Contenido

IDENTIFICACIÓN

Ciclo: **SISTEMAS MICROINFORMÁTICOS Y REDES**
Módulo profesional: **Seguridad informática**
Código: **0226**
Duración: **105 horas**
Profesor/a: **Manuel Agüera Higueras**

Año: **2018/2019**

Introducción

El módulo de SEGURIDAD INFORMÁTICA forma parte del segundo curso del ciclo formativo de grado medio de Técnico en Sistemas Microinformáticos y Redes (SMR).

El desarrollo curricular viene dado por la ORDEN de 26 de junio de 2009, de la Consejera de Educación, Cultura y Deporte. Este módulo está dividido en dos unidades formativas:

—UF0226_12. Seguridad informática. Conceptos generales y formas pasivas. Duración: 45 horas.
—UF0226_22. Seguridad informática. Implementación de formas activas. Duración: 60 horas.

Su duración es de 105 horas lectivas por curso, en periodos de 5 horas semanales, las cuales serán teórico-prácticas.

Organización de las unidades, secuenciación y temporalización

Unidad didáctica	Título de la unidad didáctica	Contenidos de la unidad didáctica	Horas	Evaluación
1	**Introducción a la seguridad informática**	• Introducción • Seguridad informática y seguridad de la información • Principios de la seguridad informática • Políticas de seguridad • Planes de contingencia	4	1
2	**Seguridad física**	• Importancia de la seguridad física • Protección física de los equipos • Centros de procesos de datos	8	1
3	**Seguridad lógica**	• Concepto de seguridad lógica • Acceso a sistemas operativos y aplicaciones	12	1

		• Acceso a aplicaciones por Internet • Otras alternativas de gestión de identidades		
4	**Criptografía**	• Introducción a la criptografía • Cifrado de clave simétrica • Cifrado de clave asimétrica • Algoritmo de cifrado hash • Sistemas híbridos	13	1
5	**Aplicaciones de la criptografía**	• Aplicaciones prácticas de la criptografía • Firma digital • Certificados digitales • DNI electrónico • SSL y TLS • Cifrado de la información	13	1
6	**Software malicioso**	• Software malicioso • Clasificación del malware • Denegación de servicio • Publicidad y correo no deseado • Ingeniería social. Fraudes informáticos	10	2
7	**Medidas de protección contra el malware**	• Medidas de protección contra el software malicioso • Centros de protección y respuestas frente a amenazas • Buenas prácticas para protegerse del malware	14	2
8	**Gestión del almacenamiento**	• Gestión y políticas de almacenamiento • Dispositivos de almacenamiento • Almacenamiento redundante y distribuido • Copias de seguridad • Gestión de imágenes del sistema • Recuperación de datos eliminados	10	2
9	**Seguridad en redes**	• Vulnerabilidades de los servicios en red • Monitorización • Técnicas de protección • Protección de redes inalámbricas • Auditorías de seguridad en redes	11	2

10	**Normativa sobre seguridad y protección de datos**	• Protección de datos de carácter personal • Legislación sobre los servicios de la sociedad de la información y comercio electrónico • Sistemas de gestión de seguridad de la información	10	2

Resultados del aprendizaje, criterios de evaluación y contenidos

CICLO FORMATIVO DE GRADO MEDIO: **SISTEMAS MICROINFORMÁTICOS Y REDES**		
MÓDULO PROFESIONAL/UNIDAD FORMATIVA: **Seguridad informática**		
RESULTADO DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN **(MÍNIMOS EN NEGRITA)**	CONTENIDOS Se indica la unidad didáctica a la que hacen referencia o los contenidos específicos.
1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	**a) Se ha valorado la importancia de mantener la información segura.** **b) Se han descrito las diferencias entre seguridad física y lógica.** **c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.** **d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.** **e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.** f) Se han seleccionado los puntos de aplicación	**UD 1, 2 y 3**

	de los sistemas de alimentación ininterrumpida. g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso. **h) Se ha valorado la importancia de establecer una política de contraseñas.** i) Se han valorado las ventajas que supone la utilización de sistemas biométricos	
2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento. **b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).** **c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.** d) Se han descrito las tecnologías de almacenamiento redundante y distribuido. **e) Se han seleccionado estrategias para la realización de copias de seguridad.** f) Se ha tenido en cuenta la frecuencia y el esquema de rotación. **g) Se han realizado copias de seguridad con distintas estrategias.** **h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.** i) Se han utilizado medios de almacenamiento remotos y extraíbles. j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	**UD 8**
3. Aplica mecanismos de	**a) Se han seguido planes de contingencia**	

seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	**para actuar ante fallos de seguridad.** **b) Se han clasificado los principales tipos de software malicioso.** **c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.** **d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.** **e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.** f) Se han aplicado técnicas de recuperación de datos.	**UD 6, 7 y 9**
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	**a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.** **b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.** c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado. d) Se han aplicado medidas para evitar la monitorización de redes cableadas. **e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.** **f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.** **g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.** **h) Se ha instalado y configurado un**	**UD 4, 5, 6 Y 9**

	cortafuegos en un equipo o servidor.	
5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	**a) Se ha descrito la legislación sobre protección de datos de carácter personal.** **b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.** **c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.** **d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.** e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. f) Se han contrastado las normas sobre gestión de seguridad de la información.	**UD 10**

Criterios de calificación

La nota de cada evaluación corresponde a la **media ponderada** de las calificaciones obtenidas hasta el momento de la evaluación y desde principio de la misma, según la siguiente fórmula:

$$\boldsymbol{NotaEvaluación} = \frac{70 * EE + 30 * TCE}{100}$$

(EE) Nota en las pruebas objetivas teóricas de la Evaluación
(TCE) Nota de las tareas y cuestionarios realizados en clase o en casa.

Siendo las notas entre 1 y 10.

Para poder realizar la media ponderada en cada evaluación será imprescindible que la valoración particular de cada uno de los apartados anteriores (EE y TCE) sea **mínimo de 4**. En caso de no llegar al mínimo la nota de la evaluación será de un máximo de 3.

Además, se podrán realizar actividades en el aula o casa que deberán ser entregadas por el alumno **aunque no se les asigne calificación**. Serán de **obligada entrega** para superar la evaluación a la que pertenezcan. En caso de no entregar las mínimas obligatorias se dará por suspensa esa evaluación con una calificación de 3. Queda a elección del docente la decisión de la repetición de las entregas si considera que no se han cumplidos los mínimos requeridos en la tarea.

Se pretende dar una formación integral a nuestros alumnos, por lo que en las calificaciones se tendrá en cuenta **la expresión precisa y correcta** haciendo especial mención en la limpieza, orden, sintaxis y semántica de informes, proyectos y cuántos documentos sean requeridos al alumno.

NOTA FINAL: La nota final se puede obtener de las siguientes maneras:

1. De la **media aritmética de las dos evaluaciones** si estas son superiores a 4 puntos.
2. De la nota del examen de la convocatoria ordinaria de **junio** que consistirá en un examen final con todos los contenidos del curso separado por evaluaciones. Este examen lo debe realizar el alumno **si cumple** uno de los siguientes supuestos:
    1. Los alumnos con nota final **menor que 5** en la media de las evaluaciones:
        - Sólo deberán realizar las partes del examen o actividades correspondientes a las evaluaciones que hayan suspendido (nota inferior a 5).
    2. Los alumnos que tengan una nota **inferior a 4** puntos en al menos una de las evaluaciones:
        - Sólo deberán realizar las partes del examen o actividades correspondientes a las evaluaciones que hayan suspendido (nota inferior a 5). La nota máxima final será de un 3 en caso de no llegar a 4 en alguna evaluación.
    3. Los alumnos que hayan perdido el derecho a la evaluación continua (15% de las horas del módulo de ausencias injustificadas):
        - Tendrán que realizar todas las partes del examen de la convocatoria ordinaria de junio de 2019 así como las tareas o actividades obligatorias, independientemente de que hubieran aprobado alguna de las evaluaciones de la evaluación continua, ya que se ha perdido el derecho a esa modalidad de evaluación.
3. Los alumnos que no superen la convocatoria ordinaria de junio tendrán derecho a la convocatoria extraordinaria.

En el procedimiento de evaluación se tendrá en cuenta tanto el grado de conocimientos adquiridos sobre los contenidos, como el grado de consecución de las actividades propuestas, valorando en todo momento el esfuerzo realizado por el alumno/a así como los razonamientos empleados.

Para conocer el nivel alcanzado por el alumnado, en su aprendizaje se valorarán distintos aspectos como son: esfuerzo, grado de integración y colaboración con el grupo, investigación y desarrollo de métodos auxiliares, correcto manejo de material, utilización adecuada de conocimientos en la resolución de problemas, utilización de nuevos materiales, etc.

Todas las actividades propuestas deberán ser entregadas en la fecha que se indique y de forma obligatoria si así se indica, salvo las tareas o cuestionarios (TCE) que puedan quedarse sin entregar pero que tendrán una nota de 0 que sí mediará con el resto de actividades de su campo (y que al final deben mediar más de 4 puntos).

Procedimientos e instrumentos de evaluación

- **Pruebas escritas**: Se realizará una prueba escrita por evaluación en la que se valorará el grado de aprendizaje del alumno de los contenidos impartidos en clase.
- **Pruebas orales**: No se contemplan este curso.
- **Montajes y prácticas de proyectos**: No se contemplan este curso.
- **Otros instrumentos**: Los trabajos y actividades entregadas por el alumno, sean en mano o en línea en una plataforma habilitada para tal uso.