PROGRAMACIÓN DEL MÓDULO:

SEGURIDAD Y ALTA DISPONIBILIDAD

PROFESOR/ES: ***En caso de más de un profesor es necesario identificar al profesor coordinador y puede ser necesario calibración.***	JULIO BARBERO GONZÁLEZ
GRUPO/S Y CICLO/S:	2º ASIR
CURSO:	2020-2021

ÍNDICE

INTRODUCCIÓN

OBJETIVOS

CONTENIDOS

DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

CRITERIOS DE EVALUACIÓN

RELACIÓN CON OTROS MÓDULOS DEL CICLO

METODOLOGÍA DIDÁCTICA

PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS

CRITERIOS DE CALIFICACIÓN

ATENCIÓN A LA DIVERSIDAD

MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

1. INTRODUCCIÓN

Este módulo se incluye en el ciclo formativo de Grado Superior Administración de Sistemas Informáticos en Red, perteneciente a la Familia Profesional de Informática y Comunicaciones, que queda establecido y regulado, en la Comunidad Autónoma de Extremadura por el DECRETO 210/2010, de 19 de noviembre, por el que se establece el currículo del Ciclo Formativo de Grado Superior de Técnico Superior en Administración de Sistemas Informáticos en Red, y por el 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.

La competencia general del 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.

Las competencias profesionales, personales y sociales se han adecuado al contexto socioeconómico y cultural del centro y a las características del alumnado, descrito en los diferentes documentos propios del centro y en el proyecto curricular de los ciclos formativos.

Las competencias profesionales, personales y sociales del ciclo formativo ASIR son las 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.

E. Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.

F. Determinar la infraestructura de redes telemáticas elaborando esquemas y seleccionando equipos y elementos.

G. Integrar equipos de comunicaciones en infraestructuras de redes telemáticas, determinando la

configuración para asegurar su conectividad.

H. Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.

I. Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

J. Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

K. Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.

L. Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.

M. 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.

N. Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.

O. 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.

P. 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.

Q. Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

R. Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

S. Participar de forma activa en la vida económica, social y cultural con actitud crítica y responsable.

T. Crear y gestionar una pequeña empresa, realizando un estudio de viabilidad de productos, de planificación de la producción y de comercialización. Artículo 4. Relación de cualificaciones y unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales.

2. OBJETIVOS

Los objetivos generales de este ciclo formativo son los siguientes:

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.

ñ) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.

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 resolver problemas y mantener una cultura de actualización e innovación.

q) Identificar formas de intervención en situaciones colectivas, analizando el proceso de toma de decisiones y efectuando consultas para liderar las mismas.

r) 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.

s) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.

t) 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.

Este módulo profesional 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.

Las funciones de la administración segura de sistemas incluyen aspectos como:
— El conocimiento y correcta manipulación de todos los elementos que forman el componente físico y lógico de los equipos.
— La adopción de prácticas seguras de acuerdo al plan de seguridad física del sistema.
— La adopción de prácticas seguras de acuerdo al plan de seguridad lógica del sistema.
— El conocimiento y uso de técnicas seguras de acceso remoto a un sistema, tanto en modo usuario como en modo administrativo.
— La selección y aplicación de técnicas y herramientas de seguridad activa que actúen como medidas preventivas y/o paliativas ante ataques a al sistema.
— La instalación y configuración de herramientas de protección perimetral, cortafuegos y servidores "proxy".
— La instalación y configuración de servicios de alta disponibilidad que garanticen la continuidad de servicios y la disponibilidad de datos.
— El conocimiento y aplicación de la legislación vigente en el ámbito del tratamiento digital de la información.

Las actividades profesionales asociadas a estas funciones se aplican en:
— Mantenimiento de equipos. Hardware y software.
— Administración de sistemas en pequeñas y medianas empresas.
— Personal técnico de administración de sistemas en centros de proceso de datos.
— Personal técnico de apoyo en empresas especializadas en seguridad informática.

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

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo están relacionados 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.

3. CONTENIDOS

Previa a la impartición de los contenidos se realiza una presentación de la asignatura, de metodología y de los criterios y procedimientos de evaluación.

Los contenidos del módulo se organizan en los siguientes bloques:

Bloque 0- Presentación del módulo.

Bloque 1 - Pautas de Seguridad Informática

- ***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.***
- ***Seguridad física y ambiental.***
- ***Seguridad lógica.***
- Análisis forense en sistemas informáticos.
- Legislación y normas de seguridad informática

Bloque 2 - Implantación de mecanismos de seguridad activa

- ***Ataques y contramedidas en sistemas personales.***
- ***Seguridad en la red corporativa.***

Bloque 3 - Implantación de técnicas de acceso remoto. Seguridad perimetral

- ***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.
- ***Técnicas de cifrado. Clave pública y clave privada.***
- Servidores de acceso remoto.

Bloque 4 - ***Instalación y configuración de cortafuegos***

- 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 un cortafuegos.

Bloque 5 - Instalación y configuración de servidores “proxy”

- 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”.***

Bloque 6 - Implantación de soluciones de alta disponibilidad

- ***Definición y objetivos.***
- ***Análisis de configuraciones de alta disponibilidad.***
- 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.

4. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

El orden de impartición de los contenidos puede variar en función de las necesidades del grupo, así como la duración planificada para cada uno de los bloques.

EVALUACIÓN	TEMA, BLOQUE O UNIDAD DIDÁCTICA	FECHA DE INICIO Y FIN	Nº HORAS LECTIVAS
1ª	Bloque 0- Presentación del módulo	21/09/2020 21/09/2020	1
	Bloque 1 - Pautas de Seguridad Informática	22/09/2020 21/10/2020	16
	Bloque 2 - Implantación de mecanismos de seguridad activa	22/10/2020 18/11/2020	15
	Bloque 3 - Implantación de técnicas de acceso remoto. Seguridad perimetral	19/11/2020 17/12/2020	15
		% AVANCE EN CONTENIDOS	**60%**
2ª	Bloque 4 - Instalación y configuración de cortafuegos	21/12/2020 01/02/2021	15
	Bloque 5 - Instalación y configuración de servidores "proxy"	02/02/2021 22/02/2021	10
	Bloque 6 - Implantación de soluciones de alta disponibilidad	23/02/2021 11/03/2021	11
		% AVANCE EN CONTENIDOS	**100%**

5. CRITERIOS DE EVALUACIÓN

El profesorado evaluará los aprendizajes del alumnado, los procesos de enseñanza y su propia práctica docente.

La evaluación en el ciclo formativo se realizará teniendo en cuenta los resultados de aprendizaje y los criterios de evaluación establecidos en los módulos profesionales, así como los objetivos generales del ciclo formativo.

Resultados de aprendizaje y criterios de evaluación según DOE nº 227 de 25 de noviembre de 2010:

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:

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en

los sistemas informáticos.
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.

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

Criterios de evaluación:

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.
Criterios de evaluación:

a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
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.

Criterios de evaluación:

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.

Criterios de evaluación:

a) Se han identificado los tipos de "proxy", sus características y funciones principales.
b) Se ha instalado y configurado un servidor "proxy-caché".
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.

Criterios de 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 "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.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado 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.

El profesorado evaluará los aprendizajes del alumnado, los procesos de enseñanza y su propia práctica docente.

La evaluación en el ciclo formativo se realizará teniendo en cuenta los resultados de aprendizaje y los criterios de evaluación establecidos en los módulos profesionales, así como los objetivos generales del ciclo formativo.

Resultados de aprendizaje y criterios de evaluación según DOE nº 227 de 25 de noviembre de 2010:

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:

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
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.

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

Criterios de evaluación:

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.
Criterios de evaluación:

a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
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.

Criterios de evaluación:

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.

Criterios de evaluación:

a) Se han identificado los tipos de "proxy", sus características y funciones principales.
b) Se ha instalado y configurado un servidor "proxy-caché".
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.

Criterios de 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 "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.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado 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.

6. RELACIÓN CON OTROS MÓDULOS DEL CICLO

Principalmente con los módulos de: Planificación y Administración de Redes (1º ASIR), Administración de Sistemas Operativos (2º ASIR), y Servicios de Red e Internet (2º ASIR), ya que el grueso de contenidos versa que sobre la seguridad de los sistemas operativos y la infraestructura de red.

Principalmente con los módulos de: Planificación y Administración de Redes (1º ASIR), Administración de Sistemas Operativos (2º ASIR), y Servicios de Red e Internet (2º ASIR), ya que el grueso de contenidos versa sobre la seguridad de los sistemas operativos y la infraestructura de red.

7. METODOLOGÍA DIDÁCTICA

El profesor, tras una breve introducción al tema a tratar, vinculará los nuevos contenidos con los ya aprendidos, dirigirá las prácticas y ejercicios necesarios para conducir al alumnado al nivel de comprensión que le capacite para desarrollar las capacidades terminales requeridas.

La investigación por grupos en Internet, la exposición de trabajos y el debate colectivo, ocuparán la mayoría del tiempo en el aula polivalente.

El desarrollo de los ejercicios se llevará a cabo principalmente en el aula bajo la dirección y supervisión del profesor, pudiendo en determinados casos completarlos en su casa.

Los ejercicios encomendados a los alumnos se remitirán por correo electrónico como norma general, o usando la plataforma de formación del centro cuando así se requiera.

El profesor, tras una breve introducción al tema a tratar, vinculará los nuevos contenidos con los ya aprendidos, dirigirá las prácticas y ejercicios necesarios para conducir al alumnado al nivel de comprensión que le capacite para desarrollar las capacidades terminales requeridas.

La investigación por grupos en Internet, la exposición de trabajos y el debate colectivo, ocuparán la mayoría del tiempo en el aula polivalente.

El desarrollo de los ejercicios se llevará a cabo principalmente en el aula bajo la dirección y supervisión del profesor, pudiendo en determinados casos completarlos en su casa.

Los ejercicios encomendados a los alumnos se remitirán por correo electrónico como norma general, o usando la plataforma de formación del centro cuando así se requiera.

8. PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS

La evaluación se realizará agrupando las unidades temáticas por evaluaciones.

Se celebrará una sesión de evaluación por cada trimestre de formación en el centro educativo; la última, tendrá la consideración de evaluación final ordinaria.

Las fechas de las mismas son las fijadas por el Claustro de profesores al inicio de curso (con las modificaciones que a este respecto pudieran ser aprobadas posteriormente, por este mismo órgano).

Los instrumentos de evaluación serán:

- Pruebas específicas de evaluación: serán escritas y/o prácticas y comprenderán los contenidos impartidos en las unidades de esa evaluación.
- Actividades de enseñanza/aprendizaje: podrán ser obligatorias u opcionales, a criterio del profesor.
- Actitud: se observará a través de su asistencia, su actitud y su comportamiento.

[Explicar convocatoria extraordinaria]
[Recuperación de evaluaciones suspensas]
[Si corresponde, explicar actividades y evaluación de alumnos que no asisten a clase del módulo por estar matriculado en 2º → se examinarán en convocatoria ordinaria de febrero/marzo y en extraordinaria de junio.]

9. CRITERIOS DE CALIFICACIÓN

La calificación en cada evaluación o recuperación será basándose en la correcta asimilación de la materia impartida, demostrada en las pruebas objetivas y ejercicios de clase con la siguiente cuantificación:
El 30% de la calificación corresponderá al resultado de las pruebas prácticas realizadas por el alumno en el aula.
El 60% de la calificación corresponderá al resultado de las pruebas teóricas realizadas por el alumno en el aula.
El 10% de la calificación atenderá a la evaluación continua del alumno durante el trimestre, teniendo en cuenta la actitud presentada en clase, la participación y asistencia.
Aquellos alumnos con un número de faltas superior al 20% de las horas asignadas al módulo perderán el derecho a la evaluación continua, y deberán realizar la entrega de prácticas pendientes y un examen final que comprenda todos los contenidos estudiados a lo largo del curso.
Además se han de tener en cuenta las siguientes consideraciones:

- Para aprobar por evaluaciones, se deberá aprobar cada evaluación por separado.
- El alumno/a que no entregue TODAS las prácticas obligatorias suspenderá la evaluación o en su caso la recuperación o examen final.
- Si no se obtiene un mínimo de 5 puntos en el examen se suspenderá la evaluación.
- Al finalizar cada tema, y a criterio del profesor, se puede llevar a cabo una prueba objetiva de los contenidos impartidos a lo largo de ese tema. Estas notas parciales se guardan para el cálculo final de la nota de la evaluación. Cuando el profesor lo estime oportuno,

realizará un examen final de los parciales que el alumno tenga pendientes. Si el alumno suspende el examen final (con uno o más parciales suspensos) iría al examen final de Marzo con todo el trimestre suspenso. En el caso de que en el examen final de Marzo no aprobará todos los trimestres que tenga pendiente (uno o más) iría a Junio con toda la materia del módulo. Los alumnos que tengan aprobados todos los trimestres no deberán realizar el examen final de Marzo.

- La nota máxima que se puede obtener en la recuperación tanto del examen como de las prácticas y trabajos es un 5.

La calificación de cada parte se obtendrá del siguiente modo:

- Actividades de enseñanza/aprendizaje: Serán evaluadas con un valor numérico comprendido entre 0 y 10 o con un APTO o NO APTO
- Prueba específica de evaluación: Tendrá una nota numérica entre 0 y 10. Se considera aprobado si es igual o mayor que 5.
- De igual manera se llevará a cabo, por parte del profesorado, un control de uso de los equipos durante las clases para hacer respetar las normas establecidas para el Ciclo (leídas al comienzo del curso a los alumnos y colgadas en los tablones de las aulas), entre las que se encuentra el no poder utilizar los equipos para jugar; siendo sancionado el alumno que lleve a cabo tal actividad con un punto negativo y el apagado inmediato del equipo durante dicha clase. Si, de esta manera, el alumno acumulara 3 negativos, perderá un punto en la evaluación final del trimestre.

Si el alumno tiene aprobadas las evaluaciones trimestrales, la nota final será la media aritmética de calificación obtenida en todas las evaluaciones.
En otro caso el alumno se presentará a un único examen de todo el módulo. La calificación se obtendrá aplicando los porcentajes señalados.

En cuanto a la promoción, se seguirán los criterios marcados en el proyecto curricular del ciclo formativo.

Normativa de exámenes y tareas:

- Los exámenes se realizarán en la fecha y hora indicadas por el profesor del módulo.
- La no asistencia a examen supone la calificación de No presentado.
- Solo se considerarán justificantes válidos los emitidos por órganos oficiales que explícitamente indiquen que no es posible o recomendable la asistencia en la fecha y hora del examen. A los estudiantes que aporten tales justificantes de ausencia a examen se les propondrá otra fecha y hora de realización.
- En caso de detectar plagios en tareas y exámenes (sea de compañeros o de otras fuentes) la calificación de la tarea o examen será de 0.
- En los exámenes no se podrá hablar ni realizar preguntas en voz alta, ni comentarios o ruidos que distraigan a los demás compañeros. En el caso de que estos se produzcan se expulsará al alumno del aula, suponiendo la anulación del examen y la calificación de 0.

10. ATENCIÓN A LA DIVERSIDAD

Si se detectan alumnos con necesidades especiales, por una parte se les ofrecerá la posibilidad de ampliar el número de ejercicios prácticos y por otra se abordarán otras metodologías (elaboración de postes, etc) encaminadas a asegurar que comprenden los distintos contenidos. Para aquellos alumnos que vayan más avanzados se les plantearán ejercicios prácticos que profundicen en los contenidos y que sean lo más motivadores posible.

11. MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

El desarrollo del módulo se hará en el aula dotada con 1 ordenador por alumno y también en el taller y en el CPD de los ciclos formativos. Se facilitará a los alumnos la utilización de los diferentes materiales y recursos disponibles.

Bibliografía:

- Manuales de las aplicaciones utilizadas.
- Especificaciones de organismos nacionales/internacionales.
- Libros relacionados con los contenidos y disponibles en la biblioteca del departamento.
- Revistas especializadas, disponibles en la biblioteca del departamento.
- Manuales, ejercicios resueltos, etc. obtenidos de Internet.

12. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Las programadas por el departamento y que estén relacionadas con los contenidos de este módulo.