IES MIGUEL ROMERO ESTEO – MÁLAGA
DEPARTAMENTO DE INFORMÁTICA

PROGRAMACIÓN DEL MÓDULO

0378. SEGURIDAD Y ALTA DISPONIBILIDAD

TOTAL HORAS: 105 **HORAS SEMANALES: 4**

CICLO FORMATIVO: **ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS Y EN RED (ASIR)**

CURSO 2026/2027

PROFESORES: ANTONIO RAMOS RAMÍREZ

Fecha de Entrega: 31 DE OCTUBRE DE 2026
Fechas de revisiones:

Índice de la programación:

COMPETENCIAS: 3

Competencia general del título: Artículo 4 del RD que lo regula. 3

Unidades de competencia asociadas al módulo. 3

Competencias profesionales, personales y sociales. 3

Normativa de Referencia 5

OBJETIVOS GENERALES ASOCIADOS AL MÓDULO 5

Relación de los Objetivos Generales del Ciclo con los Resultados de Aprendizaje. 7

CONTENIDOS 8

METODOLOGÍA, MATERIALES Y RECURSOS DIDÁCTICOS UTILIZADOS: 10

Descripción de las actividades de enseñanza y aprendizaje. 10

Materiales y recursos didácticos utilizados. 11

Relación de unidades y resultados de aprendizaje: 12

EVALUACIÓN CRITERIAL DE LAS COMPETENCIAS. ACTIVIDADES, TÉCNICAS E INSTRUMENTOS DE EVALUACIÓN: 13

PONDERACIÓN RESULTADOS DE APRENDIZAJE: 21

EVALUACIÓN ALTERNATIVA. 22

ACTIVIDADES DE RECUPERACIÓN Y MEJORA DE LOS RESULTADOS OBTENIDOS EN LA EVALUACIÓN PREVIA A LA EVALUACIÓN FINAL FP. 22

PROYECTO INTERMODULAR 23

INCORPORACIÓN DE LOS CONTENIDOS DE CARÁCTER TRANSVERSAL AL CURRÍCULO. 23

MEDIDAS DE ATENCIÓN A LA DIVERSIDAD Y ALUMNADO CON N.E.A.E. 24

ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON ESTE MÓDULO. 24

AUTOEVALUACIÓN 24

COMPETENCIAS:

Competencia general del título: Artículo 4 del RD que lo regula.

La competencia general de este título consiste en configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente.

Unidades de competencia asociadas al módulo.

UC0486_3 Asegurar equipos informáticos.

Competencias profesionales, personales y sociales.

La formación del módulo contribuye a alcanzar las **competencias profesionales, personales y sociales** del título de Técnico Superior en Administración de Sistemas Informáticos en Red que se relacionan a continuación:

a) Administrar sistemas operativos de servidor, instalando y configurando el software, en condiciones de calidad para asegurar el funcionamiento del sistema.
b) Administrar servicios de red (web, mensajería electrónica y transferencia de archivos, entre otros) instalando y configurando el software, en condiciones de calidad.
c) Administrar aplicaciones instalando y configurando el software, en condiciones de calidad para responder a las necesidades de la organización.
d) Implantar y gestionar bases de datos instalando y administrando el software de gestión en condiciones de calidad, según las características de la explotación.
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.
g) Determinar la infraestructura de redes telemáticas elaborando esquemas y seleccionando equipos y elementos.
h) Integrar equipos de comunicaciones en infraestructuras de redes telemáticas, determinando la configuración para asegurar su conectividad.
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.
l) Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.
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.
p) Mantener el espíritu de innovación y actualización en el ámbito de su trabajo para adaptarse a los cambios tecnológicos y organizativos de su entorno profesional.
q) Liderar situaciones colectivas que se puedan producir, mediando en conflictos personales y laborales, contribuyendo al establecimiento de un ambiente de trabajo agradable y actuando en todo momento de forma sincera, respetuosa y tolerante.
r) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.
s) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.
t) Participar de forma activa en la vida económica, social y cultural con actitud crítica y responsable.
u) Crear y gestionar una pequeña empresa, realizando un estudio de viabilidad de productos, de planificación de la producción y de comercialización.

Normativa de Referencia

Esta programación didáctica está fundamentada en la siguiente normativa:

- REAL DECRETO 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.
- REAL DECRETO 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.
- 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. en la Comunidad Autónoma de Andalucía.
- REAL DECRETO 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional.

OBJETIVOS GENERALES ASOCIADOS AL MÓDULO

La formación del módulo contribuye a alcanzar **los objetivos generales** del título de Técnico Superior en Administración de Sistemas Informáticos en Red que se relacionan a continuación:

a) Analizar la estructura del software de base, comparando las características y prestaciones de sistemas libres y propietarios, para administrar sistemas operativos de servidor.
b) Instalar y configurar el software de base, siguiendo documentación técnica y especificaciones dadas, para administrar sistemas operativos de servidor.
c) Instalar y configurar software de mensajería y transferencia de ficheros, entre otros, relacionándolos con su aplicación y siguiendo documentación y especificaciones dadas, para administrar servicios de red.
d) Instalar y configurar software de gestión, siguiendo especificaciones y analizando entornos de aplicación, para administrar aplicaciones.
e) Instalar y administrar software de gestión, relacionándolo con su explotación, para implantar y gestionar bases de datos.
f) Configurar dispositivos hardware, analizando sus características funcionales, para optimizar el rendimiento del sistema.
g) Configurar hardware de red, analizando sus características funcionales y relacionándolo con su campo de aplicación, para integrar equipos de comunicaciones.
h) Analizar tecnologías de interconexión, describiendo sus características y posibilidades de aplicación, para configurar la estructura de la red telemática y evaluar su rendimiento.

i) Elaborar esquemas de redes telemáticas utilizando software específico para configurar la estructura de la red telemática.
j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha 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.
n) Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios
o) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.
p) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.
q) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para resolver problemas y mantener una cultura de actualización e innovación.
r) Identificar formas de intervención en situaciones colectivas, analizando el proceso de toma de decisiones y efectuando consultas para liderar las mismas.
s) Identificar y valorar las oportunidades de aprendizaje y su relación con el mundo laboral, analizando las ofertas y demandas del mercado para gestionar su carrera profesional.
t) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
u) Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.

Relación de los Objetivos Generales del Ciclo con los Resultados de Aprendizaje.

La formación del módulo contribuye a alcanzar los objetivos generales j), k), l), m), o), p) y u) del ciclo formativo y las competencias profesionales, personales y sociales e), f), i), j), k), m), n), o), r) y s) del título.

Objetivo General	RA 1	RA 2	RA 3	RA 4	RA 5	RA 6	RA 7
j)						X	
k)	X						
l)		X	X	X	X		
m)	X					X	
o)	X	X					
p)						X	
u)							X

CONTENIDOS

UNIDAD 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.
6. Ubicación y protección física de los equipos y servidores.
7. Sistemas de alimentación ininterrumpida.
8. Seguridad lógica.
9. Criptografía.
10. Listas de control de acceso.
11. Establecimiento de políticas de contraseñas.
12. Políticas de almacenamiento.
13. Copias de seguridad e imágenes de respaldo.
14. Medios de almacenamiento.
15. Análisis forense en sistemas informáticos.

UNIDAD 2: Implantación de mecanismos de seguridad activa:

1. Ataques y contramedidas en sistemas personales.
2. Clasificación de los ataques.
3. Anatomía de ataques y análisis de software malicioso.
4. Herramientas preventivas.
5. Herramientas paliativas.
6. Actualización de sistemas y aplicaciones.
7. Seguridad en la conexión con redes públicas.
8. Pautas y prácticas seguras.
9. Seguridad en la red corporativa.
10. Monitorización del tráfico en redes.
11. Seguridad en los protocolos para comunicaciones inalámbricas.
12. Riesgos potenciales de los servicios de red.
13. Intentos de penetración.

UNIDAD 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.
6. Beneficios y desventajas con respecto a las líneas dedicadas.

UNIDAD 4: Técnicas de cifrado. Servidores VPN

1. VPN a nivel de red. SSL, IPSec.
2. VPN a nivel de aplicación. SSH.
3. Servidores de acceso remoto.
4. Protocolos de autenticación.
5. Configuración de parámetros de acceso.
6. Servidores de autenticación.

UNIDAD 5: 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.

UNIDAD 6: 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.

UNIDAD 7: Implantación de soluciones de alta disponibilidad:

1. Definición y objetivos.
2. Análisis de configuraciones de alta disponibilidad.
3. Funcionamiento ininterrumpido.
4. Integridad de datos y recuperación de servicio.
5. Servidores redundantes.
6. Sistemas de clústeres.
7. Balanceadores de carga.
8. Instalación y configuración de soluciones de alta disponibilidad.
9. Virtualización de sistemas.
10. Posibilidades de la virtualización de sistemas.
11. Herramientas para la virtualización.
12. Configuración y utilización de máquinas virtuales.
13. Alta disponibilidad y virtualización.
14. Simulación de servicios con virtualización.

UNIDAD 8: Reconocimiento de la legislación y normativa sobre seguridad y protección de datos:

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

METODOLOGÍA, MATERIALES Y RECURSOS DIDÁCTICOS UTILIZADOS:

Orientaciones pedagógicas recogidas en la Orden del Título en relación al módulo.

Descripción de las actividades de enseñanza y aprendizaje.

La metodología básica a utilizar será el aprendizaje significativo, el lenguaje utilizado en clase debe ser comprensible por el alumnado, para ello se realizarán unas pruebas iniciales para determinar el nivel de conocimiento de las competencias profesionales del módulo y que permita fijar el punto de partida del módulo, así como la adaptación de la programación al grupo.

El reparto de tiempo en las clases dependerá de los contenidos que se estén trabajando. Así por ejemplo en el bloque primero de contenido conceptual la distribución de las clases será:

1. Exposición por el profesor con toma de apuntes por el alumnado.
2. Puesta en común de los conceptos y reflexión.
3. Entrega de apuntes digitales.
4. Recogida de trabajos y realización de prácticas con ordenador.
5. Pruebas de autoevaluación y seguimiento para evaluar el grado de adquisición de los contenidos por parte del alumnado.

Se va a usar la plataforma MOODLE CENTROS como entorno de enseñanza-aprendizaje que permite poner a disposición del alumnado los materiales del módulo y la interacción con el profesor, así como la entrega de las actividades y trabajos planteados en clase.

En relación con la metodología de aprendizaje y la organización de actividades conviene resaltar su carácter activo y participativo.

Materiales y recursos didácticos utilizados.

Para el desarrollo de las actividades del curso se utilizarán los recursos y materiales presentes en el aula:

a) Infraestructura de comunicaciones

- Infraestructura de red cableada para conectar todos los ordenadores del aula y del departamento de informática.
- Acceso a Internet para todos los ordenadores del aula.

b) Hardware

- Un ordenador para cada alumno/a y un ordenador para el profesor.
- Cañón retroproyector para la realización de exposiciones teóricas y simulaciones prácticas por parte del profesor.
- Equipo servidor para virtualización de sistemas operativos.

c) Software

- Sistemas operativos: Windows y Linux.
- Paquete ofimático: LibreOffice.
- Navegador Web: Mozilla Firefox y Google Chrome
- Utilidades relacionadas con la seguridad: SysInternals, John the Ripper, LOIC, metasploits, Kali Linux, tor, etc.
- VirtualBox y Proxmox para la virtualización de sistemas informáticos.
- Diversas máquinas virtuales, ya instaladas y listas para funcionar, para la realización de ejercicios prácticos.
- Etc.

Relación de unidades y resultados de aprendizaje:

UNIDAD	Nombre	Resultado de aprendizaje	Temporalización	Observaciones
1ª EVALUACIÓN				
1	Adopción de pautas y prácticas de tratamiento seguro de la información	RA 1	5 semanas	
2	Implantación de mecanismos de seguridad activa	RA 2	3 semanas	
3	Implantación de técnicas de acceso remoto. Seguridad perimetral	RA 3	3 semanas	
4	Técnicas de cifrado. Servidores VPN	RA 2, RA 3	3 semanas	
2ª EVALUACIÓN				
5	Instalación y configuración de cortafuegos	RA 4	2 semanas	
6	Instalación y configuración de servidores proxy	RA 5	2 semanas	
7	Implantación de soluciones de alta disponibilidad	RA 6	4 semanas	
8	Reconocimiento de la legislación y normativa sobre seguridad y protección de datos	RA 7	1 semana	

EVALUACIÓN CRITERIAL DE LAS COMPETENCIAS. ACTIVIDADES, TÉCNICAS E INSTRUMENTOS DE EVALUACIÓN:

En las siguientes tablas se desarrolla el sistema de evaluación de esta programación, dentro del marco legal de la ORDEN de 29 de septiembre de 2010, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

RA 1: 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	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	1		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)
b) Se han descrito las diferencias entre seguridad física y lógica.			
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.			
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.			
e) Se han adoptado políticas de contraseñas.			
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.			
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.			
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.			
i) Se han identificado las fases del análisis forense ante ataques a un sistema.			

Contenidos del RA 1:

- 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.
- Ubicación y protección física de los equipos y servidores.
- Sistemas de alimentación ininterrumpida.
- Seguridad lógica.
- Criptografía.
- Listas de control de acceso.
- Establecimiento de políticas de contraseñas.
- Políticas de almacenamiento.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Análisis forense en sistemas informáticos.

Evaluación: 1ª	**Objetivos generales**: k) m) o)

El RA 1 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.

RA 2: Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación..
a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	2		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)
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.			
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.			
f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	4		

Contenidos del RA 2:

- Ataques y contramedidas en sistemas personales.
- Clasificación de los ataques.
- Anatomía de ataques y análisis de software malicioso.
- Herramientas preventivas.
- Herramientas paliativas.
- Actualización de sistemas y aplicaciones.
- Seguridad en la conexión con redes públicas.
- Pautas y prácticas seguras.
- Seguridad en la red corporativa.
- Monitorización del tráfico en redes.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Riesgos potenciales de los servicios de red.
- Intentos de penetración.

Evaluación: 1ª | **Objetivos generales**: l) o)

El RA 2 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.

RA 3: Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	3		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)
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.	4		
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.			

Contenidos del RA 3:

- Elementos básicos de la seguridad perimetral.
- Perímetros de red. Zonas desmilitarizadas.
- Arquitectura débil de subred protegida.
- Arquitectura fuerte de subred protegida.
- Redes privadas virtuales. VPN.
- Beneficios y desventajas con respecto a las líneas dedicadas.
- VPN a nivel de red. SSL, IPSec.
- VPN a nivel de aplicación. SSH.
- Servidores de acceso remoto.
- Protocolos de autenticación.
- Configuración de parámetros de acceso.

- Servidores de autenticación.

Evaluación: 1ª	**Objetivos generales**: l)
El RA 3 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.	

RA 4: Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
a) Se han descrito las características, tipos y funciones de los cortafuegos.	5		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)
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.			

Contenidos del RA 4:

- 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.

Evaluación: 2ª	**Objetivos generales**: l)
El RA 4 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.	

RA 5: Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
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		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)

Contenidos del RA 5:

- 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.

Evaluación: 2ª	**Objetivos generales**: l)

El RA 5 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.

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

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
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 clústeres 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		30% prácticas y ejercicios 70% prueba escrita (todos los criterios tienen el mismo peso porcentual en la evaluación)

Contenidos del RA 6:

- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad.
- Funcionamiento ininterrumpido.
- Integridad de datos y recuperación de servicio.
- Servidores redundantes.
- Sistemas de clústeres.
- 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.

Evaluación: 2ª	**Objetivos generales**: j) m) p)

El RA 6 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.

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

Criterios de evaluación	UNIDADES	% EVA	Actividad/Instrumentos evaluación.
a) Se ha descrito la legislación sobre protección de datos de carácter personal.	8		50% Producción escrita 50% Presentación oral (todos los criterios tienen el mismo peso porcentual en la evaluación)
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.			

Contenidos del RA 7:

- 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.

Evaluación: 2ª	**Objetivos generales**: u)

El RA 7 se alcanza obteniendo una calificación ponderada de 5 puntos y una calificación mínima de 4 puntos en cada uno de los instrumentos de evaluación.

Actividad de evaluación	Técnicas de evaluación	Instrumentos de evaluación
Prueba escrita	Escrita y/o prueba Moodle	Plantilla de corrección
Caso práctico	Ejecución práctica	Rúbrica o Guía de Evaluación
Exposición oral	Observación	Rúbrica o Escala de Observación
Trabajo	Ejecución oral o práctica	Plantilla de corrección

PONDERACIÓN RESULTADOS DE APRENDIZAJE:

RESULTADO DE APRENDIZAJE	PONDERACIÓN
RA 1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	20%
RA 2: Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	20%
RA 3: Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	25%
RA 4: Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	12%
RA 5: Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	8%
RA 6: Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	10%
RA 7: Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	5%
Total:	100%

La calificación de la evaluación 1ª final FP informará del resultado final del módulo, entendiéndose que una calificación positiva conlleva la superación de todos los resultados de aprendizaje y por consiguiente la superación del módulo.

EVALUACIÓN ALTERNATIVA.

El porcentaje de faltas de asistencia, justificadas e injustificadas, que originan la imposibilidad de aplicación de los instrumentos de evaluación ordinaria se establece en el 20% del total de horas lectivas de todo el curso de la materia o módulo. En la programación de cada módulo se indicará a cuántas horas corresponde dicho 20%.

Este módulo tiene 105 horas, por lo tanto, se aplicará la evaluación alternativa con 21 horas (20 %) de faltas de asistencia y se apercibirá con 10 horas (10%).

Para estos casos las competencias no superadas deberán recuperarse durante el tercer trimestre atendiendo al calendario de clases de recuperación propuesto para todo el alumnado que no supere el módulo en la evaluación ordinaria de febrero así como realizando todos los trabajos prácticos y pruebas escritas necesarias para la adquisición de las competencias profesionales del módulo.

ACTIVIDADES DE RECUPERACIÓN Y MEJORA DE LOS RESULTADOS OBTENIDOS EN LA EVALUACIÓN PREVIA A LA EVALUACIÓN FINAL FP.

Todo alumno/a que **no supere el primer y/o el segundo trimestre**, suspenderá el módulo en la evaluación 1ª final y tendrá que recuperar en la evaluación 2ª final.

Para recuperar los RA no superados en la evaluación 2ª final, el alumno/a deberá aprobar uno o más exámenes vinculados a esos RA y realizar todas las prácticas que el profesor considere necesarias para demostrar sus habilidades prácticas. Estas prácticas serán distintas de las realizadas en clase, pero le permitirán al alumno/a recuperar aquellas prácticas obligatorias que suspendió o no presentó.

PROYECTO INTERMODULAR

Para demostrar los conocimientos adquiridos en este módulo se exige para el módulo de Proyecto Intermodular del segundo curso los siguientes requisitos:

- Adopción de pautas y prácticas de tratamiento seguro de la información:
  - Criptografía
  - Políticas de almacenamiento y contraseñas
  - ACLs
- Implantación de mecanismos de seguridad activa:
  - Uso de herramientas preventivas y paliativas
  - Seguridad en red corporativa: DMZ, cortafuegos
  - Implanta técnicas de acceso remoto: redes protegidas perimetralmente y VPN
- Implanta soluciones de alta disponibilidad:
  - Sistemas redundantes
  - Virtualización

INCORPORACIÓN DE LOS CONTENIDOS DE CARÁCTER TRANSVERSAL AL CURRÍCULO.

Temas transversales que se abordarán serán:

- EDUCACIÓN MORAL Y CÍVICA: se le mostrarán al alumnado aspectos de la vida cotidiana en los que es necesario respetar unas normas básicas y adoptar actitudes positivas y solidarias para la convivencia en sociedad. Habrá que respetar normas relativas al tratamiento de datos de carácter personal, así como las relativas a proteger los derechos de propiedad intelectual.
- EDUCACIÓN PARA LA PAZ: se velará en todo momento por la comunicación a través de un lenguaje no violento, así como se prestará atención a la prevención de conflictos en el aula y a la resolución pacífica de los mismos.
- EDUCACIÓN PARA LA IGUALDAD DE OPORTUNIDADES DE AMBOS SEXOS: se debe poner de manifiesto tal igualdad a la hora de realizar los agrupamientos de alumnos y alumnas para el desarrollo de cada una de las actividades planteadas. Reflexionar sobre la igualdad de oportunidades en el mercado laboral.
- EDUCACIÓN PARA LA SALUD: se prestará especial atención a la higiene postural y a la ergonomía para prevenir los dolores de espalda, ya que se pretende reducir la carga que soporta la misma al estar sentado trabajando con el ordenador.
- EDUCACIÓN AMBIENTAL: primará el uso y generación de documentación en formato digital para evitar en la medida de lo posible el derroche de papel. Para ello, se le proporcionará al alumnado todos los ejercicios y documentación en

formato PDF, para su descarga y acceso sin necesidad de recurrir a su impresión en papel.

- EDUCACIÓN DEL CONSUMIDOR: intentaremos que el alumnado reflexione sobre el hábito de consumir, potenciando además el uso del software libre y la adquisición de licencias cuando se trate de software propietario.

MEDIDAS DE ATENCIÓN A LA DIVERSIDAD Y ALUMNADO CON N.E.A.E.

Tras la evaluación inicial y siguiendo las recomendaciones del departamento de Orientación, se medidas propuestas con el fin de atender a los diferentes ritmos de aprendizajes.

Para estos alumnos se determinan las siguientes medidas generales:

- Explicaciones alternativas de los contenidos
- Flexibilización de los tiempos de entrega
- Seguimiento más estrecho de la adquisición de competencias y supervisión constante de sus tareas
- Adecuación de las actividades/pruebas si fuera necesario. Prever actividades de refuerzo colgadas en Moodle
- Para los alumnos con mayor ritmo en esta modalidad online planificar actividades de ampliación

ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON ESTE MÓDULO.

Las actividades complementarias y extraescolares que se realicen serán las que establezca el Departamento de Informática en tiempo y forma. Relacionadas, en todo caso, con el sector de las TIC.

AUTOEVALUACIÓN

Con el fin de permitir la evaluación de la práctica docente por parte del alumnado, se plantean dos actividades:

- La primera de ellas es un cuestionario anónimo que se pasará al alumnado a final de trimestre para consultar su opinión con respecto a la dinámica de las clases y para que propongan mejoras y cambios en las mismas.

- La segunda es de tipo transversal y recoge, de forma anecdótica pero frecuente, mediante conversaciones con el grupo su opinión sobre el desarrollo normal de las clases, la temporalización o los instrumentos de evaluación, entre otras.

Octubre 2026