Departamento de Informática y Comunicaciones

Seguridad Informática y Alta Disponibilidad

Profesor:
Pedro Vargas Pérez

Curso
2016/2017

Ciclo Formativo de Grado Superior

Administración de Sistemas Informáticos en Red

1.- Contextualización

En este documento se desarrolla la programación didáctica del módulo de **Seguridad Informática y Alta Disponibilidad.** Este módulo se imparte en el segundo curso del **Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red** cuya competencia general se cita a continuación:

Consiste en configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente.

Dicho ciclo de formación profesional tiene una duración de 2000 horas, lo que equivale a cinco trimestres de formación en centro educativo más la formación en centro de trabajo correspondiente.

Este ciclo formativo dispone de una organización modular. El módulo de Seguridad Informática y Alta Disponibilidad se imparte en el segundo curso. Dispone de una carga lectiva de 84 horas que se distribuyen a razón de 4 horas semanales durante 21 semanas.

2.- Normativa de Referencia

Esta programación didáctica está fundamentada en la siguiente normativa:

- REAL DECRETO 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.
- REAL DECRETO 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.
- 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. en la Comunidad Autónoma de Andalucía.
- 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.
-

3.- Objetivos

Tal y como se enuncia en el RD 1629/2009, para el ciclo formativo de grado superior ASIR se han definido una serie de objetivos generales, que vienen a desarrollar la competencia general establecida para el mismo.

La formación del módulo de Seguridad Informática y Alta Disponibilidad, en concreto, contribuye a alcanzar los siguientes objetivos generales del módulo:

- Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.
- Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.
- Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
- Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.
- Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios
- Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.

También contribuye a la adquisición de las siguientes competencias profesionales, personales y sociales:

- Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
- Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
- Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
- Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
- Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
- Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
- 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.
- Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
- Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.
- Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

Aumentando el grado de concreción, se habla de objetivos a nivel del módulo, que vienen expresados en términos de resultados de aprendizaje, que pasamos a citar:

- Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
- Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
- Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
- Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
- Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

- Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
- Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permitirán alcanzar los objetivos anteriores estarán relacionadas 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.

4.- Contenidos

4.1.- Unidades temáticas

Los contenidos de este módulo se distribuyen en las siguientes unidades temáticas:

- U.T.1: Principios de seguridad informática y alta disponibilidad.
- U.T.2: Configuraciones de alta disponibilidad.
- U.T.3: Normativa legal en materia de seguridad informática.
- U.T.4: Seguridad Pasiva.
- U.T.5: Seguridad Lógica.
- U.T.6: Software antimalware.
- U.T.7: Criptografía.
- U.T.8: Seguridad en redes.

Veamos el desarrollo de cada una de estas unidades:

U.T.1: Principios de Seguridad Informática y Alta Disponibilidad (4 horas)

Contenidos

- Introducción a la seguridad informática
- Conceptos de fiabilidad, confidencialidad, integridad y disponibilidad.
- Análisis de los elementos vulnerables en el sistema informático: hardware, software y datos.
- Análisis de las amenazas que se pueden presentar en un sistema informático.
- Protección de los sistemas informáticos.

U.T.2: Configuraciones de Alta Disponibilidad (8 horas)

Contenidos

- Concepto de alta disponibilidad.
- Soluciones de alta disponibilidad.
    - Sistemas RAID.
    - Balanceo de carga.
    - Virtualización.
    - Servidores redundantes.
    - Sistemas de clústeres.

U.T.3: Normativa Legal en Materia de Seguridad Informática (4 horas)

Contenidos

- Ley orgánica de protección de datos.
- Ley de servicios de la sociedad de la información y del comercio electrónico.

U.T.4: Seguridad Pasiva (8 horas)

Contenidos

- Principios de seguridad pasiva.
- Copias de seguridad.
- Seguridad física y ambiental.
- Sistemas de alimentación ininterrumpida.

U.T.5: Seguridad Lógica (8 horas)

Contenidos

- Principios de seguridad lógica.
- Control de acceso lógico.
- Políticas de usuarios y grupos.

U.T.6: Seguridad Software Antimalware (8 horas)

Contenidos

- Software malicioso.
- Clasificación del malware.
- Protección y desinfección.

U.T.7: Criptografía (8 horas)

Contenidos

- Principios de criptografía.
- Tipos de algoritmos de cifrado.
- Certificados digitales.

U.T.8: Seguridad en Redes (16 horas)
Contenidos
• Amenazas y ataques en las redes. • Sistemas de detección de intrusos. • Riesgos potenciales en los servicios de red. • Comunicaciones seguras. • Seguridad en los protocolos para comunicaciones inalámbricas. • Cortafuegos. • Servidores proxy.

4.2.- Contenidos transversales

La inclusión de los temas transversales como contenido curricular permite acercar a los Centros aquellos problemas que la sociedad reconoce como prioritarios en un momento determinado. Son muchos y variados los temas transversales que se relacionan con los distintos bloques temáticos del módulo de Implantación de Aplicaciones Web, así se señalan a modo de ejemplo **algunas conexiones de los temas transversales con el módulo de Implantación de Aplicaciones Web.**

Además de los contenidos anteriormente detallados, en la dinámica diaria del proceso de enseñanza – aprendizaje, trabajaremos los siguientes temas transversales:

- ***EDUCACIÓN MORAL Y CIVICA****:* se le mostrarán al alumnado aspectos de la vida cotidiana en los que es necesario respetar unas normas básicas y adoptar actitudes positivas y solidarias para la convivencia en sociedad, lo que se pondrá en práctica con la realización de actividades en grupo así como asociando el trabajo de clase con aquél realizado en empresas de informática. La actitud de un futuro profesional debe ser correcta. Habrá que respetar normas relativas al tratamiento de datos de carácter personal, así como las relativas a proteger los derechos de propiedad intelectual.
- ***EDUCACIÓN PARA LA PAZ****:* se velará en todo momento por la comunicación a través de un lenguaje no violento, así como se prestará atención a la prevención de conflictos en el aula y a la resolución pacífica de los mismos.
- ***EDUCACIÓN PARA LA IGUALDAD DE OPORTUNIDADES DE AMBOS SEXOS****:* se debe poner de manifiesto tal igualdad a la hora de realizar los agrupamientos de alumnos y alumnas para el desarrollo de cada una de las actividades planteadas. Reflexionar sobre la igualdad de oportunidades en el mercado laboral.
- ***EDUCACIÓN PARA LA SALUD***: se prestará especial atención a la higiene postural y a la ergonomía para prevenir los dolores de espalda, ya que se pretende reducir la carga

que soporta la misma al estar sentado trabajando con el ordenador. También a la hora de configurar y diseñar sitios web se tendrán en cuenta opciones de accesibilidad.

- ***EDUCACIÓN AMBIENTAL**:* primará el uso y generación de documentación en formato digital para evitar en la medida de lo posible el derroche de papel. Para ello, se le proporcionará a los alumnos la mayoría de los ejercicios y documentación en formato PDF, para su descarga y acceso sin necesidad de recurrir a su impresión en papel.
- ***EDUCACIÓN DEL CONSUMIDOR**:* intentaremos que el alumnado reflexione sobre el hábito de consumir, potenciando además el uso del software libre y la adquisición de licencias cuando se trate de software propietario. Existen licencias destinadas a estudiantes con precios muy competitivos, también pueden beneficiarse del programa DreamSpark Premium de Microsoft que tiene suscrito el instituto.

Se consideran una serie de fechas idóneas para motivar la reflexión y el trabajo sobre estos temas, por medio de actividades normales o extraordinarias: 25 de noviembre (día internacional contra la violencia de género), 3 de diciembre (día internacional de personas con minusvalías), 30 de enero (día escolar de la no violencia y la paz), 28 de febrero (día de Andalucía), 8 de marzo (día internacional de la mujer), 15 de marzo (día internacional del consumidor), etc.

Finalmente, recordar que el objetivo de la formación profesional es formar a un PROFESIONAL cuya actitud y conducta debe estar acorde con todos estos valores.

4.3 Competencias profesionales, personales y sociales

- 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.
- Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
- Instalar, configurar y mantener servicios multiusuario, aplicaciones y dispositivos compartidos en un entorno de red local, atendiendo a las necesidades y requerimientos especificados.
- Realizar las pruebas funcionales en sistemas microinformáticos y redes locales, localizando y diagnosticando disfunciones, para comprobar y ajustar su funcionamiento.
- Mantener sistemas microinformáticos y redes locales, sustituyendo, actualizando y ajustando sus componentes, para asegurar el rendimiento del sistema en condiciones de calidad y seguridad.
- 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.
- Elaborar presupuestos de sistemas a medida cumpliendo los requerimientos del cliente.
- Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
- Organizar y desarrollar el trabajo asignado manteniendo unas relaciones profesionales adecuadas en el entorno de trabajo.
- Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.

- Utilizar los medios de consulta disponibles, seleccionando el más adecuado en cada caso, para resolver en tiempo razonable supuestos no conocidos y dudas profesionales.
- Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
- Resolver problemas y tomar decisiones individuales siguiendo las normas y procedimientos establecidos definidos dentro del ámbito de su competencia.

5.- Temporalización

5.1.- Distribución de unidades temáticas por trimestre

Al tratarse del segundo curso del ciclo formativo, sólo hay dos trimestres de formación en el centro educativo, dedicándose el tercero para la formación en centros de trabajo (FCT) y proyecto integrado (PI).

Trimestre	Unidad temática	Número de horas
1er Trimestre	U.T.1	4 horas
	U.T.2	8 horas
	U.T.3	4 horas
	U.T.4	8 horas
	U.T.5	8 horas
	U.T.6	8 horas
2º Trimestre	U.T.7	8 horas
	U.T.8	16 horas

6.- Metodología

A la hora de aplicar la metodología habrá que tener en cuenta las orientaciones pedagógicas, relacionadas con el módulo, que establecen que este módulo profesional contiene la formación necesaria para seleccionar y utilizar técnicas y herramientas específicas de seguridad informática en el ámbito de la administración de sistemas. Además, servirá para conocer arquitecturas de alta disponibilidad y utilizar herramientas de virtualización en la implantación de servicios de alta disponibilidad.

Las funciones de la administración segura de sistemas incluyen aspectos como:

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

Las actividades profesionales asociadas a estas funciones se aplican en:

- Mantenimiento de equipos. Hardware y software.
- Administración de sistemas en pequeñas y medianas empresas.
- Personal técnico de administración de sistemas en centros de proceso de datos.
- Personal técnico de apoyo en empresas especializadas en seguridad informática.

Como orientaciones metodologías se utilizarán las siguientes:

- Partir del nivel de desarrollo del alumno/a y de los conocimientos previos que posee.
- Favorecer la motivación por el aprendizaje.
- Favorecer la adquisición de aprendizajes significativos y funcionales, trasladables a situaciones de trabajo relacionadas con su ciclo formativo. De este modo, se crean relaciones entre los nuevos contenidos y lo que ya se sabe.
- Asegurarse de que el alumno sabe lo que hace y por qué lo hace, encontrándole sentido a la tarea.
- Contribuir al desarrollo de la capacidad de “aprender a aprender”, permitiendo que el alumno/a se adapte a nuevas situaciones de aprendizaje.
- Crear un clima de aceptación mutua y cooperación.

En definitiva, la metodología a utilizar será activa, participativa, creativa y reflexiva; para que el alumno/a sea protagonista de su propio aprendizaje. Para ello haremos uso de los métodos siguientes:

- Plantear y resolver problemas haciendo uso de herramientas y técnicas de seguridad. Al finalizar, los alumnos y alumnas deberán valorar los resultados alcanzados y el grado de consecución de los objetivos que se habían planteado.
- Utilizar distintas fuentes de información para el estudio: libros, documentos de ejemplo, manuales, enlaces web …
- Emplear la simulación de distintas situaciones en el ordenador para facilitar la deducción, observación y experimentación.
- Utilizar la plataforma Moodle como aula virtual, donde se publicará todo el material del curso a utilizar por los estudiantes y mediante la cual se realizará la entrega de prácticas, a la vez que servirá de apoyo a la comunicación entre profesorado y alumnado.

Para poder llevar a cabo esta labor se utilizarán los siguientes tipos de actividades de enseñanza aprendizaje:

1. De aprendizaje:

- Pruebas de conocimientos.
- Utilización de manuales (ayudas).
- Prácticas con el ordenador.
- Resolución de problemas.
- Ejercicios teórico - prácticos.

2. Docentes:

- Exposición de los contenidos teóricos que se consideren oportunos.
- Realización de prácticas como modelo.
- Planteamiento de situaciones problema.
- Supervisión y corrección del trabajo realizado por los alumnos/as.
- Asesoramiento y orientación permanente a los alumnos/as.

7.- Materiales e Infraestructura

Para el desarrollo de las actividades del curso se utilizaran los recursos y materiales presentes en el aula:

a) Infraestructura de comunicaciones

- Infraestructura de red para intercomunicar todos los ordenadores del aula.
- Acceso a Internet para todos los ordenadores del aula.

b) Hardware

- Un ordenador para cada alumno/a y un ordenador para el profesor.

- Cañón retroproyector para la realización de exposiciones teóricas y simulaciones prácticas por parte del profesor.

c) Software

- Sistemas operativos: Windows y Linux.
- Paquete ofimático: OpenOffice.
- Navegador Web: Mozilla Firefox.
- Utilidades relacionadas con la seguridad: DriverMax, DeepFreeze, Keepass Password Safe, Revealer Keylogger, …
- VirtualBox para la virtualización de sistemas informáticos.
- Diversas máquinas virtuales, ya instaladas y listas para funcionar, para la realización de ejercicios prácticos.
- Vmware ESXi y vSphere en sus versiones gratuitas y de prueba.
- Etc.

8.- Evaluación

8.1.- Criterios de evaluación

Los criterios de evaluación de los que nos valdremos para evaluar el aprendizaje del alumnado serán aquellos establecidos en la Orden de 19 de julio de 2010 para el módulo de Seguridad Informática y Alta Disponibilidad:

- En relación con el resultado de aprendizaje nº 1. *Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo*, se valorará que:
  - Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
  - Se han descrito las diferencias entre seguridad física y lógica.
  - Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
  - Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
  - Se han adoptado políticas de contraseñas.
  - Se han valorado las ventajas que supone la utilización de sistemas biométricos.
  - Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
  - Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
  - Se han identificado las fases del análisis forense ante ataques a un sistema.

- En relación con el resultado de aprendizaje nº 2. *Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema*, se valorará que:
  - Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.

- Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
- Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
- Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
- Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
- Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
- Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
- Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
- Se han descrito los tipos y características de los sistemas de detección de intrusiones.

- En relación con el resultado de aprendizaje nº 3. *Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad*, se valorará que:
  - Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
  - Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
  - Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
  - Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
  - Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
  - Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
  - Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

- En relación con el resultado de aprendizaje nº 4. *Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna*, se valorará que:
  - Se han descrito las características, tipos y funciones de los cortafuegos.
  - Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
  - Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
  - Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
  - Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
  - Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
  - Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
  - Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

- En relación con el resultado de aprendizaje nº 5. *Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio*, se valorará que:
  - Se han identificado los tipos de «proxy», sus características y funciones principales.
  - Se ha instalado y configurado un servidor «proxy-cache».
  - Se han configurado los métodos de autenticación en el «proxy».
  - Se ha configurado un «proxy» en modo transparente.
  - Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.
  - Se han solucionado problemas de acceso desde los clientes al «proxy».
  - Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.
  - Se ha configurado un servidor «proxy» en modo inverso.
  - Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».

- En relación con el resultado de aprendizaje nº 6. *Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba*, se valorará que:
  - Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
  - Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
  - Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
  - Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
  - Se ha implantado un balanceador de carga a la entrada de la red interna.
  - Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
  - Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.
  - Se han analizado soluciones de futuro para un sistema con demanda creciente.
  - Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

- En relación con el resultado de aprendizaje nº 7. *Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia*, se valorará que:
  - Se ha descrito la legislación sobre protección de datos de carácter personal.
  - Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
  - Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
  - Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
  - Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
  - Se han contrastado las normas sobre gestión de seguridad de la información.
  - Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

8.2.- Instrumentos de evaluación

La evaluación de este módulo **es continua** a lo largo de todo el curso. Por tanto requiere la **asistencia regular a clase** por parte del alumno/a, así como la realización de los ejercicios y prácticas programadas por el profesor.
Se realizarán **dos evaluaciones parciales**, la última de las cuales se desarrollará a mediados del mes de Marzo, con la finalidad de que el alumnado que haya superado todos los módulos, realice la FCT y el PI.
Además de estas evaluaciones parciales se realizará **una evaluación final** (Junio) para aquel alumnado que tenga el módulo no superado mediante evaluación parcial o desee mejorar los resultados obtenidos, teniendo otros módulos previos a la realización de la FCT con evaluación negativa.
Para evaluar el desempeño del alumnado durante todo el curso, se utilizarán las siguientes herramientas:

- Control de faltas de asistencia y **observación diaria**. Se debe tener muy en cuenta el trabajo diario que realice el alumno y su comportamiento, lo que engloba la asistencia a clase, la atención en las mismas, la realización de las diferentes actividades propuestas, la participación activa y la aplicación de los distintos contenidos actitudinales definidos para cada una de las unidades didácticas. Todos estos aspectos se valorarán numéricamente entre 0 y 10.
- Corrección individual de las actividades y **prácticas** propuestas durante el desarrollo de cada una de las unidades didácticas. Algunos trabajos de este tipo incluirán una defensa por parte de cada alumno/a, para demostrar que el alumno/a es el autor de la práctica. Para que las prácticas se consideren superadas siempre deberán ser entregadas en las fechas establecidas, a la vez que deberán obtener una calificación igual o superior a 5.
- Una serie de pruebas escritas (**exámenes teóricos**) así como haciendo uso del ordenador (**exámenes prácticos**), distribuidas para cubrir todas las unidades de trabajo. La carga teórica frente a la práctica de cada prueba dependerá de la unidad de trabajo a evaluar, si bien se intentará darle el mayor enfoque práctico posible. **Si el profesor lo considera oportuno, y en el caso de que la unidad impartida sea muy práctica, se podrá suprimir el exámen por la nota global de las prácticas, siempre y cuando el alumno/a no falte más de un 20% a las clases y tenga entregadas todas las prácticas.**

Al final de cada trimestre se realizará una **evaluación parcial en la que la** calificación para los estudiantes será la media poderada del siguiente apartado.

8.3.- Criterios de calificación

- Control de faltas de asistencia y **observación diaria**. Se tendrá en cuenta el trabajo diario que realice el alumno y su comportamiento, lo que engloba la asistencia a clase, la atención en las mismas y la participación activa. Todos estos aspectos se valorarán numéricamente entre 0 y 10.
- Los trabajos de clase escritos y prácticas, la forma de puntuar será mediante (en términos de porcentaje): 0, si la actividad no se ha entregado o el trabajo no se ha realizado;50, si se ha realizado lo anterior de la forma más básica posible e incluso con algún error;25 si se ha entregado de forma óptima, pero fuera de plazo; 75, si se ha realizado lo anterior sin errores y con medios propios; 100, si se realiza lo anterior de forma óptima, con mucho interés e incluso con ampliación de información sobre lo pedido.

- En relación a los exámenes teórico-prácticos señalar que:
  - Influirá negativamente en la nota de las evaluaciones las faltas de ortografía y una incorrecta forma de expresarse.
  - Si al alumnado se le sorprende copiando o hablando deberá abandonar el aula, se le recogerá el examen y se le calificará con un uno.
  - Tanto la calificación asignada a cada una de las preguntas o ejercicios propuestos como el número de preguntas que conforman la prueba variará en cada examen, a criterio del docente.

La calificación de los alumnos se realizará por unidades de trabajo o bien por bloques de unidades homogéneas, aplicando las calificaciones de las pruebas y de los instrumentos de evaluación, ponderados adecuadamente.
Cada uno de los instrumentos de evaluación se valorará de la siguiente manera:

- **Exámenes o pruebas objetivas**: 50%
- **Trabajos de clase escritos y prácticas de clase:** 30%
- **Observación sistemática del alumnado:** 20%

La calificación final del módulo se obtiene mediante la media aritmética ponderada de las calificaciones particulares de las unidades de trabajo o de los bloques de unidades homogéneas.
Esta ponderación de unidades o bloques se establece de acuerdo con la importancia relativa de los resultados de aprendizaje del módulo, que se encuentren incluidas en cada unidad o bloque.
Por otra parte, cabe reseñar que si el alumno/a no asiste a clase durante alguna de las pruebas y **no lo justifica debidamente** (certificado médico o comunicación de su tutor/a), se considerará SUSPENSO/A y no podrá recuperar dicha prueba hasta la recuperación o en su defecto el mes de junio. De igual modo, la falta no justificada a cualquiera de las demás pruebas (recuperaciones y finales) supone la calificación de SUSPENSO/A.
En caso de tratarse de una falta justificada, el profesor/a podrá realizar la prueba a este alumno/a el **primer día** de clase que éste se incorpore o en el momento que el profesor/a considere oportuno (sin previo aviso).
La evaluación trimestral y final de este módulo profesional, se realizará en forma de calificaciones numéricas comprendidas entre 1 y 10 sin decimales, considerándose positivas las calificaciones iguales o superiores a 5 y negativas las restantes.
La calificación correspondiente a cada trimestre seguirá la siguiente ponderación:

- 50 % exámenes
- 30 % prácticas
- 20 % observación diaria

8.4.- Recuperación

Después de cada una de las evaluaciones se dedicará un día para realizar una prueba destinada a que los alumnos que obtuvieron una calificación negativa en la evaluación puedan recuperar la evaluación correspondiente.
Puede ser que algunos alumnos necesiten un refuerzo para alcanzar los objetivos, en cuyo caso se les entregará material práctico elaborado por el profesor, en función de las carencias observadas, con un método diferente o simplemente como mayor ejercitación de un concepto.
Entre los mecanismos o **actividades de recuperación** previstos podemos destacar:

- Actividades de refuerzo y corrección de las mismas.
- Pruebas orales o escritas teórico-prácticas más flexibles sobre los contenidos de la materia objeto de recuperación.
- Solución a nuevos casos prácticos.
- Mejora de las prácticas realizadas.
- Pequeños trabajos de investigación.

Los alumnos/as pendientes podrán realizar cualquier consulta al profesor en las horas de tutoría o en cualquier hora libre acudiendo al Departamento de Informática y Comunicaciones.

8.5.- Evaluaciones parciales

Como ya se ha indicado, la evaluación será continua, por lo que la nota final del módulo para cada uno de los alumnos/as se obtendrá teniendo en cuenta las calificaciones conseguidas durante el desarrollo del curso.
Se realizarán **dos evaluaciones parciales**, la última de las cuales se desarrollará a mediados de Marzo.
La nota final del alumno será la media aritmética de las notas obtenidas en las dos evaluaciones parciales.

En caso de que el alumno o alumna, acumule un número de faltas de asistencia superior al 20% de las horas lectivas del trimestre, perderá el derecho a evaluación continua en esa evaluación parcial. Por lo que tendrá que recuperarla en el mes de junio.

8.6.- Evaluación final

Consideramos en este caso a los alumnos/as que hayan obtenido una evaluación negativa de nuestro módulo en las evaluaciones parciales o deseen mejorar los resultados obtenidos.

- **Alumnado que no haya superado el módulo**. Tendrán la obligación de efectuar las prácticas que no hayan realizado durante el curso y de mejorar aquellas realizadas. Al final del curso académico (en Junio) se tendrán que realizar pruebas teórico-prácticas con los contenidos de cada trimestre y si éstas no se superaran, una prueba que englobe todos los contenidos trabajados en el módulo, de manera que se permita la aplicación de todos los criterios de evaluación definidos para el mismo. Esta prueba constará de varias preguntas tipo test y/o de desarrollo y una serie de supuestos prácticos. La ponderación de cada actividad dependerá de la importancia del contenido que trate, conocida por el alumno con anterioridad a la realización de la prueba.

- **Alumnado que quiera mejorar los resultados**, realizarán durante este periodo la mejora de las prácticas realizadas o resolución de nuevos casos prácticos o trabajos de investigación o prueba teórico-practica, etc.

Para la superación de la evaluación final, se informará al alumnado de los contenidos mínimos de los que se les examinará en la prueba final.
En el caso de que el alumno/a no superase esta evaluación final tendría que repetir el módulo en el próximo curso.

9.- Atención a la Diversidad

Partiremos desde la premisa de que no se pueden realizar adaptaciones curriculares significativas, ya que en una enseñanza de carácter profesional con un título homologado a nivel internacional, los objetivos del módulo son irrenunciables. Los objetivos se particularizan en los Resultados de Aprendizaje, los cuales deben ser evaluados. La calificación positiva para aprobar el módulo depende de la consecución de dichos resultados. Su no consecución inhabilitaría al alumno para superar el módulo.

La diversidad de alumnado en el aula hace que existan diferentes ritmos de aprendizaje. Para detectarlos realizaremos una evaluación inicial a principio de curso así como actividades de diagnóstico o evaluación de conocimientos previos en las distintas unidades didácticas a trabajar.

Se consideran los siguientes casos:

- Atención personalizada a los alumnos/as con un ritmo de aprendizaje más lento, ayudándoles en la resolución de problemas, dándoles más tiempo para la realización de ejercicios, prácticas, trabajos, y proponiéndoles actividades de refuerzo que les permitan la comprensión de los contenidos trabajados en clase.
- Proporcionar actividades complementarias y de ampliación a los alumnos/as más aventajados para ampliar conocimientos sobre los contenidos tratados y otros relacionados. También podrán implicarse en la ayuda a sus compañeros de clase como monitores en aquellas actividades en las que demuestren mayor destreza. Con esta medida se pretende además trabajar las habilidades sociales de los alumnos y alumnas, reforzando la cohesión del grupo y fomentando el aprendizaje colaborativo.

Se considera pues el "diseño para todos" como criterio general a aplicar en todas las unidades didácticas, distinguiendo los contenidos fundamentales de los complementarios, graduando la dificultad de las actividades, realizando diferentes agrupamientos, y por último, evaluando prioritariamente contenidos fundamentales y conforme a diferentes capacidades.

10.- Bibliografía y Enlaces Web de interés

10.1.- Libros de texto

Por un lado, se utilizaran los libros de texto publicados que desarrollan los contenidos del módulo:

- Seguridad Informática y Alta Disponibilidad
  Jesús Costas Santos
  Editorial Ra-ma (2011)

10.2.- Otras publicaciones

- El Arte de la Intrusión: como ser un hacker o evitarlos
  Kevin D. Mitnick “El Condor”
  Editorial Alfaomega ra-ma

- Destripa la red
  Carlos Minguez Pérez
  Anaya Multimedia, 2007

10.3.- Enlaces web de interés

Usaremos los siguientes enlaces web, entre otros:

- http://www.hispasec.com
- http://www.penetration-testing.com/
- http://www.inteco.es
- http://www.idg.es
- http://www.newsai.es
- http://www.accesor.com
- http://www.malwarebytes.org

Adicionalmente, se utilizarán artículos de revistas, documentos extraídos de la web y cualquier otro tipo de documentación de interés para los alumnos, en el campo de las bases de datos.