la posibilidad de un segundo envío. No se aceptará ningún envío de tareas fuera de plazos indicados, salvo circunstancias excepcionales, que valorará el profesorado previa acreditación documental de las mismas.
- **Cuatrimestre:** Corresponde al cuatrimestre en el que serán vistos los contenidos. El primer cuatrimestre serán los meses comprendidos entre septiembre-enero y el 2º Cuatrimestre los meses comprendidos entre febrero-mayo.

4.- Metodología y materiales didácticos

El alumnado, a través de los contenidos que se le ofrece a lo largo del curso, irá adquiriendo los conceptos básicos para introducirse en el módulo. Las actividades de autoevaluación y las tareas afianzarán y concretarán su aprendizaje funcional.

Las tareas serán evaluadas bajo unos criterios que atenderán a la naturaleza de cada tarea y serán puestos a disposición del alumnado para su conocimiento.

Se suscitará el debate y la puesta en común de ideas, mediante la participación activa del alumnado a través del foro y del correo, respetando la pluralidad de opinión.

Se propiciará que el alumnado sea sujeto activo de su propio aprendizaje, intentando igualmente fomentar el trabajo y la participación.

Para la parte presencial del módulo profesional el profesorado fijará los siguientes tipos de sesiones presenciales según corresponda atendiendo al inicio, desarrollo y finalización del curso:

- Al finalizar cada uno de los cuatrimestres, durante los meses de febrero y junio se celebrarán las pruebas presenciales siguiendo el calendario publicado en el portal de Formación Profesional Andaluza: <https://www.juntadeandalucia.es/educacion/portals/web/formacion-profesional-andaluza/quiero-formarme/modalidades/a-distancia>

Las sesiones online las desarrollará el alumnado desde casa, pero desde el centro se le proporcionará todo el apoyo telemático necesario para resolver cualquier duda que pueda surgir. Además se le indicará al alumnado los tiempos recomendados para realizar las tareas y finalizar los temas.

En términos generales, las unidades didácticas se irán abriendo de forma gradual, y para que el alumnado pueda pasar a la unidad siguiente tendrá que esperar a la fecha de publicación de dicha unidad didáctica.

El esquema que se seguirá con carácter general en unas sesiones online en éste módulo será el siguiente:

1. Los minutos iniciales se dedicarán a orientar sobre las posibles dudas que no hayan quedado aclaradas a través de la plataforma. Debemos concienciar a los alumnos para que resuelvan las dudas en el momento que se producen a través de los cauces que proporciona la plataforma: mensajes, correos, foros, chat, etc.
2. Análisis de aquellas tareas en el aula virtual (ya entregadas) y que a juicio del profesor deban de quedar claras en su correcta elaboración.
3. Presentación de las próximas tareas en el aula virtual a realizar por los alumnos y de los materiales de apoyo que las sustentan (archivos, enlaces, videos, ...) realizándose la exposición de los contenidos más importantes o que presenten un mayor nivel de dificultad.
4. Trabajar con el alumnado sobre alguna tarea práctica de los contenidos que se estén viendo.

Se contemplan los siguientes materiales didácticos:

- Unidades de trabajo expuestas en pantalla.
- Direcciones de Internet.
- Ejercicios de autoevaluación.
- Exámenes a través de Internet.
- Casos prácticos y/o tareas..
- Cuestionarios.
- Material complementario.
- Con respecto a los sistemas operativos: Windows y/o Ubuntu (ya se irá indicando).
- Software libre que se irá indicando con Open Office, Libre Office y otros propietarios según corresponda.

5.- Criterios y procedimiento de evaluación

Tal y como establece la Orden de 29 de septiembre de 2010 (BOJA 15-10-2010) que regula la evaluación del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía en la modalidad a distancia, la evaluación continua del alumnado requerirá la realización y entrega en el plazo establecido de las tareas obligatorias, la participación activa en las diferentes herramientas de comunicación del aula virtual, así como la realización de las pruebas de evaluación online y la superación de la prueba presencial de evaluación.

El proceso de evaluación se llevará a cabo a lo largo de todo el periodo que comprende el curso, teniendo en cuenta la calificación obtenida en los criterios de evaluación asociados a diferentes actividades evaluables realizadas en el aula virtual y pruebas presenciales.

Los exámenes presenciales serán tipo **test** sin ordenador.

Para cada grupo de alumnos y alumnas, dentro del periodo lectivo, se realizarán dos sesiones de evaluación parcial. Además de éstas, se llevará a cabo una sesión de evaluación inicial y una sesión de evaluación final en cada uno de los cursos académicos, sin perjuicio de lo que a estos efectos los centros docentes puedan recoger en sus proyectos educativos.

Durante el primer mes se realizará una evaluación inicial, que servirá como valoración inicial. La evaluación inicial será el punto de referencia del equipo docente y, en su caso, del departamento de familia profesional, para la toma de decisiones relativas al desarrollo del currículo y su adecuación a las características, capacidades y conocimientos del alumnado. Esta evaluación en ningún caso conllevará calificación para el alumnado.

La prueba presencial de febrero y junio debe permitir la identificación fehaciente del alumnado y demostrar la adquisición de los resultados de aprendizaje trabajados en las tareas y otros instrumentos de aprendizaje.

Para obtener calificación positiva en el módulo, el alumnado deberá superar la prueba presencial obligatoria del mes de junio. Dicha prueba versará sobre todos los resultados de aprendizaje vinculados al módulo profesional exceptuando, en su caso, aquellos resultados de aprendizaje que hayan sido superados en la prueba de febrero.

Si la calificación obtenida en la prueba presencial del mes de junio es inferior a 5, el módulo se considerará no superado y la calificación máxima a la que podrá optar el alumnado será de un 4, con independencia de la calificación obtenida aplicando la media ponderada a los diferentes resultados de aprendizaje y criterios de evaluación.

Una vez superado el examen de junio, el alumnado superará el módulo si cuando la calificación final del módulo aplicando la media ponderada de los diferentes resultados de aprendizaje (RA) y criterios de evaluación (CE) es igual o superior a 5.

5.1.- Ponderación de los resultados de aprendizaje y criterios de evaluación

Para calcular la nota final del módulo profesional utilizaremos los Resultados de Aprendizaje obtenidos por el alumno durante todo el curso. Si criterio es evaluado con más de un instrumento la nota del criterio será la media aritmética de las notas obtenidas con cada uno de los instrumentos.

HAY QUE SUPERAR TODOS LOS RESULTADOS DE APRENDIZAJE PARA SUPERAR EL MÓDULO.

RA	Porcentaje	Criterio de Evaluación (CE)	Ponderación por CE	Instrumentos de evaluación		Unidad
				Tarea Individual	Prueba Presencial	
RA1: Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.		a) Se ha valorado la importancia de mantener la información segura.	4	X	X	1 - 2
		b) Se han descrito las diferencias entre seguridad física y lógica.	4	X	X	
		c) Se han definido las características de la ubicación física y condiciones ambientales de	3	X	X	

los equipos y servidores.			
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	3	X	X
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	3	X	X
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	3	X	
g) Se han esquematizado 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	3	X	X

		contraseñas.				
		i) Se han valorado las ventajas que supone la utilización de sistemas biométricos..	3	X	X	
RA2:		a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento..	2	X	X	3
Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información		b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).	2	X	X	
		c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento	2	X	X	

en red.			
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	2		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.	2	X	X
g) Se han realizado copias de seguridad con distintas estrategias..	2	X	
h)Se han identificado las características de los medios de almacenamiento remotos y extraíbles.	2	X	X
i) Se han creado y restaurado imágenes de	2	X	

		respaldo de sistemas en funcionamiento.				
		j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento	2	X		
RA3: Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema		a)Se han seguido planes de contingencia para actuar ante fallos de seguridad.	3	X	X	5
		b) Se han clasificado los principales tipos de software malicioso.	3	X	X	
		c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades..	3	X		
		d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan	3	X		

		en los sistemas..				
		e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	3	X		
		f) Se han aplicado técnicas de recuperación de datos.	3	X		
RA4:		a)Se ha identificado la necesidad de inventariar y controlar los servicios de red.	3	X	X	4 - 6
Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.		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	3	X	X	

volumen de trafico generado por la publicidad y el correo no deseado.			
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.	3	X	X
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	3	X	X
g))Se ha instalado y configurado un cortafuegos en un equipo o servidor.	3	X	

RA5: Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.		a) Se ha descrito la legislación sobre protección de datos de carácter personal.	2	X	X	1
		b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	2	X	X	
		c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	2	X	X	
		d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen..	2	X	X	
		e) Se ha descrito la legislación actual sobre los	2	X	X	

	servicios de la sociedad de la información y comercio electrónico.				
	f) Se han contrastado las normas sobre gestión de seguridad de la información.	2	X	X	

5.2.- Instrumentos de evaluación

Los instrumentos utilizados para la evaluación serán los siguientes:

- Pruebas presenciales.
- Tareas.
- Participación en foros y herramientas de comunicación.

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

5.2.1- Pruebas presenciales

Al finalizar cada uno de los cuatrimestres, durante los meses de febrero y junio se celebrarán las pruebas presenciales siguiendo el calendario publicado en el portal de Formación Profesional Andaluza :<https://www.juntadeandalucia.es/educacion/portals/web/formacion-profesional-andaluza/quiero-formarme/modalidades/a-distancia>

La superación de las pruebas presenciales no implica la superación del módulo de forma directa. La calificación final del módulo depende de la calificación obtenida en los diferentes instrumentos de evaluación y su ponderación en base a criterios de evaluación. Esto significa que aparte de superar la prueba presencial, para superar el módulo deberás realizar de forma satisfactoria las tareas evaluables contempladas en la programación del mismo.

Estas pruebas presenciales serán de carácter eliminatorio.

Fechas	Contenido del examen
Parcial 1er cuatrimestre de Febrero (opcional) 02/02/26	Cuatrimestre 1: Unidades: 1,2 y 3
Convocatoria ordinaria de Junio 01/06/26	*Cuatrimestre 1: Unidades: 1,2 y 3 Cuatrimestre 2: Unidades: 4,5 y 6

*Nota: Las pruebas presenciales de febrero y junio deben permitir la identificación fehaciente del alumnado. El alumnado no tendrá la obligación de presentarse a las pruebas objetivas de los cuatrimestres marcados con * (asterisco) en la correspondiente convocatoria de examen presencial si y solo si ha superado dicho cuatrimestre en la convocatoria anterior.*

IMPORTANTE:

- La no presentación del alumnado a la prueba presencial de junio implicará la NO

SUPERACIÓN del módulo.

- Una calificación de la prueba presencial de junio inferior a 5 significará la NO SUPERACIÓN del módulo.
- La calificación de la prueba presencial de junio se calculará en base a la media ponderada de los diferentes Resultados de Aprendizaje y criterios de evaluación.
- En la prueba de junio el alumnado deberá de realizar todos los ejercicios cuyos resultados de aprendizaje no haya superado de forma completa en la prueba opcional de febrero.
- La ponderación de los resultados de aprendizaje evaluados de forma parcial en la prueba opcional de febrero y su ponderación con respecto a la prueba presencial de junio será especificado en las instrucciones de la prueba presencial de junio.
- Si se detecta que se ha copiado durante la realización de las pruebas presenciales, la prueba correspondiente quedará anulada y se le dará la calificación de 0 puntos para todos los resultados de aprendizaje incluidos en la misma. Si se copia con la ayuda de un compañero, también supondrá la anulación de la prueba para el alumno o la alumna que facilita dicha información.

5.2.2.- Tareas

Cada unidad didáctica tendrá por defecto una única tarea asignada, vinculada a los resultados de aprendizaje y sus correspondientes criterios de evaluación. Se pondrán ampliar las tareas en función de la naturaleza de los resultados de aprendizaje.

Es recomendable que el **envío** de las tareas se realice de **forma escalonada y progresiva**, evitando enviar de golpe un conjunto grande de tareas. Además, es conveniente no enviar las tareas muy cerca de la fecha obligatoria de entrega para poder garantizar la corrección con suficiente antelación en caso de que se opte a un segundo envío. De no ser así, no se garantiza tener las correcciones a tiempo.

El alumnado puede disponer de dos intentos de entrega de una misma tarea, siempre y cuando, la calificación del primer intento tenga una nota inferior a 5 sobre 10, obtenida de la media ponderada de la calificación de los criterios de evaluación, y la entrega del segundo intento se realice con, al menos, una semana de antelación a la fecha límite establecida para la tarea.

El segundo intento tiene un plazo máximo de entrega de siete días naturales, contado a partir del día siguiente de la comunicación de la calificación al alumnado. Este segundo intento debe ajustarse siempre a la fecha límite de entrega indicada.

Si se detecta que una tarea ha sido copiada total o parcialmente de otra entregada, ambas tareas serán calificadas con 0 puntos.

No está permitido poner en los foros las soluciones o partes de las soluciones de las tareas. De ser así, se valorará de forma negativa.

5.2.3.- Participación en foros y herramientas de comunicación

La participación y la colaboración entre iguales del alumnado no serán evaluadas en sí mismas ni de manera general. Sin embargo, se podrán proponer tareas evaluables cuya realización dependa de determinadas herramientas de comunicación tales como foros, chats o salas de videoconferencia ...

No se permite poner en los foros las soluciones o partes de las soluciones de las tareas o de las respuestas de los exámenes online, de ser así se valorará de forma negativa.

5.3.- Cuestionarios en el aula virtual

Cuando haya cuestionarios, el alumnado podrá realizar los cuestionarios online asociados a cada unidad tantas veces como desee, debiendo transcurrir un mínimo de 24 horas entre cada intento.

Los cuestionarios online asociados a cada unidad no son evaluables, por lo que no es un instrumento de evaluación, sino de autoevaluación. Estos cuestionarios tienen como finalidad comprobar si se han comprendido bien los contenidos del módulo.

6.- Bibliografía

Recomendación

Páginas web

- Plataforma educativa (CON ESTA SERÁ SUFICIENTE)

Libros

- Seguridad Informática. Jose Fabián Roa Buendia McGraw Hill

7.- Recursos necesarios

Debes conocer

A medida que se avanza en el proceso de enseñanza-aprendizaje, el alumnado deberá ir instalando y utilizando el software que se proporciona en las sesiones presenciales a fin de que aprenda el manejo y utilización de los mismos, u otros similares. (SE IRÁ INFORMANDO DE LO QUE NECESITE)

Algunos de los recursos que necesitaremos se pueden encontrar en los siguientes enlaces:

- <https://es.libreoffice.org>
- <https://www.openoffice.org/es/>
- <https://www.youtube.com>
- <https://mail.google.com/>
- <https://shotcut.org>
- <https://www.virtualbox.org/>
- <https://www.microsoft.com/es-es/windows>
- <https://ubuntu.com/download>
- ...

Obra publicada con [Licencia Creative Commons Reconocimiento Compartir igual 4.0](#)