PROGRAMACIÓN DE SEGURIDAD Y ALTA DISPONIBILIDAD 2º CURSO ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

I. INTRODUCCIÓN

El desarrollo didáctico y la programación del módulo **Seguridad y Alta Disponibilidad** se obtienen a partir del perfil del Ciclo Formativo de Grado Medio: **Administración de Sistemas Informáticos en Red (ASIR)**.

De acuerdo con el **Decreto 147/2025**, de 17 de septiembre, y la normativa básica estatal que regula las enseñanzas mínimas del título de **Técnico Superior en Administración de Sistemas Informáticos en Red**, el ciclo queda identificado por los siguientes elementos:

Denominación	**Administración de Sistemas Informáticos en Red (ASIR)**
Nivel	Formación Profesional de Grado D, nivel 3 de CNCP (equivalente a Grado Superior)
Duración	2000 horas distribuidas en dos cursos académicos
Familia Profesional	Informática y Comunicaciones
Referente Europeo	Nivel 5 del Marco Europeo de Cualificaciones (EQF)
Carácter	Formación Profesional Dual de Carácter General, con Fase de Formación en Empresa u Organismo Equiparado
Competencia General	Configurar, administrar y mantener sistemas informáticos en red, asegurando su funcionalidad, integridad y acceso seguro a los recursos, proporcionando asistencia a las personas usuarias y aplicando criterios de calidad, accesibilidad y sostenibilidad.

Esta programación responde a este enfoque dual y al nuevo marco andaluz (Decreto 147/2025 y Orden de 18 de septiembre de 2025). Su finalidad es planificar de forma coherente el proceso de enseñanza-aprendizaje, garantizando:

- La adquisición de las competencias profesionales, personales y sociales vinculadas al desarrollo de aplicaciones y la administración de datos.
- La integración de metodologías activas y participativas, centradas en el alumnado y orientadas a la resolución de problemas reales.
- La coherencia con el Proyecto Educativo del Centro, la atención a la diversidad y la mejora continua del proceso docente.

Este módulo tiene una duración total de **105 horas anuales**, con una frecuencia de **3 horas**

semanales durante **35 semanas** y contiene la formación necesaria para *seleccionar y utilizar técnicas y herramientas específicas de seguridad informática en el ámbito de la administración de sistemas. Además, servirá para conocer arquitecturas de alta disponibilidad y utilizar herramientas de virtualización en la implantación de servicios de alta disponibilidad.*

Además, teniendo en cuenta que el ciclo formativo es Dual, ciertos resultados de aprendizaje o criterios de evaluación se desarrollarán en la Fase de Formación en Empresa u Organismo Equiparado (a partir de ahora FFEOE). La FFEOE se realizará desde el **25 de enero** hasta **19 de mayo**, cuatro días a la semana (lunes, martes, jueves y viernes). El número total de **horas duales** en empresa correspondientes el módulo serán de **51**, por lo que en el centro se impartirán **54 horas** del módulo de Seguridad y Alta Disponibilidad.

La programación consta de 7 **Unidades de Trabajo**. En el siguiente cuadro mostramos la temporalización de dichas unidades didácticas incluyendo la distribución horaria de cada una de ellas, el tiempo necesario para la realización de las pruebas diagnósticas teóricas y prácticas que evaluarán los contenidos de las mismas:

UNIDADES DE TRABAJO		Horas
Unidad 1:	Principios de seguridad y alta disponibilidad	8
Unidad 2:	Auditorías de seguridad	12
Unidad 3:	Criptografía	15
Unidad 4:	Alta disponibilidad	28
Unidad 5:	Seguridad perimetral	20
Unidad 6:	Seguridad en redes corporativas	20
Unidad 7:	Legislación y normativa sobre seguridad	2
	Número Total de Horas	105

ACTIVIDADES FORMATIVAS EN LA EMPRESA
• AF1. Verificar el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. **RA2. b)** • AF2. Analizar diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. **RA2. d)** • AF3. Implantar aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. **RA2. e)** • AF4. Utilizar técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. **RA2. f)** • AF5. Planificar y llevar a cabo la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red, documentando el proceso de instalación, configuración y uso. **RA4. c), h)**

• AF6. Configurar filtros en un cortafuegos a partir de un listado de reglas de filtrado. **RA4. d)** • AF7. Revisar los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. **RA4. e)** • AF8. Probar distintas opciones para implementar cortafuegos, tanto software como hardware. **RA4. f)** • AF9. Diagnosticar problemas de conectividad en los clientes provocados por los cortafuegos. **RA4. g)**
Total horas FFEOE = 51

Atendiendo al Decreto 327/2010 de 13 de julio (art. 29), "las programaciones didácticas de la formación profesional inicial deberán incluir las competencias profesionales, personales y sociales que hayan de adquirirse".

Según la Orden de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de **Técnico Superior en Administración de Sistemas Informáticos en Red**, la formación del módulo **Seguridad y Alta Disponibilidad** contribuye a alcanzar las **competencias profesionales, personales y sociales** de este título que se relacionan a continuación:

- e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
- f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
- i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
- j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
- k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
- m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
- n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.
- o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
- r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
- s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

II. RESULTADOS DE APRENDIZAJE. TRATAMIENTO EN CADA UNIDAD

Las Unidades Didácticas descritas en la sección anterior permiten abordar y cumplir con todos los Resultados de Aprendizaje establecidos en la normativa vigente.

En la siguiente tabla se detallan dichos resultados de aprendizaje y su relación con las unidades didácticas que los desarrollan:

RESULTADOS DE APRENDIZAJE	UNIDADES DE TRABAJO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
RA-1*: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	X						
RA-2*: Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.		X	X				
RA-3*: Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.						X	
RA-4*: Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.					X		
RA-5*: Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.					X		
RA-6*: Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.				X			
RA-7: Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.							X

Según la **Orden 18/09 de 2025, en el artículo 3b)** *La diferente contribución, en su caso, de cada resultado de aprendizaje para alcanzar las competencias profesionales en el marco de la contextualización del currículo al entorno en el que se desarrolle el proceso de enseñanza-aprendizaje y siempre asegurando la adquisición de dichas competencias, especificando si la superación del módulo o proyecto requiere la superación de la totalidad de los resultados de aprendizaje o solo la de aquellos que se determinen como imprescindibles.*

En la presente programación, los resultados de aprendizaje RA-1, RA-2, RA-3, RA-4, RA-5, RA-6 marcados con un **asterisco *** se consideran imprescindibles para la superación del módulo.

III. CRITERIOS DE EVALUACIÓN

III.1 Criterios propios del módulo

Los criterios de evaluación específicos del módulo descrito a partir de los resultados de aprendizaje correspondientes son los que se especifican y ponderan en la tabla que aparece a continuación.

La ponderación de los resultados de aprendizaje y criterios de evaluación se ha establecido mediante acuerdo de departamento, en base al principio de autonomía pedagógica y en función de la importancia de los objetivos, competencias y contenidos relacionados con el módulo, de su necesidad para la comprensión de conocimientos, de la relación con tareas principales del técnico superior en Administración de Sistemas Informáticos en Red y del grado de complejidad de las mismas. Dichos Resultados corresponden a un 100% de la nota final del módulo.

RA 1 * 10%	**Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.**	**CE %**
a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.		10%
b) Se han descrito las diferencias entre seguridad física y lógica.		10%
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.		10%
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.		10%
e) Se han adoptado políticas de contraseñas.		10%
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.		10%
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.		20%
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.		10%
i) Se han identificado las fases del análisis forense ante ataques a un sistema.		10%

RA 2 * 22%	**Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.**	**CE %**
a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.		5%
b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.		15%

c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	10%
d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	10%
e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	15%
f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	15%
g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	10%
h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	10%
i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.	10%

RA 3 * 19%	**Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.**	**CE %**
a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.		8%
b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.		8%
c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.		8%
d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.		18%
e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.		20%
f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.		18%
g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.		20%

RA 4 * 12%	**Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.**	**CE %**
a) Se han descrito las características, tipos y funciones de los cortafuegos.		6%
b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.		6%
c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.		15%
d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.		15%

e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	15%
f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	20%
g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	15%
h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	8%

RA 5 * 12%	**Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.**	**CE %**
a) Se han identificado los tipos de proxy, sus características y funciones principales.		5%
b) Se ha instalado y configurado un servidor proxy-cache.		15%
c) Se han configurado los métodos de autenticación en el proxy.		15%
d) Se ha configurado un proxy en modo transparente.		15%
e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web.		15%
f) Se han solucionado problemas de acceso desde los clientes al proxy.		10%
g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.		10%
h) Se ha configurado un servidor proxy en modo inverso.		10%
i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.		5%

RA 6 * 19%	**Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.**	**CE %**
a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.		8%
b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.		8%
c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.		10%
d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.		16%
e) Se ha implantado un balanceador de carga a la entrada de la red interna.		16%
f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.		16%
g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y		10%

productividad del sistema.	
h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	8%
i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	8%

RA 7 6%	**Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.**	**CE %**
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.		14%
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.		14%
d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.		14%
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.		14%
f) Se han contrastado las normas sobre gestión de seguridad de la información.		15%
g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.		14%

III.2 Competencias personales y sociales a tener en cuenta para la asignación del alumnado a las empresas u organismos equiparados para la realización de la FFEOE

Con el objetivo de realizar la asignación de empresas al alumnado de forma objetiva, se valorarán las siguientes competencias personales y sociales puntuándolos de la siguiente forma:

COMPETENCIA	**Siempre**	**Casi siempre**	**A veces**	**Rara vez o nunca**
Realiza las tareas programadas en el tiempo establecido	4	3	2	1
Muestra iniciativa antes los problemas que se plantean y toma decisiones adecuadas	4	3	2	1
Cuida los recursos y evita riesgos medioambientales	4	3	2	1
Capacidad de innovación y creatividad	4	3	2	1
Sabe dialogar, negociar y trabajar cooperativamente	4	3	2	1
Muestra empatía, respeto y valora la diversidad de los compañeros	4	3	2	1

Los criterios de valoración serán los siguientes:

VALORACIÓN	CRITERIO
Siempre	No existen evidencias de su incumplimiento
Casi siempre	Existe 1 evidencia de su incumplimiento
A veces	Existen 2 evidencias de su incumplimiento
Rara vez o nunca	Existen 3 o más evidencias de su incumplimiento

III.3 Valoración del desempeño de las actividades realizas en la empresa

Atendiendo al **Decreto 147/2025**, de 17 de septiembre de 2025, en su artículo 27, para la evaluación de los resultados de aprendizaje que han sido dualizados (su obtención se ha llevado a cabo tanto en el centro docente como durante la fase de formación en empresa u organismo equiparado), la evaluación de tales resultados de aprendizaje será responsabilidad del personal docente que imparta el módulo o, en su caso, de la persona experta conjuntamente con la persona titular de la jefatura de departamento correspondiente o la persona titular de la dirección del centro.

La persona que ejerza la tutoría dual de empresa colaborará en la evaluación de los resultados de aprendizaje trabajados conjuntamente entre el centro docente y la empresa u organismo equiparado mediante la valoración cualitativa en términos de “superado” o “no superado” de los resultados de aprendizaje incluidos en las actividades formativas desarrolladas en la empresa u organismo equiparado, que será recogida por la persona que ejerza la tutoría dual docente, de conformidad con el apartado 7.a) del **artículo 18** del **Real Decreto 659/2023**, de 18 de julio.

La evaluación del módulo integrará la calificación del centro y la valoración de la empresa conforme a lo recogido en la programación didáctica y será responsabilidad final del equipo docente y del centro educativo.

Atendiendo al artículo 163 del RD 659/2023, el tutor laboral valorará en términos de “superado” o “no superado” cada uno de los RAs previstos y realizará una valoración cualitativa de la estancia en la empresa y sus competencias profesionales y para la empleabilidad. Para ello, durante los períodos de formación en la empresa, los tutores laborales tomarán nota del desempeño de cada alumno. Para ello utilizarán la documentación suministrada por el profesorado de los módulos duales (aquellos que tengan resultados de aprendizaje en la empresa) que contendrá los instrumentos necesarios para valorar las actividades duales que hayan sido programadas y facilitar así la valoración de los resultados de aprendizaje. Principalmente, se hará uso de rúbricas, fichas de observación y similares. Todo ello formará parte del informe de estancia en la empresa.

El alumnado debe documentar de forma sistemática las tareas y aprendizajes realizados en la empresa. Para ello, elaborará tanto unas fichas semanales a través de la plataforma ÁTICA, como un diario de prácticas, en el que describirá las actividades realizadas, los conocimientos adquiridos, etc., pudiendo adjuntar capturas de pantalla, fragmentos de código, informes breves, fotografías o descripciones técnicas de las actividades desarrolladas. Estas evidencias serán revisadas por el profesorado y formarán parte del proceso evaluador. Cabe resaltar que a pesar de que estas evidencias constituirán una parte relevante del proceso evaluador, hay que tener en cuenta las posibles restricciones relacionadas con la confidencialidad, protección de datos o propiedad intelectual de las empresas colaboradoras, se procurará por tanto, que la documentación aportada

por el alumnado sea profesional, precisa y respetuosa con dichas limitaciones, evitando incluir información sensible y priorizando descripciones técnicas generales u observaciones sobre competencias desarrolladas.

El profesorado del módulo, responsable último de la evaluación cuantitativa, integrará las calificaciones obtenidas en el centro educativo (a través de las actividades y criterios trabajados en clase) con los resultados cualitativos obtenidos de la estancia en empresa. Esta integración se realizará de forma ponderada, considerando tanto la valoración cualitativa y numérica emitida en la rúbrica descrita anteriormente por el tutor laboral, como el análisis de las evidencias aportadas por el alumno en su diario de prácticas.

La nota final del módulo reflejará, por tanto, un enfoque global y competencial del aprendizaje, coherente con la filosofía de la Formación Profesional actual. Esta metodología dual garantiza la coherencia entre lo aprendido en el centro y lo experimentado en la empresa, refuerza la evaluación por competencias y promueve una formación conectada con la realidad del mercado laboral.

Las calificaciones estimadas en función del informe de la estancia en empresa se obtendrán de la siguiente forma:

- De las actividades propuestas para su realización, se contabilizan únicamente aquellas que hayan podido realizarse.
- Cada actividad se asocia con uno o varios criterios de evaluación de un resultado de aprendizaje.

IV. CONTENIDOS: SECUENCIACIÓN Y TEMPORALIZACIÓN POR UNIDADES Y TRIMESTRES

Los contenidos básicos que se deben exigir al alumnado en el módulo de Seguridad y Alta Disponibilidad son los siguientes:

- Adopción de pautas y prácticas de tratamiento seguro de la información.
- Implantación de mecanismos de seguridad activa.
- Implantación de técnicas de acceso remoto. Seguridad perimetral.
- Instalación y configuración de cortafuegos.
- Instalación y configuración de servidores proxy.
- Implantación de soluciones de alta disponibilidad.
- Reconocimiento de la legislación y normativa sobre seguridad y protección de datos.

A continuación se muestra un mayor nivel de concreción de los contenidos, junto con la distribución de los mismos entre las distintas unidades que componen la programación del módulo.

DESGLOSE DE CONTENIDOS POR UNIDAD

Adopción de pautas y prácticas de tratamiento seguro de la información.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**
Fiabilidad, confidencialidad, integridad y disponibilidad. Elementos vulnerables en el sistema informático. Hardware, software y datos.	X						
Análisis de las principales vulnerabilidades de un sistema informático.	X	X					
Amenazas. Tipos. Amenazas físicas y lógicas.	X						
Seguridad física y ambiental. Ubicación y protección física de los equipos y servidores. Sistemas de alimentación ininterrumpida.	X						
Seguridad lógica. Criptografía.	X		X				
Listas de control de acceso.	X						
Establecimiento de políticas de contraseñas.	X		X				
Políticas de almacenamiento. Copias de seguridad e imágenes de respaldo. Medios de almacenamiento.	X						
Análisis forense en sistemas informáticos	X	X					
Implantación de mecanismos de seguridad activa.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**
Ataques y contramedidas en sistemas personales. Clasificación de los ataques.	X						
Anatomía de ataques y análisis de software malicioso. Herramientas preventivas.	X	X					
Herramientas paliativas.	X						
Actualización de sistemas y aplicaciones. Seguridad en la conexión con redes públicas. Pautas y prácticas seguras.	X	X					
Seguridad en la red corporativa. Monitorización del tráfico en redes.	X	X					
Seguridad en los protocolos para comunicaciones inalámbricas.	X						
Riesgos potenciales de los servicios de red.	X	X					
Intentos de penetración.		X					
Implantación de técnicas de acceso remoto. Seguridad perimetral.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**

Elementos básicos de la seguridad perimetral. Perímetros de red. Zonas desmilitarizadas. Arquitectura débil de subred protegida. Arquitectura fuerte de subred protegida.					X		
Redes privadas virtuales. VPN. Beneficios y desventajas con respecto a las líneas dedicadas. Técnicas de cifrado. Clave pública y clave privada. VPN a nivel de red. SSL, IPSec. VPN a nivel de aplicación. SSH.						X	
Servidores de acceso remoto. Protocolos de autenticación. Configuración de parámetros de acceso. Servidores de autenticación.						X	
Instalación y configuración de cortafuegos.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**
Utilización de cortafuegos. Filtrado de paquetes de datos. Tipos de cortafuegos. Características. Funciones principales. Instalación de cortafuegos. Ubicación. Reglas de filtrado de cortafuegos. Pruebas de funcionamiento. Sondeo. Registros de sucesos de cortafuegos.					X		
Instalación y configuración de servidores proxy.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**
Tipos de proxy. Características y funciones. Instalación de servidores proxy. Instalación y configuración de clientes proxy. Configuración del almacenamiento en la caché de un proxy. Configuración de filtros. Métodos de autenticación en un proxy.					X		
Implantación de soluciones de alta disponibilidad.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**
Definición y objetivos. Análisis de configuraciones de alta disponibilidad. Funcionamiento ininterrumpido. Integridad de datos y recuperación de servicio. Servidores redundantes. Sistemas de clusters. Balanceadores de carga. Instalación y configuración de soluciones de alta disponibilidad. Virtualización de sistemas. Posibilidades de la virtualización de sistemas. Herramientas para la virtualización. Configuración y utilización de máquinas virtuales. Alta disponibilidad y virtualización. Simulación de servicios con virtualización.				X			
Reconocimiento de la legislación y normativa sobre seguridad y protección de datos.	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**

Legislación sobre protección de datos. Figuras legales en el tratamiento y mantenimiento de los ficheros de datos. Legislación sobre los servicios de la sociedad de la información y correo electrónico.							X

La distribución de las unidades didácticas según las tres evaluaciones queda reflejada en la tabla siguiente. En dicha tabla, se detalla también la ponderación establecida para los resultados de aprendizaje específicos del módulo en función de las horas que dedicamos durante el curso a cada uno de ellos:

Ud.	Trim	Horas Aula	Horas FFEOE	RA 1*	RA 2*	RA 3*	RA 4*	RA 5*	RA 6*	RA 7	Horas Totales
UD 1	1º	8		X							8
UD 2	2º	1	11		X						12
UD 3	2º	1	14		X						15
UD 4	3º	2	26						X		28
UD 5	1º	20					X	X			20
UD 6	1º	20				X					20
UD 7	3º	2								X	2
Horas Totales		**54**	**51**								**105**

V. ORIENTACIONES PEDAGÓGICAS

V.1 Líneas de actuación

Las líneas de actuación en el proceso enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo están relacionadas con:

- El conocimiento de las prácticas y pautas adecuadas, relativas a la seguridad física y lógica en un sistema informático.
- El conocimiento y análisis de técnicas y herramientas de seguridad activa, que actúen como medidas preventivas y/o paliativas ante ataques al sistema.
- El análisis y aplicación de técnicas y herramientas de seguridad activa.
- El análisis y aplicación de técnicas seguras de acceso remoto a un sistema.
- El análisis de herramientas y técnicas de protección perimetral para un sistema.
- La instalación, configuración y prueba de cortafuegos y servidores proxy como herramientas básicas de protección perimetral.
- El análisis de los servicios de alta disponibilidad más comunes, que garanticen la continuidad de servicios y aseguren la disponibilidad de datos.
- El conocimiento y análisis de la legislación vigente en el ámbito del tratamiento digital de la

información.

V.2 Metodología de trabajo con el alumnado que no realiza la FFEOE

El alumnado que, por algún motivo no realice la FFEOE, será atendido en el centro docente y se llevarán a cabo las siguientes actividades:

- Estudio de contenidos y realización de tareas similares a las que se estén desarrollando en la fase de formación en empresa.
- Actividades para el refuerzo y la mejora de competencias relacionadas con los contenidos impartidos con anterioridad.

VI. INSTRUMENTOS Y CRITERIOS DE CALIFICACIÓN ESPECÍFICOS DE MÓDULO

VI.1 Instrumentos de evaluación

Para comprobar si se están alcanzando los objetivos deberemos medir el nivel de consecución de los criterios de evaluación del módulo. Para ello, se utilizarán diferentes mecanismos de recogida de datos teniendo en cuenta los resultados de aprendizaje y características del alumnado.

En concreto, los instrumentos de evaluación para obtener la información que evidencie las habilidades y saberes que se han consolidando en el alumnado serán:

- **Pruebas teóricas y prácticas (P)**: cuestionarios escritos y/o ejercicios prácticos que se realizarán en clase. Permitirán comprobar la asimilación de conceptos fundamentales así como la capacidad para resolver problemas cercanos a la realidad sobre seguridad y alta disponibilidad. Se realizarán sin material de apoyo.
- **Tareas prácticas (TP):** trabajos y proyectos de carácter práctico que se realizarán en el aula y/o en casa de forma individual o en grupo, en función de los objetivos y tipo de trabajo. Se evaluará el cumplimiento de los plazos de entrega, capacidad en el uso de herramientas, la calidad técnica del trabajo y el nivel de profesionalismo.
- **Observación en el aula (OA):** trabajos, prácticas y pruebas, tanto individuales como en grupo, con la ayuda del material de apoyo necesario y que se presentarán con regularidad en horario de clase.
- **Observación en la Empresa (OE):** actividades planteadas por el docente para que el alumnado las desarrolle en la empresa. Estas actividades serán supervisadas y evaluadas tanto por el tutor laboral como por el docente del módulo, quien será el que finalmente las califique.
- En el caso del alumnado que haya interrumpido el periodo de FFEOE, éste se incorporará a partir de ese momento a las clases ordinarias, aplicándose los mismos instrumentos y criterios de calificación especificados en el presente punto. En estos casos la empresa u organismo equiparado no llegará a evaluar ninguno de los RRAA y actividades impartidas

en periodo de FFEOE.

En la siguiente tabla se muestran los instrumentos que podrán emplearse para cada RA:

UNIDAD DE TRABAJO		UD 1	UD 2	UD 3	UD 4	UD 5	UD 6	UD 7
RESULTADO DE APRENDIZAJES	**RA 1**	X						
	RA 2		X					
	RA 3				X			
	RA 4			X				
	RA 5							X
	RA 6							
	RA 7							
INSTRUMENTOS	**P**	X	X	X	X	X	X	X
	TP	X	X	X	X	X	X	
	OA	X	X	X	X	X	X	X
	OE		X	X				

VI.2 Criterios de calificación

En la siguiente tabla se resume la ponderación asignada a los diferentes resultados de aprendizajes que deben adquirir los alumnos en este módulo, así como los instrumentos que utilizaremos para valorar los correspondientes criterios de evaluación asociados.

Resultados de Aprendizaje			Ponderación general sobre el módulo	Instrumento de evaluación
Específicos del módulo	R.A. 1	10%	100%	P, TP, OA
	R.A. 2	22%		P, TP, OA, OE
	R.A. 3	19%		P, TP, OA, OE
	R.A. 4	12%		P, TP, OA, OE
	R.A. 5	12%		P, TP, OA
	R.A. 6	19%		P, TP, OA
	R.A. 7	6%		P, OA

- La calificación que corresponderá a los Criterios de evaluación asociados a los resultados de aprendizaje ponderará un 100% sobre la nota final.
- La calificación de cada alumno/a se calculará en función de la ponderación de notas

obtenidas en cada criterio de evaluación, que a su vez tendrán una ponderación sobre cada resultado de aprendizaje y en la calificación final.

- La calificación del módulo se expresará en valores numéricos de 1 a 10, sin decimales. Se considerarán positivas o superadas las calificaciones iguales o superiores a 5 y negativas o no superadas las restantes.

- Los RA marcados con asterisco (*) deberán tener una calificación igual o superior a cinco para la superación del módulo profesional, debido a su relevancia para el perfil profesional del título al que corresponde.

- El alumnado, previamente a su incorporación a la FFEOE, deberá haber superado los Resultados de Aprendizaje correspondientes a Prevención de Riesgos Laborales presentes tanto en el módulo transversal de IPE I, como en aquellos módulos profesionales en los que esté incluida la Prevención de Riesgos Laborales

VI.3 Tratamiento de la recuperación y mejora de la calificación final

Para el alumnado que, pese a asistir regularmente a clase y participar en las actividades programadas, **no consiga evaluación positiva del módulo por evaluaciones parciales**, **o bien no haya superado la FFEOE**, se plantearán opciones para mejorar las competencias necesarias de manera que pueda seguir el proceso de evaluación continua. Para ello se plantearán prácticas y/o actividades de "repaso de lo aprendido".

Según la **Orden de evaluación de 18 de septiembre de 2025** (art. 22), *"el periodo de refuerzo será el comprendido entre las dos evaluaciones finales"*. Durante el periodo comprendido entre la primera evaluación final y la segunda evaluación final, se realizarán prácticas y/o actividades de refuerzo y mejora de las competencias, que permitan al alumnado superar los resultados de aprendizaje, o en su caso, mejorar las calificaciones obtenidas en el módulo. El período previsto para **2º curso de Grado Superior e**s entre el **22 de mayo y el 15 de junio**.

VI.4 Pérdida de evaluación continua

La pérdida de la evaluación continua se aplicará al alumnado con un **absentismo superior al 20% de la duración total del módulo**, a partir de la fecha en la que el alumnado se haya matriculado.

Este Ciclo Formativo tiene carácter presencial, de manera que los alumnos y/o alumnas que no asistan un 20% de las horas de este módulo, **perderán el derecho de evaluación continua** y tendrán que realizar una serie de pruebas objetivas conforme a los criterios de evaluación que estén asociados a los RA no superados.

Según el **artículo 2 de la Orden de evaluación de 18 de septiembre de 2025**, *"el alumnado **tendrá derecho a la realización de las pruebas objetivas que el equipo docente responsable considere oportunas**, conforme a los criterios de evaluación que estén asociados a los resultados de aprendizaje no superados, a lo incluido en la correspondiente programación didáctica y en el proyecto educativo del centro. En todo caso, este alumnado **no podrá realizar***

aquellas actividades prácticas o pruebas objetivas que, a criterio del equipo docente, impliquen algún tipo de riesgo *para sí mismos, para el resto del grupo o para las instalaciones del centro".*

Concretamente, para este módulo, se podrá exigir al alumnado la realización de:

- Las prácticas y trabajos programados, así como las actividades que hayan sido realizadas en clase u otras equivalentes que estén relacionados con los RAs no superados.
- Los exámenes y pruebas teóricas y prácticas que se consideren oportunos conforme a los criterios de evaluación que estén asociados a los RA no superados.

VI.5 Situación de las pendientes del plan anterior (en los módulos que proceda)

Se van a realizar dos convocatorias finales, denominadas por la Consejería de Educación en el sistema de gestión Séneca como: Evaluación de pendientes 1º convocatoria, la cual se realizará la última semana de noviembre – primera de diciembre y evaluación de pendientes 2º convocatoria, se realizará a finales de febrero – primeros de marzo.

La no presentación en cada convocatoria y para cada módulo profesional pendiente conlleva la calificación de "No presentado" y consume convocatoria.

VII. ATENCIÓN A LA DIVERSIDAD

Según el **art. 3g) Orden de evaluación de 18 de septiembre de 2025**, *"se adecuarán las actividades formativas y los procedimientos de evaluación cuando el ciclo formativo vaya a ser cursado por alumnado que presente discapacidad o cualquier otra necesidades específica de apoyo educativo o formativo".*

A continuación, se detallan las adaptaciones metodológicas, de ampliación de tiempos y de recursos, que se podrán aplicar de forma individualizada según las necesidades concretas del alumno/a (discapacidad visual, auditiva, motriz, dificultades de aprendizaje, etc.). Se priorizará la dimensión práctica de los aprendizajes **(art. 4.2, Orden 18/09 de 2025)**.

VII.1 Adaptación Metodológica

Estas adaptaciones buscan hacer accesibles los fundamentos de la seguridad informática, priorizando su aplicación práctica y su vinculación con situaciones reales.

Estrategias de Enseñanza

- Aprendizaje Visual y Concreto: facilitar la comprensión de los procesos de seguridad y alta disponibilidad mediante esquemas, diagramas y demostraciones guiadas, a través de recursos visuales, simuladores y herramientas interactivas. Se utilizará Cisco Packet Tracer (o GNS3) para representar redes y reglas de firewall, Cryptool para representar de forma visual algoritmos de cifrado/descifrado de mensajes y uso de máquinas virtuales (con Kali

Linux y Metasploitable) como laboratorios para practicar vulnerabilidades

- Instrucciones Claras y Secuenciadas: Desglosar las tareas en pequeños pasos con objetivos claros y verificables. Proporcionar guías o plantillas paso a paso que permitan al alumnado centrarse en el objetivo y la lógica de la tarea, evitando dispersarse en búsquedas externas y asegurando que se mantenga el foco en la práctica real.
- Trabajo Colaborativo Guiado: Fomentar el aprendizaje entre iguales (tutoría entre compañeros) y la realización de proyectos prácticos y trabajos de investigación en grupo para que el alumnado se apoye mutuamente en la resolución de problemas.
- Tutoría y Apoyo Personalizado: Ofrecer atención más individualizada en el aula para la resolución de dudas específicas.

Priorización del Currículo Práctico

- Foco en la Competencia Práctica: Priorizar los objetivos de competencia profesional, resaltando la importancia de la seguridad informática y su aplicación en copias de seguridad, implementación de medidas de seguridad física y lógica, aplicación de técnicas de cifrado y protección de datos.
- Uso de herramientas de seguridad informática asistido como:
  - Veeam Agent (Windows / Linux) y comandos rsync Linux / robocopy Windows para copias de seguridad.
  - Ufw / firewalld / iptables (configuración de cortafuegos en Linux) y Wireshark (análisis de tráfico y detección de accesos sospechosos).
  - ClamAV y Autopsy para análisis de amenazas y forense básicos.
  - GnuPG, OpenSSH, BitLoccker para cifrado y protección de la información.
  - Máquina virtual Kali + Metasploitables
  - UrBackup Servidor + cliente para simular un entorno de backup real.

VII.2 Adaptación de evaluación

Estas adaptaciones aseguran que la evaluación refleje el nivel de competencia adquirido sin penalizar la dificultad de ejecución derivada de la NEAE:

- **Ampliación de tiempos** concediendo tiempo adicional en pruebas escritas y prácticas, así como flexibilidad en los plazos de entrega de las tareas evaluables.
- **Adaptaciones en el formato de la prueba** que facilite y permita la accesibilidad de todo el alumnado a los enunciado de actividades, tareas, y pruebas.
- **Evaluación práctica como referente principal** basado en la corrección funcional y comprensión de la aplicación de los contenidos de seguridad informática en un entorno real.
- **Diversificación de los procedimientos de evaluación**, adecuando determinadas pruebas o complementando las actividades propuestas mediante demostraciones prácticas, respuestas orales guiadas y el uso de un portafolio técnico, manteniendo en todo momento el mismo

nivel de exigencia y los criterios de evaluación establecidos.

VIII. MATERIAL DIDÁCTICO

Los materiales específicos necesarios para el módulo serán:

- Cuaderno de apuntes y/o ejercicios de alumno.
- Para el seguimiento del módulo, el profesor suministrará a los alumnos, la documentación necesaria a través de la plataforma Moodle del centro (específica de ciclos formativos). Dicha documentación será suministrada en PDF, donde se incluirán apuntes desarrollados por el profesor, así como los ejercicios, cuestiones y prácticas. La plataforma Moodle a su vez servirá como herramienta de comunicación para la entrega de trabajos, así como la utilización de material extra, y cuando sea posible, la resolución de dudas entre el propio alumnado y si procediera, del profesor/a mediante el foro específico del módulo. Sin embargo, se podrán dar casos en los que haya actividades, trabajos, prácticas, etc. que se entreguen presencialmente y no por vía telemática. El alumnado no utilizará ningún otro medio distinto al indicado por el profesor para la entrega de sus trabajos, prácticas, etc. En caso contrario constará será calificado como “No Entregado”
- Se intentará que cada alumno presente un equipo de trabajo para realizar diversos trabajos. Todos estos equipos dispondrán de diversos sistemas operativos (Windows y Linux), así como la posibilidad de creación de diversas máquinas virtuales (Virtual Box, VMWare). Todos los equipos estarán conectados a internet atendiendo a las normas de uso y utilización definidas por el departamento y el centro. Cada uno de estos equipos presentará instalado los siguientes programas utilizados:
  - Draw.io editor para mapas conceptuales y diagramas de flujo sobre políticas e implementaciones de seguridad informática.
  - Open Office, paquete ofimático software libre para el desarrollo de documentos que describan protocolos, medidas y estrategias de seguridad informática.

Como se indicó anteriormente, se recomienda al alumno la utilización de una memoria de almacenamiento USB para que diariamente pueda realizar diversas copias de seguridad de intercambio con los dispositivos particulares.

Se utilizarán principalmente los apuntes elaborados por el profesor y algunos recursos obtenidos de diversas fuentes como Internet. Como material de apoyo y consulta:

- Se utilizarán los materiales facilitados a través de la plataforma educativa Moodle.
- Como libro de consulta los alumnos pueden usar:

  - Seguridad y Alta Disponibilidad, Alfredo Abad Domingo, Ed. Garceta, ISBN: 978-84-1728-930-0
  - Seguridad y Alta Disponibilidad, Jesús Costas Santos, Ed. Ra-Ma, ISBN: 978-84-9964-089-1

- Webs de referencia
  - INCIBE (Instituto Nacional de Ciberseguridad de España) https://www.incibe.es/incibe
  - INTEF, recursos de Ciberseguridad https://intef.es/recursos-2/ciberseguridad/
  - RedIRIS es la red académica y de investigación española de comunicaciones. https://www.rediris.es/home/
  - CCN-CERT (Centro Criptológico Nacional) https://www.ccn-cert.cni.es/es/
  - INCIBE. Herramientas de seguridad https://www.incibe.es/ciudadania/herramientas
  - Web oficial de Kali Linux. https://www.kali.org/docs/
  - Hispasec: artículos y noticias sobre seguridad https://hispasec.com/es/inicio
  - Web Security Academy https://portswigger.net/web-security

VIII. PROTOCOLO UNIFICADO DE ACTUACIÓN TELEMÁTICA

Para haya uniformidad a la hora de trabajar de forma telemática y favorecer la atención del alumnado, todo el profesorado del centro debe adoptar las siguientes directrices:

- Se trabajará con el alumnado a través de la plataforma Moodle Centros de la Junta de Andalucía.
- En las videoconferencias con el alumnado y el profesorado se utilizará la herramienta suministrada en Moodle Centros (bbCollaborate).
- La retroalimentación entre profesorado y alumnado se producirá a través de los mecanismos suministrados por la plataforma Moodle.
- Para favorecer la coordinación entre los miembros del equipo docente, además, se podrán utilizar herramientas de Google Drive, por ejemplo:
  - Formularios para recabar información que no tenga carácter personal o confidencial.
  - Hojas de cálculo para organizar actuaciones comunes como el calendario de exámenes de tutoría.

- Uso de Séneca para recabar información de tutoría.