Introducción

La normativa de referencia a tener en cuenta para la elaboración de la programación didáctica del módulo de Seguridad Informática Locales(**SEGI**) es la siguiente:

- El Real Decreto 1147/2011, de 29 de Julio**,** por el que se establece la ordenación general de la formación profesional del sistema educativo.
- El Real Decreto 1691/2007, de 3 de Julio, establece el título de **Técnico en Sistemas Microinformaticos y Redes**, y fija sus enseñanzas mínimas.
- La ORDEN de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de **Técnico en Sistemas Microinformáticos y Redes** (***SMR***) en Andalucía.
- Resto de disposiciones de aplicación para evaluación, organización de enseñanzas a distancia, etc.

Este profesional ejerce su actividad en el área de informática de entidades que dispongan de sistemas para la gestión de datos e infraestructura de redes (intranet, internet y/o extranet).

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

La definición de esta función incluye aspectos como:

- La instalación de equipos y servidores en entornos seguros.
- La incorporación de procedimientos de seguridad en el tratamiento de la información.
- La actualización de los sistemas operativos y el software de aplicación instalado.
- La protección frente a software malicioso.
- La aplicación de la legislación y normativa sobre seguridad y protección de la información.

Las actividades profesionales asociadas a esta función se aplican en:

- La instalación de equipamiento informático.
- El tratamiento, transmisión y almacenamiento de la información.
- El mantenimiento de los sistemas informáticos.

El módulo profesional, debido a lo extenso de sus contenidos y a la enorme importancia que tiene en la adquisición de competencias del ciclo formativo, se desglosa en 6 **unidades de trabajo**.

Al tratarse de una **enseñanza en modalidad semipresencial** en la que una parte importante se desarrolla online se le ha dado mucha importancia a la información obtenida a través de Internet, por lo que se ofrece un listado de direcciones en donde se podrán ampliar los conocimientos adquiridos, aclarar dudas, etc.

Cada una de las unidades de trabajo presenta los objetivos, criterios de evaluación y algunas orientaciones sobre cómo trabajar la unidad y sobre los recursos para el desarrollo de las actividades.

En la **modalidad de enseñanza presencial**, a este módulo profesional le corresponden 105 horas de clase **(2 horas semanales y 3 horas telemáticas durante 32 semanas)**. En esta modalidad semipresencial no es posible indicar una dedicación horaria para cada módulo, ya que esto depende del alumno, entre otros condicionantes, pero puede ser interesante considerar este número de horas como una referencia relativa y utilizarlo para baremar y comparar el tiempo necesario para superar cada módulo. Debe tenerse en cuenta que los alumnos en la modalidad presencial, además de esas 5 horas semanales de clase, deben dedicar también tiempo en casa para estudiar y hacer tareas, por lo que el tiempo requerido es sin duda mayor.

1. Competencias, objetivos y resultados de aprendizaje

1.1. Competencias profesionales, personales y sociales

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

  - Las competencias profesionales, personales y sociales de este título son las que se relacionan a continuación:

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.
j) Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
l) Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
o) Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.

1.2. Objetivos generales

- La formación del **módulo profesional SEGI** contribuye a alcanzar los siguientes **Objetivos generales**, respetando la letra con la que se relaciona en la Orden que regula el ciclo formativo de **SMR** 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.

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

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

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

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

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

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

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

1.3. Resultados de aprendizaje y criterios de evaluación.

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

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

Criterios de evaluación:

a) Se ha valorado la importancia de mantener la información segura.

b) Se han descrito las diferencias entre seguridad física y lógica.

c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.

d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.

e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.

f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.

g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.

h) Se ha valorado la importancia de establecer una política de contraseñas.

i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

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

Criterios de evaluación:

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.

b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).

c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.

d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.

e) Se han seleccionado estrategias para la realización de copias de seguridad.

f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.

g) Se han realizado copias de seguridad con distintas estrategias.

h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.

i) Se han utilizado medios de almacenamiento remotos y extraíbles.

j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de

uso del sistema informático.

Criterios de evaluación:

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

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

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

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

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

f) Se han aplicado técnicas de recuperación de datos.

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

Criterios de evaluación:

a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.

b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.

c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.

d) Se han aplicado medidas para evitar la monitorización de redes cableadas.

e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.

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

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

h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

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

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.

b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.

c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.

d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.

e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.

f) Se han contrastado las normas sobre gestión de seguridad de la información.

2. Unidades de Trabajo

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

Unidad 1. Introducción a la seguridad informática (14 horas)
Unidad 2. Seguridad en el entorno físico (28 horas)
Unidad 3. Seguridad en el hardware. Almac. y recuperación de datos. (18 horas)
Unidad 4. Sistemas de identificación. Criptografía. (18 horas)
Unidad 5. Amenazas de seguridad del software. (17 horas)
Unidad 6. Redes seguras. (10 horas).

UT01: Introducción a la seguridad Informática

CP	OG	RA	Contenidos propuestos
l,n,o,p	l,m	1 5	1.- Introducción a la seguridad informática. 1.1.- Introducción a la seguridad informática. 1.2.- Clasificación de seguridad. 1.2.1.- Seguridad activa y pasiva. 1.2.2.- Seguridad física y lógica. 1.3.- Objetivos de la seguridad informática. 1.3.1.- Principales aspectos de seguridad. 1.4.- Amenazas y fraudes en los sistemas de información. 1.4.1.- Vulnerabilidades, amenazas y ataques. 1.4.2.- Tipos de ataques. 1.4.3.- Mecanismos de seguridad. 1.5.- Gestión de riesgos. 1.5.1.- Proceso de estimación de riesgos. 1.5.2.- Políticas de seguridad. 1.5.3.- Auditorías. 1.5.4.- Plan de contingencias. 1.6.- Legislación: LOPD. 1.6.1.- Ámbito de aplicación. 1.6.2.- Agencia española de protección de datos. 1.6.3.- Derechos ARCO. 1.6.4.- Niveles de seguridad y medidas asociadas. 1.6.5.- Infracciones y sanciones. 1.7.- Legislación: LSSI. 1.7.1.- Ámbito de aplicación. 1.7.2.- Obligaciones de las empresas. 1.8.- Legislación: Derechos de autor. 1.8.1.- Ley de Propiedad Intelectual. 1.8.2.- Copyright y copyleft. 1.8.3.- Licencias Creative Commons.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

UT02: Seguridad en el entorno físico

CP	OG	RA	Contenidos propuestos
a,c,	e,d,m	3	1.- Seguridad en el entorno físico. 1.1.- Acceso de personas al recinto. 1.2.- Alarma contra intrusos. 1.3.- Instalación eléctrica. 1.4.- Seguridad de materiales eléctricos y protección de personas frente a la electricidad. 1.5.- Condiciones ambientales: Humedad y temperatura. 1.6.- Enemigos de los ordenadores: Partículas de polvo, agua y fuego. 2.- Centro de proceso de datos y su entorno físico. 2.1.- Infraestructura. 2.2.- Acceso. 2.3.- Redundancia. 3.- Sistemas de control de acceso. 3.1.- Personal de vigilancia y control. 3.2.- Dispositivos de control de acceso en un datacenter. 3.3.- iButton, Touch memories o llaves electrónicas de contacto. 3.4.- Sistemas de reconocimiento de personas. 3.5.- Sistemas biométricos e identificación personal. 3.5.1.- Propiedades (ideales) de los rasgos biométricos. 3.5.2.- Sistemas biométricos más utilizados. 3.5.3.- Comparación de métodos biométricos. 4.- Políticas, planes y procedimientos de seguridad. 4.1.- Elementos de las políticas de seguridad. 4.2.- Características deseables de las políticas de seguridad. 4.3.- Definición e implantación de las políticas de seguridad. 4.4.- Inventario y auditoría. 4.5.- Elementos de las políticas de seguridad.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

UT03: Seguridad en el Hardware. Almacenamiento y recuperacion de datos.

CP	OG	RA	Contenidos propuestos

c,i,j,l,n,o,p	c,d,g,k,l,m	2	• Seguridad en el hardware. Almacenamiento y recuperación de los datos.
			  ◦ Introducción a la seguridad en el hardware.
			  ▪ Monitorización del hardware.
			  ◦ Sistemas de alimentación ininterrumpida.
			  ▪ ¿Qué es un SAI?
			  ▪ Tipos de SAI.
			  ◦ Almacenamiento redundante.
			  ▪ Sistemas de tolerancia a fallos y seguridad física redundante.
			  ▪ Sistemas RAID.
			  ▪ Configuraciones o niveles RAID básicos.
			  ▪ Configuraciones o niveles RAID avanzados.
			  ▪ RAID en Windows.
			  ◦ Clusters de servidores.
			  ▪ Clasificación de los clusters.
			  ▪ Componentes de un cluster.
			  ◦ Almacenamiento externo.
			  ▪ Cloud Computing.
			  ▪ NAS
			  ▪ SAN.
			  ◦ Copias de seguridad.
			  ▪ Políticas de copias de seguridad.
			  ▪ Clasificación.
			  ▪ Copia de seguridad del registro.
			  ▪ Copia de seguridad de datos en Windows.
			  ▪ Copia de seguridad de datos en Linux.
			  ◦ Recuperación de datos.
			  ▪ Software de recuperación de datos.
			  ▪ Creación de imágenes del sistema.
			  ▪ Restauración del sistema.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

UT04: Sistemas de identificación. Criptografía.

CP	OG	RA	Contenidos propuestos

c,j,l,n,o	c,d,e,g,l	4	1. Sistemas de identificación. Criptografía.
			2. Introducción a la criptografía.
			  1. Aspectos de seguridad.
			  2. Concepto de criptografía.
			  3. Historia.
			  4. Primeros métodos de cifrado.
			3. Técnicas criptográficas.
			  1. Criptografía simétrica.
			  2. Inconvenientes de la criptografía simétrica.
			  3. Criptografía de clave pública.
			  4. Firmas digitales.
			  5. Funciones 'hash'.
			  6. Sobres digitales.
			4. Certificados digitales.
			  1. Autoridades de certificación.
			  2. Obtener un certificado digital en España.
			  3. PKI.
			5. Herramienta GPG en Linux.
			  1. Comandos para el cifrado simétrico.
			  2. Comandos para el cifrado asimétrico (de clave pública).
			6.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

UT05. Amenazas de seguridad del software.

CP	OG	RA	Contenidos propuestos

a,c,i,j,l,n,o	a,c,d,e,g,k,l,m	3	Amenazas y seguridad del software.
			• Fraudes informáticos y robos de información.
			  ◦ Introducción.
			  ◦ Software que vulnera la seguridad.
			  ◦ Vulnerabilidad del software.
			  ◦ Tipos de ataques.
			  ◦ Atacantes.
			  ◦ Fraude en Internet.
			• Control de acceso a la información.
			  ◦ En el sistema operativo.
			  ◦ Control de acceso a la información.
			  ◦ Monitorización del sistema.
			  ◦ Recursos de seguridad en el sistema operativo.
			• Seguridad en redes.
			  ◦ Protocolos seguros.
			  ◦ Seguridad en redes cableadas.
			  ◦ Seguridad en redes inalámbricas.
			• Seguridad activa.
			  ◦ Antivirus.
			  ◦ Antimalware.
			  ◦ Congelación.
			  ◦ Correo.
			  ◦ Cómo crear una contraseña segura.
			  ◦ Firewall o cortafuegos en equipos.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

UT06: Redes seguras

CP	OG	RA	Contenidos propuestos

a,c,j,l,n,o,p	a,c,d,e,g,k,l	3 y 4	Redes seguras.
			• 6. Redes seguras.
			  ◦ Niveles OSI.
			  ▪ Seguridad en las capas.
			  ◦ Redes Privadas Virtuales.
			  ▪ Introducción a las Redes Privadas Virtuales.
			  ▪ Analogía: Cada LAN es una isla.
			  ▪ ¿Qué hace una VPN?
			  ▪ VPN de acceso remoto y VPN punto a punto.
			  ▪ Mantener el tráfico en el túnel VPN.
			  ▪ Encriptación y protocolos de seguridad en una red privada virtual.
			• Cortafuegos o Firewall.
			  ◦ Tipos de Cortafuegos.
			  ◦ Arquitecturas de firewall.
			• Proxy.
			  ◦ Funcionamiento y características.
			  ◦ Proxy web y Proxy Caché.
			  ◦ Proxy en Windows.
			  ▪ Proxy en Windows. Wingate.
			  ▪ Proxy en Windows. Free proxy.
			  ◦ Proxy en Linux.
			  ▪ Proxy en Linux. Listas de Control de acceso.
			  ▪ Proxy en Linux. Opciones avanzadas.
			• IDS Sistemas detectores de intrusos.
			  ◦ Sistemas detectores de intrusos.
			  ◦ Clasificación de sistemas IDS.
			  ◦ Arquitectura de sistemas IDS.

CP = Competencias Profesionales. OG = Objetivos Generales. RA: Resultados de Aprendizaje

3. Metodología y materiales didácticos

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

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

Se contemplan los siguientes materiales didácticos:

- Unidades de trabajo expuestas en pantalla.
- Casos prácticos.
- Cuestionarios.
- Tareas.
- Material complementario.

MATERIAL Y EQUIPOS INFORMÁTICOS

- Aula de ordenadores con PCs conectados en red local y 1 servidor de red.
- Un proyector conectado al pc del profesor.

SOFTWARE

- Sistemas operativos Windows y Linux, tanto para los PCs de los alumnos, como para el servidor del aula, y para la creación de máquinas virtuales
- Programa analizador de protocolos tipo Wireshark.
- Programa simulador de redes tipo Packet Tracer.
- Otras herramientas de gestión y monitorización de redes.
- VirtualBox: Aplicación para la virtualización de sistemas informáticos.
- Diversas máquinas virtuales, ya instaladas y listas para funcionar, para la realización de ejercicios prácticos sobre seguridad.
- Herramientas variadas para seguridad.

Para la parte presencial del módulo profesional se fijarán los siguientes tipos de sesiones presenciales:

- Sesiones de presentación de contenidos;
- Sesiones prácticas (p.ej. resolución de ejercicios, prácticas software sobre seguridad,etc...);
- Sesiones de repaso y dudas;
- Sesiones de evaluación.

4. Criterios y procedimiento de evaluación

Tal y como establece el **Decreto 359/2011 de 7 de diciembre** que regulan las modalidades semipresencial y a distancia de las enseñanzas de Formación Profesional Inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía, las enseñanzas ofertadas en la modalidad semipresencial se impartirán mediante la combinación de **sesiones lectivas colectivas presenciales, de obligada asistencia para el alumnado**. Así mismo, los criterios de evaluación recogidos en las programaciones didácticas de las enseñanzas impartidas en las modalidades semipresencial y a distancia, recogerán de forma cuantificada o porcentual el peso en la evaluación de cada una de las actividades que intervienen en el proceso de aprendizaje y, en el caso de enseñanzas impartidas en la modalidad semipresencial, se valorarán de forma proporcional, además, las actividades realizadas por el alumnado en las sesiones presenciales.

El proceso de evaluación se llevará a cabo a lo largo de todo el periodo que comprende el curso, siendo el resultado la media ponderada de la suma de una serie de componentes ASOCIADOS A SUS RESPECTIVOS R.A.

Estos componentes son los siguientes:

Ponderación de los diferentes elementos que intervienen en la evaluación

Componente a evaluar
Actividades realizadas de forma presencial (TP)
Exámenes presenciales (EP)
Tareas en el aula virtual. (TAV)
Cuestionarios en el aula virtual (CU)

Los diferentes apartados que intervienen en la evaluación se puntuarán los R.A.e de **0 a 10 puntos**. Se considerará superado el módulo profesional, cuando la media ponderada comentada anteriormente sea **mayor o igual a 5, siempre y cuando la calificación media ponderada de las distintas pruebas presenciales haya sido superior o igual a 5.**

En el caso que el alumnado tenga más del 20% de faltas de asistencia en las sesiones lectivas presenciales, perderá el derecho a la evaluación continua.

El alumnado que haya perdido el derecho a la evaluación continua podrá presentarse a la convocatoria final de Junio, siempre que haya entregado todas las tareas y actividades que se han realizado durante el curso.

Los exámenes presenciales podrán ser escritos o prácticos con o sin ordenador según lo requiera la materia a evaluación.

Para cada grupo de alumnos y alumnas, dentro del periodo lectivo, se realizarán al menos **tres 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.

Durante el primer mes, desde el comienzo de las actividades lectivas de los ciclos formativos o de los módulos profesionales ofertados, 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**.

Con respecto a las evaluaciones parciales se realizará una por cada trimestre, la última se desarrollará en la última semana de mayo.

Las **calificaciones obtenidas trimestralmente** permiten conocer la evolución del proceso de enseñanza de aprendizaje del alumno/a, pero **son meramente informativas**.

Para calcular la **nota de cada evaluación** se tendrán en cuenta los RA impartidos en dicha evaluación y se aplicarán las siguientes fórmulas:

NOTA 1E = 40% RA1 + 50% RA3 + 10% RA5

NOTA 2E = 30% RA2 + 70% RA4

NOTA 3E = 50% RA3 + 50% RA4

La **nota final** del módulo profesional se calculará con la siguiente fórmula:

TOTAL = RA1 *20% + RA2 * 20% + RA3 *25% + RA4 *30% + RA5 * 5% .

Se considera **superado** el módulo si la **nota final es igual o superior a 5**.

Aportación de cada unidad a la nota de cada Evaluación

EVALUACIONES	UNIDAD	RA1	RA2	RA3	RA4	RA5	Total por Evaluación
1ª Evaluación	U1	40%				10%	100%
	U2			50%			
2ª Evaluación	U3		60%				100%
	U4				40%		
3ª Evaluación	U5				40%		100%
	U6			50%	10%		

Aportación de cada Unidad a la nota final

EVALUACIONES	UNIDAD	RA1	RA2	RA3	RA4	RA5	Total por Evaluación

1ª Evaluación	**U1**	20%				5%	35%
	U2			10%			
2ª Evaluación	**U3**		20%				35%
	U4				15%		
3ª Evaluación	**U5**				10%		30%
	U6			15%	5%		

Los criterios de evaluación son los que se recogen en la **ORDEN de 7 de julio de 2009** del BOJA 25 de Agosto 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, de conformidad con el Decreto 436/2008, de 2 de septiembre. A continuación, indicamos los **criterios de calificación para cada RA**:

1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
Aplicación de medidas de seguridad pasiva
NOTA Σ(**100%**): 20

- Resultado de aprendizaje 1: Criterios de evaluación ponderados correctamente (20% del resultado de aprendizaje).
- **1.a) Se ha valorado la importancia de mantener la información segura.**
  NOTA (%): 3
- **1.b) Se han descrito las diferencias entre seguridad física y lógica.**
  NOTA (%): 3
- **1.c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.**
  NOTA (%): 2
- **1.d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.**
  NOTA (%): 2
- **1.e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.**
  NOTA (%): 2
- **1.f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.**
  NOTA (%): 2
- **1.g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.**
  NOTA (%): 1
- **1.h) Se ha valorado la importancia de establecer una política de contraseñas.**
  NOTA (%): 3
- **1.i) Se han valorado las ventajas que supone la utilización de sistemas biométricos**
  NOTA (%): 2

2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.
Gestión de dispositivos de almacenamiento
NOTA Σ(**100%**): 20

- Resultado de aprendizaje 2: Criterios de evaluación ponderados correctamente (20% del resultado de aprendizaje).
- **2.a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.**
  NOTA (%): 2
- **2.b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).**
  NOTA (%): 2
- **2.c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.**
  NOTA (%): 2
- **2.d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.**
  NOTA (%): 2
- **2.e) Se han seleccionado estrategias para la realización de copias de seguridad.**
  NOTA (%): 2
- **2.f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.**
  NOTA (%): 2
- **2.g) Se han realizado copias de seguridad con distintas estrategias.**
  NOTA (%): 2
- **2.h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.**
  NOTA (%): 2
- **2.i) Se han utilizado medios de almacenamiento remotos y extraíbles.**
  NOTA (%): 2
- **2.j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.**
  NOTA (%): 2

3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
Aplicación de mecanismos de seguridad activa
NOTA Σ(**100%**): 25

- Resultado de aprendizaje 3: Criterios de evaluación ponderados correctamente (25% del resultado de aprendizaje).
- **3.a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.**
  NOTA (%): 4
- **3.b) Se han clasificado los principales tipos de software malicioso.**
  NOTA (%): 4
- **3.c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.**
  NOTA (%): 4
- **3.d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.**
  NOTA (%): 4

- **3.e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.**
  NOTA (%): 5
- **3.f) Se han aplicado técnicas de recuperación de datos**
  NOTA (%): 4

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico.
Aseguramiento de la privacidad.
NOTA Σ(**100%**): 30

- Resultado de aprendizaje 4: Criterios de evaluación ponderados correctamente (30% del resultado de aprendizaje).
- **4.a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.**
  NOTA (%): 2
- **4.b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.**
  NOTA (%): 2
- **4.c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.**
  NOTA (%): 2
- **4.d) Se han aplicado medidas para evitar la monitorización de redes cableadas.**
  NOTA (%): 6
- **4.e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.**
  NOTA (%): 3
- **4.f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.**
  NOTA (%): 6
- **4.g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.**
  NOTA (%): 6
- **4.h) Se ha instalado y configurado un cortafuegos en un equipo o servidor**
  NOTA (%): 3

5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.
Cumplimiento de la legislación y de las normas sobre seguridad
NOTA Σ(**100%**): 5

- Resultado de aprendizaje 5: Criterios de evaluación ponderados correctamente (5% del resultado de aprendizaje).
- **5.a) Se ha descrito la legislación sobre protección de datos de carácter personal.**
  NOTA (%): 1
- **5.b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.**
  NOTA (%): 1
- **5.c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.**
  NOTA (%): 1
- **5.d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.**
  NOTA (%): 1
- **5.e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.**
  NOTA (%): 0,5
- **5.f) Se han contrastado las normas sobre gestión de seguridad de la información**
  NOTA (%): 0,5

4.1. Actividades presenciales

El alumnado, a lo largo del curso, irá realizando en las sesiones presenciales una serie de actividades prácticas. El profesorado evaluará la actitud y la destreza de los alumnos en el desarrollo de estas actividades. El profesor enviará a los alumnos tareas y/o custrionarios referidos a dichas actividades presenciales.

En el apartado 5.1. Sesiones presenciales puede ver un listado de todas las actividades presenciales a realizar en el curso así como su planificación.

4.2. Exámenes presenciales

El decreto 359/2011 establece en su artículo 9.2 que *la realización de pruebas de evaluación, requerirán la identificación personal fehaciente del alumnado que las realice y se corresponden con el enfoque práctico empleado, como elemento validador de las actividades presenciales o virtuales desarrolladas a lo largo del curso.*

En virtud de lo anterior, en los exámenes presenciales prevalece el enfoque práctico y debe tener en cuenta que la prueba presencial está basada en los resultados de aprendizaje del módulo profesional.

Se prevé la realización de mínimo tres pruebas presenciales. una en cada trimestre. Además, se realizará el examen final FP presencial en junio. La planificación de las pruebas es la siguiente:

Prueba Presencial Escrita y/o Practica	Contenido del examen	R.A.
1ª evaluación	Unidades 1 y 2 .	1,5 y 3
2ª evaluación	Unidades 3 y 4.	2, 4
3ª evaluación	Unidades 5 y 6	3 y 4

Las fechas previstas para la realización de las pruebas presenciales (exámenes) son:

Prueba Presencial	Fechas previstas Examen Presencial
1ª evaluación	Diciembre de 2022
2ª evaluación	Abril de 2023
3ª evaluación	Mayo de 2023
FINAL FP (JUNIO)	Junio de 2023

Nota: Las fechas de la tabla anterior son orientativas. Las fechas y horas definitivas de los exámenes se comunicarán al alumnado con suficiente antelación a lo largo del curso.

IMPORTANTE:

- Las pruebas tienen carácter eliminatorio.
- La nota final de pruebas presenciales será, aproximadamente, la media ponderada de los exámenes de las tres evaluaciones.
- En caso de que la media ponderada de los distintos componentes de la evaluación (citados en el apartado 4.) no sea superior a 5 se realizará la prueba final.
- Para superar el módulo profesional es indispensable que la nota media ponderada de todos los componentes de los tres trimestres sea superior o igual a 5, o se supere la prueba final.

4.3. Tareas en el aula virtual

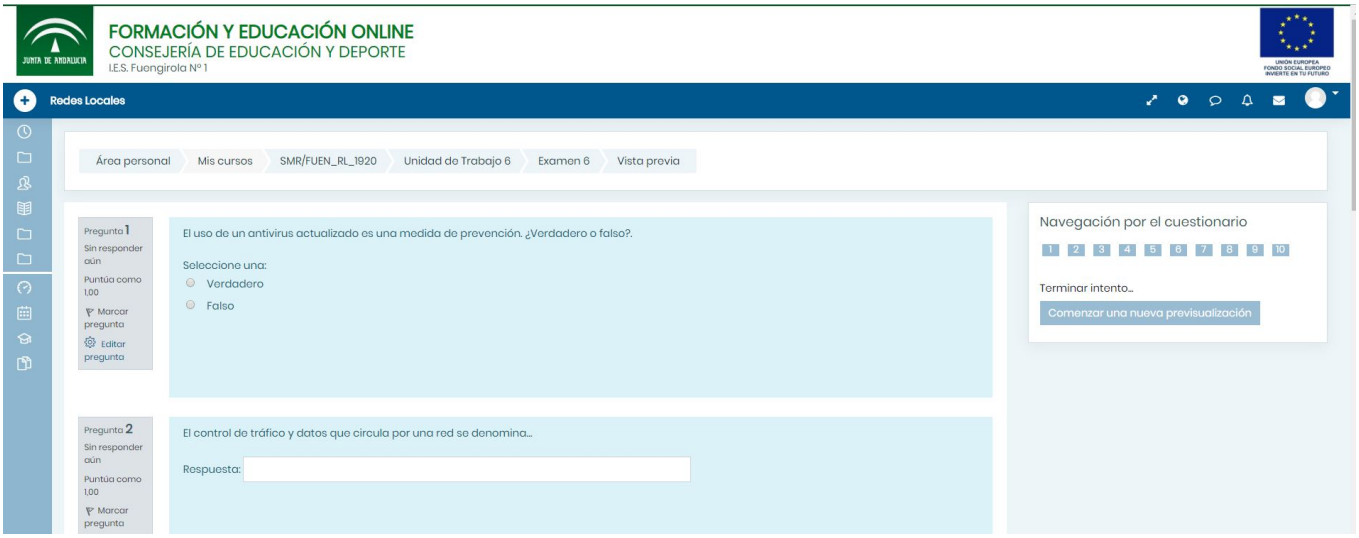
El alumnado **podrá entregar hasta un máximo de 2 veces la solución de una misma tarea**, siempre que la primera entrega tenga una nota inferior a 5 y superior a 1 sobre 10.

El segundo intento tendrá un plazo máximo de entrega de 7 días naturales después de que el profesor/a haya calificado como suspensa la tarea. Este segundo intento deberá ajustarse siempre a la fecha obligatoria de entrega indicada en la tabla de temporalización de cada unidad y/o bloque. **La nota de esta segunda entrega será como maximo un 5**.

Es recomendable que el envío de las tareas se realice de forma escalonada y progresiva, evitando enviar un conjunto grande de tareas. En los supuestos casos que la entrega de tareas se realice sobre la fecha límite de la misma, no se garantiza respetar la posibilidad del segundo reenvío, ya que podría darse el caso en que el docente no cuente con tiempo suficiente para responder al envío masivo de tareas.

4.4. Cuestionarios en el aula virtual

El alumnado deberá realizar los cuestionarios on-line asociados a cada unidad que el profesor proponga, **pudiendo realizar un máximo de tres intentos de cada uno, y conservándose la mayor nota de todos los intentos que haya realizado.**

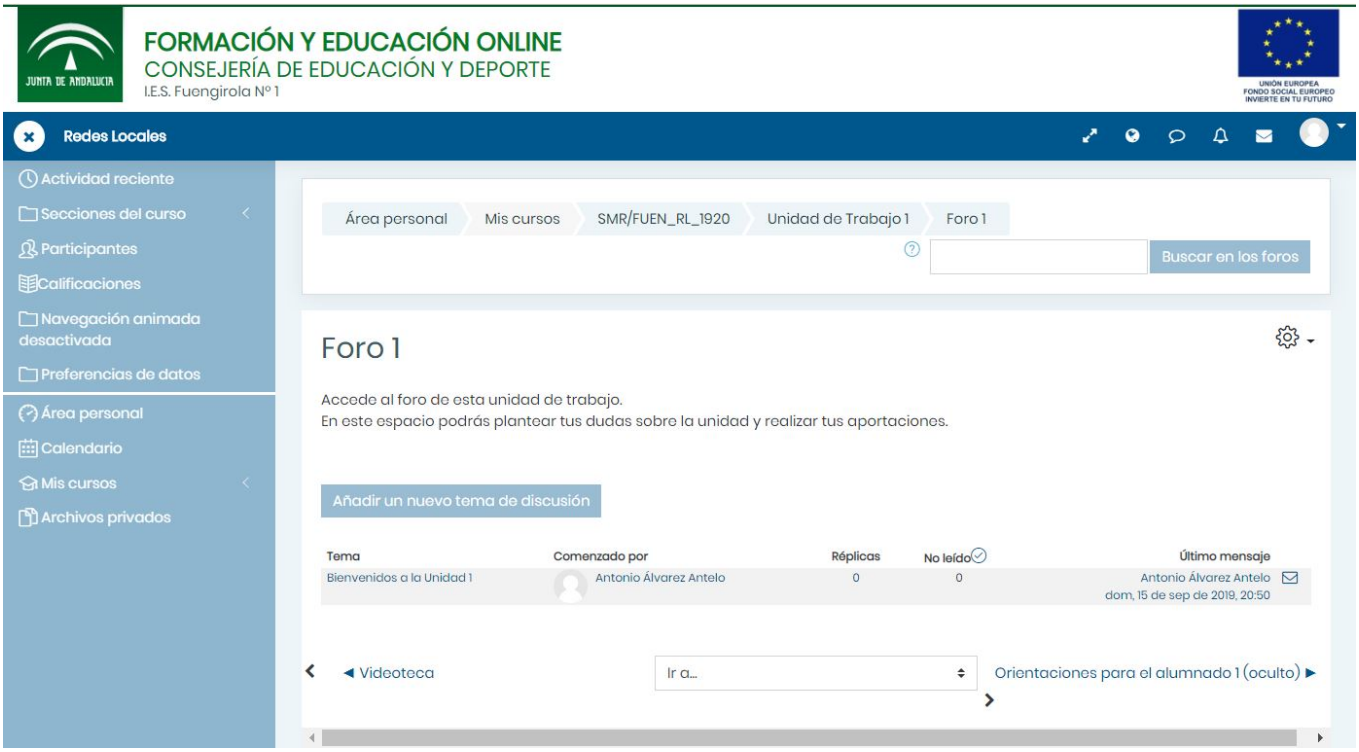


Captura de pantalla de la plataforma de FPaD

4.5. Participación en foros y herramientas de comunicación

El profesorado fomentará la particiáción activa del alumnado en el aula virtual a traves de foros y otros elementos de comunicación.

La participación del alumnado no será evaluada en si misma.



Captura de pantalla de la plataforma de FPaD

5. Secuenciación de Unidades de Trabajo y temporalización

Las fechas aproximadas previstas de presentación de cada Unidad de Trabajo son las siguientes:

Unidad	Fecha de inicio	Fecha de finalización	Fecha tope obligatoria de entrega de tareas
BLOQUE 1ª Evaluación.			
UT1:Introducción a la seguridad informática	19/09/2022	19/10/2022	20/12/2022
UT2: Seguridad en el entorno físico	19/10/2022	17/12/2022	
BLOQUE 2ª Evaluación:			
UT3: Seguridad en el hardware. Almac. y recuperación de datos.	09/01/2023	13/02/2023	20/03/2023
UT4:Sistemas de identificación. Criptografía.	13/02/2023	20/03/2023	
BLOQUE 3ª Evaluación			
UT5: Amenazas de seguridad del software.	20/03/2023	08/05/2023	28/05/2023
UT6: Redes seguras.	08/05/2023	22/05/2023	

- La **fecha tope obligatoria de entrega** indica el último día que se recogerán las tareas indicadas (incluido el segundo envío en caso de que fuera necesario) si estuviese **fuera de la fecha indicada en la tarea se valoraría los RA asociados como máximo un 5**.
- Se recomienda al alumnado la entrega progresiva de tareas conforme se vayan finalizando las unidades didácticas, garantizándose así la posibilidad de un segundo reenvío.
- No se aceptará ningún envío de tareas fuera de esos plazos, salvo circunstancias excepcionales, que valorará el profesor o profesora previa acreditación documental de las mismas

5.1. Sesiones presenciales

El artículo 3.2. establece que l*as sesiones de docencia presencial tendrán como objetivo facilitar al alumnado las ayudas pertinentes en la realización de tareas, resolver dudas respecto a los aspectos esenciales del currículo, orientar hacia el uso de las herramientas de comunicación empleadas por esta modalidad de enseñanza, afianzar las interacciones cooperativas entre el alumnado, promover la adquisición de los conocimientos, competencias básicas o profesionales que correspondan y, en su caso, reforzar la práctica de las destrezas orales.* Por lo tanto, se establece tres tipos de sesiones presenciales:

- Las **sesiones de acogida del alumnado** se realizan en la primera semana del curso para explicar al alumnado los aspectos generales del ciclo, características de la enseñanza semipresencial, el uso del Aula Virtual, las características más importantes de cada módulo, etc.
- El objetivo de las **sesiones presenciales** es la exposición de los contenidos de una unidad, resolución de dudas, realización de prácticas en el Centro, etc.
- Al final de cada trimestre se fijarán **sesiones de recuperación** para que el alumnado pueda recuperar las actividades presenciales que no haya podido realizar.

Tal y como establece el horario del grupo, las clases de este módulo profesional se realizan los Lunes.

1ª evaluación

Fechas	Unidad	Descripción
19/09/22	-	Sesión de acogida del alumnado Cuestionario inicial del alumnado
19/09/22 - 17/10/22	UT01	Presentación de la unidad - Ejercicios y dudas
17/10/22 - 19/12/22	UT02	Presentación de la unidad - Ejercicios, dudas. Examen

2ª evaluación

Fecha	Unidad	Descripción
09/01/23 - 13/02/23	UT03	Presentación de la unidad - Ejercicios y dudas. .
13/02/23 - 20/03/23	UT04	Presentación de la unidad - Ejercicios y dudas, Examen

3ª evaluación

Fecha	Unidad	Descripción
20/03/23 - 08/05/23	UT05	Presentación de la unidad - Ejercicios y dudas.
08/05/23 - 22/05/23	UT06	Presentación de la unidad - Ejercicios y dudas. Examen.

6. Planificación de las actividades de refuerzo o mejora de las competencias.

En este apartado se describe la determinación y planificación de las actividades de refuerzo o mejora de las competencias, que permitan al alumnado matriculado en la modalidad semipresencial la superación de los módulos profesionales pendientes de evaluación positiva o, en su caso, mejorar la calificación obtenida en los mismos.

Dichas actividades se realizarán durante el periodo comprendido entre la última evaluación parcial y la evaluación final, que será antes del 22 de junio.

Las actividades que se desarrollarán durante este periodo se centrarán en:

a. Sesiones presenciales en las que se repasarán aquellos contenidos que presenten especial dificultad para los alumnos del módulo.
b. Sesiones presenciales en las que se realizarán ejercicios y prácticas bajo la coordinación del profesor del módulo.
c. Sesiones presenciales para resolución de las dudas que planteen los alumnos.
d. Resolución de dudas a través de los medios telemáticos ofrecidos por la plataforma de aprendizaje (foro, chat, mensajes).
e. Entrega de tareas online no realizadas durante el curso.
f. Realización de los cuestionarios pendientes.

7. Bibliografía

Recomendación

Libros

- Seguridad Informatica. Editorial Rama
- Seguridad Informatica. Editorial Sintesis.
- Seguridad Informatica. Editorial Mc graw hill
- Seguridad Informática 2ºedicion, Ethical Hacking. Editorial Eni
- Kevin Mitnick. El arte de la intrusion como ser un hacker. Editorial Alfaomega
- Merce Molist. Hackstory.es (Historia del hacking en España) (www.hackstory.es)..

- **Páginas web**

  - *http://www.elotroladodelmal.com/*
  - *http://www.inteco.es/*
  - *http://www.hispasec.com/*

8. Recursos necesarios

👀 Debes conocer

En los materiales suministrados por el profesor se incluirán enlaces a las distintas páginas de las que debemos descargar el software necesario para realizar las tareas, las prácticas en las sesiones presenciales y los exámenes presenciales.

Por ejemplo la herramienta maquinas virtuales de seguridad, Kali Linux, Packet Tracer, etc..

9.Anexo Covid

Protocolo a Seguir en el Caso de...

Reducción del Grupo Presencial.

- Si en la materia asistieran más de 20 alumnos al aula de forma presencial, la clase se dividirá en 2 grupos: uno asistiría presencialmente una semana y el otro grupo la siguiente; así hasta que no sea necesario aplicar el protocolo de distanciamiento Covid en el aula o el ratio baje de 20. El alumnado que no esté presencialmente deberá seguir la clase a distancia utilizando la **"Sala virtual".**

Confinamiento Total o Parcial.

- En el caso que tuviésemos que pasar a confinamiento total o parcial, por positivo en el aula u otra situación similar, las sesiones presenciales seguirán impartiéndose a distancia durante el mismo horario. Utilizando para ello la **"Sala virtual"** que hay dentro de la plataforma Semipresencial.
- Si uno o varios alumnos pasaran a estar confinados en casa, por contacto o por positivo en Covid; se les permitirán que puedan seguir las clases presenciales a distancia; utilizando para ello la **"Sala virtual".**