IES GUADALPEÑA

ARCOS DE LA FRONTERA (CÁDIZ)

PROGRAMACIÓN DIDÁCTICA

NIVEL

CICLO FORMATIVO DE GRADO SUPERIOR

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED.

MÓDULO

SEGURIDAD Y ALTA DISPONIBILIDAD

IND	Departamento de	Informática.

16. ANEXO-II: PLAN DE REFUERZO

17. ANEXO-III: PLAN DE MEJORA

1. INTRODUCCIÓN

La presente programación didáctica se desarrolla en el centro IES Guadalpeña de Arcos de la Frontera en la provincia de Cádiz, destinada al módulo profesional de "Seguridad y Alta Disponibilidad", del segundo curso del Ciclo Formativo de Grado Superior correspondiente al título de Técnico en Administración de Sistemas Informáticos y Redes. La duración del mismo es de 84 horas, impartiéndose 4 horas semanales.

Este módulo se encuadra dentro del título de formación profesional Técnico en Administración de Sistemas Informáticos en Red, que tiene una duración de 2000 horas distribuidas en módulos que se desarrollarán durante dos cursos académicos.

La referencia del sistema productivo de este módulo profesional y sus enseñanzas mínimas se encuentran en el Real Decreto por el que se establece el título en Técnico de Administración de Sistemas Informáticos y Redes (Real Decreto 1629/2009, de 30 de octubre), por el que se establece el título de Administración de Sistemas Informáticos y Redes y se fijan sus enseñanzas mínimas y en la ORDEN de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de Administración de Sistemas Informáticos y Redes. También nos basamos en 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.

1.1. Nuestro Centro

- **Ubicación**: El centro IES Guadalpeña se encuentra ubicado en Arcos de la Frontera, localidad de unos 30.000 habitantes.
- **Edificio**: Es un edificio de reciente construcción, que se encuentra en buen estado.
- **Materiales**: El centro tiene una dotación aceptable. Existiendo al menos un ordenador por cada dos alumnos/as en todas las aulas.
- **Unidades**: Existe primer y segundo ciclo de Educación Secundaria Obligatoria, Bachillerato de las ramas de Humanidades y ciencias sociales, y Ciencias y tecnología, Formación Profesional Básica de Informática de Oficina, un ciclo formativo de Formación Profesional Inicial de Grado Medio de Sistemas Microinformáticos y Redes y por último un ciclo formativo de Formación Profesional Inicial de Grado Superior de Administración de sistemas informáticos en red.

1.2. Nuestro entorno.

El I.E.S. Guadalpeña se encuentra dentro del denominado Barrio Bajo de la localidad de Arcos de la Frontera (Cádiz). Arcos de la Frontera es un municipio que cuenta con una importante población dentro de los Pueblos Blancos de la Sierra de Cádiz (30.000 habitantes aprox.), pero el reparto geográfico de la misma es desigual.

Esta situación geográfica condiciona en gran medida las posibilidades educativas que van a encontrar los alumnos/as dentro de su entorno, no existiendo mas ciclos tecnológicos en un radio de 15 kms, existiendo solo un ciclo de chapa y pintura y otro de hostelería en la misma localidad.

1.3. Características del alumnado.

- Son de la localidad o municipios cercanos.
- Disparidad de edades, lo que provoca distintos niveles de conocimientos iniciales.
- Los alumnos/as que se han matriculado en este ciclo provienen de: Prueba de acceso, bachillerato y 4o de ESO.

Por todas estas características, nos encontramos con una gran diversidad de niveles en la clase, aunque todos con una base sólida en informática a nivel de usuario.

1.4. Marco Legal

El marco legal del que parte esta programación se detalla a continuación:

- **Ley Orgánica 5/2002**, de 19 de junio, de las Cualificaciones y de la Formación Profesional.

- **El Real Decreto 1147/2011**, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo, fija la estructura de los nuevos títulos de formación profesional, que tendrán como base el Catálogo Nacional de las Cualificaciones Profesionales, las directrices fijadas por la Unión Europea y otros aspectos de interés social, dejando a la Administración educativa correspondiente el desarrollo de diversos aspectos contemplados en el mismo.

- **El Decreto 436/2008,** de 2 de septiembre, por el que se establece la ordenación y las enseñanzas de la Formación Profesional inicial que forma parte del sistema educativo, regula los aspectos generales de estas enseñanzas. Esta formación profesional está integrada por estudios conducentes a una amplia variedad de titulaciones, por lo que el citado Decreto determina en su artículo 13 que la Consejería competente en materia de educación regulará mediante Orden el currículo de cada una de ellas.

- **El Decreto 327/2010,** de 13 de julio, por el que se aprueba el Reglamento Orgánico de los Institutos de Educación Secundaria.

- **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.

- **El Real Decreto 1629/2009** del Ministerio de Educación, 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 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.

1.5 Descripción del Módulo

El módulo en el que se centra esta Programación se denomina “Seguridad y alta disponibilidad” y se ubica dentro de los módulos profesionales impartidos en el Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red. Así mismo, este ciclo se enmarca dentro de la Familia Profesional de Informática y se corresponde con la figura profesional de Técnico Superior en Administración de Sistemas Informáticos en red, ubicada en cualquier empresa que tenga automatizada su gestión y en empresas más específicas del sector informático.

El módulo se desarrolla durante **84 horas** distribuidas en 4 horas semanales, que estarían incluidas en el total de 2.000 horas de duración del Ciclo Formativo completo.
Este módulo será cursado por los/as alumnos/as a lo largo del segundo año académico correspondiente a este ciclo.

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.

2. OBJETIVOS

2.1. Objetivos generales del Ciclo Formativo.

De los **Objetivos Generales** enunciados en la **ORDEN de 19 de julio de 2010**, por la que se desarrolla el currículo correspondiente al título de **Técnico Superior en Administración de Sistemas Informáticos en Red**, corresponden, específicamente, para este módulo, 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 especifico 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.

2.2. Resultados de Aprendizaje del Módulo.

Los **Objetivos del Módulo** se expresan en términos de **Resultados de Aprendizaje**, y son los que se espera que alcance el alumno al concluir el módulo.

Los **Resultados de Aprendizaje** establecidos en la normativa vigente (Orden del 19 julio de 2010), para este módulo son las siguientes:

1. **RA.1.** Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. (SEGURIDAD PASIVA-FÍSICIA, BACKUPS, ACLs, CUOTAs, HERRAMIENTAS DE DETECCIÓN Y MONITORIZACIÓN DE AMENAZAS Y VULNERABILIDADES, PROTECCIÓN CUENTA ADMINISTRACIÓN, POLITICA CLAVES SEGURAS, PROTECCIÓN CARGADOR ARRANQUE, TÉCNICAS DE SUPLANTACIÓN CUENTAS ADMINISTRACIÓN y ANÁLISIS FORENSE).

2. **RA.2.** Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema. (SEGURIDAD ACTIVA-LOGICA. CRIPTOGRAFÍA(Cifrado de Archivos, Directorios y Comunicaciones). SEGURIDAD EN REDES LOCALES. HERRAMIENTAS DE DETECCIÓN, MONITORIZACIÓN DE VULNERABILIDADES).

3. **RA.3.** Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad. (SSH y VPN).

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

5. **RA.5.** Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio. (PROXY).

6. **RA.6.** Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba. (ALTA DISPONIBILIDAD: VIRTUALIZACIÓN EN SERVIDORES…).

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

2.3. Actividades Profesionales asociadas al Módulo.

Las actividades profesionales asociadas a esta función 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.

2.4. Orientaciones Pedagógicas.

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.

3. UNIDAD DE COMPETENCIA ASOCIADA AL MÓDULO.

De acuerdo a lo establecido en el artículo 8 de la Ley Orgánica 5/2002, de 19 de junio, la unidad de competencia asociada al módulo de **Seguridad y Alta Disponibilidad** son "**Asegurar equipos informáticos**" (**UC0486_3**) y "**Administrar los dispositivos hardware del sistema**" (**UC0484_3**) de la Cualificación Profesional de "**Gestionar sistemas informáticos**" (**IFC152_3**).

4. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

La formación del módulo de Seguridad y Alta Disponibilidad contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

<table>
<tr><th>COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES</th><th>OBJETIVOS GENERALES</th><th>RESULTADOS DE APRENDIZAJE</th></tr>
<tr><td rowspan="3">(a) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
(b) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades
de funcionamiento.
(c) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
(d) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
(e) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
(f) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
(g) 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.
(h) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados,
informando cuando sea conveniente.
(i) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
(j) Resolver problemas y tomar decisiones individuales, siguiendo</td><td>(a) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para implementar soluciones de alta disponibilidad.
(b) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de
fabricante, para supervisar la seguridad física.</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.</td></tr>
<tr><td>(c) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
(d) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.</td><td>RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.</td></tr>
<tr><td>(e) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.</td><td>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 RA5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el
funcionamiento seguro del servicio.

RA5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.</td></tr>
</table>

las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.		
	(f) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para mantener el espíritu de innovación.	**RA7.** Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

5. CONTENIDOS

5.1. Contenidos del Currículum.

Los contenidos básicos que figuran en el Currículo oficial son:

- **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.
  - Ejemplos de amenazas.
  - Estadísticas.
  - 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.
  - Utilización de sistemas biométricos de identificación.
  - Copias de seguridad e imágenes de respaldo.
  - Medios de almacenamiento.
  - Recuperación de datos.
  - Realización de Auditorías de seguridad.
  - Análisis forense en sistemas informáticos:
    - Objetivo del análisis forense.
    - Recogida y análisis de evidencias.
    - Herramientas del análisis.

- **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: Identificación digital. Firma electrónica y certificado digital. Publicidad y correo no deseado. Otros.
  - Elaboración de un manual de seguridad y planes de contingencia.
  - Pautas y prácticas seguras.
  - Seguridad en la red corporativa:
  - Monitorización del tráfico en redes: aplicaciones para la captura y análisis del tráfico, Aplicaciones para la monitorización de redes y equipos.
  - Seguridad en los protocolos para comunicaciones inalámbricas.
  - Riesgos potenciales de los servicios de red.
  - Intentos de penetración: craqueado de contraseñas, forzado de recursos, puertas traseras. Sistemas de detección de intrusiones.

- **Implantación de técnicas de acceso remoto. Seguridad perimetral:**
  - Elementos básicos de la seguridad perimetral:
  - «Router» frontera.
  - Cortafuegos.
  - Redes privadas virtuales.
  - Perímetros de red. Zonas desmilitarizadas.
  - Arquitectura débil de subred protegida.

- Arquitectura fuerte de subred protegida.
- Políticas de defensa en profundidad:
- Defensa perimetral.
- Defensa interna.
- Factor Humano.
- 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 enlace.
- VPN a nivel de red. SSL, IPSec.
- VPN a nivel de aplicación. SSH.
- Intérprete de comandos SSH.
- Gestión de archivos 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.
  - Cortafuegos integrados en los sistemas operativos.
  - Cortafuegos libres y propietarios.
  - Distribuciones libres para implementar cortafuegos en máquinas dedicadas.
  - Cortafuegos hardware.

- **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».
  - «Proxys» inversos.
  - «Proxys» encadenados.
  - Pruebas de funcionamiento. Herramientas gráficas.

- **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:
  - Entornos personales.
  - Entornos empresariales.
  - Configuración y utilización de máquinas virtuales.
  - Alta disponibilidad y virtualización.
  - Simulación de servicios con virtualización.

- Servicios reales con virtualización.
- Análisis de la actividad del sistema virtualizado.
- Pruebas de carga. Cargas sintéticas.
- Modelos predictivos y análisis de tendencias.

- **Legislación y normas sobre seguridad:**
  - Legislación sobre protección de datos.
  - Legislación sobre los servicios de la sociedad de la información y correo electrónico.
  - Normas ISO sobre gestión de seguridad de la información.
  - Organismos de gestión de incidencias.

5.3. Distribución contenidos en Unidades Didácticas y Temporalización.

Unidades Didácticas y Temporalización	
UD.1 – Principios de Seguridad y Alta Disponibilidad. Seguridad Pasiva. • Legislación sobre Seguridad informática. • Técnicas de Respaldo de Sistemas Linux y Windows. • Técnicas de Respaldo de Sistemas Linux y Windows en red. • Creación y Restauración de Cargadores de arranque para Sistemas Linux y Windows. • Técnicas de Intrusión en Sistemas Linux y medidas preventivas. • Técnicas de Intrusión en Sistemas Windows y medidas preventivas.	**1ª EVALUACIÓN**
UD.2 – Seguridad Activa. • Criptografía. Cifrado de Archivos, Directorios y Unidades. • Autoridades de Certificación, Certificados Digitales de Servidor y Certificados Digitales de Cliente. • Servicios en Red cifrados: HTTPS. • Seguridad en Redes y Comunicaciones.	**1ª EVALUACIÓN**
UD.3 – SSH. • SSH y SSHFS. • VPNs.	**1ª EVALUACIÓN**
UD.4 – Firewalls. • Reglas de Filtrado de tráfico. • Reglas de Ruteo de tráfico. • Reglas de Registro de tráfico.	**1ª EVALUACIÓN**
UD.5 – Alta Disponibilidad. • Cluster en Proxmox. • SAS en Proxmox. • AD en Proxmox.	**2ª EVALUACIÓN**
UD.6 – PROXY. • ACLs • ACLs basada en tiempos y grupos.	**2ª EVALUACIÓN**
UD.7 – Legislación y Normativa en Seguridad Informática.	**2ª EVALUACIÓN**
Total Horas: **84 horas.**	

5.3. Relación de Unidades Didácticas con los Resultados de Aprendizaje.

En el siguiente cuadro resumen, se especifica la concordancia entre los objetivos específicos de este módulo y las unidades de trabajo (la X muestra correspondencia):

UDs / RAs	[RA1] Seg. Pasiva	[RA2] Seg. Activa	RA3 [SSH]	RA4 [Firew.]	RA5 [Proxys]	RA6 [HA]	RA7 [Legisl. y Normat.]
UD.1 – Principios de Seguridad y Alta Disponibilidad. Seguridad Pasiva.	**100%**						
UD.2 – Seguridad Activa.		**100%**					
UD.3 – SSH.			**100%**				
UD.4 – Firewalls.				**100%**			
UD.5 – Alta Disponibilidad.						**100%**	
UD.6 – Proxys.					**100%**		
UD.7 – Legislación y Normativa en Seguridad Informática.							**100%**

La calificación de cada RA se obtendrá mediante media ponderada de los respectivos pesos indicados en la tabla.

6. CONTENIDOS TRANSVERSALES

Los temas transversales deben integrarse en los objetivos, contenidos y criterios de evaluación de todos módulos profesionales. Es evidente que no todos se prestan por igual al tratamiento de estos temas.

Unos tienen más posibilidades que otros. Los temas transversales que se relacionan más directamente con nuestro módulo y que por tanto pueden tratarse de una forma natural serían los siguientes:

- **El respeto de los valores cívicos:** Será un tema que trataremos en nuestra práctica docente diariamente a través de nuestra actitud hacia los alumnos y alumnas, fomentando el trato igualitario, tanto entre sexos como entre las diversa culturas, y el respeto entre los integrantes del grupo.

- **Educación para la Paz y la Tolerancia:** el profesor procurará ser tolerante tanto con sus compañeros y compañeras como por supuesto con todo el alumnado, procurará debatir las ideas y razonar con aquellas personas de opiniones contrarias.

- **Desarrollo de hábitos de vida saludable:** Este tema podemos concretarlo en diversos aspectos como los hábitos en la postura para el uso del ordenador así como otros problemas de salud que pudieran derivarse de una utilización inadecuada o excesiva del mismo.

- **Desarrollo de hábitos de consumo:** En este tema será conveniente incidir en los siguientes aspectos: la necesidad de estudio detallado de precio/prestaciones a la hora de adquirir cualquier producto hardware o software; el fomento del uso de software legal y estudio de la problemática del uso de software pirata, y por último, las ventajas del software de distribución libre o con licencia copyleft.

- **Utilización del tiempo de ocio:** Aquí podemos tratar el uso adecuado de Internet.

7 . METODOLOGÍA

Nuestro planteamiento metodológico estará orientado a favorecer en el alumnado la integración de contenidos científicos, tecnológicos y organizativos, la capacidad de aprendizaje y la capacidad para trabajar en equipo. Promoveremos en el alumnado, una visión global y coordinada de los procesos productivos en los que debe intervenir.

A lo largo del desarrollo de las unidades didácticas se alternarán las explicaciones teóricas de los contenidos conceptuales con la puesta en práctica de los mismos, realizando actividades en las que el alumno pueda analizar el avance que se ha producido respecto a sus ideas previas.

En la secuenciación de unidades didácticas se puede observar, cómo en algunas de ellas priman los contenidos teóricos sobre los prácticos, mientras que en otras ocurre lo contrario, sobre todo en la segunda mitad del módulo. En cualquier caso, siempre se buscará la alternancia de los mismos propiciando la construcción de aprendizajes significativos y la motivación del alumno, con el objetivo de que se interese profesionalmente en esta materia técnica.

En las exposiciones teóricas de los temas, utilizaremos un lenguaje sencillo a la vez que técnico, para que el alumno, futuro profesional, vaya conociendo la terminología y el argot que se utiliza en el campo de la administración de sistemas informáticos.

Las prácticas se plantearán en base al orden de ejecución de las tareas y de la exactitud, las verificaciones necesarias y respetando las normas básicas de seguridad.

El profesor propondrá un conjunto de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser resueltos por los alumnos, bien en horas de clase o bien en casa.

Algunos ejercicios prácticos se realizarán en los ordenadores utilizando el entorno de desarrollo adecuado a la Unidad de Trabajo en la que estemos trabajando. Las prácticas se resolverán de forma individual o en grupo, depende del número de alumnos que haya por cada ordenador, siendo aconsejable que no haya más de dos alumnos por cada equipo informático.

La intervención del profesor estará enmarcada en una concepción constructivista del aprendizaje, para lo cual:

- **a)** Partiremos de lo que el alumno ya sabe antes de proceder a programar. Ello facilitará el aprendizaje del alumno.

- **b)** Facilitaremos la construcción de aprendizajes significativos. La interacción profesor-alumno es esencial para que se produzcan estos aprendizajes.

- **c)** Tendremos en cuenta las peculiaridades de cada alumno y su ritmo de aprendizaje para adaptar los métodos y los recursos a las diferentes situaciones. En este sentido, utilizaremos una gran variedad de recursos y diferentes estrategias de aprendizaje para atender precisamente a esta heterogeneidad del grupo.

- **d)** Propiciaremos que el alumno sea un agente activo de su proceso de aprendizaje.

- **e)** Promoveremos la capacidad de “aprender a aprender” evitando la asimilación pasiva de los contendidos.

- **f)** La metodología seguida será flexible, motivadora y participativa.

- **g)** Se atenderá a los principios didácticos de “la investigación como eje de aprendizaje del alumno/a”.

- **h)** Facilitaremos todo tipo de interacciones, trabajo en grupo, individual, organización del espacio, del tiempo.

En el presente curso, debido a la situación socio-sanitaria y considerando Circular de 3 de septiembre de 2020, de la viceconsejería de educación y deporte, relativa a medidas de flexibilización curricular y organizativas para el curso escolar 2020/2021, de las opciones que en ella se indican, el centro ha adoptado por el modelo 6.c) indicada en el apartado quinto: Modelos para la organización curricular flexible para el alumnado que curse tercero y cuarto de ESO, Bachillerato, Formación Profesional Inicial y Enseñanzas de Régimen Especial

8. EVALUACIÓN

De acuerdo con 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, y tal y como aparece recogido en el Plan de Centro:

- La Evaluación del alumnado será realizada por el profesorado que imparta cada módulo profesional del ciclo formativo, de acuerdo con los resultados de aprendizaje, los criterios de evaluación y contenidos de cada módulo profesional, así como las competencias y objetivos generales del ciclo formativo asociados a los mismos.

- La Evaluación del aprendizaje del alumnado de las enseñanzas de formación profesional será continua y se realizará por módulos profesionales.

  Por Evaluación continua se entiende que el/la alumno/a será evaluado constantemente a lo largo de todo el curso escolar. Es decir, de manera continua en el tiempo, usando diferentes técnicas e instrumentos de evaluación, que se ajustarán a los criterios de evaluación del módulo.

- La aplicación del proceso de evaluación continua del alumnado requerirá, en la modalidad presencial, su asistencia regular a clase y su participación en las actividades programadas para los distintos módulos profesionales del ciclo formativo.

8.1. Criterios de Evaluación del Módulo asociados a cada Resultado de Aprendizaje.

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **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.

Ver **ANEXO I** con desglose de ponderación de cada uno de los resultados de aprendizajes y sus criterios de evaluación correspondientes.

8.2. Procedimientos de Evaluación

De acuerdo con 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, los procedimientos de evaluación quedan establecidos de la siguiente forma:

- **EVALUACIONES PARCIALES.**

Se realizarán 3 evaluaciones parciales en 1º curso y 2 en 2º correspondientes a cadauno de los trimestres del curso. Para tener aprobada cada evaluación parcial se tendrá en cuenta el grado de consecución de cada uno de los resultados de aprendizaje que se evalúen en dicho trimestre. No obstante, la nota del boletín será meramente informativa ya que no refleja la calificación de cada uno de los resultados de aprendizaje por separado. Por ello, puede darse el caso en que alguno de los resultados de aprendizaje desarrollados, total o parcialmente, durante el trimestre no esté conseguido, con lo que la nota que aparecerá en el boletín será inferior a 5.

La calificación informativa que se dará al alumnado en cada una de las evaluaciones parciales, corresponderá al resultado de la media, ponderada o no, de las calificaciones obtenidas en cada uno de los Resultados de Aprendizaje evaluados desde el inicio de curso hasta el momento de la evaluación parcial correspondiente.

- **EVALUACIÓN FINAL.**

Se realizará una evaluación final, en el mes de junio antes de que finalice el período lectivo, para que aquellos alumnos/as que no hayan conseguido todos los resultados de aprendizaje puedan hacerlo.

De acuerdo con la normativa, el alumnado que tenga módulos profesionales no alcanzados mediante evaluación parcial, tendrá obligación de asistir a clase y continuar con las actividades lectivas hasta la fecha de finalización de la evaluación final. A lo largo del periodo de evaluación final, será evaluado de los contenidos de todos los resultados de aprendizaje no conseguidos en el módulo. En el caso de que un resultado de aprendizaje no conseguido, incluya criterios de evaluación distribuidos en varias unidades didácticas, deberá ser evaluado de cada una de ellas.

Así mismo, el alumnado de primer curso, que desee mejorar los resultados obtenidos, tendrá obligación de asistir a clase y continuar con las actividades lectivas hasta la fecha de la evaluación final. Se evaluará de los contenidos de todos los resultados de aprendizaje que deben alcanzarse en el módulo.

8.3. Instrumentos de evaluación.

En las Actividades Evaluables que se propongan a lo largo del curso, podrán ser utilizados los siguientes instrumentos de evaluación por cada Resultado de Aprendizaje:

- Cuestionarios
- Mapas conceptuales o esquemas
- Tareas y Actividades desarrolladas dentro y fuera del aula
- Trabajos de Investigación
- Proyectos
- Pruebas escritas
- Pruebas prácticas
- Pruebas orales

8.4. Plan De Recuperación.

De forma extraordinaria, y por acuerdo del departamento, aquellos/as alumnos/as que no hayan conseguido superar algún resultado de aprendizaje tendrán una opción de recuperación del mismo a través de la realización de las actividades evaluables correspondientes. En el caso de que un resultado de aprendizaje no conseguido, incluya criterios de evaluación distribuidos en varias unidades didácticas, deberá ser evaluado de cada una de ellas.

Se realizará recuperación del primer y segundo trimestre en el caso de los grupos de 1º, y solo del primer trimestre en el caso de los grupos de 2º. Estas recuperaciones podrán llevarse a cabo antes de finalizar el trimestre correspondiente o al comienzo del siguiente, quedando a criterio del docente correspondiente.

En el caso de 2º al final del 2º trimestre se realizará una recuperación de los resultados no conseguidos en los dos trimestres para que el alumnado pueda superar el módulo y promocionar a FCT.

Aquellos/as alumnos/as que no hayan asistido a clase durante la realización de alguna actividad evaluable y que tras la aplicación de la media ponderada correspondiente de las calificaciones alcanzadas en los distintos criterios de evaluación que corresponden a un Resultado de Aprendizaje, la calificación obtenida en el mismo no sea positiva, es decir inferior a 5, tendrán opción a recuperar dicha actividad evaluable.

El profesorado decidirá en qué fecha se realizará dicha actividad, pudiendo ser a lo largo del trimestre, al final del mismo o en su caso, al comienzo del siguiente.

9. PROGRAMA DE REFUERZO PARA LA RECUPERACIÓN DE APRENDIZAJES NO ADQUIRIDOS

9.1. Metodología

Tal y como se indicó en el punto 7 de esta programación, la metodología que se utilizará durante el período de Refuerzo coincidirá con la aplicada a lo largo del curso para el desarrollo habitual de las clases, haciendo un mayor hincapié en trabajar las actividades evaluables.

9.2. Tipo de Actividades

En el **ANEXO II** se planifican las actividades 'tipo' de refuerzo de las competencias, que permitan al alumnado conseguir los resultados de aprendizajes no alcanzados.

9.3. Temporalización

Como establece 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, en el mes de junio se procederá a realizar la determinación y planificación de las actividades de refuerzo o mejora de las competencias, que permitan al alumnado matriculado en la modalidad presencial la superación de los módulos profesionales pendientes de evaluación positiva o, en su caso, mejorar la calificación obtenida en los mismos.

Dichas actividades se realizarán en primer curso durante el periodo comprendido entre la 2ª evaluación parcial y la evaluación final.

Durante este período, el número de sesiones dedicadas al refuerzo de los distintos resultados de aprendizajes que el alumnado debe alcanzar, se repartirá entre los distintos resultados de aprendizajes que no hayan sido adquiridos, destinando más sesiones a aquellos que tengan mayor dificultad.

9.4. Instrumentos de evaluación

En las Actividades Evaluables que se propongan a lo largo del curso, podrán ser utilizados los siguientes instrumentos de evaluación por cada Resultado de Aprendizaje:

- Cuestionarios
- Mapas conceptuales o esquemas
- Tareas y Actividades desarrolladas dentro y fuera del aula
- Trabajos de Investigación
- Proyectos
- Pruebas escritas
- Pruebas prácticas
- Pruebas orales

9.5. Criterios de Evaluación

Tal y como establece La **Orden de 19 de julio de 2010**, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red, los criterios de Evaluación serán los indicados en dicha norma y detallados en el punto 8.1 de esta programación, coincidiendo con los aplicados durante el desarrollo del curso.

10. PROGRAMA DE MEJORA DE CALIFICACIONES

10.1. Metodología

Tal y como se indicó en el punto 7 de esta programación, la metodología que se utilizará durante el período de Refuerzo coincidirá con la aplicada a lo largo del curso para el desarrollo habitual de las clases, haciendo un mayor hincapié en trabajar las actividades evaluables.

10.2. Tipo de Actividades

En el **ANEXO III** se planifican las actividades 'tipo' de mejora de las competencias, que permitan al alumnado mejorar sus calificaciones en los diferentes resultados de aprendizajes.

10.3. Temporalización

Como establece 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, en el mes de junio se procederá a realizar la determinación y planificación de las actividades de refuerzo o mejora de las competencias, que permitan al alumnado matriculado en la modalidad presencial la superación de los módulos profesionales pendientes de evaluación positiva o, en su caso, mejorar la calificación obtenida en los mismos.

Dichas actividades se realizarán en primer curso durante el periodo comprendido entre la 2ª evaluación parcial y la evaluación final.

Durante este período, el número de sesiones dedicadas al refuerzo de los distintos resultados de aprendizajes que el alumnado debe alcanzar, se repartirá entre los distintos resultados de aprendizajes, destinando más sesiones a aquellos que tengan un mayor peso en la calificación final del módulo (indicado en el Anexo I).

10.4. Instrumentos de evaluación

En las Actividades Evaluables que se propongan a lo largo del curso, podrán ser utilizados los siguientes instrumentos de evaluación por cada Resultado de Aprendizaje:

- Cuestionarios
- Mapas conceptuales o esquemas
- Tareas y Actividades desarrolladas dentro y fuera del aula
- Trabajos de Investigación
- Proyectos
- Pruebas escritas
- Pruebas prácticas
- Pruebas orales

10.5. Criterios de Evaluación

Tal y como establece La **Orden de 19 de julio de 2010**, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red, los criterios de Evaluación serán los indicados en dicha norma y detallados en el punto 8.1 de esta programación, coincidiendo con los aplicados durante el desarrollo del curso.

11. MEDIDAS DE ATENCIÓN A LA DIVERSIDAD

De acuerdo con 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, así como con lo establecido en el Proyecto de Centro, a la hora de elaborar las programaciones didácticas de los módulos se tendrá en cuenta la adecuación de las actividades formativas, así como de los criterios y los procedimientos de evaluación cuando el ciclo formativo vaya a ser cursado por alumnado con algún tipo de discapacidad, garantizándose el acceso a las pruebas de evaluación. Esta adaptación en ningún caso supondrá la supresión de resultados de aprendizaje y objetivos generales del ciclo que afecten a la adquisición de la competencia general del título.

La diversidad es un hecho inherente al desarrollo humano, a lo largo de esta programación intentaremos asegurar un equilibrio entre la necesaria adquisición de competencias profesionales del currículo y la innegable diversidad del alumnado.

Se distinguirán principalmente dos tipos de casos:

- Alumnos/as con diferentes niveles de conocimientos, intereses y motivaciones (Atención a la diversidad).

- Alumnos/as en los que se aprecian con dificultades físicas, materiales, de comunicación (ceguera, sordera…) (Adaptaciones de acceso)

Lógicamente todos los alumnos/as parten de conocimientos y destrezas distintas y por tanto la situación de partida es muy diferente para cada uno de ellos. Para mitigar estas diferencias se debe plantear un seguimiento individual de cada uno de los alumnos/as a través de los siguientes métodos, considerando que se debe atender a la diversidad en todos los sentidos, es decir, facilitar y favorecer el aprendizaje a los grupos “por abajo” y “por arriba”.

- Propuesta de actividades al final de cada unidad didáctica en las cuales se vaya incrementando el nivel de dificultad conforme se avance en ellas.

- Integración de los alumnos/as en grupos de trabajos mixtos y diversos en los cuales se fomentará la ayuda entre los integrantes del grupo y así los más rezagados se verán beneficiados por los que poseen un mayor nivel de conocimiento.

- Apoyo de los profesores cuando lo consideren necesario y en la forma que se estime.

- Facilitarle a los alumnos/as material complementario tales como libros, apuntes, ejercicios resueltos, revistas, artículos …

- Realización de actividades complementarias propuestas por los profesores.

- Realización de trabajos por parte de los alumnos/as fomentando la capacidad creativa.

- Exposición de algunos de los trabajos realizados por los grupos de trabajo.

11.1 Adaptaciones De Acceso

Las adaptaciones de acceso son modificaciones o provisión de recursos espaciales, materiales, personales o de comunicación que van a facilitar que algunos alumnos/as con necesidades educativas especiales puedan desarrollar el currículo ordinario. Tales como eliminación de barreras arquitectónicas, modificar los materiales o utilizar otros especiales, sonorización del aula, acondicionamiento de espacios, iluminación…

En este curso, tenemos un alumno con movilidad reducida, por lo que le proporcionaremos un lugar en la clase cómodo y de fácil accesibilidad procurando tener siempre el pasillo libre y amplio.

12 MATERIALES Y RECURSOS DIDÁCTICOS

12.1 Materiales

La mayoría de los apuntes serán elaborados por el profesor y colocados en la plataforma digital del departamento para que el alumnado pueda usarlos desde allí.

Al mismo tiempo, las actividades que se realicen en clase se entregarán al alumno en formato digital o quedarán expuestas en la pizarra para su seguimiento y desarrollo.

De todas formas y siempre que el profesor lo considere oportuno podrá citar alguna que otra referencia bibliográfica o dirección web mediante la cual se pueda complementar ciertos contenidos o aspectos del módulo.

12.2 Recursos Didácticos

- Puestos: ordenadores en red con los que los alumnos/as realizarán su trabajo.
- Red de comunicaciones y acceso a Internet.
- Impresora.
- Software de Sistemas Operativos: Windows y Linux.
-
- Software de Virtualización tipo KVM.
-
- Pizarra.
- Cañón de proyección.
- Apuntes de clase, recogidos por el alumnado y en los casos en que así se requiera, elaborados por el profesor.
- Plataforma Moodle.

13 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

13.1 Actividades Complementarias

- Feria del libro. Propuesta por el Departamento de Lengua para todo el alumnado del centro.
- Contra la violencia de género. Mes de noviembre. Todo el alumnado implicado.
- Día de la Constitución. 1ª semana de diciembre. Propuesta por del Departamento de Historia para todo el alumnado del centro.
- La paz y la no violencia. Finales de enero. Todo el alumnado implicado.

13.2 Actividades ExtraEscolares

- Visita a un Centro de Procesamiento de Datos.
- Visita al CICA de Sevilla.
- Viaje de fin de estudios.

14 PERSPECTIVA DE GÉNERO

La **Constitución Española** proclama en su **artículo 14** el principio de igualdad ante la Ley y en el **artículo 9.2**. establece que los poderes públicos promoverán las condiciones para que la libertad y la igualdad sean reales y efectivas, removerán los obstáculos que impidan o dificulten su plenitud y facilitarán la participación de la ciudadanía en la vida política, económica, cultural y social. A partir de aquí, se articularon las primeras políticas a favor de las mujeres, en la etapa de inicio de la democracia, y se ha inspirado la normativa que le ha ido dando desarrollo y concreción.

La **Comunidad Autónoma de Andalucía** asume en su **Estatuto de Autonomía** un fuerte compromiso con la igualdad de género, disponiendo en el **artículo 10.2** que «la Comunidad Autónoma propiciará la efectiva igualdad del hombre y de la mujer andaluces...» y en su **artículo 15** que «se garantiza la igualdad de oportunidades entre hombres y mujeres en todos los ámbitos».

El II Plan Estratégico de Igualdad de Género en Educación 2016-2021, que tendrá una vigencia de seis años, se concibe como el marco de actuación y la herramienta para continuar impulsando la igualdad dentro del sistema educativo.

Una de las líneas de actuación de este nuevo Plan de Igualdad de Género se centra en el **Plan de Centro de los Institutos**, de la siguiente manera: "Los órganos competentes en los centros docentes integrarán la perspectiva de género en la elaboración de las programaciones didácticas de los distintos niveles y materias, visibilizando la contribución de las mujeres al desarrollo de la cultura y las sociedades, poniendo en valor el trabajo que, histórica y tradicionalmente, han realizado, su ausencia en determinados ámbitos y la lucha por los derechos de ciudadanía de las mujeres".

Desde el presente módulo proponemos las siguientes actuaciones que incluyen la perspectiva de género :

En nuestro módulo proponemos las siguientes actuaciones que incluyen la perspectiva de género:

Por trimestre:

- Búsqueda de información en Internet y comentario de la misma, relativa a figuras femeninas y masculinas representativas de las unidades didácticas tratadas.
- Visualización de vídeos y películas con temática relativa a la figura de las mujeres en el mundo de las ciencias y las tecnologías.

15. ANEXO-I. PONDERACIÓN DE LOS CRITERIOS DE EVALUACIÓN Y DE LOS RESULTADOS DE APRENDIZAJE

METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

Se seguirá la **Metodología** descrita en el **Apartado 7** y los **Criterios de Evaluación** contemplados en el **Apartado 8**.

RAs	%/RA	CRITERIOS DE EVALUACIÓN	%/CEv
RA1. **Seguridad Pasiva.** Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. **UD1: Introducción a la Seguridad Pasiva-Física.** 1). Políticas de Seguridad para Credenciales de Acceso. Amenazas Credendicales Administrador. 2). Políticas de BACKUP. Restauración y Clonado de Sistemas. 3). Técnicas de intrusión a sistemas atacando la cuenta de administrador. 4). Optimizando el particionado del sistema para mejorar el rendimiento y la seguridad del mismo.	**15%**	**[b]. Se han descrito las diferencias entre seguridad física y lógica.**	**2%**
		[c]. Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	**2%**
		[d]. Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	**2%**
		[f]. Se han valorado las ventajas que supone la utilización de sistemas biométricos.	**2%**
		[h]. Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.	**2%**
		[a]. Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. Importancia de los BACKUPS/RESTAURACION en los distintos sistemas Linux y Windows. RESPALDO de Sistemas completos y su restauración en caso de incidente, incluyento el arranque y la gestión de sus particiones internas.	**25%**
		[e]. Se han adoptado políticas de contraseñas. Importancia de contar con contraseñas seguras. Suplantación de cuentas de Administración en Sistemas Windows y Linux.	**25%**
		[g]. Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. Respaldo de sistemas en Red mediante canales seguros SSH, tipo RSYNC.	**25%**
		[i]. Se han identificado las fases del análisis forense ante ataques a un sistema. Estudio y Análisis de un incidente de seguridad en sistemas Linux y Windows. Respaldo previo del entorno para evitar alteración del escenario y pruebas.	**25%**
RA2. **Seguridad Activa.** Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema. **UD2: Seguridad Activa-Lógica.** 1). Criptografía. Cifrado de Directorios/Archivos mediante Criptografía Simétrica y Asimétrica. Firma Digital. 2). Cifrado de Unidades. 3). Cifrado de Servicios mediante Certificados Digitales. 4). Seguridad en Redes Locales.	**15%**	**[a]. Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.**	**2%**
		[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.	**2%**
		[g]. Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	**2%**
		[h]. Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	**2%**
		[i]. Se han descrito los tipos y características de los sistemas de detección de intrusiones.	**2%**
		[c]. Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	**20%**

		[d]. Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	**10%**
		[e]. Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	**10%**
		[f]. Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. Instalación y Configuración de la infraestructura necesaria para la Emisión y Firmado de Certificados Digitales en la creación y configuración de Sitios Web HTTPS. Instalación y Configuración de Software para el cifrado de archivos como GPG. Instalación y Configuración de Software para el cifrado de particiones con LUKS.	**50%**
RA3. **SSH**. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad. **UD3: Servicio SSH** 1). Acceso SSH remoto. 2). Acceso SSH usando Túneles SSH. 3). Montaje remoto de Sistemas de Ficheros mediante SSHFS. 4). Redes VPN con OpenVPN, IPSEC(OpenSWAN).	**15%**	**[a]. Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.**	**2,5%**
		[b]. Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	**2,5%**
		[c]. Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.	**5%**
		[d]. Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.	**25%**
		[e]. Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	**25%**
		[f]. Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.	**20%**
		[g]. Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	**20%**
RA4. **FWs**. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna. **UD4: FireWalls[IPTABLES]** 1). Reglas de Filtrado. 2). Reglas de Ruteo. 3.) Reglas de Registro.	**15%**	**[a]. Se han descrito las características, tipos y funciones de los cortafuegos.**	**2,5%**
		[h]. Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	**2,5%**
		[c]. Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. Se conoce la definición de reglas de ruteo para limitar el acceso a redes externas.	**30%**
		[b]. Se han clasificado los niveles en los que se realiza el filtrado de tráfico. Se conoce los distintos tipos de reglas para limitar el tráfico.	**10%**
		[d]. Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. Se conoce la definición y uso correcto de reglas de filtrado para limitar el tráfico.	**20%**
		[e]. Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	**30%**
		[f]. Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	**2,5%**
		[g]. Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	**2,5%**
RA5. **PROXYs.** Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento	**15%**	**[a]. Se han identificado los tipos de proxy, sus características y funciones principales.**	**2,5%**
		[i]. Se ha elaborado documentación relativa a la instalación,	**2,5%**

seguro del servicio. **UD5: Proxys[SQUID]** 1). Filtrado a nivel de red. 2). Filtrado a nivel de contenido.		**configuración y uso de servidores proxy.**	
		[c]. Se han configurado los métodos de autenticación en el proxy.	**5%**
		[d]. Se ha configurado un proxy en modo transparente.	**15%**
		[e]. Se ha utilizado el servidor proxy para establecer restricciones de acceso web.	**15%**
		[f]. Se han solucionado problemas de acceso desde los clientes al proxy.	**15%**
		[g]. Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.	**15%**
		[h]. Se ha configurado un servidor proxy en modo inverso.	**15%**
		[b]. Se ha instalado y configurado un servidor proxy-cache.	**15%**
RA6. **Alta Disponibilidad.** Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba. **UD6: Virtualización y Alta Disponibilidad con Proxmox:** 1) MVs/CTs en Proxmox. 2) Redes en Proxmox. 3) Montaje de Clusters para Servicios de Alta Disponibilidad con Proxmox. 4) Sistemas de Almacenamiento en Cluster(GlusterFS y CephFS). 5)Réplicas en Proxmox. 6) Migraciones en Proxmox.	**15%**	**[a]. Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.**	**2%**
		[b]. Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	**2%**
		[c]. Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	**2%**
		[i]. Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	**2%**
		[h]. Se han analizado soluciones de futuro para un sistema con demanda creciente.	**2%**
		[d]. Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	**30%**
		[e]. Se ha implantado un balanceador de carga a la entrada de la red interna.	**20%**
		[f]. Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	**20%**
		[g]. Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema.	**20%**
RA7. **Legislación y Normativa.** Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia. **UD7: Legislación y Normativa sobre Seguridad Informática.** 1). Estudio e Interpretación de la Ley LOPDGDD respecto al RGPD.	**10%**	**[a]. Se ha descrito la legislación sobre protección de datos de carácter personal.**	**10%**
		[b]. Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	**15%**
		[c]. Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	**15%**
		[d]. Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	**15%**
		[e]. Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	**15%**
		[f]. Se han contrastado las normas sobre gestión de seguridad de la información.	**15%**
		[g]. Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	**15%**

16. ANEXO II: PROGRAMA DE REFUERZO DEL MÓDULO "SEGURIDAD Y ALTA DISPONIBILIDAD"

METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

Se seguirá la **Metodología** descrita en el **Apartado 7** y los **Criterios de Evaluación** contemplados en el **Apartado 8**.

RAs	%RA	UD	ACTIVIDADES DE APRENDIZAJE	Crit. Eval.
RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	**20%**	**UD1 [100%]**	**Actividad Tipo1:** Backups/Restauración locales de Sistemas con Clonezilla en Sistemas **Linux(Ubuntu/Debian) y Windows-2012.**	**a, b, c**
			Actividad Tipo2: Backups/Restauración con Rsync en Sistemas **Linux(Ubuntu/Debian) y Windows-2012.**	**a, b, c**
			Actividad Tipo3: Backups/Restauración en red con Clonezilla en Sistemas **Linux(Ubuntu/Debian) y Windows-2012.**	**a, b, c**
			Actividad Tipo4: Backups/Restauración con Rsync en Sistemas **Linux(Ubuntu/Debian) y Windows-2012.**	**a, b, c**
			Actividad Tipo5: Instalación/Recuperación de BOOT y BOOTLOADERs en Sistemas **Linux(Ubuntu/Debian) y Windows-2012.**	**a, b, c**
			Actividad Tipo6: Ataques contra la cuenta de administración en sistemas **Linux(Ubuntu/Debian)**.	**a, b, c**
			Actividad Tipo7: Ataques contra la cuenta de administración en sistemas **Windows-2012**.	**a, b, c**
RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	**20%**	**UD2 [100%]**	**Actividad Tipo1:** Creación de Entidad Certificadora en Sistemas **Linux(Ubuntu/Debian)**	**f, g**
			Actividad Tipo2: Creación de Entidad Certificados Digitales en Sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo3: Configuración de Servicios HTTPS en Sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo5: Cifrado de ficheros con GPG en Sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo6: Cifrado y firmado de ficheros con GPG en sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo7: Cifrado de Unidades y Directorios con ENCFS en sistemas **Linux(Ubuntu/Debian).**	**f, g**
RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	**15%**	**UD2 [100%]**	**Actividad Tipo1:** Creación de Entidad Certificadora en sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo2: Creación de Entidad Certificados Digitales en sistemas **Linux(Ubuntu/Debian).**	**f, g**
			Actividad Tipo3: Configuración de Servicios HTTPS en sistemas **Linux(Ubuntu/Debian).**	**f, g**
RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	**20%**	**UD3 [100%]**	**Actividad Tipo1:** Configuración y creación de Reglas de Filtrado de tráfico en sistemas **Linux(Ubuntu/Debian).**	**b, d, g**
			Actividad Tipo2: Configuración y creación de Reglas de Ruteo de tráfico en sistemas **Linux(Ubuntu/Debian).**	**c**
			Actividad Tipo3: Configuración y creación de Reglas de Registro en sistemas **Linux(Ubuntu/Debian).**	**e**

RA5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	**10%**	**UD6 [100%]**	**Actividad Tipo1:** Configuración y creación de Reglas de Filtrado a nivel de puertos en sistemas **Linux(Ubuntu/Debian).**	**d, e, f**
			Actividad Tipo2: Configuración y creación de Reglas de Filtrado a nivel de contenido web en sistemas **Linux(Ubuntu/Debian).**	**d, e, f**
			Actividad Tipo3: Monitorización del Proxy en sistemas **Linux(Ubuntu/Debian).**	**g**
RA6. Implanta soluciones de alta disponibilidad empleando técnicas devirtualización y configurando los entornos de prueba.	**10%**	**UD5 [100%]**	**Actividad Tipo1:** Creación de un Cluster de Alta disponibilidad en servicio Web en sistemas **Linux(Ubuntu/Debian).**	**b, c, d, g**
			Actividad Tipo2: Creación de un Cluster de Alta disponibilidad para almacenamiento compartido en sistemas **Linux(Ubuntu/Debian).**	**b, c, f, g**
			Actividad Tipo3: Creación de un Balanceador de Carga en sistemas **Linux(Ubuntu/Debian).**	**e**
RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	**5%**	**UD1 [50%]**	**Actividad Tipo1:** Conocimiento y estudio de la Ley de Protección de datos.	**a, d**
		UD2 [50%]	**Actividad Tipo1:** Creación de un Cluster de Alta disponibilidad en servicio Web en sistemas **Linux(Ubuntu/Debian).**	**a, d**

17. ANEXO-III: PROGRAMA DE MEJORA.

METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

Se realizarán todas las actividades del plan de refuerzo en Servidores **CentOS** y **Windows2016**.

Se seguirá la **Metodología** descrita en el **Apartado 7** y los **Criterios de Evaluación** contemplados en el **Apartado 8**.

RAs	%RA	UD	ACTIVIDADES DE APRENDIZAJE	Crit. Eval.
RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	**15%**	**UD1 [100%]**	**Actividad Tipo1:** Backups/Restauración locales de Sistemas con Clonezilla en Sistemas **Linux(CentOS) y Windows-2016.**	**a, b, c**
			Actividad Tipo2: Backups/Restauración con Rsync en Sistemas **Linux(CentOS) y Windows-2016. .**	**a, b, c**
			Actividad Tipo3: Backups/Restauración en red con Clonezilla en Sistemas **Linux(CentOS) y Windows-2016.**	**a, b, c**
			Actividad Tipo4: Backups/Restauración con Rsync en Sistemas **Linux(CentOS) y Windows-2016.**	**a, b, c**
			Actividad Tipo5: Instalación/Recuperación de BOOT y BOOTLOADERs en Sistemas **Linux(CentOS) y Windows-2016.**	**a, b, c**
			Actividad Tipo6: Ataques contra la cuenta de administración en sistemas **Linux(CentOS).**	**a, b, c**
			Actividad Tipo7: Ataques contra la cuenta de administración en sistemas **Windows-2016.**	**a, b, c**
RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	**15%**	**UD2 [100%]**	**Actividad Tipo1:** Creación de Entidad Certificadora en Sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo2: Creación de Entidad Certificados Digitales en Sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo3: Configuración de Servicios HTTPS en Sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo5: Cifrado de ficheros con GPG en Sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo6: Cifrado y firmado de ficheros con GPG en sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo7: Cifrado de Unidades y Directorios con ENCFS en sistemas **Linux(CentOS).**	**f, g**
RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	**15%**	**UD2 [100%]**	**Actividad Tipo1:** Creación de Entidad Certificadora en sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo2: Creación de Entidad Certificados Digitales en sistemas **Linux(CentOS).**	**f, g**
			Actividad Tipo3: Configuración de Servicios HTTPS en sistemas **Linux(CentOS).**	**f, g**
RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	**15%**	**UD3 [100%]**	**Actividad Tipo1:** Configuración y creación de Reglas de Filtrado de tráfico en sistemas **Linux(CentOS).**	**b, d, g**
			Actividad Tipo2: Configuración y creación de Reglas de Ruteo de tráfico en sistemas **Linux(CentOS).**	**c**
			Actividad Tipo3: Configuración y creación de Reglas de Registro en sistemas **Linux(CentOS).**	**e**

RA5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	**15%**	**UD6 [100%]**	**Actividad Tipo1:** Configuración y creación de Reglas de Filtrado a nivel de puertos en sistemas **Linux(CentOS).**	**d, e, f**
			Actividad Tipo2: Configuración y creación de Reglas de Filtrado a nivel de contenido web en sistemas **Linux(CentOS).**	**d, e, f**
			Actividad Tipo3: Monitorización del Proxy en sistemas **Linux(CentOS).**	**g**
RA6. Implanta soluciones de alta disponibilidad empleando técnicas devirtualización y configurando los entornos de prueba.	**15%**	**UD5 [100%]**	**Actividad Tipo1:** Creación de un Cluster de Alta disponibilidad en servicio Web en sistemas **Linux(CentOS).**	**b, c, d, g**
			Actividad Tipo2: Creación de un Cluster de Alta disponibilidad para almacenamiento compartido en sistemas **Linux(CentOS).**	**b, c, f, g**
			Actividad Tipo3: Creación de un Balanceador de Carga en sistemas **Linux(CentOS).**	**e**
RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	**10%**	**UD1 [50%]**	**Actividad Tipo1:** Conocimiento y estudio de la Ley de Protección de datos.	**a, d**
		UD2 [50%]	**Actividad Tipo1:** Creación de un Cluster de Alta disponibilidad en servicio Web en sistemas **Linux(CentOS).**	**a, d**