IES JUAN DE MAIRENA (Mairena del Aljarafe)

PROGRAMACIÓN DIDÁCTICA
DEPARTAMENTO DE INFORMÁTICA

Seguridad Informática
2º C.F.G.M. Sistemas Microinformáticos y Redes
Curso 2026-2027

2. Programación de seguridad informática 3
2.1. Resultados de Aprendizaje y Criterios de Evaluación 4
2.2 Contenidos 5
2.2.1. UNIDADES DIDÁCTICAS 6
2.3. Objetivos 30
2.4. Competencias profesionales, personales y sociales 31
2.5. Metodología 32
2.6 Temporalización de los contenidos 32
2.7. Docencia telemática 33
2.8. Acuerdos modificaciones tras la Evaluación Inicial 33
3. Evaluación 34
3.1. Aspectos generales 34
3.2. Criterios e instrumentos de evaluación 35
3.3. Criterios de calificación generales 37
3.3.1 EVALUACIÓN CONTINUA 37
3.3.2 EVALUACIÓN PARCIAL 40
3.3.3 EVALUACIÓN FINAL PRIMERA 45
3.3.4 EVALUACIÓN FINAL SEGUNDA 45
3.3.5 CRITERIOS DE CORRECCIÓN 46
3.4. Plan Personalizado de Recuperación 47
3.5. Medidas de atención a la diversidad 47
3.6. Dualización del módulo 48
3.6.1. SECUENCIACIÓN Y TEMPORALIZACIÓN 48
3.6.2. REPARTO DE RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN 48

2. PROGRAMACIÓN DE SEGURIDAD INFORMÁTICA

2.1. Resultados de Aprendizaje y Criterios de Evaluación

Los resultados de aprendizaje (RA) se refieren a los conocimientos, habilidades y actitudes aprendidas por el estudiante y que pueden ser evaluadas aplicando determinados métodos de evaluación con el fin de determinar la adquisición de las competencias propias de cada materia. Por otro lado, los criterios de evaluación son el conjunto de previsiones que, para cada resultado de aprendizaje, indican el grado de concreción aceptable del mismo.

Se enumeran a continuación los RA asociados con el presente módulo junto con sus criterios de evaluación y que serán necesarios para adquirir las competencias propias de la materia:

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 específico.
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 cortafuego 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.

2.2 Contenidos

Los contenidos básicos que se le exigirán al alumno para la superación del módulo, vienen recogidos en el RD 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, y son los siguientes:

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.

Gestión de dispositivos de almacenamiento:

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.
- Almacenamiento remoto y extraíble.
- Criptografía.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Política de almacenamiento.
- Recuperación de datos.

Aplicación de mecanismos de seguridad activa:

- Identificación digital.
- Sistemas biométricos de identificación.
- Firma electrónica y certificado digital.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Utilización de cortafuegos en un sistema o servidor.
- Listas de control de acceso.
- Política de contraseñas.
- Recuperación de datos.
- Software malicioso. Clasificación, protección y desinfección.
- Auditorias de seguridad.

- Actualización de sistemas y aplicaciones.

Aseguramiento de la privacidad:
- Métodos para asegurar la privacidad de la información transmitida.
- Fraudes informáticos y robos de información.
- Control de la monitorización en redes cableadas.
- Seguridad en redes inalámbricas.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos en equipos y servidores.
- Publicidad y correo no deseado.

Cumplimiento de la legislación y de las normas sobre seguridad:
- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

2.2.1. UNIDADES DIDÁCTICAS

A la vista de los contenidos mínimos y los resultados de aprendizaje anteriores, se ha decidido estructurar este módulo en dos bloques (que coinciden con las evaluaciones) que suman un total de diez unidades de trabajo que se presentan a continuación.

Unidad 1. Introducción a la seguridad informática
- 1.1 Seguridad informática. Introducción. Objetivos.
- 1.2 Clasificación de seguridad
  - Seguridad física y lógica
  - Seguridad activa y pasiva
- 1.3 Principios de seguridad
- 1.4 Tipos de amenazas y fraudes en los sistemas de la información
- 1.5 Vulnerabilidades
- 1.6 Planes de contingencia y políticas de seguridad.

Unidad 2. Seguridad física. Instalaciones, Hardware, CPDs y control de acceso.
- 2.1 Ubicación y protección física de los equipos y servidores.
  - Sistemas de control de acceso
- 2.2 Condiciones ambientales de los equipos
- 2.3 Sistemas de alimentación ininterrumpida (SAI)
  - Tipos de SAI. Modo de funcionamiento
- 2.4 Centros de proceso de datos (CPD)
  - Características constructivas y de disposición
  - Sistemas de seguridad del CPD
  - Climatización
  - Centros de respaldo

Unidad 3. Seguridad Lógica. Sistemas de identificación y control de acceso.
- 3.1 Concepto de seguridad lógica
- 3.2 Acceso a sistemas operativos y aplicaciones
  - Contraseñas
  - Listas de control de acceso
- 3.3 Acceso a aplicaciones por Internet
- 3. 4 Otras alternativas de gestión de identidades
  - Autenticación de usuarios
  - Autorización de usuarios

Unidad 4. Seguridad Lógica. Criptografía.
- 4.1 Introducción a la criptografía
  - Definiciones. Conceptos básicos
  - Elementos de un criptosistema
  - Tipos de sistema de cifrado
- 4.2 Cifrado de clave simétrica
  - Confidencialidad con claves simétricas
  - Algoritmos de cifrado

- 4.3 Cifrado de clave asimétrica
  - Autentificación con claves asimétricas
  - Confidencialidad con claves asimétricas
  - Algoritmos de cifrado
- 4.4 Algoritmo de cifrado hash
- 4.5 Sistemas híbridos

Unidad 5. Seguridad Lógica. Aplicaciones prácticas de la Criptografía.

- 5.1 Aplicaciones prácticas de la criptografía. Conceptos y procedimientos
- 5.2 Firma digital
  - Mecanismo de firma
  - Firma digital con árbitro
  - Firma digital ordinaria
- 5.3 Certificados digitales
  - Concepto y características
  - Autoridades de certificación
  - Solicitud de certificados
  - Clases de certificados
- 5.4 DNI electrónico
- 5.5 SSL y TLS
- 5.6 Cifrado de información

Unidad 6. Gestión de almacenamiento

- 6.1 Gestión y políticas de almacenamiento
- 6.2 Dispositivos de almacenamiento
  - Servicios de almacenamiento remoto
  - Almacenamiento externo
- 6.3 Almacenamiento redundante y distribuido
  - RAIDs
  - Clusters
- 6.4 Copias de seguridad
  - Clases de copias de seguridad
  - Realización de copias de seguridad
- 6.5 Otras copias de seguridad
  - Imágenes de respaldo
  - Copia de seguridad del registro
  - Puntos de restauración del sistema operativo.
  - Copias de seguridad de los datos de correo electrónico
- 6.6 Recuperación de datos.

Unidad 7. Software Malicioso.

- 7.1 Concepto de software malicioso
- 7.2 Clasificación del malware.
- 7.3 Denegación de servicio
- 7.4 Publicidad y correo no deseado
- 7.5 Ingeniería social. Fraudes informáticos

Unidad 8. Medidas de protección contra el Malware

- 8.1 Medidas de protección contra el software malicioso
  - Medidas preventivas contra el malware
  - Medidas paliativas contra el malware
- 8.2 Centros de protección y respuestas frente a amenazas
- 8.3 Buenas prácticas para protegerse del malware

Unidad 9. Seguridad en redes. Ataques y contramedidas

- 9.1 Métodos para asegurar la privacidad de la información transmitida.
- 9.2 Seguridad en redes
  - Servicios de red
  - Vulnerabilidades
  - Monitorización de redes. Escaneo de puertos.
  - Detección de intrusos
  - Permisos de recursos compartidos en red

Seguridad en los navegadores
Seguridad en las redes sociales
9.3. Seguridad en redes inalámbricas
Tecnologías Wi-Fi
Seguridad Wi-Fi.
Monitorización de redes Wi-Fi
Detección de intrusos.
9.4 Sistemas cortafuegos en equipos y servidores.
Tipos de Cortafuegos
Instalación y configuración de proxys.
Instalación y configuración de cortafuegos.
Registros de actividad del cortafuegos
9.5 Auditorías de seguridad en redes
Tipos de auditorías de red
Herramientas para auditorías

Unidad 10. Normativa sobre seguridad y protección de datos.

10.1 Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD-GDD).
Disposiciones generales
Principios de protección de datos
Derechos de las personas
Medidas básicas de cumplimiento (políticas de privacidad, consentimiento, derechos ARCO).
Obligación legal, interés público
Consecuencias del incumplimiento normativo
Infracciones penales
Derechos digitales de los trabajadores
Figuras legales que intervienen en el tratamiento de datos.
Legislación existente sobre los servicios de la sociedad de la información y el comercio electrónico.
Normas ISO sobre gestión de la seguridad de la información.

A continuación, se detalla el plan de trabajo para cada una de las unidades didácticas anteriores.

<table>
<tr><th colspan="2">UNIDAD 1: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA</th><th>TEMP: SEP</th><th>10 HORAS</th></tr>
<tr><th colspan="2">OBJETIVOS</th><th colspan="2">CONTENIDO</th></tr>
<tr><td colspan="2">• Conocer las diferencias entre seguridad de la información y seguridad informática.
• Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
• Describir cuales son los principios básicos de la seguridad.
• Conocer qué son y qué utilidad tienen las políticas de seguridad.
• Aprender en qué consisten los planes de contingencia.</td><td colspan="2">1.1 Seguridad informática. Introducción. Objetivos.
1.2 Clasificación de seguridad
Seguridad física y lógica
Seguridad activa y pasiva
1.3 Principios de seguridad
1.4 Tipos de amenazas y fraudes en los sistemas de la información
1.5 Vulnerabilidades
1.6 Planes de contingencia y políticas de seguridad.</td></tr>
<tr><th colspan="4">RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO</th></tr>
<tr><td colspan="4">RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.</td></tr>
<tr><td colspan="4">a) Se ha valorado la importancia de mantener la información segura. (1,875%)
b) Se han descrito las diferencias entre seguridad física y lógica. (1,250%)</td></tr>
<tr><td colspan="4">RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.</td></tr>
<tr><td colspan="4">a) Se ha identificado la necesidad de inventariar y controlar los servicios de red (1,0%).
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información. (0,4%)</td></tr>
<tr><td colspan="4">RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.</td></tr>
<tr><td colspan="4">b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada (0,5%).</td></tr>
<tr><th colspan="4">INSTRUMENTOS DE EVALUACIÓN</th></tr>
<tr><td colspan="4">Pruebas escritas o por ordenador
Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo.
Observación diaria de la actividad en clase de cada alumno.</td></tr>
<tr><th colspan="4">ACTIVIDADES</th></tr>
<tr><td colspan="4">- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual.
- Exposición de los contenidos.</td></tr>
<tr><td colspan="4">- Práctica 1. Amenazas y riesgos.
- Práctica 2. Análisis de vulnerabilidades.
- Práctica 3. ZENMAP.
- Práctica 4. Planes de contingencia</td></tr>
<tr><td colspan="4">- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones.
- Prueba de conocimiento (Examen).
- Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.</td></tr>
<tr><th colspan="4">REFUERZO Y AMPLIACIÓN</th></tr>
<tr><td colspan="4">Revisión vídeos y material adicional.</td></tr>
<tr><td colspan="4">TRABAJO EN CASA: Actividades de consolidación</td></tr>
</table>

VALORACIÓN DE LO APRENDIDO UD1			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
1	a	Observación	0,188%
		Examen	1,125%
		Actividades	0,563%
	b	Observación	0,125%
		Examen	0,750%
		Práctica 1	0,375%
4	a	Observación	0,100%
		Examen	0,600%
		Práctica 2	0,300%
	b	Observación	0,040%
		Examen	0,240%
		Práctica 3	0,120%
5	b	Práctica 4	0,500%
			5,025%

<table>
<tr><th colspan="2">UNIDAD 2: SEGURIDAD FÍSICA</th><th>TEMP: OCT</th><th>10 HORAS</th></tr>
<tr><th colspan="2">OBJETIVOS</th><th colspan="2">CONTENIDO</th></tr>
<tr><td colspan="2">• Tomar conciencia sobre la importancia de la seguridad de los sistemas informáticos.
• Identificar los riesgos físicos a los que están sometidos los equipos informáticos.
• Aplicar las medidas preventivas adecuadas para proteger los equipos informáticos.
• Describir las características y medidas de seguridad de un CPD.
• Valorar la importancia de los centros de respaldo de datos.</td><td colspan="2">2.1 Ubicación y protección física de los equipos y servidores.
Sistemas de control de acceso
2.2 Condiciones ambientales de los equipos
2.3 Sistemas de alimentación ininterrumpida (SAI)
Tipos de SAI
Modo de funcionamiento
2.4 Centros de proceso de datos (CPD)
Características constructivas y de disposición
Sistemas de seguridad del CPD
Climatización
Centros de respaldo.</td></tr>
<tr><th colspan="4">RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO</th></tr>
<tr><td colspan="4">RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.</td></tr>
<tr><td colspan="4">c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores. (2,5%)
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos (1,25%).
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida (1,25%).
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida (1,25%)
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos (1,25%).</td></tr>
<tr><th colspan="4">INSTRUMENTOS DE EVALUACIÓN</th></tr>
<tr><td colspan="4">Pruebas escritas o por ordenador
Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo.
Observación diaria de la actividad en clase de cada alumno.</td></tr>
<tr><th colspan="4">ACTIVIDADES</th></tr>
<tr><td colspan="4">- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual.
- Exposición de los contenidos.</td></tr>
<tr><td colspan="4">- Práctica 1. SAI
- Práctica 2. Cámaras IP
- Práctica 3. Huellas dactilares
- Práctica 4. Traslado CPD
- Práctica 5. CPD y centros de respaldo</td></tr>
<tr><td colspan="4">- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones.
- Prueba de conocimiento (Examen).
- Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.</td></tr>
<tr><th colspan="4">REFUERZO Y AMPLIACIÓN</th></tr>
<tr><td colspan="4">Revisión vídeos y material adicional.</td></tr>
<tr><td colspan="4">TRABAJO EN CASA: Actividades de consolidación</td></tr>
</table>

VALORACIÓN DE LO APRENDIDO UD2			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
1	c	Observación	0,250%
		Examen	1,500%
		Actividades	0,250%
		Práctica 4	0,500%
	d	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 3	0,125%
		Práctica 4	0,125%
	e	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 2	0,125%
		Práctica 5	0,125%
	f	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 3	0,125%
	i	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 2	0,125%
			7,50%

UNIDAD 3: SEGURIDAD LÓGICA	**TEMP: OCT-NOV**	**12 HORAS**
OBJETIVOS	**CONTENIDO**	
• Conocer qué es la seguridad lógica y apreciar su importancia. • Describir los sistemas de protección de acceso a sistemas operativos y aplicaciones mediante contraseñas y listas de control de acceso. • Analizar los sistemas de protección de acceso a las aplicaciones a través de internet. • Identificar diversas alternativas de gestión de identidades, explicando las diferencias entre autenticación y autorización.	3.1 Concepto de seguridad lógica 3.2 Acceso a sistemas operativos y aplicaciones Contraseñas Listas de control de acceso 3.3 Acceso a aplicaciones por Internet 3.4 Otras alternativas de gestión de identidades Autenticación de usuarios Autorización de usuarios	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
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 (1,875%). b) Se han descrito las diferencias entre seguridad física y lógica (1,25%). g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso (1,875%). h) Se ha valorado la importancia de establecer una política de contraseñas (2%).		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
f) Se han aplicado técnicas de recuperación de datos (3,75%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos. - Respuesta común en parejas – Debates sobre un tema de actualidad/noticia relacionada con los contenidos de la unidad.		
- Práctica 1. John the Ripper - Práctica 2. Actualización Software - Práctica 3. ACL - Práctica 4. Actividad Administración de contraseñas y Actividad de pagos seguros		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD3			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
1	a	Observación	0,188%
		Examen	1,125%
		Práctica 1	0,563%
	b	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 2	0,250%
	g	Observación	0,188%
		Examen	1,125%
		Actividades	0,188%
		Práctica 3	0,375%
	h	Observación	0,250%
		Examen	1,500%
		Actividades	0,250%
		Práctica 1	0,250%
		Práctica 4	0,250%
3	f	Observación	0,375%
		Práctica 4	3,375%
			11,25%

UNIDAD 4: CRIPTOGRAFÍA	**TEMP: NOV**	**10 HORAS**
OBJETIVOS	**CONTENIDO**	
• Conocer qué es la criptografía y para qué se utiliza. • Distinguir los tipos de sistemas de cifrados utilizados en la criptografía. • Describir las ventajas e inconvenientes de los criptosistemas. • Conocer y apreciar las ventajas de los criptosistemas híbridos.	4.1 Introducción a la criptografía Definiciones. Conceptos básicos Elementos de un criptosistema Tipos de sistema de cifrado 4.2 Cifrado de clave simétrica Confidencialidad con claves simétricas Algoritmos de cifrado 4.3 Cifrado de clave asimétrica Autentificación con claves asimétricas Confidencialidad con claves asimétricas Algoritmos de cifrado 4.4 Algoritmo de cifrado hash 4.5 Sistemas híbridos	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
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 (1,875%). b) Se han descrito las diferencias entre seguridad física y lógica (1,25%). g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso (1,875%).		
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.		
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red (1%). b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes y robos de información (0,4%). f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital entre otros (2%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. Esteganografía - Práctica 2. Cifrado Simétrico RSA - Práctica 3. Thunderbird		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD4			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
1	a	Observación	0,188%
		Examen	1,125%
		Actividades	0,563%
	b	Observación	0,125%
		Examen	0,750%
		Práctica 1	0,375%
	g	Observación	0,188%
		Examen	1,125%
		Actividades	0,188%
		Práctica 2	0,375%
4	a	Observación	0,100%
		Examen	0,600%
		Actividades	0,100%
		Práctica 3	0,200%
	b	Observación	0,040%
		Examen	0,240%
		Práctica 3	0,120%
	f	Observación	0,200%
		Examen	1,200%
		Práctica 3	0,600%
			8,40%

UNIDAD 5: APLICACIONES DE LA CRIPTOGRAFÍA	**TEMP: NOV-DIC**	**10 HORAS**
OBJETIVOS	**CONTENIDO**	
• Aprender qué es la firma digital y qué aplicaciones tiene. • Conocer qué son los certificados digitales. • Describir las funciones del DNI electrónico y conocer los mecanismos de seguridad que tiene. • Estudiar los protocolos SSL y TLS para las conexiones seguras. • Aprender a cifrar archivos y unidades de almacenamiento.	5.1 Aplicaciones prácticas de la criptografía. Conceptos y procedimientos 5.2 Firma digital Mecanismo de firma Firma digital con árbitro Firma digital ordinaria 5.3 Certificados digitales Concepto y características Autoridades de certificación Solicitud de certificados Clases de certificados 5.4 DNI electrónico 5.5 SSL y TLS 5.6 Cifrado de información	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
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 (1,875%).		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas (2,3%).		
RA4. 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 y robos de información (0,4%). f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital entre otros (2%). g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros (4%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. Certificados - Práctica 2. Certificados y firmas - Práctica 3. Verifirma - Práctica 4. GPG		
FINALES: Síntesis y Evaluación (3 h.)		
-- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD5			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
1	a	Observación	0,188%
		Examen	1,125%
		Práctica 2	0,563%
3	d	Actividades	0,230%
		Examen	1,380%
		Práctica 1	0,690%
4	b	Observación	0,040%
		Práctica 3	0,360%
	f	Observación	0,200%
		Examen	1,200%
		Actividades	0,200%
		Práctica 4	0,400%
	g	Observación	0,400%
		Examen	2,400%
		Actividades	0,400%
		Práctica 4	0,800%
			10,575%

UNIDAD 6: GESTIÓN DEL ALMACENAMIENTO	**TEMP: ENE**	**8 HORAS**
OBJETIVOS	**CONTENIDO**	
• Conocer las características de la gestión del almacenamiento. • Diseñar políticas de almacenamiento. • Utilizar los medios de almacenamiento y saber cómo protegerlos. • Reconocer las tecnologías de almacenamiento redundante más utilizadas. • Realizar copias de seguridad e imágenes del sistema. • Aprender a recuperar datos borrados.	6.1 Gestión y políticas de almacenamiento 6.2 Dispositivos de almacenamiento Clasificación Servicios de almacenamiento remoto Almacenamiento externo 6.3 Almacenamiento redundante y distribuido RAIDs Clusters 6.4 Copias de seguridad Clases de copias de seguridad Realización de copias de seguridad 6.5 Otras copias de seguridad Imágenes de respaldo Copia de seguridad del registro Puntos de restauración del sistema operativo. Copias de seguridad de correo electrónico 6.6 Recuperación de datos.	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.		
a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento (1,25%). b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros) (1,25%). c)Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red (1,25%). d)Se han descrito las tecnologías de almacenamiento redundante y distribuido (1,25%). e) Se han seleccionado estrategias para la realización de copias de seguridad (1,25%). f) Se ha tenido en cuenta la frecuencia y el esquema de rotación (1,25%). g) Se han realizado copias de seguridad con distintas estrategias (1,25%). h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles (1,25%). i) Se han utilizado medios de almacenamiento remotos y extraíbles (1,25%). j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento (1,25%).		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad (0,60%). f) Se han aplicado técnicas de recuperación de datos (3,75%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. Copias de seguridad. Programación. - Práctica 2. Creación de imágenes. Clonación. - Práctica 3. Restauración de imágenes. - Práctica 4. Técnicas de recuperación de datos en diferentes unidades.		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD6			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
2	a	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 2	0,125%
	b	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 3	0,250%
	c	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 3	0,250%
	d	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 2	0,125%
	e	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 3	0,125%
	f	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 2	0,125%
		Práctica 3	0,125%
	g	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 2	0,125%
		Práctica 3	0,125%
	h	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 1	0,125%
		Práctica 3	0,125%
	i	Observación	0,125%
		Examen	0,750%
		Actividades	0,125%
		Práctica 3	0,250%
	j	Observación	0,125%
		Examen	0,750%

		Práctica 3	0,375%
3	a	Examen	0,360%
		Práctica 4	0,240%
	f	Observación	0,375%
		Examen	2,250%
		Actividades	0,375%
		Práctica 4	0,750%
			16,85%

UNIDAD 7: SOFTWARE MALICIOSO	**TEMP: ENE**	**4 HORAS**
OBJETIVOS	**CONTENIDO**	
• Diferenciar entre los diferentes tipos de software malicioso que existen. • Conocer los ataques de denegación de servicio. • Distinguir entre publicidad y correo no deseado. • Conocer en qué consiste la ingeniería social.	7.1 Concepto de software malicioso 7.2 Clasificación del malware. 7.3 Denegación de servicio 7.4 Publicidad y correo no deseado 7.5 Ingeniería social. Fraudes informáticos	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
b) Se han clasificado los principales tipos de software malicioso (4,5%). d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas (2,3%).		
RA4. 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 y robos de información (0,4%). c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado (0,667%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
INICIACIÓN: Presentación y explicación | Metodología: Aprendizaje Cooperativo y Activo		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. Análisis de un tipo de malware. Estudio de casos reales. Daños y soluciones.		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD7			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
3	b	Observación	0,450%
		Examen	2,700%
		Actividades	1,350%
	d	Observación	0,230%
		Examen	1,380%
		Actividades	0,690%
4	b	Observación	0,040%
		Examen	0,240%
		Práctica 1	0,120%
	c	Observación	0,067%
		Examen	0,400%
		Práctica 1	0,200%
			7,87%

UNIDAD 8: MEDIDAS DE PROTECCIÓN CONTRA EL MALWARE	**TEMP: FEB**	**6 HORAS**
OBJETIVOS	**CONTENIDO**	
• Conocer cómo se puede proteger un equipo para evitar infecciones de malware. • Aprender a actuar ante una infección por malware. • Diferenciar entre antivirus personales y corporativos. • Aprender a evitar infecciones en correos corporativos.	8.1 Medidas de protección contra el software malicioso Medidas preventivas contra el malware Medidas paliativas contra el malware 8.2 Centros de protección y respuestas frente a amenazas 8.3 Buenas prácticas para protegerse del malware	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades (4,5%). d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas (2,3%).		
RA4. 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 y robos de información (0,4%). c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado (0,667%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. Infección controlada. - Práctica 2. Software congelador. - Práctica 3. SpyBot.		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD8			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
3	c	Observación	0,450%
		Examen	2,700%
		Actividades	0,450%
		Práctica 1	0,900%
	d	Observación	0,230%
		Examen	1,380%
		Práctica 1	0,690%
4	b	Observación	0,040%
		Examen	0,240%
		Práctica 2	0,120%
	c	Observación	0,067%
		Examen	0,400%
		Actividades	0,067%
		Práctica 3	0,133%
			7,87%

UNIDAD 9: SEGURIDAD EN REDES	**TEMP: FEB**	**10 HORAS**
OBJETIVOS	**CONTENIDO**	
• Estudiar las vulnerabilidades existentes en la comunicación entre equipos. • Conocer qué es una herramienta de monitorización y cómo nos puede ayudar a mejorar la seguridad de una red. • Aprender cómo funcionan y cómo nos pueden ayudar algunas herramientas de protección de redes como cortafuegos, proxies o detectores de intrusos. • Conocer los mecanismos de seguridad en redes inalámbricas y sus vulnerabilidades. • Aprender qué es una auditoría de seguridad informática y para qué se utiliza.	9.1 Métodos para asegurar la privacidad de la información transmitida. 9.2 Seguridad en redes Servicios de red Vulnerabilidades Monitorización de redes. Escaneo de puertos. Detección de intrusos Permisos de recursos compartidos en red Seguridad en los navegadores Seguridad en las redes sociales 9.3. Seguridad en redes inalámbricas Tecnologías Wi-Fi Seguridad Wi-Fi. Monitorización de redes Wi-Fi Detección de intrusos. 9.4 Sistemas cortafuegos en equipos y servidores. Tipos de Cortafuegos Instalación y configuración de proxys. Instalación y configuración de cortafuegos. Registros de actividad del cortafuegos 9.5 Auditorías de seguridad en redes Tipos de auditorías de red Herramientas para auditorías	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso. (6%)		
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.		
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red (1%). c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado (0,667%). d) Se han aplicado medidas para evitar la monitorización de redes cableadas (2%). e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas (2%). h) Se ha instalado y configurado un cortafuegos en un equipo o servidor (1%).		
INSTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos.		
- Práctica 1. NMAP - Práctica 2. ARP Poisoning - Práctica 3. Configuración Proxy. - Práctica 4. IDS Snort.		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD9			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
3	e	Observación	0,600%
		Examen	5,400%
4	a	Observación	0,100%
		Examen	0,600%
		Práctica 1	0,300%
	c	Observación	0,067%
		Examen	0,400%
		Práctica 1	0,200%
	d	Observación	0,200%
		Examen	1,200%
		Actividades	0,200%
		Práctica 2	0,400%
	e	Observación	0,200%
		Examen	1,200%
		Actividades	0,200%
		Práctica 3	0,400%
	h	Observación	0,100%
		Práctica 4	0,900%
			12,67%

Para el caso del alumnado en régimen ordinario, los contenidos asignados a la Unidad 10 están pensados para ser trabajados de forma íntegra en la empresa, esto implica que las actividades para adquirir los criterios de evaluación serán las que decida la empresa según el plan de formación (Tabla A). No obstante, si por cualquier situación o contingencia no se pudiera cursar en la empresa, los contenidos asignados a la Unidad 10 y los criterios de evaluación asociados serán trabajados en forma de actividades y pruebas evaluables, cuya planificación aparece detallada en la tabla B.

Tabla A: Formación dual

UNIDAD 10: NORMATIVA SOBRE SEGURIDAD Y PROTECCIÓN DE DATOS.	**TEMP: MAR-MAY**	**DUALIZADO**
OBJETIVOS	**CONTENIDO**	
• Tomar conciencia de la importancia de la protección de datos. • Describir la legislación existente sobre protección de datos. • Identificar las figuras legales que intervienen en el tratamiento de datos. • Conocer la legislación existente sobre los servicios de la sociedad de la información y el comercio electrónico. • Contrastar las normas ISO sobre gestión de la seguridad de la información.	Plan formativo de la empresa que incluirá: Conocer la Ley Orgánica de Protección de Datos y el RGPD. Analizar las consecuencias del incumplimiento normativo. Aplicar medidas básicas de cumplimiento (políticas de privacidad, consentimiento, derechos ARCO).	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
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 (1,875%). b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada (2,000%). c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos (1,875%). d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen (1,875%). e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico (2,5%) f) Se han contrastado las normas sobre gestión de seguridad de la información (1,875%).		
INSTRUMENTOS DE EVALUACIÓN		
Valoración del cumplimiento de buenas prácticas en el entorno laboral.		
ACTIVIDADES		
Actividades formativas en la empresa		
REFUERZO Y AMPLIACIÓN		
Actividades formativas en la empresa		

VALORACIÓN DE LO APRENDIDO UD10			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
5	a	Actividades formativas en la empresa	1,875%
	b	Actividades formativas en la empresa	2,000%
	c	Actividades formativas en la empresa	1,875%
	d	Actividades formativas en la empresa	1,875%
	e	Actividades formativas en la empresa	2,500%
	f	Actividades formativas en la empresa	1,875%
			12,000%

Tabla B: En caso de no poder cursar las prácticas en empresa.

UNIDAD 10: NORMATIVA SOBRE SEGURIDAD Y PROTECCIÓN DE DATOS.	**TEMP: MARZO-MAYO**	
OBJETIVOS	**CONTENIDO**	
• Tomar conciencia de la importancia de la protección de datos. • Describir la legislación existente sobre protección de datos. • Identificar las figuras legales que intervienen en el tratamiento de datos. • Conocer la legislación existente sobre los servicios de la sociedad de la información y el comercio electrónico. • Contrastar las normas ISO sobre gestión de la seguridad de la información.	Conocer la Ley Orgánica de Protección de Datos y el RGPD. Analizar las consecuencias del incumplimiento normativo. Aplicar medidas básicas de cumplimiento (políticas de privacidad, consentimiento, derechos ARCO).	
RESULTADOS DE APRENDIZAJE - CRITERIOS DE EVALUACIÓN – PESO		
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 (1,875%). b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada (2,000%). c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos (1,875%). d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen (1,875%). e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico (2,5%) f) Se han contrastado las normas sobre gestión de seguridad de la información (1,875%).		
INTRUMENTOS DE EVALUACIÓN		
Pruebas escritas o por ordenador Realización de trabajos prácticos o de investigación, tanto a nivel individual como en grupo. Observación diaria de la actividad en clase de cada alumno.		
ACTIVIDADES		
- Breve cuestionario inicial sobre el contenido de la unidad en formulario on-line. Individual. - Exposición de los contenidos. - Respuesta común en parejas – Debate sobre un tema de actualidad/noticia relacionada con los contenidos de la unidad.		
- Práctica 1. Análisis de datos de naturaleza heterogénea. Caracterización y protección según su tipología. Consecuencias del incumplimiento normativo. Figuras legales que intervienen en el tratamiento de datos.		
- Resolución dudas. Corrección de ejercicios. Repaso para reforzar contenidos y extraer conclusiones. - Prueba de conocimiento (Examen). - Rúbrica de autoevaluación y rúbrica de evaluación práctica docente.		
REFUERZO Y AMPLIACIÓN		
Revisión vídeos y material adicional.		
TRABAJO EN CASA: Actividades de consolidación		

VALORACIÓN DE LO APRENDIDO UD10			
RA	**CE**	**Procedimiento**	**Peso parcial CE**
5	a	Observación	0,187%
		Examen	1,688%
	b	Observación	0,200%
		Examen	1,200%
		Actividades	0,600%
	c	Examen	0,187%
		Actividades	1,125%
		Práctica 1	0,563%
	d	Examen	0,187%
		Actividades	1,125%
		Práctica 1	0,563%
	e	Observación	0,250%
		Examen	1,500%
		Actividades	0,250%
		Práctica 1	0,500%
	f	Observación	0,187%
		Examen	1,125%
		Actividades	0,188%
		Práctica 1	0,375%
			12,000%

2.3. Objetivos

Los objetivos generales de este ciclo formativo a los que contribuye a alcanzar este módulo de Seguridad Informática son los siguientes:

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

b) Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.

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

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.

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.

2.4. Competencias profesionales, personales y sociales

La competencia general del título de "Técnico en Sistemas Microinformáticos y Redes" 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. Dentro de la Orden del 7 de julio de 2009, también se recogen las principales competencias profesionales, personales y sociales del título. De todas ellas, la superación de este módulo contribuirá a alcanzar las siguientes:

- 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.
- Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
- 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.
- Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
- Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
- Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
- Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.
- Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
- Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y aprendizaje.

En cuanto a las **competencias transversales,** se persigue:

1. Analizar con una visión crítica la realidad actual, contrastando la información de los distintos medios de comunicación, y fomentando el respeto a las opiniones de los demás (alumnos, profesores, etc.). Para la consecución de esta competencia podemos realizar:

    a) Se realizarán actividades de grupo con exposiciones para favorecer el trabajo colaborativo.
    b) Se analizarán en clase noticias actuales relacionadas con los contenidos del módulo, analizando los diferentes puntos de vista de los interesados y favoreciendo el debate.

2. Valorar la importancia de la conservación del medio ambiente, fomentando el uso racional y eficiente de la energía, el agua y el papel, respetándolo y contribuyendo a su cuidado y mejora. Para la consecución de esta competencia podemos realizar:

    a) Toda la información y documentación manejada en clase estará en formato digital, fomentado el uso racional del papel.
    b) Se insistirá en la importancia de mantener una clase limpia, en orden y con un uso adecuado de su iluminación.

2.5. Metodología

Dado el enfoque que requiere el presente módulo, las clases serán fundamentalmente prácticas. Las clases expositivas tendrán un carácter complementario. Al comienzo de la unidad se hará una presentación en la que se explicarán los conceptos esenciales de cada tema que sirva de punto de partida para que los alumnos y alumnas puedan afrontar las actividades que se propondrán a continuación, ya sea para complementar lo expuesto por la profesora o para aplicarlo.

En cada unidad se realizará una exposición teórica de los contenidos del mismo y se realizarán exposiciones prácticas para explicar los procedimientos necesarios para llevar a cabo las capacidades profesionales en estudio. Los temas se expondrán en un lenguaje sencillo, a la vez que técnico, para que el alumno, futuro profesional, vaya conociendo la terminología y el argot que se utiliza en el campo del uso de seguridad informática.

La profesora resolverá las dudas que puedan tener los alumnos del ciclo, tanto teóricas como prácticas, incluso si él lo considerase necesario se realizarán ejercicios específicos que aclaren los conceptos que más cueste comprender a los alumnos. La profesora propondrá un conjunto de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser resueltos por los alumnos, bien en horas de clase o en casa.

Si las circunstancias lo permiten, se inculcará la idea de trabajo en equipo a través de trabajos y actividades a realizar por equipos de alumnos (2 ó 3 por actividad). La profesora propondrá también la resolución de ejercicios que conlleven un proceso de investigación y búsqueda de información. Finalmente la profesora corregirá y resolverá junto a los alumnos dichos ejercicios. Además se propondrá algún trabajo que englobe conocimientos de varios bloques temáticos para comprobar que los conocimientos mínimos exigidos en cada uno de ellos han sido satisfactoriamente asimilados por los alumnos del Ciclo Formativo.

Las prácticas se resolverán de forma individual o en grupo, en función del tipo de práctica que se esté realizando. También se propondrá resolver casos prácticos reales relacionados con la materia que se esté impartiendo (por ejemplo: instalación de la red del aula, añadir conexiones nuevas en el edificio, configurar las propiedades de red de equipos que estén prestando servicio en el centro, etc.) para que los alumnos vayan habituándose a resolver situaciones análogas a las que se enfrentarán en el futuro en el mundo laboral.

Todos los materiales, actividades y ejercicios se facilitarán a través de la plataforma educativa online de aprendizaje tipo Moodle o Classroom, para que el alumnado esté habituado al uso de estas herramientas de cara a posibles escenarios.

Dentro del uso de nuevas tecnologías acorde con la participación del centro en el programa TDE, los alumnos y alumnas podrán utilizar sus dispositivos móviles para actividades de distinto tipo (individuales y/o grupales), siempre con finalidad pedagógica, tras el permiso de sus profesores/as y bajo su supervisión. Tal uso podrá hacerse en las actividades lectivas, complementarias y extraescolares en las condiciones anteriormente especificadas.

2.6 Temporalización de los contenidos

A continuación se muestra una tabla con la temporalización y horas estimadas para cada uno de los bloques y unidades de trabajo que se han establecido para este módulo. Dado que en este módulo se cuenta con 4 horas semanales, se puede establecer una previsión de 52 horas aproximadas de septiembre a diciembre (coincidiendo con el primer trimestre) y 28 horas aproximadas al periodo comprendido entre enero y febrero, resultando una duración de 80 horas antes de irse a la empresa para la formación dual (en la cual estarán hasta finales de mayo en torno a 40 horas). En su secuenciación, se tomará como referente el inicio del curso escolar el 15 de septiembre y la finalización del periodo ordinario en febrero/marzo, comenzando a partir de dicho mes el periodo de recuperación extraordinario hasta el 23 de junio.

En la secuenciación y temporalización de los contenidos mostrada en las siguientes tablas se tendrá en cuenta su carácter flexible y revisable, atendiendo al ritmo de aprendizaje del alumnado, circunstancias escolares imprevistas y las dificultades o intereses planteados. En dicha tabla también se reflejan los RA y CE de los correspondientes al módulo que serán abordados en cada unidad didáctica.

Periodo	**RA(CE)**	**UD**	***TEMPORALIZACIÓN***	***HORAS***	
1 eval parcial	RA1(a,b), RA4(a,b), RA5(b)	UD1	Septiembre	10	**52**
	RA1(c,d,e,f,i)	UD2	Octubre	10	
	RA1(a,b,g,h), RA3(f)	UD3	Octubre/noviembre	12	
	RA1(a,b,g), RA4(a,b,f)	UD4	Noviembre	10	
	RA1(a), RA3(d) RA4(b,f,g)	UD5	Noviembre/diciembre	10	
2ª eval. parcial	RA2(a,b,c,d,e,f,g,h,i,j),RA3(a,f)	UD6	Enero	8	**28**
	RA3(b,d),RA4(b,c)	UD7	Enero	4	
	RA3(c,d),RA4(b,c,)	UD8	Febrero	6	
	RA3(e),RA4(a,c,d,e,h)	UD9	Febrero	10	
				80 horas	
DUAL	RA5(a,b,c,d,e,f)	UD10	Marzo-mayo	Dualizado	

2.7. Docencia telemática

En caso de suspensión de la actividad presencial en el aula debido a pandemia u otra eventualidad, el uso de las plataformas digitales de formación tales como Moodle y Classroom tendrá más protagonismo. En dichas plataformas se colocarán tanto los materiales audiovisuales y contenidos teóricos, como las prácticas y tareas que deban realizar el alumnado, a fin de asegurar la continuidad formativa en cuanto a transmisión de conocimientos y corrección de las tareas asignadas, todo ello siguiendo las recomendaciones de la Consejería de Educación y Deporte.

El uso de estas plataformas digitales de formación facilita al alumnado el acceso, en tiempo y forma, de todo lo que se va trabajando en clase, por lo que tanto los días que no pudieran acudir al centro, como si tuvieran que permanecer en casa, siempre tendrían acceso, gracias a estas plataformas, a todos los materiales, ejercicios y pruebas que se van realizando en clase. Además, se usarán herramientas tipo Moodle o Meet para las videoconferencias, intentando, siempre que sea posible que el método de trabajo sea el mismo para facilitar el estudio a los alumnos y alumnas.

Se podrán habilitar otras herramientas de comunicación tales como iPasen, emails y aplicaciones de mensajería instantánea para la correcta comunicación tanto de los alumnos presenciales como de aquellos que deban estar en casa. Si hubiera que realizarse alguna prueba de evaluación, se le facilitará la realización de la misma, bien en casa a través de las plataformas trabajadas en clase, siempre que el alumno se encuentre bien, o se le fijará una fecha para que pueda realizarla cuando vuelva a las aulas.

2.8. Acuerdos modificaciones tras la Evaluación Inicial

Tras la sesión de evaluación inicial, se han propuesto cambios en la distribución de la clase de 2ºSMR A para evitar ruidos y distracciones, ubicando a algunos alumnos con mayores dificultades para mantener la atención con otros con los que se puedan relacionar de forma satisfactoria y se favorezca su aprendizaje. Con esta medida se persigue favorecer la concentración durante la realización de las actividades y el seguimiento de las clases, así como fomentar hábitos de comportamiento adecuados a un entorno laboral real.

3. EVALUACIÓN

3.1. Aspectos generales

La evaluación del aprendizaje del alumnado se regirá por la **Orden de 18 de septiembre de 2025**, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de los grados D y E del Sistema de Formación Profesional en la Comunidad Autónoma de Andalucía y el **Decreto 147/2025** que establece la **ordenación general y la organización** de las enseñanzas de los Grados D y E del Sistema de **Formación Profesional** en Andalucía.

El proceso de evaluación será **objetiva, continua, formativa e integradora** de las competencias adquiridas en el centro y, en su caso, en la empresa u organismo equiparado. La evaluación se realizará tomando como referencia los resultados de aprendizaje (RA) y los criterios de evaluación establecidos.

A continuación se describen los principios del proceso de evaluación y asistencia:

1. **Carácter de la Evaluación:** La evaluación es **continua, formativa e integradora**. El profesorado responsable de la impartición del módulo es quien realiza la evaluación.
2. **Asistencia Obligatoria:** Para la modalidad presencial (en la que se imparte este módulo), la evaluación continua de los aprendizajes requerirá la **asistencia regular y obligatoria de al menos el 80 por ciento de la duración total del módulo**.
3. **Pérdida del Derecho a la Evaluación Continua:**
    - En caso de incumplimiento del porcentaje de asistencia obligatoria (80%), el alumno perderá el derecho a la evaluación continua.
    - El alumnado que pierda este derecho será notificado mediante medios que garanticen su constancia, utilizando para ello el Anexo I de la Orden de 18 de septiembre de 2025.
    - La primera evaluación final se calificará con la expresión «No evaluado» conforme a lo establecido en el artículo 27 del Decreto 147/2025, de 17 de septiembre. Esta calificación de «No evaluado» comportará, a todos los efectos, el cómputo de dicha convocatoria a efectos del límite máximo de convocatorias establecido.
    - Este alumnado deberá asistir a clase en el periodo comprendido entre la primera evaluación final y la segunda evaluación final. El equipo docente le indicará las tareas y pruebas necesarias, conforme a los criterios de evaluación asociados a los resultados de aprendizaje no superados.
2. **Situaciones Extraordinarias:** Las situaciones extraordinarias (como enfermedad prolongada, trabajo incompatible, o cuidado de familiares graves, entre otras) que impidan la asistencia con regularidad serán estudiadas por el equipo educativo del curso, que determinará las reglas de actuación según la legalidad vigente.
3. El profesorado informará al alumnado a principios de curso, acerca de criterios e instrumentos de evaluación del módulo profesional, así como de los requisitos mínimos exigibles para obtener una calificación positiva. Esta información estará disponible en la página Web del instituto https://iesjuandemairena.org/, así como en el tablón habilitado para ello.
4. **El alumnado dispondrá de un máximo de cuatro convocatorias,** con independencia de la oferta o modalidad en que los curse.
5. **La convocatoria extraordinaria** se concede excepcionalmente y por una sola vez, previa solicitud, una vez agotadas las cuatro convocatorias ordinarias. Esta convocatoria solo podrá autorizarse si concurren circunstancias excepcionales debidamente acreditadas (como enfermedad prolongada, desempeño de puesto de trabajo incompatible, cuidado de dependientes o NEAE). El procedimiento a seguir está regulado en la **Orden de 18 de septiembre de 2025.**

Para llevar a cabo la evaluación en dichos términos, se realizarán las siguientes sesiones de evaluación:

- **Evaluación Inicial**: Se realizará durante el primer mes y tiene por objetivo conocer las características, capacidades y conocimientos previos del alumnado. En ningún caso conlleva calificación.
- **Evaluaciones Parciales**: Se realizarán **dos sesiones de evaluación** parciales. La primera en el mes de diciembre y la segunda en los meses de febrero-marzo. La calificación se expresará en valores numéricos del 1 al 10, sin decimales, siendo positiva a partir de 5 puntos. Estas sesiones son meramente informativas.

- **Evaluaciones Finales**: Se llevarán a cabo **dos sesiones de evaluación fina**l. La fecha de la primera sesión de la evaluación final, no podrá ser anterior al 30 de mayo para 2º curso. La fecha de la segunda sesión de la evaluación final se corresponderá con la finalización del régimen ordinario de clase y no podrá ser anterior al 23 de junio.

Además, siguiendo la normativa de aplicación en la evaluación y calificación de la Formación Profesional, para poder superar este módulo, es requisito imprescindible que el alumno/a haya demostrado poseer los resultados de aprendizaje correspondientes. Para ello, al comenzar el curso, **el profesorado informará al alumnado** de los resultados de aprendizaje, contenidos, criterios de evaluación del módulo, así como de la metodología a aplicar y los requisitos mínimos exigibles para obtener una calificación positiva. De forma que, para superar el módulo el alumnado **deberá obtener una calificación igual o mayor a 5 en cada uno de los resultados de aprendizaje.**

El alumnado que no haya alcanzado con calificación positiva el módulo profesional en la primera evaluación final, **tendrá obligación de asistir a clases y continuar con las actividades lectivas hasta la fecha de finalización del régimen ordinario de clase que no será anterior al día 22 de junio de cada año y que culmina con la segunda evaluación final donde deberá obtener una calificación positiva para tener definitivamente superado el módulo.**

El alumnado que resulte aprobado en la Evaluación final primera, podrá optar a **subir nota** en la evaluación final segunda, para esto deberá realizar una serie de tareas propuestas por el profesor.

3.2. Criterios e instrumentos de evaluación

Se enumeran a continuación los resultados de aprendizaje (RA) asociados con el presente módulo junto con sus criterios de evaluación y que serán necesarios para adquirir las competencias propias de la materia:

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 específico.
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 cortafuego 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:

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

A continuación, se establecen los instrumentos comunes de evaluación que se utilizarán para valorar la adquisición de cada uno de los Resultados de Aprendizajes del módulo formativo, a través de sus correspondientes criterios de evaluación:

- **Producciones del alumnado**: resolución de ejercicios, trabajos realizados en clase o propuestos, en definitiva, el trabajo diario. Se valorarán:

  - **Actividades en el aula**: Se realizarán de forma individual. Se realizarán varias actividades en cada unidad didáctica que se evaluarán en la misma aula y se entregarán a través de la plataforma educativa usada (Moodle o Classroom), siempre que sea posible
  - **Trabajos prácticos o de investigación**: Se realizarán de forma individual o en grupos reducidos de dos o tres alumnos/as, y se entregarán a través de la plataforma educativa usada, siempre que sea posible. Algunos deberán ser realizados en el horario lectivo, y otros de mayor extensión, en casa.
  - **Exposiciones orales** de trabajos realizados tanto de forma individual como en grupo.

- **Pruebas de evaluación específicas: referidas a los contenidos del módulo.**

  - **Orales y escritas:** Los alumnos/as deberán contestar una serie de cuestiones de carácter teórico.
  - **Pruebas de evaluación práctica:** Los alumnos/as deberán resolver unos supuestos planteados aplicando un determinado instrumento o modelo a la situación descrita. En algunos casos tendrán la posibilidad de consultar libros, apuntes y documentación previamente preparados por el alumno/a.

Se trata de evaluar la capacidad de obtener información, analizarla y resolver problemas prácticos, más que la memorización de unos conocimientos teóricos.

- Los **alumnos/as que no se presenten a una prueba de evaluación** tendrán la oportunidad de hacerlo en la **prueba de recuperación** programada por el profesor/a.

- **Participación cívica e interés**: la observación directa y sistemática es un instrumento eficaz para informarnos sobre las motivaciones, intereses, progresos y dificultades, nos ayudan a conocer el estilo de aprendizaje del alumnado. Se realizarán anotaciones en el cuaderno del profesor/a. Se tendrán en cuenta la ***asistencia puntual a clase***, ***participación*** en clase y en las actividades propuestas, ***actitud colaboradora*** en los trabajos en grupo, ***interés*** por investigar. ***Orden***, ***claridad*** y ***limpieza en la elaboración de trabajos***. ***Respeto*** a las opiniones y trabajo desarrollado por los compañeros/as y a toda la comunidad educativa. Cumplimiento de las normas de actuación establecidas en el aula. Mantenimiento y cuidado de los equipos informáticos.

3.3. Criterios de calificación generales

3.3.1 EVALUACIÓN CONTINUA

Para disfrutar de esta evaluación continua se requerirá la asistencia regular y obligatoria de al menos el 80 por ciento de la duración total del módulo. La **evaluación continua consta de 2 evaluaciones parciales** (diciembre y febrero-marzo) de carácter informativo y **de una evaluación final primera** (no podrá ser anterior al 30 de mayo para 2º curso) que sí contempla una calificación final del módulo.

Si en la evaluación final primera el alumno tiene **una nota igual o superior a 5, teniendo todos los RA superados**, habrá aprobado el módulo. En caso contrario deberá seguir viniendo a clase para superar los RA pendientes, tal y como se detalla en el apartado 3.3.3.

El término calificar, en el contexto educativo, significa atribuir un valor (nota) al aprendizaje logrado por el alumnado que servirá para verificar aquello que el alumnado ha superado y/o asimilado atendiendo a una calificación. **Esta calificación se expresará en una escala numérica de 1 a 10**.

De cara a la obtención de dicha calificación, se considera que la evaluación del mismo estará basada en los resultados de aprendizaje (RA) y en los criterios de evaluación (CE) indicados en el apartado anterior. Cada RA y CE tendrá asociado un porcentaje que fije su peso específico para determinar la categorización de los mismos y será la herramienta de referencia para el cálculo de la calificación.

La siguiente tabla muestra los **pesos que tendrán los resultados de aprendizaje** de este módulo profesional. Esta tabla también incluye el porcentaje de cada RA que se desarrollará en la empresa de modo exclusivo o compartido. En el caso de compartición del resultado de aprendizaje, se detalla el porcentaje en que se calificarán las actividades desarrolladas en la empresa.

Resultados de aprendizaje (RA)	***Peso%***	***Peso% IES***	***Peso% Empresa***
RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	25,00%	25% (100%)	0% (0%)
RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	12,50%	25% (100%)	0% (0%)
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	30,00%	25% (100%)	0% (0%)
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	20,00%	20% (100%)	0% (0%)
RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	12,50%	0,5% (4%)	12% (96%)

Dado que esta medición de la adquisición de los RA y CE será realizada a través de las unidades didácticas impartidas en las distintas evaluaciones, y que cada unidad cubre parcialmente los RA y CE indicados a continuación, es posible también obtener el **peso de cada unidad didáctica**. Este peso es distinto dentro de las unidades que componen el desarrollo del módulo. En la siguiente tabla se presentan los porcentajes correspondientes a cada una de las unidades didácticas, indicando también el grado de participación parcial en cada uno de los RA asociados.

Mes	UD	RA(CE)	RA1	RA2	RA3	RA4	RA5	%UD CALIFICACIÓN TOTAL	%RA
SEP-DIC	UD1	RA1(a,b), RA4(a,b), RA5(b)	3,13%			1,40%	0,50%	5,03%	42,75%
	UD2	RA1(c,d,e,f,i)	7,50%					7,50%	
	UD3	RA1(a,b,g,h), RA3(f)	7,50%		3,75%			11,25%	
	UD4	RA1(a,b,g), RA4(a,b,f)	5,00%			3,40%		8,40%	
	UD5	RA1(a), RA3(d) RA4(b,f,g)	1,88%		2,30%	6,40%		10,58%	
ENE-FEB	UD6	RA2(a,b,c,d,e,f,g,h,i,j), RA3(a,f)		12,50%	4,35%			16,85%	45,25%
	UD7	RA3(b,d),RA4(b,c)			6,80%	1,07%		7,87%	
	UD8	RA3(c,d),RA4(b,c,)			6,80%	1,07%		7,87%	
	UD9	RA3(e),RA4(a,c,d,e,h)			6,00%	6,67%		12,67%	
DUAL	UD10	RA5(a,b,c,d,e,f)					12,00%	12,00	12,00%
			25%	**12,50%**	**30%**	**20%**	**12,50%**	**100%**	**100%**

Así, entre septiembre y diciembre se cubrirán el 42,75% de los RA, mientras que entre enero y febrero será el 45,25% y durante la formación dual el 12,00%. Estos porcentajes se obtienen de los RA y CE trabajados en cada periodo de tiempo según la temporalización, teniendo en cuenta las distribuciones de pesos de los RA y CE mostradas en las siguientes tablas:

Resultados de aprendizaje (RA)	Peso %	Criterios de evaluación (CE)	%CE en RA
RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	25%	a) Se ha valorado la importancia de mantener la información segura.	30%
		b) Se han descrito las diferencias entre seguridad física y lógica.	15%
		c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.	10%
		d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	5%
		e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	5%
		f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	5%
		g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.	15%
		h) Se ha valorado la importancia de establecer una política de contraseñas.	10%
		i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	5%
RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	12,5%	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	10%
		b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).	10%
		c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.	10%
		d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	10%
		e) Se han seleccionado estrategias para la realización de copias de seguridad.	10%

		f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.	10%
		g) Se han realizado copias de seguridad con distintas estrategias.	10%
		h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.	10%
		i) Se han utilizado medios de almacenamiento remotos y extraíbles.	10%
		j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	10%
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	30%	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.	2%
		b) Se han clasificado los principales tipos de software malicioso.	15%
		c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.	15%
		d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.	23%
		e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	20%
		f) Se han aplicado técnicas de recuperación de datos.	25%
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	20%	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.	15%
		b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.	10%
		c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	10%
		d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	10%
		e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	10%
		f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	20%
		g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	20%
		h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	5%
RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	12,5%	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	15%
		b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	20%
		c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	15%
		d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	15%
		e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	20%
		f) Se han contrastado las normas sobre gestión de seguridad de la información.	15%

Para esta asignación de pesos se ha tenido en cuenta tanto la dedicación horaria que va a tener cada RA así como la importancia del RA en sí mismo dentro del mercado laboral actual.

La valoración del grado de adquisición de los RA es medida a través de los criterios de evaluación (CE) sirviéndonos de actividades de enseñanza-aprendizaje diseñadas para tal fin en las unidades didácticas. Estas **actividades de evaluación contenidas en cada unidad serán valoradas de 0 a 10 puntos**. Dichas actividades estarán asociadas a uno o más criterios de evaluación (e indirectamente, a uno o más RAs).

Así, los **criterios de evaluación serán calificados con una nota numérica** utilizando dichas actividades y, para cada Unidad Didáctica evaluada, se consignará la calificación obtenida en los CE tratados en la misma. Se entenderá superados los RA y CE asociados si se obtiene una **valoración positiva** en los mismos (**puntuación igual o superior a cinco puntos**).

3.3.2 EVALUACIÓN PARCIAL

Para obtener la calificación de cada evaluación, al final de la misma, se calculará la calificación correspondiente, que será la media ponderada de los RA vistos en la evaluación. En este punto, conviene recordar que el peso del criterio de evaluación se enmarca dentro del resultado de aprendizaje al que se asocia, por lo que será necesario calcular el **peso efectivo del CE** que resultará de multiplicar el peso del CE de un RA dentro de la unidad por la ponderación correspondiente al RA ($\%RA_i$*$\%CE_j$_enRA_i).

Para la obtención de la calificación final de cada evaluación se tendrá en cuenta únicamente los RA y CE trabajados en dicha evaluación. De forma que la nota final se obtendrá como el sumatorio de los productos de la calificación (expresada en valores de 0 a 10) para cada CE trabajado por el peso efectivo expresado en porcentaje para cada criterio. Es decir, se usará **la media ponderada** por los pesos efectivos de las **calificaciones de cada uno de los CE trabajados** antes de cada sesión de evaluación parcial calculada de la siguiente forma.

$$Nota_{eval} = \frac{nota_{CE1}{}^{*}peso_{efect_{CE1}} + nota_{CE2}{}^{*}peso_{efect_{CE2}} + \ldots + nota_{CEn}{}^{*}peso_{efect_{CEn}}}{\sum_{i} peso_{efect_{CEi}}}$$

Así, al final de cada evaluación se calculará la calificación (*$Nota_{eval}$*) correspondiente, que será la media ponderada de los RA vistos desde el principio de curso. En caso de no haber visto un RA completo se calculará la media ponderada de los criterios de evaluación vistos de ese RA. En este sentido, conviene destacar que:

- Entre septiembre y diciembre (primera evaluación parcial) se evaluará totalmente el RA 1, y parcialmente los RA 3, RA 4 y RA 5, calificándose con el sistema de ponderación establecido, llevándolo al 100% para puntuar en Séneca por el sistema tradicional. Es decir, un alumno/a que tenga un diez en todas las unidades del citado periodo habrá obtenido un 42,75% de los RA, pero se calificará con un 10 la evaluación.
- Entre enero y febrero (segunda evaluación parcial), se le añadirán del mismo modo los RA 2, 3 y 4, por lo que en el anterior porcentaje se incrementará un 45,25%, resultando un 88% de los RA.
- Durante el periodo dualizado, es decir, durante la formación en la empresa, se evaluará el RA 5, cubriendo el 12% de los RA.
- Para calcular la nota en las sesiones de evaluaciones finales, se aplicarán los porcentajes de todos los RAs, es decir, sobre el 100%.

Se llevará un registro en hoja de cálculo para obtener la calificación de cada RA, unidad, actividad y criterio, y así poder realizar un mejor seguimiento y control de las calificaciones.

Para superar el módulo, debe obtenerse una calificación **igual o superior a 5** en cada RA. En caso contrario, **sólo deben recuperarse los RA y CE no superados**. La recuperación de los RAs no superados se realizará en el periodo comprendido entre la primera evaluación final y la segunda evaluación final de la siguiente manera, dependiendo de las características de las actividades evaluables y del criterio docente:

- Realización o rectificación de las mismas actividades evaluables asociadas al CE/RA siempre que no se haya proporcionado las soluciones y/o no exista riesgo de copia.
- Actividades de recuperación complementarias que sustituyan a las no superadas, atendiendo a los principios de evaluación continua, formativa y formadora.

- Pruebas escritas finales con contenido teórico-práctico. Cada elemento de la prueba deberá indicar el RA asociado y su puntuación.

El docente completará el informe de recuperación indicando al estudiante los RAs no superados y las actividades de recuperación asociadas, que deberán ser realizables en tiempo y forma. Igualmente, la calificación será numérica, entre 0 y 10.

El alumnado que resulte aprobado en la primera evaluación final, podrá optar a subir nota en la evaluación final segunda, para esto deberá realizar una serie de tareas propuestas por el profesorado.

Los criterios de calificación de cada resultado de aprendizaje se detallan en las siguientes tablas, indicando para cada RA: los criterios de evaluación, las ponderaciones de los CE, las actividades en las que se materializan, así como las unidades en las que se integran:

RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.					**PondRA: 25%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
1	1	a	UD1: Observación UD1: Examen UD1: Actividades	0,188% 1,125% 0,563%	7,50%
	3		UD3: Observación UD3: Examen UD3: Práctica 1	0,188% 1,125% 0,563%	
	4		UD4: Observación UD4: Examen UD4: Actividades	0,188% 1,125% 0,563%	
	5		UD5: Observación UD5: Examen UD5: Práctica 2	0,188% 1,125% 0,563%	
	1	b	UD1: Observación UD1: Examen UD1: Práctica 1	0,125% 0,750% 0,375%	3,75%
	3		UD3: Observación UD3: Examen UD3: Actividades UD3: Práctica 2	0,125% 0,750% 0,125% 0,250%	
	4		UD4: Observación UD4: Examen UD4: Práctica 1	0,125% 0,750% 0,375%	
	1	c	UD1: Observación UD1: Examen UD1: Actividades UD1: Práctica 2	0,250% 1,500% 0,250% 0,500%	2,50%
	2	d	UD2: Observación UD2: Examen UD2: Actividades UD2: Práctica 3 UD2: Práctica 4	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	2	e	UD2: Observación UD2: Examen UD2: Actividades UD2: Práctica 2 UD2: Práctica 5	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	2	f	UD2: Observación UD2: Examen UD2: Actividades UD2: Práctica 1 UD2: Práctica 3	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	3	g	UD3: Observación	0,188%	3,75%

			UD3: Examen UD3: Actividades UD3: Práctica 3	1,125% 0,188% 0,375%	
	4		UD4: Observación UD4: Examen UD4: Actividades UD4: Práctica 2	0,188% 1,125% 0,188% 0,375%	
	3	h	UD3: Observación UD3: Examen UD3: Actividades UD3: Práctica 1 UD3: Práctica 4	0,250% 1,500% 0,250% 0,250% 0,250%	2,50%
	2	i	UD2: Observación UD2: Examen UD2: Actividades UD2: Práctica 1 UD2: Práctica 2	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%

RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.					**PondRA: 12,50%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
2	6	a	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 1 UD6: Práctica 2	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	6	b	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 3	0,125% 0,750% 0,125% 0,250%	1,25%
	6	c	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 3	0,125% 0,750% 0,125% 0,250%	1,25%
	6	d	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 1 UD6: Práctica 2	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	6	e	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 1 UD6: Práctica 3	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	6	f	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 2 UD6: Práctica 3	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	6	g	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 2 UD6: Práctica 3	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%
	6	h	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 1 UD6: Práctica 3	0,125% 0,750% 0,125% 0,125% 0,125%	1,25%

	6	i	UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 3	0,125% 0,750% 0,125% 0,250%	1,25%
	6	j	UD6: Observación UD6: Examen UD6: Práctica 3	0,125% 0,750% 0,375%	1,25%

RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.					**PondRA: 30,00%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
3	6	a	UD6: Examen UD6: Práctica 4	0,360% 0,240%	0,60%
	7	b	UD7: Observación UD7: Examen UD7: Actividades	0,450% 2,700% 1,350%	4,50%
	8	c	UD8: Observación UD8: Examen UD8: Actividades UD8: Práctica 1	0,450% 2,700% 0,450% 0,900%	4,50%
	5	d	UD5: Actividades UD5: Examen UD5: Práctica 1	0,230% 1,380% 0,690%	6,90%
	7		UD7: Observación UD7: Examen UD7: Actividades	0,230% 1,380% 0,690%	
	8		UD8: Observación UD8: Examen UD8: Práctica 1	0,230% 1,380% 0,690%	
	9	e	UD9: Observación UD9: Examen	0,600% 5,400%	6,00%
	3	f	UD3: Observación UD3: Práctica 4	0,375% 3,375%	7,50%
	6		UD6: Observación UD6: Examen UD6: Actividades UD6: Práctica 4	0,375% 2,250% 0,375% 0,750%	

RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.					**PondRA: 20,00%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
4	1	a	UD1: Observación UD1: Examen UD1: Práctica 2	0,100% 0,600% 0,300%	3,00%
	4		UD4: Observación UD4: Examen UD4: Actividades UD4: Práctica 3	0,100% 0,600% 0,100% 0,200%	
	9		UD9: Observación UD9: Examen UD9: Práctica 1	0,100% 0,600% 0,300%	
	1	b	UD1: Observación UD1: Examen UD1: Práctica 3	0,040% 0,240% 0,120%	2,00%
	4		UD4: Observación UD4: Examen UD4: Práctica 3	0,040% 0,240% 0,120%	

	5		UD5: Observación UD5: Práctica 3	0,040% 0,360%	
	7		UD7: Observación UD7: Examen UD7: Práctica 1	0,040% 0,240% 0,120%	
	8		UD8: Observación UD8: Examen UD8: Práctica 2	0,040% 0,240% 0,120%	
	7	c	UD7: Observación UD7: Examen UD7: Práctica 1	0,067% 0,400% 0,200%	2,00%
	8		UD8: Observación UD8: Examen UD8: Actividades UD8: Práctica 3	0,067% 0,400% 0,067% 0,133%	
	9		UD9: Observación UD9: Examen UD9: Práctica 1	0,067% 0,400% 0,200%	
	9	d	UD9: Observación UD9: Examen UD9: Actividades UD9: Práctica 2	0,200% 1,200% 0,200% 0,400%	2,00%
	9	e	UD9: Observación UD9: Examen UD9: Actividades UD9: Práctica 3	0,200% 1,200% 0,200% 0,400%	2,00%
	4	f	UD4: Observación UD4: Examen UD4: Práctica 3	0,200% 1,200% 0,600%	4,00%
	5		UD5: Observación UD5: Examen UD5: Actividades UD5: Práctica 4	0,200% 1,200% 0,200% 0,400%	
	5	g	UD5: Observación UD5: Examen UD5: Actividades UD5: Práctica 4	0,400% 2,400% 0,400% 0,800%	4,00%
	9	h	UD9: Observación UD9: Práctica 4	0,100% 0,900%	1,00%

Para el módulo Seguridad Informática se dualiza el Resultado de Aprendizaje 5 de manera coparticipada con la empresa, a razón de 4% por parte del instituto y 96% por la empresa. Atendiendo a estos porcentajes, y teniendo en cuenta que el RA5 tiene un peso del 12,5% respecto al resto de RAs, la empresa tendrá un peso total del 12% respecto a la evaluación del módulo.

CASO 1: Formación dual en la empresa.

RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.					**PondRA: 12,50%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
5	10	a	Actividades formativas en la empresa	1,887%	1,875%
	1	b	UD1: Práctica 4	0,50%	2,500%
	10		Actividades formativas en la empresa	2,00%	
	10	c	Actividades formativas en la empresa	1,887%	1,875%
	10	d	Actividades formativas en la empresa	1,887%	1,875%

	10	e	Actividades formativas en la empresa	2,500%	2,500%
	10	f	Actividades formativas en la empresa	1,875%	1,875%

CASO 2: Para alumnado que no pueda cursar la formación dual en empresa.

RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.					**PondRA: 12,50%**
RA	**Unidad Didáctica**	**Criterios evaluación**	**Actividad - Instrumento**	**Contribución**	**Peso efect CE %**
5	10	a	UD10: Observación UD10: Examen	0,187% 1,688%	1,875%
	1	b	UD1: Práctica 4	0,500%	2,50%
	10		UD10: Observación UD10: Examen UD10: Actividades	0,200% 1,200% 0,600%	
	10	c	UD10: Examen UD10: Actividades UD10: Práctica 1	0,187% 1,125% 0,563%	1,875%
	10	d	UD10: Examen UD10: Actividades UD10: Práctica 1	0,187% 1,125% 0,563%	1,875%
	10	e	UD10: Observación UD10: Examen UD10: Actividades UD10: Práctica 1	0,250% 1,500% 0,250% 0,500%	2,50%
	10	f	UD10: Observación UD10: Examen UD10: Actividades UD10: Práctica 1	0,187% 1,125% 0,188% 0,375%	1,875%

3.3.3 EVALUACIÓN FINAL PRIMERA

La calificación **final primera** será la **media ponderada de todos los RA** vistos en el curso, siempre que estén todos superados. Si alguno no hubiese sido superado la nota en ningún caso será superior a 4.

La recuperación de los RAs no superados se realizará en el periodo comprendido entre la primera evaluación final y la segunda evaluación final. En este periodo los alumnos/as tendrán que seguir asistiendo a clase hasta que tenga lugar la segunda evaluación final del módulo.

El alumnado que resulte aprobado en la Evaluación final primera, podrá optar a subir nota en la evaluación final segunda, para esto deberá realizar una serie de tareas y/o pruebas propuestas por el profesor.

3.3.*4* EVALUACIÓN FINAL SEGUNDA

Aquellos alumnos/as que no obtengan el aprobado en la evaluación continua, plasmada en la evaluación final primera **tendrán que asistir a clase en el periodo comprendido entre la primera evaluación final y la segunda evaluación final**. El equipo docente le indicará las tareas y pruebas necesarias, conforme a los criterios de evaluación asociados a los resultados de aprendizaje no superados.

Durante este tiempo, los alumnos/as tendrán que realizar las siguientes actividades de recuperación o mejora:

- Repaso de los contenidos.
- Resolución de dudas.
- Elaboración de actividades, resúmenes y esquemas.

- Realización de pruebas de evaluación específicas.
- Realización de pruebas prácticas.

Todas ellas orientadas a lograr superar los resultados de aprendizaje no alcanzados para poder superar todos los objetivos del módulo.

El alumno/a sólo tendrá que recuperar los resultados de aprendizaje no superados, del resto conservará sus calificaciones, volviendo a aplicar las ponderaciones para el cálculo de la calificación explicadas en el apartado 3.3.1.

3.3.5 CRITERIOS DE CORRECCIÓN

Los **criterios de corrección** de las pruebas escritas o sobre el ordenador se basarán en:

- Funcionamiento.
- Cumplimiento de los requisitos expuestos en el examen.
- Seguimiento de las normas de actuación desarrolladas en el aula.
- Ausencia total de errores sintácticos y semánticos.

Las consideraciones sobre las **Producciones del alumnado** *son las siguientes*:

- Son de entrega obligatoria a través del medio y plazo establecido por el profesorado, siempre que no se indique su voluntariedad.

- Aquellos alumnos/as que no asistieron a clase durante el desarrollo de alguna actividad y justifiquen su falta de asistencia mediante documento acreditado, podrán entregarla en la plataforma en un nuevo plazo establecido por el profesor/a.

- Cuando la tarea sea de obligada entrega y existan alumnos/as que, estando en clase, no entreguen la tarea en el plazo establecido, el profesor/a podrá fijar, si lo considera necesario, un segundo plazo de entrega para aquellos alumnos/as que lo necesiten. En este caso se penalizarán acorde con la demora, siendo la penalización del 10-40% de la nota obtenida en la misma si se entregan entre 1-4 días de retraso.

- Pasados cuatro días del día de entrega (o llegado el momento de su corrección), la práctica se considera no entregada.

- Se tendrá en cuenta la presentación, la ortografía y la gramática en las entregas escritas y presentación de trabajos.

- En caso de encontrar dos trabajos iguales, se anularán los dos y se tomarán las medidas oportunas.

- Ciertas prácticas requerirán la asistencia a clase en un día concreto.

La observación directa y sistemática es un instrumento eficaz para informarnos sobre las motivaciones, intereses, progresos y dificultades, nos ayudan a conocer el estilo de aprendizaje del alumnado. Se realizarán anotaciones en el cuaderno del profesor/a. Para evaluar la **Participación cívica e interés** se tendrá en cuenta lo siguiente:

- Asistencia puntual a clase.
- Participación activa en las prácticas realizadas.
- Actitud colaboradora en los trabajos en grupo
- Trabajo y esfuerzo (individual o en grupo) en clase.
- Responsabilidad con el material de trabajo.
- Orden, claridad y limpieza.
- Iniciativa propia. Resolutivo/a.
- Interés por la materia tratada y curiosidad por investigar. Atención.

- Atención. Predisposición a tomar apuntes y buscar información complementaria.
- Participación activa en las exposiciones y debates.
- Educación y respeto hacia el/la profesor/a, compañeros/as y el resto de la comunidad educativa.

3.4. Plan Personalizado de Recuperación

El alumnado de segundo que repita curso o haya promocionado con módulos pendientes de primer curso asistirá a clase y participará en las actividades de manera ordinaria como el resto del alumnado. En este curso hay cuatro alumnos en esta situación, dos en 2º SMR A y otros dos en 2ª SMR B. En base a ello, se ha establecido que el plan de recuperación incluya la realización de las **mismas actividades y pruebas evaluables asociadas al CE/RA dentro del periodo ordinario**. Para el cálculo de la calificación se utilizará se utilizará el **mismo sistema de pesos asignado a los criterios de evaluación** siguiendo el procedimiento del apartado 3.3.1.

No obstante, se les realizará un seguimiento a fin de identificar dificultades de aprendizaje e introducir mejoras si fuese oportuno:

- Sesión de evaluación inicial: se establecerá el perfil del alumnado y el estilo de aprendizaje, punto de partida para elaborar el plan individualizado.
- Revisión del trabajo del alumnado para comprobar, el grado de realización de actividades, y valoración del avance del alumnado.
- Reuniones periódicas, haciéndolas coincidir con las sesiones de evaluación parciales y/o finales.
- Valoración del plan de actividades y su idoneidad para el alumnado.

3.5. Medidas de atención a la diversidad

De forma genérica, se plantea la atención a la diversidad en los siguientes casos:

- **Alumnos con dificultades de aprendizaje:** Son aquellos alumnos/as que tienen más dificultades que sus compañeros para acceder al aprendizaje determinado en los currículos que corresponden a su edad.
- **Alumnos con discapacidades:** Aquí englobamos al alumnado con dificultades físicas o de comunicación tales como invidentes, sordos, problemas de movilidad, etc. Antes de tomar cualquier medida, siempre solicitaremos la colaboración y asesoramiento del departamento de orientación.
- **Alumnos con mayor capacidad intelectual:** En general son aquellos alumnos cuya capacidad intelectual es superior a la media, presentan un alto nivel de creatividad y un alto grado de dedicación a las tareas. En este curso escolar no se ha detectado alumnado con estas características en las pruebas iniciales. No obstante, en caso de identificar más adelante estas características en el alumnado, se plantea un seguimiento individualizado del alumno/a que consistirá fundamentalmente en la **realización de actividades de ampliación** en cada unidad didáctica y cuyo resultado sea un enriquecimiento del alumno y una mayor motivación. Estas actividades estarán enfocadas a configuraciones más complejas y funcionalidades adicionales de algunas de las prácticas de cada unidad, para ello se le darán al alumno algunas directrices para la realización de trabajos de investigación que después, con apoyo de la profesora, deberán poner aplicar a la actividad encomendada.

En este curso, en 2º SMR contamos con un grupo de alumnos/as con dificultades de aprendizaje (algunos de ellos/as tienen informe en Séneca de años anteriores), cabe destacar a los siguientes alumnos/as con necesidades específicas de apoyo educativo que requieren medidas específicas para apoyar el aprendizaje distinguiendo por grupo tenemos:

2º SMR A

El grupo está formado por 18 alumnos y tiene un carácter heterogéneo, con una parte del alumnado con buenos resultados y otra parte que tiene ciertas dificultades. El ambiente de trabajo es bueno, la mayoría del alumnado se conoce del curso anterior, salvo un alumno que se ha incorporado nuevo al centro. Hay dos alumnos que están repitiendo con algunos módulos pendientes. En el grupo hay varios alumnos con NEAE:

- 2 alumnos con TDAH, uno de ellos toma medicación.
- 1 alumno con dificultades específicas en el aprendizaje de la lectura o dislexia.
- 1 alumno con dificultades de aprendizaje por retraso en el lenguaje.

2º SMR B
El grupo tiene un carácter heterogéneo, donde hay alumnos con muy buenas notas y otros que aprobaron en el periodo de recuperación del curso anterior. El ambiente de trabajo es bueno, la mayoría del alumnado se conoce del curso anterior. El grupo de 2º SMR B está formado por 18 alumno/as, 17 chicos y 1 chica. Este curso se han incorporado 3 alumnos nuevos procedentes de otros centros , y también hay 2 alumnos repetidores con todos los módulos. En el grupo hay varios alumnos con NEAE:

- 1 alumno/a con Hipoacusia (discapacidad reconocida del 38%)
- 1 alumnos/as con Asperger.

Siguiendo las recomendaciones del Departamento de Orientación, se proponen las siguientes medidas:

- Tener muy presente las relaciones entre el alumnado a la hora de realizar los grupos, de forma que estén integrados dentro un grupo que los acepte y puedan desarrollar su actividad diaria en un ambiente favorable.
- Situar al alumnado dentro del aula en posiciones cercanas al profesorado y a la pizarra, así como próximos a compañeros/as con los que se puedan relacionar de forma satisfactoria y se ayuden unos a otros.
- Cuando trabajan en grupo integramos a los alumnos/as con más carencias en grupos de trabajo mixtos.
- Para favorecer la comprensión de las explicaciones los docentes se apoyarán en distintos medios audiovisuales, transparencias, videoproyector, etc.
- La prioridad será ayudarlos a que accedan a una comunicación eficaz que le permita preservar y desarrollar su capacidad cognitiva.

Las adaptaciones de contexto que actúan sobre la estructura grupal y el clima emocional del aula, flexibilizan el uso de tiempos y espacios y modifican los agrupamientos en el aula, entre otras cosas, se concretarán en lo siguiente:

- Proporcionar a los alumnos/as más tiempo para realizar las pruebas de evaluación.
- Evitar en las pruebas de evaluación preguntas interrogativas negativas o enunciados enlazados que dificulten a estos alumnos/as la comprensión de los mismos.
- Proporcionar a los alumnos/as más tiempo para realizar las actividades previstas en el aula.
- Trabajar en grupos pequeños.
- Sensibilizar al resto del grupo para que utilicen recursos comunicativos adecuados que faciliten la comprensión de los mensajes en el aula.
- Atender de manera más individualizada aquellas necesidades que demanden los alumnos/as

3.6. Dualización del módulo

3.6.1. SECUENCIACIÓN Y TEMPORALIZACIÓN

Las prácticas en empresa se realizarán entre el segundo y tercer trimestre, teniendo previsto su comienzo en la segunda quincena de febrero y su finalización la segunda quincena de mayo.

Para este módulo corresponden un total de 40 horas de formación en la empresa aproximadamente.

3.6.2. REPARTO DE RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

Para el módulo Seguridad Informática se dualiza el Resultado de Aprendizaje 5 de manera coparticipada con la empresa, a razón de 4% por parte del instituto y 96% por la empresa. Atendiendo a estos porcentajes, y teniendo en cuenta que el RA5 tiene un peso del 12,5% respecto al resto de RAs**, la empresa tendrá un peso total del 12% respecto a la evaluación del módulo**.

Centrándonos en los criterios de evaluación del RA5, a continuación se indican los CE trabajados en la empresa y los trabajados en el instituto.

Criterios de Evaluación en la empresa: a,b,c,d,e,f

Criterios de Evaluación en el instituto: b

3.6.3. INSTRUMENTOS DE EVALUACIÓN

Los instrumentos de evaluación serán actividades formativas desarrolladas en la empresa, estas actividades irán asociadas a uno o varios Criterios de Evaluación.

Estas actividades formativas en la empresa estarán detalladas de manera general en el documento “Plan de Formación Inicial” y para cada alumno en el “Plan de Formación Individualizado”.

3.6.4. EVALUACIÓN DE LOS RA DUALIZADOS

Para las actividades formativas desarrolladas en la empresa el tutor laboral emitirá una valoración cualitativa. El profesor del módulo es el que debe decidir la nota cuantitativa de los criterios de evaluación asociadas a cada tarea.

Cuando el alumno no pueda realizar las prácticas en empresas, tendrá que superar los Criterios de Evaluación en el instituto siguiendo los instrumentos de evaluación determinados por el profesor.