PROGRAMACIÓN DIDÁCTICA

CURSO 2023-2024

MÓDULO **Seguridad y Alta Disponibilidad**

FAMILIA PROFESIONAL INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO DE GRADO SUPERIOR

Administración de Sistemas Informáticos en Red

CURSO: SEGUNDO

PROFESORES:

DIURNO: **Nuria Aragón Miralles**

ÍNDICE

1. INTRODUCCIÓN

El módulo de Seguridad y Alta Disponibilidad, se encuadra dentro de las especificaciones del título de Técnico Superior en Administración de Sistemas Informáticos en Red, integrado en la Familia Profesional de Informática y Comunicaciones, recogidas en el Real Decreto 1629/2009, de 30 de octubre. Este módulo tiene una duración total de 100 horas a razón de 5 horas semanales.

Referente europeo: CINE-5b (Clasificación Internacional Normalizada de la Educación)

2. OBJETIVOS

2.1 Competencia general del Título

"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".

2.2 Cualificaciones profesionales y unidades de competencia

a) Gestión de sistemas informáticos IFC152_3 (R.D. 1087/2005, de 16 de septiembre), que comprende las siguientes unidades de competencia:

UC0484_3 Administrar los dispositivos hardware del sistema.

UC0485_3 Instalar, configurar y administrar el software de base y de aplicación del sistema.

2.3 Competencias profesionales, personales y sociales del módulo

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

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

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

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

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

2.4 Objetivos generales del ciclo que contribuye a alcanzar el módulo

10. Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.

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

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

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

14. Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios

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

2.5 Objetivos del módulo

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

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

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

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

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

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

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

3. CONTENIDOS Y DISTRIBUCIÓN TEMPORAL

3.1 Contenidos básicos

Adopción de 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:
  - Amenazas físicas.
  - Amenazas 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:

Implantación de mecanismos de seguridad activa:

- Ataques y contramedidas en sistemas personales:
  - Clasificación de los ataques.
  - Anatomía de ataques y análisis de software malicioso.
  - Herramientas preventivas. Instalación y configuración.
  - Herramientas paliativas. Instalación y configuración.
  - 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.

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:
  - 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.

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.

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».

Implantación de soluciones de alta disponibilidad:

- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad.
  - Funcionamiento ininterrumpido.
  - Integridad de datos y recuperación de servicio.
  - Servidores redundantes.
  - Sistemas de «clusters».
  - Balanceadores de carga.

- Instalación y configuración de soluciones de alta disponibilidad.
- Virtualización de sistemas.
- Posibilidades de la virtualización de sistemas.
- Herramientas para la virtualización.
- Configuración y utilización de máquinas virtuales.
- Alta disponibilidad y virtualización.
- Simulación de servicios con virtualización.

Legislación y normas sobre seguridad:

- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

3.2 Contenidos actitudinales

Los contenidos actitudinales, aquellos que contribuyen a que la realización de actividades adquiera un carácter profesional, merecen especial atención ya que son necesarios para poder integrarse en el mundo laboral. Es por ello que existen algunas actitudes asociadas al comportamiento y a la realización de trabajo, de forma individual o en grupo, cuya adquisición se ha de contemplar y fomentar en el desarrollo de todas las unidades didácticas programadas para este módulo:

Actitudes Personales:

- Aceptar y cumplir el reglamento interno del Instituto
- Aceptar y cumplir las normas de comportamiento y trabajo establecidas durante el curso
- Utilizar los equipos y programas informáticos cumpliendo las normas establecidas, las de seguridad e higiene y los requisitos legales
- Ser puntual.
- Mantener su puesto de trabajo en perfecto estado
- Respetar y valorar la utilización de técnicas y procedimientos para mantener la seguridad, integridad y privacidad de la información
- Participar activamente en los debates y en los grupos de trabajo
- Valorar la evolución de la técnica para adaptarse al puesto de trabajo
- Interesarse por la formación permanente en cuestiones relacionadas con su trabajo
- Perseverar en la búsqueda de soluciones
- Valorar la constancia y el esfuerzo propio y ajeno en la realización del trabajo. Querer aprender y mejorar.
- Demostrar interés, participar, realizar aportaciones y comprometerse con el desarrollo del módulo.

- Mostrar interés por la utilización correcta del lenguaje
- Realizar su trabajo personal de forma autónoma y responsable. No apropiarse del trabajo ajeno.
- Saber rodearse de los materiales necesarios para desarrollar correctamente su trabajo. Traer siempre el material necesario.
- Responsabilizarse de la ejecución de su propio trabajo y de los resultados obtenidos
- Orden y método en la realización de tareas
- El esmero, la pulcritud y la puntualidad en la entrega de actividades. Evitar las faltas de ortografía y cuidar la redacción.
- Demostrar interés por la conclusión total de un trabajo antes de comenzar el siguiente

Actitudes relacionales:

- Respeto por otras opiniones, ideas y conductas. Saber estar en todos los sentidos.
- Tener conciencia de grupo, integrándose en un grupo de trabajo, participando activamente en las tareas colectivas y respetando las opiniones ajenas
- Respetar la ejecución del trabajo ajeno en el grupo, compartiendo las responsabilidades derivadas del trabajo global
- Valorar el trabajo en equipo como el medio más eficaz para la realización de ciertas actividades
- Mantener actitudes de solidaridad y compañerismo

3.3 Distribución temporal

RESULTADOS DE APRENDIZAJE							UNIDADES DIDÁCTICAS SECUENCIADAS	DURACIÓN (horas)
RA1	RA2	RA3	RA4	RA5	RA6	RA7		
X							UT1. Adopción de pautas de seguridad informática	10
X	X						UT2. Implantación de mecanismos de seguridad activa	30
X	X	X					UT3. Implantación de técnicas de acceso remoto	10
X	X	X	X				UT4. Instalación y configuración de cortafuegos.	20
X				X			UT5. Instalación y configuración de un servidor proxy.	15
X					X		UT6. Implantación de soluciones de alta disponibilidad	10
						X	UT7. Legislación y normas sobre seguridad	5
							TOTAL	**100h.**

4. UNIDADES DIDÁCTICAS

Unidad 01: Adopción de pautas de seguridad informática.

Competencias	Objetivos	Contenidos según normativa	Resultados de aprendizaje
10,13	1,2	Adopción de 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.	RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
– Criptografía asimétrica. – Análisis Forense. – Análisis forense digital (secuencia de recogida de información volátil)			GPG (**GPG4Win**) FTK Imager https://cybercamp.es/videos/analisis-forense-digital
		Nº horas de la unidad:	**10**

Unidad 02: Implantación de mecanismos de seguridad activa.

Competencias	Objetivos	Contenidos según normativa	Resultados de aprendizaje
11,13	1,2,3	- Elaboración de un manual de seguridad y planes de contingencia. - Ataques y contramedidas en sistemas personales. o Anatomía de ataques y análisis de software malicioso. o Clasificación de los ataques. o Footprinting o Information Gathering. o FingerPrinting. o Explotación de las vulnerabilidades. Metasploit. o Ataques según el principio de seguridad vulnerado. o Ataques web. o Ataques a contraseñas. Fases de registro y autenticación. - Seguridad en la conexión con redes públicas. - Seguridad en la red corporativa.	RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema
Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
– Herramientas de Footprinting (Google, Shodan, Maltego, Foca,…) – Herramientas de Fingerprinting. NMAP – Explotación de las vulnerabilidades. Metasploit – Meterpreter y escalada de privilegios – Ocultar y mantener el acceso – Ataques web – Ataques a contraseñas			Máquina virtual de Kali Máquinas vulnerables dadas por la profesora
		Nº horas de la unidad:	**30**

<table>
<tr><th colspan="4">Unidad 03: Implantación de técnicas de acceso remoto</th></tr>
<tr><th>Competencias</th><th>Objetivos</th><th>Contenidos según normativa</th><th>Resultados de aprendizaje</th></tr>
<tr><td>11,13</td><td>1,4</td><td>- Elementos básicos de la seguridad perimetral.
o Router frontera.
o Cortafuegos.
o Redes privadas virtuales.
o Perimetros de red. Zonas desmilarizadas.
o Subred protegida débil Vs subred protegida fuerte.
- Políticas de defensa en profundidad.
o Defensa perimetral.
o Defensa interna.
o Factor humano.
- Protocolo SSH.
- Redes privadas virtuales. VPN.
- Servidores de acceso remoto.
o Protocolos de autenticación.
o Servidores de autenticación. Ataques y contramedidas en sistemas personales.
o Acceso remoto centralizado: Apache Guacamole.
o Servidores de autenticación. Ataque y contraseñas en sistemas personales.</td><td>RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad</td></tr>
<tr><td colspan="3">Actividades de enseñanza-aprendizaje y de evaluación</td><td>Recursos necesarios para su realización</td></tr>
<tr><td colspan="3">– Secure Shell: SSH
– VPN</td><td>Máquinas virtuales linux</td></tr>
<tr><td></td><td></td><td>Nº horas de la unidad:</td><td>10</td></tr>
</table>

Unidad 04: Instalación y configuración de cortafuegos

Competencias	Objetivos	Contenidos según normativa	Resultados de aprendizaje
11	1,5	- Utilización de cortafuegos. - Filtrado de paquetes de datos. - Tipos de cortafuegos. - Utilización de cortafuegos. - Reglas de filtrado de cortafuegos. - Pruebas de funcionamiento. - Registros de sucesos de un cortafuegos. - Cortafuegos integrados en los sistemas operativos. - Distribuciones libres para implementar cortafuegos en máquinas dedicadas. - Cortafuegos hardware. - Sistemas Detectores de Intrusos. Técnicas.	RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema. RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad. RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna
Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
– Instalación de PFSENSE – Configuración de las interfaces + DHCP – Configuración de reglas de firewall – Configuración de NAT – Configuración de VPN			Máquina virtual pfsense
		Nº horas de la unidad:	**20**

Unidad 05: Instalación y configuración de un servidor proxy

Competencias	Objetivos	Contenidos según normativa	Resultados de aprendizaje
11	1,6	- ¿Qué es un proxy. - Instalación y configuración de un servidor proxy. - Instalación y configuración de un cliente proxy. - Métodos de autenticación en un proxy. - Proxy inverso. - Proxy encadenado. - Pruebas de funcionamiento. - Herramientas gráficas.	RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. RA5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
Configuración del proxy SQUID: - Filtros - En modo caché - Acceso a usuarios - Generación de informes con SARG			Máquinas virtuales linux
		Nº horas de la unidad:	**15**

Unidad 06: Implantación de soluciones de alta disponibilidad

Competencias	Objetivos	Contenidos según normativa	Resultados de aprendizaje
9	1, 7	- Análisis de configuraciones de alta disponibilidad: o Funcionamiento ininterrumpido. o Integridad de datos y recuperación de servicio. o Servidores redundantes. Sistemas de Clusters. o Balanceadores de carga. - Virtualización de sistemas. o Herramientas para la virtualización. o Entornos personales Vs entornos empresariales. o Alta disponibilidad y virtualización. o Análisis de la actividad del sistema virtualizado. - Pruebas de carga. o Cargas sintéticas. - Modelos predictivos y análisis de tendencias.	RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
– Instalación y configuración de ldirector para alta disponibilidad – Alta disponibilidad en el entorno NetInVM			Máquinas virtuales
		Nº horas de la unidad:	**10**

Unidad 07: Legislación y normas sobre seguridad			
Competencias	**Objetivos**	**Contenidos según normativa**	**Resultados de aprendizaje**

18	8	- Legislación sobre protección de datos.
		  ○ RGPD y LOPDGDD. Tratamiento de los datos.
		- Legislación sobre los servicios de la sociedad de la información y correo electrónico.
		- Normas ISO sobre gestión de seguridad de la información.
		  ○ PDCA.
		- Organismos de gestión de incidencias
			RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia

Actividades de enseñanza-aprendizaje y de evaluación			**Recursos necesarios para su realización**
Responder a las cuestiones planteadas			Apuntes del tema
		Nº horas de la unidad:	**5**

5. METODOLOGÍA

La Ley Orgánica 2/2006, de 3 de mayo, de Educación, especifica en su artículo 40, como uno de los objetivos de la formación profesional: aprender por sí mismos y trabajar en equipo. Teniendo en cuenta esto, en todo momento, se proponen las siguientes pautas de actuación:

- Favorecer la motivación del alumnado, haciéndoles sentir protagonistas del proceso de enseñanza-aprendizaje y relacionando en todo momento los nuevos conocimientos con la vida real.
- Motivar que los alumnos/as realicen aprendizajes significativos por sí mismos.
- Proponer actividades que despierten el interés del alumno/a, siempre ajustándose a sus posibilidades de realización (ni demasiado fáciles ni excesivamente difíciles)
- Favorecer la comunicación interpersonal
- Favorecer una metodología activa e investigadora, mediante el desarrollo del pensamiento crítico e investigador tanto en el alumnado como en el docente.
- Promover técnicas de grupo como los debates, las discusiones guiadas, foros etc.

También se utilizará el aula ATECA (Aula de Tecnología Aplicada) como aula dinámica para la realización de prácticas y trabajos grupales, contribuyendo al desarrollo de las competencias personales, sociales y profesionales del alumnado. En dicha aula, se trabajará siguiendo la metodología ABP (Aprendizaje Basado en Proyectos), planteando un proyecto a diferentes grupos de alumnos para abordar entre todos su solución.

5.1 Materiales y recursos didácticos

Los materiales y recursos necesarios para el correcto desarrollo del módulo por parte de los alumnos serán los siguientes:

- Ordenador con acceso a Internet.
- Procesador de textos para la realización de las prácticas.
- Software de virtualización.

6. EVALUACIÓN

6.1 Criterios de evaluación

RA1. 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.

RA2. 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.

RA3. 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.

RA4. 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.

RA5. 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-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».

RA6. 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.

RA7. 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.

6.2 Instrumentos y procedimientos de evaluación

Mediante la evaluación se determina si la planificación del curso ha permitido alcanzar los objetivos propuestos o bien si es necesario reestructurar dicha planificación.

Por cada unidad didáctica se plantearán una serie de ejercicios teórico-prácticos que el alumnado deberá resolver individualmente, disponiendo para ello del material didáctico que necesite: libros, apuntes, etc. Posteriormente dichos ejercicios serán enviados para ser corregidos por el profesor/a, permitiendo de esta forma conocer al mismo/a la marcha académica de los alumnos y pudiendo el alumnado servirse de ellos como apoyo en el estudio y/o repaso de los contenidos de la evaluación. Así mismo en cada unidad didáctica se incluirán ejercicios de autoevaluación que permitan conocer al alumno/a su propio progreso.

Pruebas presenciales

Las pruebas objetivas presenciales se organizan:

- Se realizarán dos evaluaciones, una por trimestre, en las que se verificarán los resultados de aprendizaje adquiridos a través de los contenidos conceptuales, procedimentales y actitudinales desarrollados por el alumno y mediante los criterios de evaluación.
- Las convocatorias ordinarias serán en marzo y junio.

6.3 Criterios de calificación

Los porcentajes asignados a cada uno de los apartados en los que se divide la materia son:

a) Los exámenes presenciales realizados durante la evaluación supondrán un **75%** de la nota.

UNIDADES DIDÁCTICAS	Bloque
UT1. Adopción de pautas de seguridad informática	**55%**
UT2. Implantación de mecanismos de seguridad activa	
UT3. Implantación de técnicas de acceso remoto	
UT4. Instalación y configuración de cortafuegos.	**45%**
UT5. Instalación y configuración de un servidor proxy.	
UT6. Implantación de soluciones de alta disponibilidad	
UT7. Legislación y normas sobre seguridad	
TOTAL	**100%**

b) Los ejercicios y/o prácticas encomendadas por el profesor supondrán un **25%** de la nota.

UNIDADES DIDÁCTICAS	Porcentaje
UT1. Adopción de pautas de seguridad informática	**10**
UT2. Implantación de mecanismos de seguridad activa	**30**
UT3. Implantación de técnicas de acceso remoto	**10**
UT4. Instalación y configuración de cortafuegos.	**20**
UT5. Instalación y configuración de un servidor proxy.	**15**
UT6. Implantación de soluciones de alta disponibilidad	**10**
UT7. Legislación y normas sobre seguridad	**5**
TOTAL	**100%**

Para obtener la calificación de cada evaluación se realizará la media ponderada de los resultados obtenidos en cada uno de los exámenes y prácticas realizadas hasta el momento de la evaluación. La nota de evaluación resultará del truncamiento de esta media ponderada, pero se guardará la nota con 2 decimales para el cálculo de la calificación final ordinaria del módulo.

De acuerdo con la normativa vigente la calificación del módulo profesional es numérica entre 1 y 10, sin decimales. Se considerarán positivas las calificaciones iguales o superiores a cinco puntos y negativas las restantes.

Otros aspectos a considerar sobre las prácticas y pruebas son:

- Las prácticas marcadas como obligatorias deberán entregarse en las fechas/horas establecidas sin excusa. La no entrega en las fechas/horas marcadas serán calificados con un 0. Posteriormente a dicha fecha/hora, podrán ser entregados y corregidos, con el fin de que sirvan como base para la práctica siguiente.
- Aquellos proyectos, trabajos, prácticas o ejercicios de diferentes alumnos en los que haya una manifiesta similitud entre ellos o con otros de años anteriores o de Internet serán calificados con un 0.
- Podrá requerirse la exposición oral de las prácticas por parte de los alumnos.
- Es responsabilidad del alumno guardar en el lugar especificado por el profesor las pruebas y prácticas realizadas, de forma que, si no aparecen en el lugar indicado, serán calificados con un 0.

Serán calificados con un 0 aquellos exámenes y/o pruebas en los que se detecte que ha habido copia entre diferentes compañeros y/o se hayan utilizado medios no autorizados por el profesor

6.4 Criterios de recuperación

El profesor debe facilitar el éxito de sus alumnos, por lo que deben establecerse unos criterios para permitir la recuperación de las partes no superadas. Al ser la evaluación individualizada, las actividades de recuperación podrán variar en función del alumno y de los conocimientos y capacidades que sean objeto de recuperación.

Los procedimientos de recuperación son detección de las carencias del alumno, realización de tareas específicas que refuercen la carencia detectada y reevaluación de los conocimientos y/o capacidades no superadas.

La reevaluación de los conocimientos y/o capacidades no superadas se realizará:

En las evaluaciones ordinarias (primera y segunda), que se llevarán a cabo en los meses de marzo y junio y serán realizadas por:

- **Alumnos que no hayan superado la materia a lo largo del curso.**

  Estos alumnos realizarán un examen de los bloques no superados. La calificación final del módulo se calculará con los porcentajes establecidos en los criterios de calificación, cogiendo la mejor nota entre la nota del examen original de un bloque o la del examen de la recuperación del mismo realizado en esta evaluación.

- **Alumnos que han perdido el derecho a evaluación continua**.

Se llevará a cabo la evaluación de toda la materia impartida en la asignatura en un examen llevado a cabo en la convocatoria ordinaria (primera y/o segunda), que se llevarán a cabo en los meses de marzo y junio. En este tipo de evaluación, la nota del módulo corresponderá con la calificación obtenida en el examen final. Este examen podrá tener contenidos de las prácticas realizadas durante el curso. La calificación final del módulo será la resultante del redondeo de la nota de este examen, siempre y cuando ésta sea igual o mayor que 5.

6.5 Actividades de refuerzo o recuperación

Se explica en el apartado anterior.

6.6 Recuperación de módulos pendientes

Los alumnos con este módulo pendiente de otros años deberán cursarlo de nuevo en las mismas condiciones que los alumnos nuevos (excepto el número de convocatoria).

7. ATENCIÓN AL ALUMNADO CON NECESIDADES ESPECÍFICAS DE APOYO EDUCATIVO

La atención a la diversidad en este módulo se centra en prestar apoyo a aquellos alumnos que sufran algún retraso en la adquisición de determinados contenidos del curso ya que no hay ningún alumno con necesidades educativas específicas de carácter físico que exija la adaptación de las pruebas.

Se atenderá cada alumno de forma individual y en todo caso se procurará aclarar cuantas dudas surjan por parte de los alumnos de forma que aquellos que no hayan alcanzado los conocimientos y procedimientos mínimos harán actividades de apoyo o de refuerzo para que cubran las lagunas que tengan y puedan seguir el curso en mejores condiciones, mientras que otros alumnos pueden hacer actividades de profundización o ampliación.

8. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se intentará que los alumnos participen en jornadas tecnológicas o talleres que estén relacionados con el módulo y se promoverá la participación en concursos de nivel autonómico o nacional relacionados con el módulo.

9. NECESIDADES Y PROPUESTAS DE FORMACIÓN DEL PROFESORADO

El profesorado de este módulo demandaría formación avanzada en ciberseguridad.

10. BIBLIOGRAFÍA DE REFERENCIA

Como bibliografía de referencia para el desarrollo del módulo, se utilizarán, además de los apuntes proporcionados en el aula virtual (*https://aulavirtual-educacion.larioja.org/*), libros de consulta y prensa especializada, vídeos explicativos, manuales de Internet etc.