Programación del Módulo Profesional
“Seguridad y Alta Disponibilidad”
Del Ciclo Formativo de Grado Superior
“Administración de Sistemas Informáticos en Red”

Contenido

1 Objetivos generales del módulo profesional.

Los objetivos del módulo, según el BOE, son:

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

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

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

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

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

16. Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.

17. Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para resolver problemas y mantener una cultura de actualización e innovación.

21. Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.

2 Unidades de competencia asociadas al módulo profesional.

Según el BOE, las unidades de competencia son “Asegurar equipos informáticos” (UC0486_3) y “Administrar los dispositivos hardware del sistema” (UC0484_3) de la Cualificación Profesional de “Gestionar sistemas informáticos” (IFC152_3).

3 Contenidos y secuenciación

La duración del módulo, según el BOCM, es de 95 horas, repartidas en 6 horas semanales. En el presente curso**, las horas reales disponibles para docencia son 88: 42 en el primer trimestre y 46 en el segundo trimestre**.

Se prevé la siguiente distribución de tiempos:

PRIMER TRIMESTRE	42 horas
U.T. 0 Repaso del curso anterior y Preparación de la red virtual	5
U.T. 1 Principios de Seguridad y Alta Disponibilidad	5
U.T. 2 Seguridad pasiva	5
U.T. 3 Seguridad lógica	5
U.T. 4 Seguridad perimetral	20
EVALUACIÓN	2
SEGUNDO TRIMESTRE	46 horas
U.T. 5 Malware	5
U.T. 6 Criptografía	7
U.T. 7 Seguridad corporativa	5

U.T. 8 Alta Disponibilidad	21
U.T. 9 Legislación sobre seguridad.	2
EVALUACIÓN	4
EVALUACIÓN FINAL	2 horas

Antes de especificar los contenidos de cada Unidad, es necesario decir que podrían verse alterados debido a las necesidades de adaptación y que se abordarán en una parte significativa de una manera práctica.

El BOCM establece los siguientes contenidos, que han sido reestructurados en 9 Unidades Temáticas:

U.T. 1. Principios de Seguridad y Alta Disponibilidad	
Contenidos	
• Visión global de la seguridad informática. • Fiabilidad, confidencialidad, integridad y disponibilidad. • Elementos vulnerables en el sistema informático: hardware, software y datos. • Análisis de las principales vulnerabilidades de un sistema informático. • Amenazas. Tipos: físicas y lógicas. Tipos de ataques. • Protección. Valoración de los riesgos. Impactos y repercusión. Análisis forense.	

U.T. 2. Seguridad Pasiva	
Contenidos	
• Principios de la seguridad pasiva. • Copias de seguridad e imágenes de respaldo. Políticas de almacenamiento. Medios de almacenamiento externo. • Seguridad física y ambiental: Ubicación y protección física. Condiciones ambientales. Protección del hardware. Control de acceso físico. Plan de seguridad física. Plan recuperación en caso de desastres. • Sistemas de alimentación ininterrumpida. Funciones. Tipos.	

U.T. 3. Seguridad Lógica	
Contenidos	
• Principios de la seguridad lógica. • Control de acceso lógico. Políticas de contraseñas. Seguridad en gestores arranque. Seguridad en BIOS. Control de acceso al sistema operativo. • Política de usuarios y grupos. Autenticación para el acceso al sistema. Control de acceso a datos y aplicaciones. • Actualización de sistemas y aplicaciones.	

U.T. 4: Seguridad perimetral	
Contenidos	
• Elementos básicos de la seguridad perimetral. • Arquitecturas de seguridad perimetral • Cortafuegos. Características. Tipos. Instalación y configuración. Integración con otras tecnologías. • Proxies. Tipos. Características. Instalación y configuración.	

U.T. 5. Malware	
Contenidos	

- Software malicioso.
- Clasificación del malware. Métodos de infección.
- Protección y desinfección. Herramientas preventivas y paliativas. Pautas y prácticas seguras. Seguridad en la conexión con redes públicas. Seguridad en el particionado de discos.

U.T. 6. Criptografía	
Contenidos	
• Principios de criptografía. • Tipos de algoritmos de cifrado: de clave secreta o de clave pública. • Funciones de mezcla. • Firma electrónica. • Certificados digitales. • DNI electrónico.	

U.T. 7. Seguridad corporativa	
Contenidos	
• Amenazas y ataques. • Sistemas de detección de intrusos. • Riesgos potenciales de los servicios de red. Monitorización del tráfico de redes. • Comunicaciones seguras. IPsec, SSL/TSL, PGP, S/MIME... • VPN. Elementos de una VPN. Arquitecturas. Protocolos. • Redes inalámbricas. Seguridad en WAN.	

U.T. 8: Alta disponibilidad	
Contenidos	
• Definición y objetivos. • RAID. • Balanceo de carga. • Virtualización para alta disponibilidad. NAS virtual. • Análisis de configuraciones de alta disponibilidad.	

U.T. 9: Legislación sobre seguridad	
Contenidos	
• Legislación sobre protección de datos (LOPD) • Legislación sobre los servicios de la sociedad de la información y correo electrónico (LSSICE)	

4 Contenidos mínimos

Para superar el módulo es necesario **controlar**, como mínimo, los siguientes contenidos:

- Visión global de la seguridad informática. Elementos vulnerables.
- Análisis y valoración de riesgos de las principales vulnerabilidades, amenazas y ataques de un sistema informático.
- Copias de seguridad
- Almacenamiento externo.

- Seguridad física y lógica. Control de acceso físico y lógico.
- Sistemas de alimentación ininterrumpida.
- Software malicioso. Clasificación. Métodos de infección. Protección y desinfección.
- Criptografía de clave secreta o de clave pública. Funciones de mezcla. Firma electrónica. Certificados digitales.
- Sistemas de detección de intrusos. Monitorización del tráfico de redes.
- Comunicaciones seguras.
- VPN.
- Seguridad en WAN.
- Arquitecturas de seguridad perimetral.
- Cortafuegos.
- Proxies.
- Alta disponibilidad: RAID, balanceo de carga, virtualización.
- LOPD y LSSICE

5 Metodología y estrategias didácticas

Metodología

El profesor explicará a los alumnos la mayor parte de los contenidos, tanto teóricos como prácticos, del módulo. El resto deberán ser auto-aprendidos por ellos, de forma guiada o autónoma.

Los alumnos deberán generar memorias de las prácticas escogidas por el profesor, que el profesor evaluará.

Estrategia

Se busca que los alumnos:

- Disfruten del aprendizaje. Para lo cual es preciso hacerlo dinámico y participativo.
- Asuman la responsabilidad de su propio aprendizaje. Para ello, se les orientará para que se impliquen y que desarrollen su autonomía.

6 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 disponibilida 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 lasmedidas 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.

7 Procedimientos e instrumentos de evaluación

Se celebrará una sesión de evaluación por cada trimestre de formación en el centro educativo. La última tendrá la consideración de evaluación final ordinaria, por lo que no aparecerá en ningún acta de evaluación parcial; no obstante constará como parcial a efectos de la calificación del módulo.

La primera acabará el día 29-11-2017 y la segunda el día 1-3-2018, según lo aprobado en Claustro.

La evaluación se realizará agrupando las unidades temáticas por evaluaciones.

Los instrumentos de evaluación serán:

- **Prueba específica de evaluación:** Comprenderá todos los contenidos impartidos en esa evaluación.
- **Actitud**: Se observará a través de su presencia, su disposición, su conocimiento y su interés por aumentar y profundizar en la materia. Se medirá a través de la observación en clase del alumno y de la entrega de prácticas, en caso de ser considerado necesario por el profesor

8 Los criterios de calificación

La calificación del módulo se hará conforme a la siguiente tabla de convocatorias y pesos.

	Prueba específica de evaluación	Recuperación
Evaluación 1	100%	Sí
Evaluación 2	100%	No
Convocatoria ordinaria	100%	-
Convocatoria extraordinaria	100%	-

El profesor **podrá** proponer prácticas a los alumnos, orientadas a consolidar o profundizar en aspectos de la materia y servir como instrumento de evaluación. Cada práctica se definiría con una nota máxima. El alumno obtendría una valoración de dicha práctica y ese valor se sumaría al del examen de la evaluación correspondiente.

En cada evaluación se obtendrá una nota con una precisión de un decimal. Esta nota se redondeará: los decimales inferiores o iguales a 0,5 más bajo; los superiores, al más alto (con dos excepciones: la franja entre 4 y 5 se redondeará siempre a 4 y las notas inferiores a 1 se redondearán a 1). No obstante, en los futuros cálculos en los que se utilicen estos resultados del alumno, se empleará la nota previa al redondeo.

Las faltas de ortografía cometidas en todo tipo de escritos (ejercicios, prácticas, exámenes, etc.) se penalizarán, hasta un máximo de un punto, con arreglo al siguiente baremo:

- Cada error en el empleo de las grafías: 0'2 puntos.
- Cada error de acentuación o puntuación: 0'1 puntos

Además se han de tener en cuenta las siguientes consideraciones:

- **La nota por evaluaciones será la media ponderada de las notas de las dos evaluaciones.**
- La recuperación consistirá en una nueva prueba específica de evaluación. La nota final de la prueba específica de evaluación será la mejor de las dos notas.
- En el examen de la convocatoria ordinaria, sólo será necesario examinarse de las evaluaciones suspensas. Si lo están las dos, habrá un único examen de todo el módulo.
- El examen de la convocatoria extraordinaria abarcará todos los contenidos mínimos del módulo.
- **Para aprobar el módulo es imprescindible no presentar actitudes contrarias a las normas de convivencia**.
- **La calificación final del módulo será la media aritmética de las calificaciones obtenidas en las dos evaluaciones trimestrales, si tal nota es mayor o igual que 5. Si no lo es, será la nota obtenida en la convocatoria extraordinaria.**

9 Recursos didácticos

Se precisarán los siguientes medios:

- **Recursos de información:** No se usará libro de texto, por lo que la carga teórica se basará principalmente en las explicaciones del profesor, y las recomendaciones bibliográficas concretas para cada unidad (libros, artículos, revistas, páginas web…).

- **Recursos informáticos:** Los alumnos dispondrán de un ordenador a su disposición y de una cuenta de usuario en el servidor de dominio de la clase, con un directorio asociado en el que podrán depositar los ficheros que necesiten conservar en el aula. También podrán acceder al curso virtual de la plataforma Moodle, asociado al módulo.
- **Bibliografía**:
    - HACKER Edición 2006 – Justo Pérez Agudín y otros – Anaya Multimedia
    - Seguridad y Alta Disponibilidad – Jesús Costas – Ra-Ma
    - Seguridad y Alta Disponibilidad – Garceta

10 Atención a la diversidad y adaptaciones curriculares

En el caso en que este módulo sea cursado por un alumno con discapacidad, se realizará la adaptación de las actividades de formación, los criterios y los procedimientos de evaluación necesarios, de modo que se garantice su accesibilidad a las pruebas de evaluación; esta adaptación en ningún caso supondrá la supresión de objetivos, o resultados de aprendizaje que afecten a la competencia general del título. La adaptación curricular se archivará en el expediente del alumno.

11 Utilización de las TIC

Se hará uso intensivo de los recursos informáticos, como queda reflejado en el punto 9.

12 Actividades de recuperación de módulos profesionales pendientes

Este apartado no es de aplicación para este módulo.

13 Procedimiento para que el alumnado y sus familias conozcan los contenidos, criterios de evaluación, los criterios de calificación, los procedimientos y los instrumentos de evaluación

Se publicará la presente programación en la página web del Centro (www.iesjovellanos.org).

14 Actividades complementarias y extraescolares

Se tratará de realizar una visita guiada al Instituto Nacional de Tecnología Aeroespacial (INTA), situado en Torrejón de Ardoz.

15 Referencias

- **DECRETO 12/2010, de 18 de marzo**, por el que se establece para la Comunidad de Madrid el currículo del ciclo formativo de grado superior correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red (BOCM nº 89, de 15/04/2010).
- **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 (BOE nº 278, de 18/11/2009).
- **Orden 2694/2009, de 9 de junio**, por la que se regula el acceso, la matriculación, el proceso de evaluación y la acreditación académica de los alumnos que cursen en la Comunidad de Madrid la modalidad presencial de la formación profesional del sistema educativo establecida en la Ley Orgánica 2/2006, de 3 de mayo, de Educación (BOCM lunes 22 de Junio de 2009).
- **Proyecto Educativo de Centro**. IES Gaspar Melchor de Jovellanos, Fuenlabrada.