JUNTA DE ANDALUCIA

CONSEJERIA DE EDUCACION
IES Gonzalo Nazareno

Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red

Programación del módulo profesional de Seguridad y Alta Disponibilidad

Curso 2018/2019

Profesor: José Rafael Luque Giráldez

Índice

1 Introducción....3
2 Actividades de exploración inicial....5
3 Objetivos....6
4 Contenidos y secuenciación temporal....7
4.1 Secuenciación temporal....9
4.2 Desarrollo de las unidades....10
5 Metodología....20
6 Materiales y recursos didácticos....21
7 Evaluación....22
7.1 Criterios de evaluación....22

1 Introducción

En este documento se presenta la programación didáctica para el módulo profesional Seguridad Informática, y se basa en la siguiente legislación:

- REAL DECRETO 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas 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 en Red (BOJA Nº 168 de 27 de agosto de 2010).

Este módulo profesional se imparte durante el segundo curso y tiene asignadas un total de 88 horas, a razón de 4 horas semanales.

Esta programación didáctica está compuesta de dos partes: este documento y el curso virtual de la plataforma educativa del departamento de informática del IES Gonzalo Nazareno, accesible en la dirección:

http://dit.gonzalonazareno.org/moodle/course/view.php?id=18

Este documento no incluye las actividades a desarrollar en cada una de las unidades didácticas, ya que éstas se encuentran en la plataforma educativa que es un medio mucho más eficaz para mantenerlas actualizadas.

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

a) Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos, interpretando la documentación técnica asociada y organizando los recursos necesarios.
c) Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
i) Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información.
j) Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
l) Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
n) Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
o) Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.
p) Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
t) Gestionar su carrera profesional, analizando las oportunidades de empleo,

autoempleo y aprendizaje.

Las líneas de actuación en el proceso enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

– La protección de equipos y redes informáticas.
– La protección de la información transmitida y almacenada.
– La legislación y normativa vigente en materia de seguridad.

2 Actividades de exploración inicial

El desarrollo de la evaluación inicial tendrá lugar durante las primeras horas del módulo. Como herramienta se utilizará el siguiente cuestionario escrito, que servirá para recabar información personal y relevante sobre el alumno, y para determinar los conocimientos previos desde los que el alumno parte.

1. ¿Tienes ordenador en casa?

2. ¿Es tuyo?

3. ¿Tienes más de un ordenador?

4. ¿Tienes acceso a Internet? ¿De qué tipo?

5. Explica qué significa para ti el concepto de Seguridad Informática.

6. ¿Qué es un hacker?

7. ¿Sabes qué es la criptografía? Pon un ejemplo de uso.

8. Explica a continuación para qué sirven los siguientes dispositivos:

    Cortafuegos

    Servidor VPN

    Lector DNIe

    SAI

9. ¿Has realizado alguna vez una copia de seguridad? ¿Con qué sistema o herramientas?

10. ¿Qué es un sistema biométrico?

11. ¿Qué son los metadatos de un fichero?

12. ¿Qué es el malware?

13. Marca con un círculo las siguientes técnicas que conozcas y sepas para qué se utilizan: spoofing, sniffing, hijacking, man in the middle

3 Objetivos

Los objetivos generales de este módulo para el curso 2016/2017 son los siguientes:

1. Aplicar medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
2. Gestionar dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.
3. Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
4. Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico.
5. Reconocer la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

4 Contenidos y secuenciación temporal

A continuación se presenta un relación secuenciada de los contenidos de este módulo:

1. **Introducción**
    1. Importancia de la seguridad informática.
    2. Definición de seguridad informática.
    3. Objetivos de la seguridad informática.
    4. Clasificaciones de las medidas de seguridad.
2. **Aspectos Éticos y Legales.**
    1. Código Penal.
    2. LOPD.
    3. LSSI/CE.
    4. Ética del administrador de sistemas.
3. **Implantación de una Política de Seguridad.**
    1. Identificación de activos.
    2. Tipos de ataques y atacantes.
    3. Análisis de riesgos.
    4. Planes de seguridad.
    5. Planes de contingencia.
4. **Monitorización de sistemas y redes**
    1. Introducción a la monitorización.
    2. Monitorización de sistemas y redes con Nagios.
5. **Contramedidas**
    1. Herramientas de Seguridad.
        1. Escáner de vulnerabilidades.
        2. Sistemas de detección de intrusos.
        3. Herramientas de fortaleza de contraseñas.
        4. Herramientas de control de la integridad de ficheros.
    2. Medidas de prevención. Hardening de servidores Linux.
    3. Medidas de detección.
    4. Medidas de recuperación.
6. **Técnicas criptográficas**
    1. Criptografía simétrica
    2. Criptografía asimétrica
    3. Funciones Hash
    4. SSL
    5. Firma digital
7. **Sistemas de cortafuegos**
    1. Tipos de cortafuegos. Características. Funciones principales.
    2. Instalación de cortafuegos. Ubicación.
    3. DMZ
    4. Reglas de filtrado de cortafuegos.
    5. Pruebas de funcionamiento. Sondeo.
    6. Registros de sucesos de cortafuegos.
8. **Redes Privadas Virtuales**
    1. Beneficios y desventajas con respecto a las líneas dedicadas.
    2. VPN a nivel de red. SSL, IPSec.

3. Protocolos de autenticación.
4. Configuración de parámetros de acceso.
5. Servidores de autenticación.

9. Alta Disponibilidad y Sistemas Redundantes

1. Análisis de configuraciones de alta disponibilidad.
2. Funcionamiento ininterrumpido.
3. Integridad de datos y recuperación de servicio.
4. Servidores redundantes.
5. Sistemas de clusters.
6. Balanceadores de carga.
7. Instalación y configuración de soluciones de alta disponibilidad.

4.1 Secuenciación temporal

A continuación se presenta una tabla con la temporalización que se seguirá durante el curso:

Unidad	N.º Horas	Primer Trimestre	Segundo Trimestre
1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA	4	X	
2. ASPECTOS ÉTICOS Y LEGALES	6	X	
3. IMPLANTACIÓN DE UNA POLÍTICA DE SEGURIDAD	8	X	
4. MONITORIZACIÓN DE SISTEMAS Y REDES	8	X	
5. CONTRAMEDIDAS	12	X	
6. TÉCNICAS CRIPTOGRÁFICAS	18	X	X
7. SISTEMAS DE CORTAFUEGOS.	12		X
8. VPN	10		X
9. ALTA DISPONIBILIDAD Y SISTEMAS REDUNDANTES	10		X

4.2 Desarrollo de las unidades

UNIDAD DIDÁCTICA Nº: 1 Introducción a la Seguridad Informática	
Duración: 4 h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.
• Conocer los conceptos básicos de la seguridad informática: fiabilidad, confidencialidad, integridad, disponibilidad, autenticación y no repudio. • Conocer distintos métodos de seguridad. • Clasificar los métodos de seguridad: activos, pasivos y físicos, lógicos.
B. CONTENIDOS.
Conceptuales y procedimentales
• Objetivos de la seguridad: Fiabilidad, confidencialidad, integridad, disponibilidad, autenticación y no repudio. • Clasificación de los métodos de seguridad: activos / pasivos, físicos / lógicos • Métodos de seguridad
Actitudinales.
• Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos. • Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad. • Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.
C. CRITERIOS E INSTRUMENTOS 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, activos y pasivos. c. Se conocen distintos métodos para conseguir sistemas seguros. d. Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.

UNIDAD DIDÁCTICA Nº: 2 Aspectos éticos y legales	
Duración: 6h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Conocer la legislación sobre protección de datos de carácter personal.
- Determinar la necesidad de controlar el acceso a la información personal almacenada.
- Identificar las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Contrastar el deber de poner a disposición de las personas los datos personales que les conciernen.
- Conocer la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Contrastar las normas sobre gestión de seguridad de la información.
- Comprender la necesidad de conocer y respetar la normativa legal aplicable.

B. CONTENIDOS.

Conceptuales y procedimentales

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

Actitudinales.

- Valorar la importancia de conocer la legislación sobre protección de datos de carácter personal.
- Respetar la normativa legal aplicable descrita en la unidad.
- Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad.
- Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.

C. CRITERIOS E INSTRUMENTOS 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.

UNIDAD DIDÁCTICA Nº: 3 Implantación de una Política de Seguridad	
Duración: 8h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Reconocer los elementos vulnerables en un sistema informático.

- Analizar las vulnerabilidades de un sistema informático.
- Identificar las amenazas y sus tipos.
- Identificar y realizar los distintos tipos de ataques informáticos
- Identificar los distintos tipos de malware
- Valorar la probabilidad y el impacto de cada una de las amenazas que sufren los activos de la empresa.
- Conocer las medidas que pueden tomarse para hacer frente a las amenazas más comunes.
- Redactar un plan de seguridad que incluya el conjunto de reglas que debe seguir el personal de una empresa para minimizar los riesgos de un ataque.
- Redactar planes de contingencia para minimizar el impacto de las consecuencias de un ataque informático.

B. CONTENIDOS.

Conceptuales y procedimentales

- Elementos vulnerables en el sistema informático. Hardware, software y datos.
- Análisis de las principales vulnerabilidades de un sistema informático.
- Amenazas. Tipos. Amenazas físicas y lógicas.
- Ataques en sistemas personales.
- Clasificación de las amenazas y los ataques.
- Técnicas de análisis de riesgos.
- Planes de Seguridad.
- Planes de Contingencia.

Actitudinales.

- Valorar la importancia de identificar los activos a proteger dentro de la empresa.
- Valorar la necesidad de tener un plan de seguridad en la empresa.
- Valorar la importancia de elaborar planes de contingencia para recuperarse de los ataques.
- Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad.
- Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.

C. CRITERIOS E INSTRUMENTOS 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 clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
c) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
d) Se han adoptado políticas de contraseñas.
e) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
f) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
g) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
h) Se han identificado la anatomía de los ataques más habituales.
i) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.

UNIDAD DIDÁCTICA Nº: 4 Monitorización de sistemas y redes

Duración: 8 h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Conocer soluciones de monitorización de sistemas y redes.
- Instalar y configurar un sistema de monitorización con Nagios
- Instalar y configurar un sistema de monitorización con Pandora

B. CONTENIDOS.

Conceptuales y procedimentales
• Introducción a la monitorización • Monitorización de sistemas y redes con Nagios. • Monitorización de sistemas y redes con Pandora.
Actitudinales.
• Valorar la importancia de la monitorización de sistemas y redes. • Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos. • Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad. • Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.
C. CRITERIOS E INSTRUMENTOS DE EVALUACIÓN.
a. Se ha instalado y configurado un sistema de monitorización con Nagios. b. Se ha instalado y configurado un sistema de monitorización con Pandora.

UNIDAD DIDÁCTICA Nº: 5 Contramedidas	
Duración: 12h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Conocer las vulnerabilidades de los sistemas y redes.
- Instalar, configurar y utilizar la información recogida por una herramienta de escaneo de vulnerabilidades.
- Instalar, configurar y utilizar la información recogida por un sistema de detección de intrusos.
- Instalar, configurar y utilizar la información recogida por una herramienta de verificación de la integridad de los ficheros del sistema.
- Instalar, configurar y utilizar la información recogida por una herramienta de comprobación de la fortaleza de las contraseñas.
- Conocer las herramientas de prevención, detección y recuperación frente a ataques informáticos.
- Conocer los mecanismos conducentes al aseguramiento de servidores Linux.

B. CONTENIDOS.

Conceptuales y procedimentales

- Herramientas de Seguridad.
  - Escáner de vulnerabilidades.
  - Sistemas de detección de intrusos.
  - Herramientas de fortaleza de contraseñas.
  - Herramientas de control de la integridad de ficheros.
- Medidas de prevención. Hardening de servidores Linux.
- Medidas de detección.
- Medidas de recuperación.

Actitudinales.

- Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos.
- Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad.
- Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.

C. CRITERIOS E INSTRUMENTOS DE EVALUACIÓN.

a. Se han aplicado políticas correctas de control de acceso lógico.
b. Se han verificado las políticas de usuarios y grupos.
c. Se han definido aspectos importantes para auditar los sistemas informáticos.
d. Se han tomado las medidas oportunas para la protección frente a los distintos tipos de malware
e. Se han tomado las medidas oportunas para la desinfección de los distintos malware.
f. Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
g. Se han descrito los tipos y características de los sistemas de detección de intrusiones.
h. Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización de las aplicaciones y del sistema operativo.

UNIDAD DIDÁCTICA Nº: 6 Técnicas criptográficas	
Duración: 12h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.
• Comprender los conceptos básicos de la criptografía • Distinguir los distintos métodos criptográficos. • Comprobar la integridad de los archivos utilizando funciones de dispersión. • Utilizar técnicas criptográficas para la autentificación y establecimiento de comunicaciones seguras.
B. CONTENIDOS.
Conceptuales y procedimentales

• Criptografía:
  • Conceptos básicos de criptografía.
  • Tipos: simétrica, asimétrica e híbrida.
  • Integridad. Funciones de dispersión.
  • Firma digital.
  • Autoridades de certificación.
  • Certificados digitales.
  • SSL

Actitudinales.
• Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos. • Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad. • Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.
C. CRITERIOS E INSTRUMENTOS DE EVALUACIÓN.
i. Se ha reconocido la necesidad de utilizar la criptografía en el ámbito de la seguridad informática. j. Se han valorado las distintas técnicas de encriptación: simétrica y asimétrica, conociendo sus ventajas e inconvenientes. k. Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información, así como en la comprobación de la integridad de la información (funciones de dispersión). l. Se ha aplicado el proceso de firma digital a documentos, así como la comprobación de la autenticidad de los mismos. m. Se ha reconocido la importancia del uso de certificados digitales, de la existencia de autoridades de certificación y del uso de SSL para las comunicaciones seguras.

UNIDAD DIDÁCTICA Nº: 7 Sistemas cortafuegos	
Duración: 12 h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.
• Instalación y configuración de cortafuegos. • Decidir la mejor ubicación de los cortafuegos. • Establecer reglas de filtrado seguras y acordes a la situación particular de la red a proteger. • Registrar y analizar los sucesos de cortafuegos.
B. CONTENIDOS.
Conceptuales y procedimentales
• Utilización de cortafuegos. • Filtrado de paquetes de datos. • Tipos de cortafuegos. Características. Funciones principales. • Instalación de cortafuegos. Ubicación. • Reglas de filtrado de cortafuegos. • Pruebas de funcionamiento. Sondeo. • Registros de sucesos de cortafuegos.
Actitudinales.
• Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos. • Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad. • Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.
C. CRITERIOS E INSTRUMENTOS DE EVALUACIÓN.
c. Se han descrito las características, tipos y funciones de los cortafuegos. d. Se han clasificado los niveles en los que se realiza el filtrado de tráfico. e. Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. f. Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. g. Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. h. Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. i. Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. j. Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

UNIDAD DIDÁCTICA Nº: 8 Redes privadas virtuales	
Duración: 10h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Describir escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
- Clasificar las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
- Identificar los protocolos seguros de comunicación y sus ámbitos de utilización.
- Configurar redes privadas virtuales mediante protocolos seguros a distintos niveles.
- Implantar un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
- Identificar y configurar los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
- Instalar, configurar e integrar en la pasarela un servidor remoto de autenticación.

B. CONTENIDOS.

Conceptuales y procedimentales

- 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.

Actitudinales.

- Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos.
- Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad.
- Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.

C. CRITERIOS E INSTRUMENTOS 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.

UNIDAD DIDÁCTICA Nº: 9 Alta disponibilidad y sistemas redundantes	
Duración: 10h	**Bloque Temático:**

A. OBJETIVOS. Capacidades Terminales.

- Analizar supuestos y situaciones en las que se hace necesario implementar soluciones de alta

disponibilidad.

- Identificar soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
- Evaluar las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
- Implantar un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
- Implantar un balanceador de carga a la entrada de la red interna.
- Implantar sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
- Evaluar la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema.
- Analizar soluciones de futuro para un sistema con demanda creciente.
- Esquematizar y documentar soluciones para diferentes supuestos con necesidades de alta disponibilidad.

B. CONTENIDOS.

Conceptuales y procedimentales

- 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.

Actitudinales.

- Grado de motivación al realizar las prácticas, que conducen a verificar los conocimientos teóricos.
- Interés en conseguir nuevas aptitudes, mediante las destrezas que propone esta unidad.
- Grado de autonomía en la resolución de dudas, valorando positivamente una investigación previa por parte del alumnado en busca de las resoluciones.

C. CRITERIOS E INSTRUMENTOS 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.
j. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

5 Metodología

Las unidades didácticas seguirán, en su mayor parte, la siguiente secuencia de actividades didácticas:

1) Actividad de introducción-motivación. Se trata de una exposición a modo de introducción de los contenidos básicos que se van a desarrollar. Ésta incluirá una justificación de la necesidad de impartir dichos contenidos y los objetivos que se pretenden alcanzar a la conclusión de la unidad didáctica y, de forma general, cómo contribuyen estos en la obtención de las capacidades terminales de un Técnico en Administración de Sistemas Informáticos.

2) Determinación de los conocimientos previos de los alumnos sobre la materia a impartir. Se trata de conocer las ideas, las opiniones, los aciertos o los errores conceptuales de los alumnos sobre los contenidos a desarrollar. Esta actividad se llevará a cabo principalmente mediante charla o coloquio con los alumnos y, en ocasiones, mediante prueba escrita informal.

3) Desarrollo de contenidos. Con esta actividad se trata de dar a conocer los conceptos, los procedimientos o las actitudes nuevas, propias de la unidad didáctica que se va a desarrollar. El profesor expondrá los contenidos fomentando, en la medida de lo posible, la participación del alumnado mediante la formulación de cuestiones teóricas o ejercicios prácticos, relativos a dichos contenidos, que den lugar a una secuenciación lógica y significativa de la exposición en la que el alumno participe activamente. Cuando los contenidos sean eminentemente prácticos y desarrollados sobre el ordenador, el profesor guiará al alumno durante el desarrollo de éstos, fomentando nuevamente la iniciativa de éste en la construcción de su aprendizaje y haciendo hincapié en la relación existente entre los contenidos teóricos y prácticos.

4) Planteamiento de problemas o ejercicios prácticos a modo actividades de consolidación en las cuales se contrastan las nuevas ideas con las ideas previas de los alumnos y se aplican los nuevos aprendizajes.

5) Actividades de refuerzo para aquellos alumnos con necesidades educativas especiales.

6) Actividades de recuperación para aquellos alumnos que no han adquirido los conocimientos mínimos de la unidad didáctica.

7) Actividades de ampliación de conocimientos. Consistente en el desarrollo, por parte de los alumnos, de trabajos de investigación guiados por el profesor.

6 Materiales y recursos didácticos

Los Materiales y recursos didácticos a utilizar son los siguientes:

- Dos pizarras blancas para rotuladores.
- Equipamiento informático: Red Gigabit Ethernet de 15 ordenadores x86_64 con 2 GiB de RAM.
- Acceso a Internet de banda ancha a través de ADSL
- Un vídeo-proyector (cañón) y una pantalla de 2x2 metros para proyectar la salida RGB de un PC.
- Curso en la plataforma educativa moodle: http://informatica.gonzalonazareno.org/plataforma/course/view.php?id=43
- Software
  - Sistema Operativo Debian GNU/Linux (squeeze)
  - Sistema Operativo Ms. Windows Server 2008.
  - Sistema Operativo Ms. Windows 7.
  - Aplicaciones incluidas en los repositorios de las distribuciones utilizadas.
- Documentación
  - Apuntes elaborados por el profesor.
  - Presentaciones elaboradas por el profesor.
  - Documentación elaborada de forma colaborativa por el alumnado.
  - Documentación publicada en los sitios web de los fabricantes de los dispositivos utilizados.
  - Consultas a la comunidad de usuarios: listas de correo, foros, etc.
  - Tutoriales, libros electrónicos, cursos y cualquier tipo de recurso educativo útil de Internet.

7 Evaluación

Las calificaciones del módulo están sujetas a 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. (Boja 202, de 15 de octubre de 2010).

Debido a que el contenido organizador debe ser de tipo procedimental, se empleará una metodología basada en la realización de prácticas o pequeños proyectos. Siempre que sea posible, se emplearán técnicas de aprendizaje cooperativo, definiendo equipos de trabajo compensados.

Dentro de los citados equipos de trabajo, se definirán para cada práctica o proyecto responsabilidades individuales y grupales. Además, se establecerán los roles a desempeñar por cada alumno y las funciones asociadas a los mismos.

De esta forma, se evaluará el trabajo del alumno en los siguientes aspectos:

- responsabilidades individuales en la realización de las prácticas o proyectos de aprendizaje cooperativo
- desempeño de las funciones asociadas al rol asignado
- responsabilidad grupal en la realización de las prácticas o proyectos de aprendizaje cooperativo
- prácticas o proyectos realizados individualmente.

La calificación de cada evaluación se obtendrá realizando la media ponderada de todas las prácticas y proyectos llevados a cabo durante el curso.

Se realizarán uno o varios trabajos prácticos en cada evaluación, correspondientes a las actividades previstas en cada unidad didáctica. Algunos de ellos deberán ser realizados durante el horario lectivo, otros, de mayor extensión, fuera del horario de clases. Será necesario entregar más de un 75% de las prácticas evaluables para superar el módulo.

Se habilitará una fecha de entrega de prácticas durante el periodo de recuperación.

7.1 Criterios de evaluación

A continuación se detallan los resultados del aprendizaje y los criterios de evaluación.

1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
Criterios de evaluación:

a) Se ha valorado la importancia de mantener la información segura.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han definido las características de la ubicación física y condiciones

ambientales de los equipos y servidores.
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
h) Se ha valorado la importancia de establecer una política de contraseñas.
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.
Criterios de evaluación:
a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.
e) Se han seleccionado estrategias para la realización de copias de seguridad.
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
g) Se han realizado copias de seguridad con distintas estrategias.
h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
i) Se han utilizado medios de almacenamiento remotos y extraíbles.
j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
Criterios de evaluación:
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
b) Se han clasificado los principales tipos de software malicioso.
c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.
f) Se han aplicado técnicas de recuperación de datos.

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico.
Criterios de evaluación:
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.

c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.
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 la obligación 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.