IES PADRE POVEDA

DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo:

SEGURIDAD Y ALTA DISPONIBILIDAD

Familia profesional:

INFORMÁTICA

Ciclo Formativo de Grado Superior:

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS

Profesor/a: Arcadio Ortega Reinoso

Curso: 2022/23

ÍNDICE

1. Objetivos

La formación del módulo contribuye a alcanzar los objetivos generales de este ciclo formativo que se relacionan a continuación:

j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para implementar 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.
o) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.
p) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para mantener el espíritu de innovación.

2. Resultados de aprendizaje y criterios de evaluación

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
Criterios de evaluación:
a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
e) Se han adoptado políticas de contraseñas.
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.

i) Se han identificado las fases del análisis forense ante ataques a un sistema.

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

Criterios de evaluación:

a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático

b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.

c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.

d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.

e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.

f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.

g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.

h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.

i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

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

Criterios de evaluación:

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

b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.

c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.

e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.

f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.

g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

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

Criterios de evaluación:

a) Se han descrito las características, tipos y funciones de los cortafuegos.

b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.

c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.

d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.

e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.

f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.

g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.

h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

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

Criterios de evaluación:

a) Se han identificado los tipos de proxy, sus características y funciones principales.

b) Se ha instalado y configurado un servidor proxy-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. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

Criterios de evaluación:

a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.

b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un

sistema.

c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.

d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.

e) Se ha implantado un balanceador de carga a la entrada de la red interna.

f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.

g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema.

h) Se han analizado soluciones de futuro para un sistema con demanda creciente.

i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad

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

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.

b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.

c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.

d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.

e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.

f) Se han contrastado las normas sobre gestión de seguridad de la información.

g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

3. Duración del módulo

Este módulo profesional tiene una duración de 84 horas lectivas distribuidas en 4 horas semanales, durante dos trimestres.

4. Contenidos básicos

Adopción de pautas y prácticas de tratamiento seguro de la información:

– Fiabilidad, confidencialidad, integridad y disponibilidad.

– Elementos vulnerables en el sistema informático. Hardware, software y datos.

– Análisis de las principales vulnerabilidades de un sistema informático.

– Amenazas. Tipos. Amenazas físicas y lógicas.

– Seguridad física y ambiental.

- Ubicación y protección física de los equipos y servidores.

- Sistemas de alimentación ininterrumpida.

– Seguridad lógica.

- Criptografía.

- Listas de control de acceso.

- Establecimiento de políticas de contraseñas.

- Políticas de almacenamiento.

- Copias de seguridad e imágenes de respaldo.

- Medios de almacenamiento

– Análisis forense en sistemas informáticos.

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.

- Herramientas paliativas.

- Actualización de sistemas y aplicaciones.

- Seguridad en la conexión con redes públicas.

- Pautas y prácticas seguras.

– Seguridad en la red corporativa.

- Monitorización del tráfico en redes.

- Seguridad en los protocolos para comunicaciones inalámbricas.

- Riesgos potenciales de los servicios de red.

- Intentos de penetración.

Implantación de técnicas de acceso remoto. Seguridad perimetral:

– Elementos básicos de la seguridad perimetral.

– Perímetros de red. Zonas desmilitarizadas.

– Arquitectura débil de subred protegida.

– Arquitectura fuerte de subred protegida.

– Redes privadas virtuales. VPN.

– Beneficios y desventajas con respecto a las líneas dedicadas.

Técnicas de cifrado. Clave pública y clave privada.

- VPN a nivel de red. SSL, IPSec.

- VPN a nivel de aplicación. SSH.

– Servidores de acceso remoto.

- Protocolos de autenticación.

- Configuración de parámetros de acceso.

- Servidores de autenticación.

Instalación y configuración de cortafuegos:

– Utilización de cortafuegos.

– Filtrado de paquetes de datos.

– Tipos de cortafuegos. Características. Funciones principales.

– Instalación de cortafuegos. Ubicación.

– Reglas de filtrado de cortafuegos.

– Pruebas de funcionamiento. Sondeo.

– Registros de sucesos de cortafuegos.

Instalación y configuración de servidores proxy:

– Tipos de proxy. Características y funciones.

– Instalación de servidores proxy.

– Instalación y configuración de clientes proxy.

– Configuración del almacenamiento en la caché de un proxy.

– Configuración de filtros.

Implantación de soluciones de alta disponibilidad:

– Definición y objetivos.

– Análisis de configuraciones de alta disponibilidad.

- Funcionamiento ininterrumpido.

- Integridad de datos y recuperación de servicio.

- Servidores redundantes.
- Sistemas de clusters.
- Balanceadores de carga.

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

5. 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.

6. Competencias profesionales, personales y sociales que se adquieren:

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

e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.
o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

7. Líneas de actuación en el proceso de enseñanza-aprendizaje

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

- El conocimiento de las prácticas y pautas adecuadas, relativas a la seguridad física y lógica en un sistema informático.
- El conocimiento y análisis de técnicas y herramientas de seguridad activa, que actúen como medidas preventivas y/o paliativas ante ataques al sistema.
- El análisis y aplicación de técnicas y herramientas de seguridad activa.

- El análisis y aplicación de técnicas seguras de acceso remoto a un sistema.
- El análisis de herramientas y técnicas de protección perimetral para un sistema.
- La instalación, configuración y prueba de cortafuegos y servidores proxy como herramientas básicas de protección perimetral.
- El análisis de los servicios de alta disponibilidad más comunes, que garanticen la continuidad de servicios y aseguren la disponibilidad de datos.
- El conocimiento y análisis de la legislación vigente en el ámbito del tratamiento digital de la información.

8. Contenidos de carácter transversal.

En nuestro tiempo se dan unas expectativas y demandas de la sociedad, hay una serie de cuestiones que los hombres y mujeres deben estar preparados para abordarlas adecuadamente. La sociedad está clamando por la **paz**, por la **igualdad de derecho y oportunidades entre hombres y mujeres**, por un **respeto al medio ambiente**, por **vivir de una manera más saludable**, por un **desarrollo de la afectividad y de la sexualidad** que permita desarrollar las relaciones interpersonales; una sociedad que necesita forjar personalidades autónomas y cívicas, capaces de respetar la opinión de los demás y, a la vez, defender sus derechos, etc…

Para dar respuesta a esta necesidad de la sociedad actual se tratan, en el marco escolar, los **Temas Transversales**. Hay que considerar, consecuentemente, estos temas como algo necesario para vivir en una sociedad como la nuestra; de ahí la especial relevancia e importancia de estos temas no sólo para el desarrollo personal y la **formación integral de los alumnos**, sino para un proyecto de sociedad más libre y respetuosa, y eso ha de hacerse desde los centros educativos.

Los ejes transversales son grandes temas que engloban múltiples contenidos y difícilmente pueden adscribirse a un Módulo específico, sino que se considera que deben impregnar toda la acción educativa, es decir, **deben estar presentes en todas los Módulos del Ciclo Formativo** (de ahí su nombre de transversales).

Para conseguir que el alumno y la alumna los interiorice y sea capaz de hacerlos operativos en su conducta, extrapolándolos a cualquier situación que se le presente, es necesario desarrollar una serie de estrategias.

Las estrategias previstas para los contenidos de valor no se pueden limitar a aconsejar,

recomendar o moralizar, sino que existen otras que parecen particularmente indicadas:

- La habituación por repetición de actos.
- La imitación, propuesta de modelos, el ambiente…
- La experimentación o práctica activa, consciente y libre.
- La confrontación: poner en situaciones que obliguen a reaccionar frente a un determinado valor.

Como ya se indicó anteriormente, **las enseñanzas transversales se deben trabajar entre todos los Módulos del Ciclo Formativo** y, por tanto, los contenidos referidos a estas enseñanzas transversales se deben distribuir entre los distintos Módulos; por eso, dependiendo de los contenidos propios de este Módulo y de lo que se puede realizar desde el mismo, se le prestan especial atención a algunos de ellos.

A continuación se enuncian los objetivos propuestos para las diferentes enseñanzas del Ciclo Formativo:

- **Educación Moral y Cívica**: Realizar un tratamiento adecuado de la información sensible almacenada en una aplicación, respetando el derecho a la privacidad y a la intimidad de las personas, de acuerdo a lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personal. Trabajar en grupo aceptando las responsabilidades y compromiso que conlleva y respetando las iniciativas de los compañeros y compañeras.
- **Educación Ambiental**: Realizar un uso responsable y moderado de los materiales consumibles propios de la actividad informática, usar correctamente los contenedores de reciclado de papel, usar materiales "digitales" (PDFs, Plataformas Educativas, email, etc.…), ahorrar energía apagando los monitores en aquellos momentos en que no sea necesario el uso del ordenador.
- **Educación para la Salud**: Trabajar en condiciones de seguridad y salud, abordando aspectos de prevención de riesgos laborales como por ejemplo: adoptando una posición corporal correcta al sentarse, donde el ángulo correcto de las rodillas, y el de las piernas en relación con la espalda, así como el formado por los codos, debe ser de 90 grados, colocar la silla a una distancia adecuada, los ojos deben de estar a una distancia de 70-80 centímetros del monitor y quedar a la altura del borde superior de la pantalla, etc. El

Real Decreto 488/97 establece las disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.

- **Educación para el consumo:** Mediante el análisis del software libre y de pago, atendiendo a sus ventajas e inconvenientes, se intentará crear una conciencia crítica ante el consumo.

Existen otra serie de temas transversales que en algunos casos serán abordados puntualmente en determinadas unidades didácticas: cultura andaluza, educación del consumidor y del usuario, educación para la igualdad de oportunidades de ambos sexos, educación para la paz, educación sexual, educación vial.

Las enseñanzas transversales van a impregnar el quehacer educativo a través de la **metodología utilizada**, promoviendo las **actividades grupales**, pues ayudan a la interiorización y compresión de los comportamientos que rigen la vida de un grupo, las normas básicas que hacen que esa **convivencia** sea posible y también a apreciar la **importancia del trabajo cooperativo para lograr un fin común**.

9. Contenidos. Secuenciación por unidades didácticas.

PRIMER TRIMESTRE

UNIDAD DIDÁCTICA 1: Adopción de pautas y prácticas de tratamiento seguro de la información.

– Fiabilidad, confidencialidad, integridad y disponibilidad.

– Elementos vulnerables en el sistema informático. Hardware, software y datos.

– Análisis de las principales vulnerabilidades de un sistema informático.

– Amenazas. Tipos. Amenazas físicas y lógicas.

– Seguridad física y ambiental.

- Ubicación y protección física de los equipos y servidores.

- Sistemas de alimentación ininterrumpida.

– Seguridad lógica.

- Criptografía.

- Listas de control de acceso.

- Establecimiento de políticas de contraseñas.

- Políticas de almacenamiento.

- Copias de seguridad e imágenes de respaldo.

- Medios de almacenamiento.

– Análisis forense en sistemas informáticos.

UNIDAD DIDÁCTICA 2: 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.

- Herramientas paliativas.

- Actualización de sistemas y aplicaciones.

- Seguridad en la conexión con redes públicas.

- Pautas y prácticas seguras.

– Seguridad en la red corporativa.

- Monitorización del tráfico en redes.

- Seguridad en los protocolos para comunicaciones inalámbricas.

- Riesgos potenciales de los servicios de red.

- Intentos de penetración.

UNIDAD DIDÁCTICA 3: Implantación de técnicas de acceso remoto. Seguridad perimetral.

– Elementos básicos de la seguridad perimetral.

– Perímetros de red. Zonas desmilitarizadas.

– Arquitectura débil de subred protegida.

– Arquitectura fuerte de subred protegida.

– Redes privadas virtuales. VPN.

– Beneficios y desventajas con respecto a las líneas dedicadas.

UNIDAD DIDÁCTICA 4: 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.

SEGUNDO TRIMESTRE

UNIDAD DIDÁCTICA 5: 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 cortafuegos.

UNIDAD DIDÁCTICA 6: 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.

UNIDAD DIDÁCTICA 7: Implantación de soluciones de alta disponibilidad.

– Definición y objetivos.

– Análisis de configuraciones de alta disponibilidad.

- Funcionamiento ininterrumpido.

- Integridad de datos y recuperación de servicio.

- Servidores redundantes.

- Sistemas de clusters.

- Balanceadores de carga.

– Instalación y configuración de soluciones de alta disponibilidad.

– Virtualización de sistemas.

– Posibilidades de la virtualización de sistemas.

– Herramientas para la virtualización.

– Configuración y utilización de máquinas virtuales.

– Alta disponibilidad y virtualización.

– Simulación de servicios con virtualización.

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

– 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.

10. Metodología

10.1. Actividades del profesor en el aula

La metodología general que se llevará a lo largo del curso se basará en los siguientes aspectos:

- **Exposición:** Presentar la información de manera verbal, instrumental o audiovisual.
- **Mostración:** Se muestra una habilidad o se ejecuta una tarea de manera práctica, como modelo para que el alumno la reproduzca posteriormente. Siempre el aprendizaje será mejor cuando el alumno primero ve lo que tiene que hacer y después lo realiza él de forma autónoma. Hay que tener cuidado con esto ya que el alumno se puede acostumbrar a tener siempre un guía que le muestre lo que tiene que hacer, y en este Módulo, uno de los principales objetivos es fomentar la autonomía en el trabajo de los alumnos.
- **Orientación:** Se dan pautas, instrucciones, pistas, vías, guiones, información escrita, etc., para que el alumno realice una tarea o para que utilice fuentes de información. De esta forma se fomentará la autonomía del alumno en la realización del trabajo y el trabajo en grupo, dependiendo de la situación propuesta.
- **Supervisión:** El profesor corrige, mientras el alumno realiza una tarea para garantizar el éxito del trabajo.

La impartición de la asignatura se fundamentará en los siguientes aspectos:

- Hacer un breve resumen de los conceptos que se van a tratar en las tareas a realizar.
- Dar una guía al alumnado en la que se presenta una descripción de los pasos a seguir con el ordenador para la actividad propuesta.
- Comprobar que los alumnos y alumnas son capaces de llevar a cabo la tarea planteada, ayudando a aquellos que muestren dificultad, y detectando aquellos otros que son capaces de hacerlas por si mismos. Por tanto, se llevara a cabo una comprobación diaria y personal de las actividades prácticas a realizar.
- Para la explicación de cada Unidad de Trabajo, se realizará una

exposición teórica de los contenidos de la misma por parte del profesor.

- Posteriormente, se realizarán una serie de ejercicios propuestos por el profesor y resueltos y corregidos por él en clase. El objetivo de estos ejercicios, es llevar a la práctica los conceptos teóricos que se asimilaron en la exposición anterior.
- El profesor resolverá todas las dudas que puedan tener los alumnos del ciclo, tanto teóricos como prácticos. Incluso si él lo considerase necesario se realizarán ejercicios específicos que aclaren los conceptos que más cueste comprender al alumnado.
- El profesor propondrá una serie de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser realizados por los alumnos, bien en horas de clase o bien en casa.
- Algunos ejercicios prácticos, se realizarán en el aula de ordenadores, utilizando el entorno correspondiente a la Unidad Didáctica 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, de todas formas no es aconsejable que haya más de dos alumnos por cada equipo informático.
- Además se podrá proponer algún trabajo que englobe conocimientos de varias unidades didácticas para comprobar que los conocimientos mínimos exigidos en cada una de las unidades han sido satisfactoriamente asimilados. Sería recomendable un trabajo por cada evaluación.

Sería conveniente utilizar la Web del centro, en la sección del departamento de informática, para facilitar al alumnado el material que se va dando en clase (apuntes, practicas, páginas Web relacionadas con el modulo,…) con el fin de evitar el excesivo uso de fotocopias y facilitar que el alumnado almacene el material en formato digital.

10.2. Actividades habituales de los alumnos/as

– Se realizarán en clase una serie de ejercicios teórico-prácticos por cada unidad de acuerdo al contenido que se especifica en cada una de ellas en el apartado anterior.

– El alumnado realizará pequeñas exposiciones ante sus compañeros y compañeras que versarán sobre resolución de ejercicios propuestos en la unidad, trabajos voluntarios propuestos por el profesor relacionados con los contenidos de las unidades y trabajos libres

propuestos por el alumnado relacionados con los contenidos de las unidades.

10.3. Materiales didácticos

Materiales

- □□□□□□□□ Un PC por persona con Windows XP y un software de Virtualizacion como podría ser VMWAre, VirtualPC o VirtualBOX. Preferentemente VirtualBOX al ser gratuito.
- □□□□□□□□ Un Router o Switch en el aula para conectar todos los PC en red.
- □□□□□□□□ Sistemas operativos servidores: Windows 2003/2008 Server, Linux Ubuntu Server.
- □□□□□□□□ También serán positivos todos aquellos instrumentos que faciliten la tarea de exposición del profesor, por ejemplo, pantallas de cristal líquido, cañones de exposición, televisión, video, etc.

Bibliografía

Para apoyar el proceso de enseñanza-aprendizaje se propone usar alguna de las referencias citadas a continuación, aunque no serán imprescindibles, ya que el profesor elaborará los apuntes y materiales necesarios para el desarrollo del módulo, y serán suministrado al alumnado mediante fotocopias o cualquier otro método que se estime conveniente.

Se intentará tener en todo momento a disposición de los alumnos los siguientes libros para consulta:

– Seguridad y alta disponibilidad. Edit. Ra-Ma. (Libro recomendado)

- Computer Security, Principles and Practice. Third EditioN. William Stallings/Lawrie Brown.

UNSW Canberra at the Australian Defence Force Academy. PEARSON.

- CCNA SECURITY de CISCO

– Diversos manuales y cursos sobre Servicios de Red e Internet..

– Apuntes del departamento de Informática

Direcciones de Internet

https://www.khanacademy.org/

https://www.elladodelmal.com/

11. Procedimientos de evaluación y criterios de calificación

11.1. Estrategia de evaluación

La evaluación es una herramienta que permitirá comprobar el grado de consecución de los objetivos por parte del alumnado. Se lleva a cabo a lo largo del proceso de enseñanza-aprendizaje y en su conjunto debe servir para facilitar el proceso de aprendizaje y mejorar los resultados educativos.

Al comienzo del curso se realizara una evaluación inicial para lo cual se pasara un cuestionario con preguntas, con el fin de conocer los estudios y experiencias del alumnado, así como obligar a hacer un esfuerzo de auto evaluación sobre lo que éste cree que sabe y el nivel que cree poseer sobre los temas que deben ser objeto de aprendizaje durante el curso.

Se efectuarán dos o tres evaluaciones correspondientes a los trimestres naturales del curso. La evaluación será independiente para cada una de las tres evaluaciones, siendo necesario superar los conocimientos mínimos exigibles de cada una de ellas para superar el módulo completo

Para poder superar los módulos del ciclo es obligatorio la asistencia diaria a clase, ahora bien, dicha obligatoriedad podría estudiarse de forma especial para aquellos alumnos en los que concurran circunstancias especiales como:

- □□□□□□□□ Alumnos que hayan encontrado trabajo y quieran seguir realizando sus estudios.
- □□□□□□□□ Alumnos que por necesidades familiares, o de transporte no puedan asistir con regularidad a todas sus clases.
- □□□□□□□□ Cualquier otra circunstancia que el departamento estime oportuna siempre que sea lo suficientemente justificada.

Alumnos de asistencia regular. (Menos del 20 % de faltas)

Los trimestres serán evaluados mediante una serie de controles teórico y/o prácticos. Para superar dichos controles habrá que obtener una calificación igual o superior a cinco sobre

diez en cada uno de ellos. La nota final de cada evaluación, así como la nota final de la convocatoria ordinaria se calculará según se establezca en la programación de cada módulo.

Los alumnos que no aprueben alguna evaluación deberán realizar un control de características similares a cada una de las partes no superadas en su momento. Para recuperar la evaluación el alumno deberá superar cada una de las partes que la forman. La recuperación de dichas partes se hará en una sola convocatoria por evaluación.

Debido a que las materias dadas en cada trimestre son independientes, las evaluaciones aprobadas durante el curso se guardarán para la evaluación final ordinaria (evaluaciones completas, en ningún caso temas sueltos).

En caso de tener que examinarse en la convocatoria final extraordinaria, los alumnos, además de superar la prueba escrita, deberán presentar y superar aquellas prácticas obligatorias que debieran haber superado durante el desarrollo del curso y que aún no las tengan entregadas y superadas. La nota final será la nota obtenida en la prueba extraordinaria siempre y cuando se hayan entregado y superado las prácticas obligatorias.

Para que el alumno pueda realizar un perfecto seguimiento del módulo, no deberá faltar a clase, se comportará correctamente y participará activamente en todas las cuestiones planteadas. Así, si un alumno no realiza alguna de las indicaciones anteriores, la nota de la evaluación se verá afectada a la baja.

Alumnos de asistencia irregular. (más de un 20% de faltas)

Estos alumnos se presentarán obligatoriamente a una recuperación final en la convocatoria ordinaria y deberán superar la prueba con una nota igual o superior a 5 sobre 10. En algunos casos, a criterio del profesor, el alumno deberá defender su examen ante varios profesores del Departamento.

En todo caso, estos alumnos estarán obligados a presentar y superar las prácticas de evaluación exigidas al grupo, calificándoseles de la misma forma que se ha especificado en el apartado anterior.

Ortografía y falta de puntualidad

Los alumnos deberán prestar atención especial con las faltas de ortografía. A cada alumno se le quitará 0’25 por cada falta de ortografía, hasta un máximo de 2,5 puntos.

La puntualidad será tenida en cuenta a la hora de la calificación de los alumnos. Además, a los alumnos que lleguen tarde a clase de forma injustificada reiteradamente se les aplicará la normativa establecida en el Plan de Convivencia del Centro.

Calificación

Para la calificación de cada alumno se seguirán los siguientes criterios:

- **Criterios comunes a todas las actividades o pruebas realizadas:**
  - Para que una prueba, ya sea teórica o práctica, haga media con el resto de pruebas deberá tener una calificación como mínimo de un 4.
  - Para poder hacer media, el alumno solo podrá tener una prueba suspensa en cada trimestre. Con dos o más pruebas suspensas, no se hará media y tendrá que recuperar el trimestre.
- **Actividades de enseñanza-aprendizaje 10%**
  - Para este 10 % se tendrá en cuenta los siguientes apartados:
    - Asistencia y Puntualidad del alumno a clases.
    - Participación en debates.
    - Realización de ejercicios de carácter voluntario.
    - Participación en el propio proceso de enseñanza-aprendizaje ayudando a resolver dudas a alumnos menos aventajados.
    - Comportamiento en clase.
- **Actividades especificas de la evaluación 90%**
  - **Prueba escrita 70%**
    - Se realizarán pruebas escritas para comprobar que los alumnos efectivamente han afianzado correctamente los conceptos principales de las distintas unidades. Esta prueba escrita podrá constar, según el caso, de una serie de cuestiones teóricas a desarrollar, o de una serie de preguntas test y uno o varios problemas a desarrollar sobre las unidades que se están evaluando. Para superar la prueba será necesario obtener un 5, pero, teniendo que superar al menos un 30% de la puntuación que valga la teoría. En cada prueba escrita que se le haga al alumno vendrá especificado la valoración específica de cada cuestión de la misma y como se va a puntuar.
  - **Realización de Prácticas-Trabajos 20%**

- Al alumno se le podrá solicitar que realice una serie de prácticas por evaluación (que podrán ser de carácter obligatorio o de carácter optativo) que podrán ser calificadas de dos formas distintas:

  a) Las prácticas de carácter optativo podrán ser realizadas por los alumnos para afianzar sus conocimientos, pudiendo subir su nota hasta en 0,25 puntos por práctica.

  b) La práctica de carácter obligatorio será calificada con "Apto" o "No Apto", siendo en este caso necesaria obtener la calificación "Apto" para ser evaluado en la evaluación correspondiente, si no es así, al alumno se le restará hasta 2 puntos de la nota de su evaluación. La práctica de carácter obligatorio dependiendo de su complejidad podrá aumentar hasta en 2 puntos la calificación de la evaluación

  El profesor tras corregir las prácticas podrá exigir a los alumnos según crea conveniente la exposición de dicha práctica así como su defensa ante el resto de compañeros.

11.2. Procedimientos e instrumentos de evaluación

Los instrumentos de evaluación incluirán alguna o todas entre las siguientes:

- □□□□□□□□ Observación sistemática del proceso de aprendizaje del alumno.
- □□□□□□□□ Valoración de la solución tomada ante las diversas dificultades que se les puedan presentar.
- □□□□□□□□ Valoración del planteamiento y solución dada a los problemas, evitando improvisaciones y el uso del ordenador de forma indiscriminada sin un esquema de trabajo claro.
- □□□□□□□□ Pruebas abiertas escritas, y pruebas objetivas para la comprobación de los conocimientos adquiridos.
- □□□□□□□□ Pruebas prácticas de los conocimientos desarrollados en el aula.
- □□□□□□□□ Entrevistas personales o reuniones en pequeños grupos, comprobando las aportaciones individuales al grupo.
- □□□□□□□□ Prácticas de carácter obligatorio para la superación de la evaluación.
- □□□□□□□□ Prácticas de carácter voluntario para afectar al alza la nota de la

evaluación.

- □□□□□□□□ Responsabilidad en el trabajo.

Se aplicarán los siguientes porcentajes:

UNIDAD	RESULTADOS A LOS QUE CONTRIBUYE	%
UNIDAD DIDÁCTICA 1: Adopción de pautas y prácticas de tratamiento seguro de la información.	RA1	15
UNIDAD DIDÁCTICA 2: Implantación de mecanismos de seguridad activa.	RA2	10
UNIDAD DIDÁCTICA 3: Implantación de técnicas de acceso remoto. Seguridad perimetral.	RA3	15
UNIDAD DIDÁCTICA 4: Técnicas de cifrado. Clave pública y clave privada.	RA3, RA2, RA1	10
UNIDAD DIDÁCTICA 5: Instalación y configuración de cortafuegos.	RA4, RA5	15
UNIDAD DIDÁCTICA 6: Instalación y configuración de servidores proxy.	RA4, RA5	15
UNIDAD DIDÁCTICA 7: Implantación de soluciones de	RA6	10

alta disponibilidad.

UNIDAD DIDÁCTICA 8: Reconocimiento de la legislación y normativa sobre seguridad y protección de datos.	RA7	10

11.3. Formas de recuperación

Evaluación ordinaria

Durante el desarrollo de las unidades didácticas emplearemos unos mecanismos de recuperación, para reforzar o recuperar la materia aún no asimilada antes de realizar alguna prueba o práctica específica. Al ser la evaluación continua permitirá ajustar el desarrollo de la misma al rendimiento de estos alumnos mediante las técnicas e instrumentos ya expuestos. Los mecanismos que utilizaremos para realizar, en caso necesario, este ajuste (mecanismos de recuperación) son los siguientes: las explicaciones individualizadas (con más y distintos ejemplos, con una guía por nuestra parte,…) y la corrección de las actividades de refuerzo para cada unidad (proporcionando más actividades y con la graduación de dificultad precisa).

Aquellos alumnos y alumnas que una vez realizadas pruebas o prácticas específicas en la que no hayan obtenido evaluación positiva, dispondrán de varias oportunidades de recuperar dicha parte de materia o práctica en la evaluación ordinaria:

En cada prueba específica trimestral del primer o segundo trimestre, además de la propia materia a evaluar al final del trimestre, los alumnos que no hubiesen superado alguna práctica o prueba específica durante dicho trimestre, podrán entregar esas prácticas y presentarse a dichos contenidos respectivamente (sólo correspondientes al trimestre). En caso de no superar alguna parte trimestral quedará pendiente el trimestre completo para la prueba final de evaluación ordinaria.

En la prueba final de evaluación ordinaria (en el tercer trimestre), además de la propia materia a evaluar al final del tercer trimestre y de la recuperación de alguna práctica o prueba específica durante el mismo, los alumnos que tengan que recuperar uno o varios trimestres deberán presentarse a esta prueba para examinarse del trimestre/s a recuperar.

Por tanto, en las pruebas específicas trimestral del primer y segundo trimestre y en la final (u ordinaria), los alumnos se evaluarán de contenidos teórico-prácticos trabajados desde la anterior prueba específica del mismo trimestre. Además, se da la opción de recuperar la parte o materia pendiente durante el mismo trimestre. Y en el caso de la final u ordinaria, también se da la opción de evaluar los anteriores 2 trimestres por separado.

Como apoyo a los alumnos con algún trimestre pendiente durante la evaluación ordinaria, se mantendrán los contenidos, enlaces y cualquier material existente en el servidor del departamento así como los recursos hardware de clase. Además se atenderán dudas.

Evaluación extraordinaria

En el caso de que el alumno no supere el módulo en la convocatoria ordinaria o aquellos que hayan perdido el derecho a evaluación continua, tendrán derecho a volver a intentarlo en la convocatoria extraordinaria.

Es importante destacar que los alumnos que hayan perdido el derecho a la evaluación continua, no podrán presentarse a la prueba final de evaluación ordinaria y por tanto deben examinarse en esta evaluación extraordinaria de todos los contenidos del curso.

Para superar con éxito dicha convocatoria, será necesaria superar la prueba específica, en la que se evaluarán los contenidos relativos a todo el módulo.

La calificación del módulo seguirá los mismos criterios que lo detallados en el apartado de calificación.

GUÍA DE RECUPERACIÓN

UNIDAD DIDÁCTICA 1: Adopción de pautas y prácticas de tratamiento seguro de la información.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase

durante la explicación de esta unidad.

3. Objetivos Mínimos

Conocer y analizar de las principales vulnerabilidades de un sistema informático.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Buscar recursos en la página web de Hispasec y busca noticias relacionadas con seguridad informática en dicha página web

UNIDAD DIDÁCTICA 2: Implantación de mecanismos de seguridad activa.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer y analizar las principales herramientas preventivas y paliativas.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Investiga sobre las opciones de configuración de contraseñas y cifrado de archivos ofimáticos.

Investiga sobre la finalidad y opciones de la aplicación Windows SteadyState

UNIDAD DIDÁCTICA 3: Implantación de técnicas de acceso remoto. Seguridad Perimetral.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer los elementos básicos de la seguridad perimetral.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Busca información sobre Iptables

Investiga las opciones de algún proxy.

Investiga el uso de la utilidad Webmin

UNIDAD DIDÁCTICA 4: Técnicas de cifrado. Clave pública y clave privada.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer los Servidores de acceso remoto y la configuración de parámetros de acceso

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Busca información al respecto de esta unidad didáctica en la página web de la Fábrica Nacional de Moneda y Timbre, y del DNI electrónico

UNIDAD DIDÁCTICA 5: Instalación y configuración de cortafuegos.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer los tipos de cortafuegos, características, funciones principales e instalación.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Analiza el cortafuegos que incorpora por defecto Windows 7

UNIDAD DIDÁCTICA 6: Instalación y configuración de servidores proxy.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer los tipos de proxy, características, funciones, e instalación.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Analiza el uso y utilidad del proxy Winproxy

UNIDAD DIDÁCTICA 7: Implantación de soluciones de alta disponibilidad.

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. Objetivos Mínimos

Gestionar la instalación y configuración de soluciones de alta disponibilidad, así como la virtualización de sistemas, y las herramientas de virtualización actuales.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Investiga sobre los conceptos “Balanceo”, “Virtualización”, y sobre la aplicación FreeNAS

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

1. Metodología

Para recuperar esta unidad el alumno dispondrá de algún tiempo en clase, dentro de las horas dedicadas a la realización de prácticas y búsqueda autónoma de información, para afianzar sus conocimientos, y del mismo modo poder ir preguntando al profesor las dudas que le vayan surgiendo. Igualmente se propondrán trabajos de refuerzo para realizar en casa.

2. Materiales de Recuperación.

Apuntes del profesor. Páginas web propuestas durante el curso. Software utilizado en clase durante la explicación de esta unidad.

3. **Objetivos Mínimos**

Conocer la legislación sobre protección de datos y sobre los servicios de la sociedad de la información y correo electrónico.

4. Temporización

La recuperación de esta unidad se empezará a trabajar de forma paralela la semana siguiente a la terminación de la unidad didáctica en cuestión.

5. Actividades.

Busca las normativas aplicables a esta unidad didáctica, identificando el ámbito de las mismas, así como las sanciones aplicables en caso de incumplimiento de sus disposiciones imperativas.