PROGRAMACIÓN DIDÁCTICA.		
I.E.S. JULIO VERNE	DEPARTAMENTO DE INFORMÁTICA	
C.F.G.S. ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED		2º CURSO
MÓDULO: SEGURIDAD Y ALTA DISPONIBILIDAD		

CURSO:	2025 – 2026
PROFESOR:	PEDRO BLANCH LEIVA

ÍNDICE

Índice de contenido

1 INTRODUCCIÓN

Esta Programación Didáctica se prepara para el módulo formativo **Seguridad y Alta Disponibilidad** (en adelante SAD) que forma parte del segundo curso del ciclo de Administración de Sistemas Informáticos en Red (en adelante ASIR).

Dicho ciclo se distribuye en dos cursos con un total de 2.000 horas. Nuestro módulo se imparte en el segundo curso a razón de 3 horas semanales durante el curso, según la Orden que regula el título y se detalla a continuación en el apartado correspondiente. Se encargará de impartirlo profesorado de Enseñanza Secundaria de la especialidad de Informática.

El cambio normativo iniciado en el pasado curso, con la implantación de la legislación autonómica derivada de la aplicación de la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional, lleva a considerar que este módulo profesional, según la Resolución de 26 de Junio de 2024 de y sus correcciones de la Consejería de Educación, tiene un periodo de formación Dual donde se desarrollarán horas que no son de docencia efectiva.

2 MARCO LEGISTATIVO

El marco legislativo que regula el ciclo formativo viene determinado por:

2.1. Marco normativo estatal.

- Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional.

  https://www.boe.es/buscar/act.php?id=BOE-A-2022-5139
- Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional.

https://www.boe.es/buscar/doc.php?id=BOE-A-2023-16889

1. Real Decreto 658/2024, de 9 de julio, por el que se modifican el Real Decreto 132/2010, de 12 de febrero, por el que se establecen los requisitos mínimos de los centros que impartan las enseñanzas del segundo ciclo de la educación infantil, la educación primaria y la educación secundaria, y el Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional.

   https://www.boe.es/buscar/doc.php?id=BOE-A-2024-14079

2.1.1. Marco normativo para los grados superiores.

- Real Decreto 500/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen títulos de Formación Profesional de grado superior y se fijan sus enseñanzas mínimas.

  https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-10685

2.2. Marco normativo autonómico.

1. Decreto 147/2025, de 17 de septiembre de 2025, “por el que se establece la ordenación de las enseñanzas de los Grados D y E del Sistema de Formación Profesional” en Andalucía.

   https://www.juntadeandalucia.es/boja/2025/179/c01/1

2. Orden de 18 de septiembre de 2025 que 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”.

   https://www.juntadeandalucia.es/boja/2025/180/c01/1

3. Orden de 26 de septiembre de 2025, por la que se regula la fase de formación en empresa u organismo equiparado de los grados D y E del Sistema de Formación Profesional de la Comunidad Autónoma de Andalucía.

   https://www.juntadeandalucia.es/boja/2025/187/c01/2

4. Resolución de 26 de junio de 2024, de la Dirección General de Formación Profesional, por la que se dictan Instrucciones para regular aspectos relativos a la organización y al funcionamiento del curso 2024/2025 en la Comunidad Autónoma de Andalucía.

https://www.juntadeandalucia.es/educacion/portales/documents/270701/1852728/Correccio%C2%BFn%20de%20Errores%20de%20la%20de%20la%20Resolucio%C2%BFn%20de%2026%20de%20junio%20de%202024.pdf/fc9ce21f-e557-8542-f621-07d82b3b9918?version=1.1

1. 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.
   https://www.juntadeandalucia.es/boja/2010/168/4

Plan de Centro del IES Julio Verne.

3 REFERENTE CONTEXTUAL

El referente contextual viene determinado por el proyecto educativo del centro

4 OBJETIVOS GENERALES QUE SE DESARROLLAN EN EL CICLO

Recogidos en la programación del departamento

5 OBJETIVOS GENERALES QUE SE DESARROLLAN EN EL MÓDULO

j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para implementar soluciones de alta disponibilidad.

k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.

l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.

m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

o) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.

p) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para mantener el espíritu de innovación.

6 COMPETENCIAS QUE SE DESARROLLAN EN EL MÓDULO.

La formación del módulo 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.

7 ADAPTACIÓN AL ENTORNO DE LA ECONOMÍA ANDALUZA.

El presente módulo tiene una vigencia máxima en el entorno andaluz. Puede afirmarse esto debido a que el perfil de técnico especialista capacitado para diseñar, instalar, configurar y administrar servicios de red es muy demandado en la actualidad en Andalucía debido a que el perfil de las empresas es mayoritariamente pequeña y mediana empresa.

8 RESULTADOS DE APRENDIZAJE Y SUS CRITERIOS DE EVALUACIÓN

Resultados de aprendizaje	Criterios de evaluación
1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	a) Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. b) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. c) Se han descrito las diferencias entre seguridad física y lógica. d) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. e) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. f) Se han adoptado políticas de contraseñas. g) Se han valorado las ventajas que supone la utilización de sistemas biométricos. h) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.

	l) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. j) Se han identificado las fases del análisis forense ante ataques a un sistema.
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. 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. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela

	de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	a) Se han descrito las características, tipos y funciones de los cortafuegos. b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico. c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.
5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	a) Se han identificado los tipos de proxy, sus características y funciones principales. b) Se ha instalado y configurado un servidor proxy-cache. c) Se han configurado los métodos de autenticación en el proxy. d) Se ha configurado un proxy en modo transparente. e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web. f) Se han solucionado problemas de acceso desde los clientes al proxy.

	g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor proxy en modo inverso. i)Se ha elaborado documentación. relativa a la instalación, configuración y uso de servidores proxy.
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal. e) Se ha implantado un balanceador de carga a la entrada de la red interna. f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	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 el deber 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. g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

9 METODOLOGÍA GENERAL

Recogida en la programación del departamento.

10 CONTENIDOS BÁSICOS DEL MÓDULO

1. Adopción de pautas y prácticas de tratamiento seguro de la información:

1. Fiabilidad, confidencialidad, integridad y disponibilidad.
2. Elementos vulnerables en el sistema informático. Hardware, software y datos.
3. Análisis de las principales vulnerabilidades de un sistema informático.
4. Amenazas. Tipos. Amenazas físicas y lógicas.
5. Seguridad física y ambiental.
    a) Ubicación y protección física de los equipos y servidores.
    b) Sistemas de alimentación ininterrumpida.
6. Seguridad lógica.
    a) Criptografía.
    b) Listas de control de acceso.
    c) Establecimiento de políticas de contraseñas.
    d) Políticas de almacenamiento.
    e) Copias de seguridad e imágenes de respaldo.
    f) Medios de almacenamiento.
    g) Análisis forense en sistemas informáticos.

2. Implantación de mecanismos de seguridad activa:

1. Ataques y contramedidas en sistemas personales.
    a) Clasificación de los ataques.
    b) Anatomía de ataques y análisis de software malicioso.

c) Herramientas preventivas.

d) Herramientas paliativas.

e) Actualización de sistemas y aplicaciones.

f) Seguridad en la conexión con redes públicas.

g) Pautas y prácticas seguras.

2. Seguridad en la red corporativa.

a) Monitorización del tráfico en redes.

b) Seguridad en los protocolos para inalámbricas.

c) Riesgos potenciales de los servicios de red.

d) Intentos de penetración.

3. Implantación de técnicas de acceso remoto. Seguridad perimetral:

1. Elementos básicos de la seguridad perimetral.

2. Perímetros de red. Zonas desmilitarizadas.

3. Arquitectura débil de subred protegida.

4. Arquitectura fuerte de subred protegida.

5. Redes privadas virtuales. VPN. Beneficios y desventajas con respecto a las líneas dedicadas. Técnicas de cifrado. Clave pública y clave privada.

a) VPN a nivel de red. SSL, IPSec.

b) VPN a nivel de aplicación. SSH.

6. Servidores de acceso remoto.

a) Protocolos de autenticación.

b) Configuración de parámetros de acceso.

c) Servidores de autenticación.

4. Instalación y configuración de cortafuegos:

1. Utilización de cortafuegos.

2. Filtrado de paquetes de datos.
3. Tipos de cortafuegos. Características. Funciones principales.
4. Instalación de cortafuegos. Ubicación.
5. Reglas de filtrado de cortafuegos.
6. Pruebas de funcionamiento. Sondeo.
7. Registros de sucesos de cortafuegos.

5. Instalación y configuración de servidores proxy:

1. Tipos de proxy. Características y funciones.
2. Instalación de servidores proxy.
3. Instalación y configuración de clientes proxy.
4. Configuración del almacenamiento en la caché de un proxy.
5. Configuración de filtros.
6. Métodos de autenticación en un proxy

6. Implantación de soluciones de alta disponibilidad:

1. Definición y objetivos.
2. Análisis de configuraciones de alta disponibilidad.
    a) Funcionamiento ininterrumpido.
    b) Integridad de datos y recuperación de servicio.
    c) Servidores redundantes.
    d) Sistemas de clusters.
    e) Balanceadores de carga.
3. Instalación y configuración de soluciones de alta disponibilidad.
4. Virtualización de sistemas.
5. Posibilidades de la virtualización de sistemas.
6. Herramientas para la virtualización.
7. Configuración y utilización de máquinas virtuales.
8. Alta disponibilidad y virtualización.

9. Simulación de servicios con virtualización.

7. Legislación y normas de seguridad.

1. Legislación sobre protección de datos.

11 CONTENIDOS.

Las unidades didácticas en las que se distribuye la asignatura son las siguientes:

1. Adopción de pautas de seguridad informática
2. Seguridad perimetral y cortafuegos
3. Redes privadas virtuales
4. Proxy
5. Hacking ético
6. Alta disponibilidad
7. Legislación y normativa sobre seguridad y protección de datos.

Tanto la temporización como la división en unidades didácticas, ha sido realizado atendiendo a distintos factores, como son la experiencia obtenida de años anteriores, la carga teórica y práctica de las distintas unidades así como las capacidades profesionales que se desarrollan en cada una de las unidades. Además de las capacidades profesionales que necesita el alumnado para afrontar con éxito el segundo curso del ciclo.

12 TEMPORIZACIÓN

El reparto de unidades didácticas en evaluaciones será así:

- Primera Evaluación: Unidades 1 y 2.
- Segunda Evaluación: Unidades 3, 4 y 5.
- Tercera Evaluación: Unidades 6 y 7 (formación dual).

13 TABLA DE UNIDAD CON RESULTADO APRENDIZAJE

UNIDAD	RESULTADOS APRENDIZAJE	CRITERIOS DE EVALUACIÓN
1. Adopción de pautas de seguridad informática	1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i
2. Seguridad Perimetral y cortafuegos	4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	4.a, 4.b, 4.c, 4.d, 4.e, 4.f, 4.g, 4.h, 4.i, 4.h
3. Redes privadas virtuales	3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g
4. Proxy	5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	5.a, 5.b, 5.c, 5.d, 5.e, 5.f, 5.g, 5.h y 5.i
5. Hacking ético	2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	2.a, 2.b, 2.c, 2.d, 2.e, 2.f, 2.g, 2.h, 2.i
6. Alta disponibilidad	6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización yconfigurando los entornos de prueba.	6.a, 6.b, 6.c, 6.d, 6.e, 6.f, 6.g, 6.h, 6.i
7. Legislación y normativa sobre seguridad y protección de datos	7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	7.a, 7.b, 7.c, 7.d, 7.e, 7.f, 7.g

14 ESPECIFICACIÓN DE LAS UNIDADES DIDÁCTICAS

UNIDAD DIDÁCTICA 1: Adopción de pautas de seguridad informática

Descripción: Pretende dotar al alumnado de las competencias profesionales "Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo "

Criterios de evaluación: 1.a,1.b, …, 1.g	**Nº horas**: 20
Contenidos	**Metodología**
- Fiabilidad, confidencialidad, integridad y disponibilidad. - Elementos vulnerables en el sistema informático. Hardware, software y datos. - Análisis de las principales vulnerabilidades de un sistema informático. - Amenazas. Tipos. Amenazas físicas y lógicas. - Seguridad física y ambiental. a) Ubicación y protección física de los equipos y servidores. b) Sistemas de alimentación ininterrumpida. - Seguridad lógica. a) Criptografía. b) Técnicas de cifrado. Clave pública y clave privada. c) Listas de control de acceso. d) Establecimiento de políticas de contraseñas. e) Políticas de almacenamiento. f) Copias de seguridad e imágenes de respaldo. g) Medios de almacenamiento. h) Análisis forense en sistemas informáticos.	• Exposiciones teóricas. • Ejercicios prácticos. • Ejercicios de investigación.

Observaciones:

UNIDAD DIDÁCTICA 2: Seguridad Perimetral y cortafuegos	
Descripción: Pretende dotar al alumnado de las competencias profesionales "Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna"	
Criterios de evaluación: 3.a, …, 3.g	**Nº horas**: 20
Contenidos	**Metodología**
- 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. - Elementos básicos de la seguridad perimetral. - Perímetros de red. Zonas desmilitarizadas. - Arquitectura débil de subred protegida. - Arquitectura fuerte de subred protegida.	• Exposiciones teóricas. • Ejercicios prácticos. • Ejercicios de investigación.
Observaciones:	

UNIDAD DIDÁCTICA 3. Redes Privadas Virtuales	
Descripción: Pretende formar al alumnado en implantar técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad"	
Criterios de evaluación: 4.a, …, 4.i	**Nº horas**: 3
Contenidos	**Metodología**
- Redes privadas virtuales. VPN. Beneficios y desventajas con respecto a las líneas dedicadas. a) VPN a nivel de red. SSL, IPSec. b) VPN a nivel de aplicación. SSH. - Servidores de acceso remoto. a) Protocolos de autenticación. b) Configuración de parámetros de acceso. c) Servidores de autenticación.	• Exposiciones teóricas. • Ejercicios prácticos. • Ejercicios de investigación.
Observaciones:	

UNIDAD DIDÁCTICA 4: Proxy	
Descripción: Pretende dotar al alumnado de la competencia profesional "Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio."	
Criterios de evaluación:5.a, ..., 5.i	**Nº horas**: 3
Contenidos	**Metodología**
- 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	• Exposiciones teóricas. • Ejercicios prácticos. • Ejercicios de investigación.
Observaciones:	

UNIDAD DIDÁCTICA 5: Hacking ético	
Descripción: Pretende dotar al alumnado de la competencia profesional "Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema."	
Criterios de evaluación: 1.a, …, 1.j	**Nº horas**: 12
Contenidos	**Metodología**
- Ataques y contramedidas en sistemas personales. a) Clasificación de los ataques. b) Anatomía de ataques y análisis de software malicioso. c) Herramientas preventivas. d) Herramientas paliativas. e) Actualización de sistemas y aplicaciones. f) Seguridad en la conexión con redes públicas. g) Pautas y prácticas seguras. - Seguridad en la red corporativa. a) Monitorización del tráfico en redes. b) Seguridad en los protocolos para comunicaciones inalámbricas. c) Riesgos potenciales de los servicios de red. d) Intentos de penetración.	• Exposiciones teóricas. • Ejercicios prácticos. • Ejercicios de investigación.
Observaciones:	

UNIDAD DIDÁCTICA 6: Alta disponibilidad	
Descripción: Pretende dotar al alumnado de las siguientes competencias profesionales: “Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.”	
Criterios de evaluación: 7.a, ..., 7.h, 8.a, ..., 8.i.	**Formación dual**
Contenidos	
- Definición y objetivos. - Análisis de configuraciones de alta disponibilidad. a) Funcionamiento ininterrumpido. b) Integridad de datos y recuperación de servicio. c) Servidores redundantes. d) Sistemas de clusters. e) 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.	
Observaciones:	

UNIDAD DIDÁCTICA 7: Legislación y normativa sobre seguridad y protección de datos	
Descripción: Pretende dar al alumnado una visión general sobre la normativa que afecta a la seguridad.	
Criterios de evaluación: 6.a, ..., 6.h	**Formación dual**
Contenidos	
- Legislación sobre protección de datos.	
Observaciones:	

15 CONTENIDOS ACTITUDINALES

Recogidos en la programación del departamento.

16 PROCESO DE EVALUACIÓN – CALIFICACIÓN. Relación de instrumentos de evaluación con las unidades, criterios de evaluación e indicadores

Se usarán, según los casos, los siguientes instrumentos de evaluación:

- **Test:** Prueba de conocimientos individual y vigilada tipo test, sin poder consultar información.
- **Proyecto:** Trabajo individual o en equipo, dilatado en varios días, que el alumnado realiza teniendo a su disposición cualquier tipo de material o fuente de documentación. Tiene un marcado carácter de investigación.
- **Práctica:** Trabajo práctico, en el que el alumnado desarrolla sobre los ordenadores alguna función explicada en clase con acceso a cualquier tipo de fuente de documentación. Normalmente se permiten varios días para su realización. Puede ser individual o en grupo.
- **Examen teórico:** Tiene carácter individual. Se realiza sobre papel y se trata de supuestos prácticos de diseño y resolución de problemas en las que aplicar los conocimientos y habilidades adquiridas.
- **Examen práctico:** Tiene carácter individual y consiste en la ejecución práctica de determinadas funcionalidades sobre equipos reales. El alumnado podrá contar con todo tipo de documentación y acceso a Internet, aunque NO se permite la ayuda de otras personas.
- **Examen teórico-práctico:** puede contener una mezcla de los 2 anteriores.

Cada resultado de aprendizaje está asociado a una unidad didáctica. Cada uno de ellos debe ser superado por separado, y teniendo en cuenta que los contenidos de dichos resultados no tienen relación unos con otros, la superación de un resultado no puede implicar la superación de otros.

La separación de unidades por evaluaciones será la siguiente:

Unidades didácticas	Evaluación
1, 2	1ª
3, 4, 5	2ª
6, 7	3ª

U.D. 1:Adopción de pautas de seguridad informática										
Criterios de Evaluación	3									
Indicadores	3.a	3.b	3.c	3.d	3.e	3.f	3.g	3.h	3.i	3.j
Práctica		x	x	x	x	x	x	x	x	x
Examen	x	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Examen práctico con un peso de 70% • Examen teórico con un peso de 20% • Prácticas evaluables realizadas en clase y/o en casa 10%										

U.D. 2: Seguridad perimetral y cortafuegos							
Criterios de Evaluación	2						
Indicadores	2.a	2.b	2.c	2.d	2.e	2.f	2.g
Práctica			x	x	x	x	x
Examen	x	x	x	x	x	x	
Criterios de Calificación: • Examen práctico con un peso de 70% • Examen teórico con un peso de 20% • Prácticas evaluables realizadas en clase y/o en casa 10%							

U.D. 3: Redes privadas virtuales										
Criterios de Evaluación	1									
Indicadores	1.a	1.b	1.c	1.d	1.e	1.f	1.g	1.h	1.i	1.j
Práctica	x			x			x	x	x	x
Examen	x	x	x	x	x	x	x	x	x	

Criterios de Calificación:

- Examen práctico con un peso de 70%
- Examen teórico con un peso de 20%
- Prácticas evaluables realizadas en clase y/o en casa 10%

U.D. 4: Proxy									
Criterios de Evaluación	5								
Indicadores	5.a	5.b	5.c	5.d	5.e	5.f	5.g	5.h	5.i
Práctica		x	x	x	x	x	x	x	x
Examen	x	x	x	x	x	x	x	x	

Criterios de Calificación:

- Examen práctico con un peso de 70%
- Examen teórico con un peso de 20%
- Prácticas evaluables realizadas en clase y/o en casa 10%

U.D. 5: Hacking ético									
Criterios de Evaluación	4								
Indicadores	4.a	4.b	4.c	4.d	4.e	4.f	4.g	4.h	4.i
Práctica		x	x	x	x	x	x	x	x
Examen	x	x	x	x	x	x	X	x	

Criterios de Calificación:

- Examen práctico con un peso de 70%
- Examen teórico con un peso de 20%
- Prácticas evaluables realizadas en clase y/o en casa 10%

U.D. 6: Alta disponibilidad																	
Criterios de Evaluación	7,8																
Indicadores	7.a	7.b	7.c	7.d	7.e	7.f	7.g	7.h	8.a	8.b	8.c	8.d	8.e	8.f	8.g	8.h	8.i
Práctica		x	x	x	x	x	x	x		x	x	x	x	x	x	x	x
Examen Práctico 1	x	x	x	x	x	x			x	x	x	x		x			

Criterios de Calificación:

- Informe del tutor dual en la empresa

U.D. 7: Legislación y normativa sobre seguridad y protección de datos								
Criterios de Evaluación	6							
Indicadores	6.a	6.b	6.c	6.d	6.e	6.f	6.g	6.h
Práctica		x	x	x	x	x	x	x
Examen	x	x	x	x	x	x	x	

Criterios de Calificación:

- Informe del tutor dual en la empresa

Criterios de calificación generales

Un resultado de aprendizaje estará aprobado o superado si su nota es igual a superior a cinco (5).

Los resultados de aprendizaje aprobados se guardan hasta el final del curso.

No se admitirá la entrega de trabajos fuera de fecha.

La nota de la primera evaluación saldrá de la media aritmética de las notas obtenidas en todos los resultados de aprendizaje evaluados hasta ese momento. Si la media aritmética es igual o superior a 5, pero se tiene una nota inferior a 5 en cualquiera de los resultados de aprendizaje, la nota de la primera evaluación será de un 4.

La nota de la segunda evaluación saldrá de la media aritmética de las notas obtenidas en todos los resultados de aprendizaje evaluados hasta ese momento. Si la media aritmética es igual o superior a 5, pero se tiene una nota inferior a 5 en cualquiera de los resultados de aprendizaje, la nota de la segunda evaluación será de un 4.

La nota de la tercera evaluación saldrá de la media aritmética de las notas obtenidas en todos los resultados de aprendizaje evaluados hasta ese momento. Si la media aritmética es igual o superior a 5, pero se tiene una nota inferior a 5 en cualquiera de los resultados de aprendizaje, la nota de la tercera evaluación será de un 4.

La nota de la convocatoria ordinaria del curso saldrá de la media aritmética de las

notas obtenidas en todos los resultados de aprendizaje. Si la media aritmética es igual o superior a 5, pero se tiene una nota inferior a 5 en cualquiera de los resultados de aprendizaje, la nota de la convocatoria ordinaria será de un 4.

En el periodo comprendido entre la fecha de la convocatoria ordinaria y la convocatoria extraordinaria los alumnos que tengan algún resultado de aprendizaje no superado recibirán clases para preparar la prueba de la convocatoria extraordinaria que tendrá lugar en junio.

En Junio habrá una prueba para recuperar cada uno de los resultados de aprendizaje no superados en la convocatoria ordinaria.
La nota de la convocatoria extraordinaria del curso saldrá de la media aritmética de las notas obtenidas en todos los resultados de aprendizaje. Si la media aritmética es igual o superior a 5, pero se tiene una nota inferior a 5 en cualquiera de los resultados de aprendizaje, la nota de la convocatoria extraordinaria será de un 4.

17 ADAPTACIONES CURRICULARES.

Recogidas en la programación del departamento

18 FP DUAL

Según se recoge en la programación del departamento, el régimen de dual será el general y siguiendo un modelo condensado. Las fechas de incorporación de los alumnos a empresas u organismo equiparado quedan también recogidas en la programación del departamento. En ese período de formación en la empresa el alumno deberá alcanzar los siguientes RA's:

- RA-6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

- RA-7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

FORMACIÓN EN EMPRESAS

La formación profesional dual en el sistema de formación profesional para el empleo se materializará a través del contrato para la formación y aprendizaje. La característica principal que define a la FP Dual es que el alumnado es evaluado tanto por su centro educativo como por la empresa, en este sentido.

Los alumnos y alumnas de este módulo deben tener designado un tutor responsable para hacer el seguimiento del alumno, asegurarse de que se cumple el programa establecido y que se adquieren todos los conocimientos para poder desempeñar el trabajo según lo aprendido en el ciclo.

Los contenidos serán impartidos de acuerdo con la programación general del módulo, con la diferencia de que el alumnado adquirirá y aplicará sus conocimientos tanto teóricos como prácticos no solamente en el aula sino también en la empresa sin que ello afecte a la coherencia del módulo.

Se intentará que todo el alumnado (que esté en disposición según normativa) realice la fase de formación en empresa. En caso de que haya alumnado que no se pudiera incorporar a la fase de formación en empresa (por cualquier motivo justificado), éste deberá continuar con el desarrollo normal de las clases en el aula, adquiriendo los RA’s que se han planificado en la formación en empresa en el centro educativo.

19 RECURSOS DIDÁCTICOS.

En el caso de este módulo los recursos los dividimos en dos tipos: Humanos y Materiales.

a) **Recursos Humanos:** El módulo cuenta con un profesor titular.
b) **Recursos Materiales:** Se pueden inventariar los siguientes:
    - *Un aula taller,* donde se ubican todas las clases del grupo tanto prácticas como teóricas
    - *Un proyector de video.*
    - Un ordenador por cada alumno/a.
    - Una LAN cableada GigabitEth que integra todos los ordenadores de los talleres del Departamento de Informática.
    - Una red Wifi de soporte conectada a la red del Departamento.
    - *Linux* de libre distribución.
    - Plataforma Moodle *aula.iesjulioverne.es*.
    - Servidor de virtualización Proxmox administrado por el profesor para prácticas y exámenes. Con acceso desde fuera del centro.
    - Servidor de virtualización Proxmox administrado por los alumnos para prácticas de alumnos. Con acceso desde fuera del centro.
    - Acceso a Internet.

20 BIBLIOGRAFÍA RECOMENDADA.

- Toda la bibliografía recomendada consiste en documentos y webs técnicas, de acceso libre y gratuito. Su uso varía mucho con el tiempo, estando siempre referenciadas en la plataforma Moodle de esta asignatura.