PROGRAMACIÓN DIDÁCTICA:

SEGURIDAD INFORMÁTICA (2º SMR)

PROFESOR: LUIS MANUEL DEL CERRO VILLALUENGA

1. Introducción

2. Objetivos

3. Contenidos (Asumiendo escenario de presencialidad)

4. Metodología y recursos (Asumiendo escenario de presencialidad)
    a. Tipos de actividades de E/A
    b. Agrupamiento del alumnado
    c. Organización de espacios y tiempos
    d. Fuentes bibliográficas, documentales y de información
    e. Recursos materiales

5. Evaluación (Asumiendo escenario de presencialidad)
    a. Criterios de evaluación
    b. Procedimientos de evaluación
    c. Criterios de calificación
    d. Medidas de recuperación y profundización
    e. Evaluación del proceso de enseñanza/aprendizaje

6. Alumnado con la materia pendiente (si procede)
    a. Seguimiento y actuaciones.
    b. Medios de comunicación con el alumnado.
    c. Evaluación.
        i. Criterios de evaluación
        ii. Procedimientos
        iii. Criterios de calificación

7. Atención al alumnado con necesidades específicas de atención educativa.

8. Actividades complementarias y extraescolares.

9. Indicadores (Asumiendo escenario de presencialidad).

1.Introducción

En el REAL DECRETO 1691/2007 de 14 de diciembre (BOE nº. 15 del 17 de enero de 2008) se establece el título de *Técnico en sistemas microinformáticos y redes* y se fijan sus enseñanzas mínimas. Este título queda identificado por los siguientes elementos:

- **Denominación:** Sistemas microinformáticos y redes.
- **Nivel:** Formación Profesional de grado medio.
- **Duración:** 2.000 horas.
- **Familia profesional:** Informática y comunicaciones.
- **Referente europeo:** CINE-3 (Clasificación Internacional Normalizada de la Educación).

2. Objetivos

Los objetivos generales de este ciclo formativo, especificados en el BOE nº 15 del 17 de enero de 2008, son los siguientes:

1. Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
2. Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.
3. Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
4. Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de la red.
5. Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
6. Interconectar equipos informáticos, dispositivos de red local y de conexión con redes de área extensa, ejecutando los procedimientos para instalar y configurar redes locales.
7. Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
8. Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
9. Interpretar y seleccionar información para elaborar documentación técnica y administrativa.

10. Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.
11. Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
12. Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
13. Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.
14. Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.
15. Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción.
16. Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.
17. Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
18. 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.

3. **Contenidos** (Asumiendo escenario de presencialidad)

Los contenidos se han estructurado de manera que quedan englobados en 8 Unidades de Trabajo:La siguiente tabla resume los períodos lectivos dedicados a cada unidad.

En cada uno se combinará una parte teórica con otra práctica. Duración: 104 horas.

Unidad	Temporalización
Unidad 1.Conceptos básicos de la seguridad informática	8
Unidad 2. Criptografía	32
Unidad 3. Hardware y almacenamiento	15
Unidad 4. Pentesting	14
Unidad 5. Cortafuegos	12

Unidad 6. Proxies	12

c. Distribución de las Unidades por evaluación:

Evaluación	**Unidad**
Primera (52 periodos lectivos)	Unidad 1.Conceptos básicos de la seguridad informática
	Unidad 2. Sistemas de identificación. Criptografía
	Unidad 3. Hardware y almacenamiento
Segunda (52 periodos lectivos)	Unidad 4. Pentesting
	Unidad 5.Cortafuegos
	Unidad 6. Proxies

4. Metodología y recursos (Asumiendo escenario de presencialidad)

4.1. Tipos de actividades de E/A

Los contenidos y prácticas a realizar por los alumnos, se transmitirán por los siguientes medios:

- Papás.
- Aula virtual de Educamos CLM.
- Blogs personales del profesor:

  https://seguridadfuensalida.blogspot.com/

- Google:
  - Classroom.

La materia se divide en clases teóricas y clases prácticas en el aula se distribuirán, siempre que se pueda, un alumno por ordenador.

No se debe interpretar la exposición oral como una metodología marcadamente expositiva sino como una forma de colaboración o de engranaje en la que, en algunos puntos, será el propio alumno el que individualmente o en grupos tenga que preparar e indagar sobre algún contenido propuesto y exponerlo al resto o realizar puestas en común con sus compañeros.

El nivel de profundización estará en función del grado inicial de formación de los alumnos en esta materia, incluyendo tanto teoría como práctica.

4.2. Agrupamiento del alumnado

1 alumno por ordenador

4.3. Organización de espacios y tiempos

Las clases se dan en periodos lectivos de 55 minutos.

4.4. Fuentes bibliográficas, documentales y de información

4.5. Recursos materiales

Los contenidos y prácticas a realizar por los alumnos, se transmitirán por los siguientes medios:

- Papás.
- Classroom de Google.

Las prácticas tendrán una fecha de entrega máxima y se podrá utilizar algún procedimiento telemático de evaluación si fuera necesario.

Recursos informáticos del aula.

Para los puestos de los alumnos:

16 Ordenadores clientes de prestaciones actuales. Estos equipos deberán estar interconectados en red con Windows 10.

Para el puesto del profesor:

- 1 Ordenador cliente de prestaciones actuales, conectado a la red, con Windows 10. (semejante al de los alumnos).
- Proyector de pantallas conectado al ordenador del profesor.

Sistemas operativos.

Sistema Servidor tipo Microsoft Windows 2003,2008,2016 Server. Sistema Operativo Microsoft Windows 10 y Ubuntu en cada uno de los puestos.

Sistema de protección Antivirus.

Antivirus Nod32 u otro.

Recursos bibliográficos.

No

5. Evaluación (Asumiendo escenario de presencialidad)

5.1. Criterios de evaluación

Se definen para cada uno de los resultados de aprendizaje.

1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades:

b) Se ha valorado la importancia de mantener la información segura.

c) Se han descrito las diferencias entre seguridad física y lógica.

d) Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.

e) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.

f) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.

g) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.

h) Se han indicado las características de una política de seguridad basada en listas de control de acceso.

i) Se ha valorado la importancia de establecer una política de contraseñas.

j) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar 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.

3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático:

a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.

b) Se han clasificado los principales tipos de software malicioso.

c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.

d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.

e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

f) Se han aplicado técnicas de recuperación de datos.

4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar 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 y utilizado sistemas de identificación como la firma electrónica o certificado digital, entre otros.

g) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar 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.

5.2. Procedimientos de evaluación

Se realizarán exámenes escritos de teoría, prácticas, trabajos y ejercicios durante todo el curso. Las prácticas podrán ser individuales o en grupo dependiendo lo que demanden las mismas.

Habrá un examen final al finalizar las clases para todos aquellos alumnos que tengan suspendida la asignatura.

5.3. Criterios de calificación

Los criterios de calificación se establecen en la siguiente tabla:

<table>
<tr><td colspan="3">1ª Ordinaria</td></tr>
<tr><td>Primera Evaluación</td><td>● Prácticas 20%
● Examen 80%</td><td rowspan="2">Calificación final:

Se calcula realizando la media aritmética de las dos evaluaciones. En el caso de alumnos suspensos o con pérdida de evaluación continua, esta calificación será la correspondiente a la media obtenida entre la calificación del examen final y la calificación obtenida en las prácticas entregadas</td></tr>
<tr><td>Segunda Evaluación</td><td>● Prácticas 20%
● Examen 80%</td></tr>
<tr><td colspan="3">Para aplicar los porcentajes en cada una de las evaluaciones, la calificación obtenida en cada una de las partes ha de ser MAYOR O IGUAL A 4; por debajo de esta calificación no se realizará el cálculo de porcentajes considerándose la evaluación como NO SUPERADA</td></tr>
</table>

Para considerar una evaluación como SUPERADA, la calificación obtenida en la misma debe ser MAYOR O IGUAL QUE 5, en caso contrario, la evaluación se considerará NO SUPERADA.
2ª Ordinaria: examen teórico y práctico

5.4. Medidas de recuperación y profundización

Durante el primer y segundo periodo evaluativo.

El alumno que no vaya adquiriendo los elementos de capacidad en este periodo será objeto de un seguimiento y refuerzo especial por parte del profesor. Si aún así no se consigue una nota positiva al final del periodo evaluativo queda a criterio del profesor la realización de pruebas de recuperación y evaluación en posteriores periodos evaluativos.

Durante el último periodo evaluativo.

El alumno que no vaya adquiriendo los elementos de capacidad en este periodo podrá, a criterio del profesor y atendiendo a los Proyectos curriculares del centro y del ciclo, realizar pruebas evaluativas para demostrar que ha adquirido las competencias básicas del módulo con el peso de calificación señalado en la programación.

Así mismo, los alumnos también tendrán que presentar aquellos trabajos que no hubieran presentado o que fueran desechados en el plazo solicitado.

Las pruebas de recuperación final de la primera evaluación ordinaria y la segunda evaluación ordinaria serán de aquellas que el alumno no haya superado y será una prueba escrita y en base a los mínimos exigibles de la evaluación.

5.5. Evaluación del proceso de enseñanza/aprendizaje

Al final del curso, se pasará una encuesta al alumnado para valorar el proceso.

6. Alumnado con la materia pendiente (si procede)

Seguimiento y actuaciones

Se hará uso de la herramienta de mensajería de la plataforma, foros abiertos en cada unidad de trabajo para que el alumnado pueda interactuar

Se utilizará también para organizar y poner a disposición del alumnado con la materia pendiente los contenidos de cada unidad de trabajo en formato electrónico.

Evaluación

La evaluación del alumnado con la materia pendiente sigue los mismos criterios de evaluación, calificación y superación que el resto del alumnado.

Los instrumentos de evaluación serán una prueba práctica que agrupe los distintos resultados de aprendizaje. Estas pruebas se realizan antes de la primera evaluación ordinaria.

Si, tras la primera evaluación ordinaria, el alumno no ha superado el módulo, se realizarán nuevas pruebas prácticas que agrupen los resultados de aprendizaje no superados.

7. Atención al alumnado con necesidades específicas de atención educativa.

La normativa impide las adaptaciones curriculares. Para atender las necesidades específicas de apoyo educativo, se propone:

A nivel de aula:

- Se fomentará el trabajo en grupo para favorecer la inclusión.
- Se propondrán sesiones voluntarias de refuerzo de contenidos cuando se considere necesario (en el tiempo de recreo).
- Se adaptarán los espacios del aula, despejando rutas y reservando espacios para casos la entrada de sillas de ruedas y reservando equipos y espacios más cercanos a la pizarra o profesor para alumnado con dificultades visuales o auditivas.

A nivel individual, se pueden tomar medidas como:

- Adaptaciones metodológicas, si fueran necesarias, a cada caso.

- Sesiones voluntarias de refuerzo (en el tiempo de recreo).
- Adaptaciones temporales y/o procedimentales en la entrega de prácticas y pruebas.

Dispondremos de elementos (teclados, ratones o monitores) adaptados a necesidades específicas, así como facilitar el uso de los elementos propios de interacción, si dispone de ellos.

8. Actividades complementarias y extraescolares.

No se contemplan.

9. Indicadores (Asumiendo escenario de presencialidad).

RELACIÓN ENTRE CRITERIOS DE EVALUACIÓN, INDICADORES Y CRITERIOS DE CALIFICACIÓN						
RESULTADOS DEL APRENDIZAJE	CRITERIOS DE EVALUACIÓN	%	**INDICADORES**	**% de peso sobre el criterio**	**Procedimientos de evaluación**	**COMPETENCIAS PROFESIONALES**
Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades.	*k)* Se ha valorado la importancia de mantener la información segura. *l)* Se han descrito las diferencias entre seguridad física y lógica. *m)* Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores. *n)* Se ha identificado la necesidad de proteger físicamente los sistemas informáticos. *o)* Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida. *p)* Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida. *q)* Se han indicado las características de una política de seguridad basada en listas de control de acceso. *r)* Se ha valorado la importancia de establecer una política de contraseñas. *s)* Se han valorado las ventajas que supone la utilización de sistemas biométricos.	**25%**	Identifica y comprende los requisitos y mecanismos de seguridad de un sistema informático	**30%**	Exámenes, prácticas y trabajos	UC959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas microinformáticos. UC_958_2 Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes. UC_957_2 Mantener y regular el subsistema físico en sistemas informáticos.
			Reconoce la diferencia entre seguridad física y lógica	**20%**	Exámenes, prácticas y trabajos	
			Comprende el funcionamiento de los sistemas de alimentación ininterrumpida, así como listas de control de acceso y políticas de contraseñas	**40%**	Exámenes, prácticas y trabajos	
			Valora la importancia de utilizar sistemas biométricos	**10%**	Exámenes, prácticas y trabajos	
Gestionar dispositivos de		**25%**	Identifica los principales mecanismos de almacenamiento	**20 %**	Exámenes, prácticas y trabajos	

almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información.	*k)* Se ha interpretado la documentación técnica relativa a la política de almacenamiento. *l)* Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad entre otros). *m)* Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red. *n)* Se han descrito las tecnologías de almacenamiento redundante y distribuido. *o)* Se han seleccionado estrategias para la realización de copias de seguridad. *p)* Se ha tenido en cuenta la frecuencia y el esquema de rotación. *q)* Se han realizado copias de seguridad con distintas estrategias. *r)* Se han identificado las características de los medios de almacenamiento remotos y extraíbles. *s)* Se han utilizado medios de almacenamiento remotos y extraíbles. *t)* Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.		Comprende y sabe aplicar los principales mecanismos de almacenamiento	**80 %**	Exámenes, prácticas y trabajos	UC959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas microinformáticos. UC_958_2 Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes. UC_957_2 Mantener y regular el subsistema físico en sistemas informáticos

Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático. .	*g)* Se han seguido planes de contingencia para actuar ante fallos de seguridad. *h)* Se han clasificado los principales tipos de software malicioso. *i)* Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades. *j)* Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas. *k)* Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso. *l)* Se han aplicado técnicas de recuperación de datos.	**35 %**	Identifica los principales mecanismos de seguridad activa	**30%**	Exámenes, prácticas y trabajos	UC959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas microinformáticos. UC_958_2 Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes. UC_957_2 Mantener y regular el subsistema físico en sistemas informáticos
			Comprende y sabe aplicar los principales mecanismos de seguridad activa	**70%**	Exámenes, prácticas y trabajos	
Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico.	*h)* Se ha identificado la necesidad de inventariar y controlar los servicios de red. *i)* Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información. *j)* Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado. *k)* Se han aplicado medidas para evitar la monitorización de redes cableadas.	**10%**	Identifica y comprende las principales técnicas de monitorización de redes	20 %	Exámenes escritos, prácticas y trabajos	UC959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas microinformáticos. UC_958_2 Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes. UC_957_2 Mantener y regular el subsistema físico en sistemas informáticos
			Clasifica y valora las propiedades de los protocolos utilizados en redes inalámbricas	**20%**	Exámenes escritos, prácticas y trabajos	
			Instala y configura cortafuegos y proxies.	**60%**	Exámenes escritos, prácticas y trabajos	

	l) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas. *m)* Se han descrito y utilizado sistemas de identificación como la firma electrónica o certificado digital, entre otros. *n)* Se ha instalado y configurado un cortafuegos en un equipo o servidor.					
Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento	6. Se ha descrito la legislación sobre protección de datos de carácter personal. 7. Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. 8. Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. 9. Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen. 10. Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. 11. Se han contrastado las normas sobre gestión de seguridad de la información.	**5%**	Comprende y contrasta la legislación sobre protección de datos	**100%**	Exámenes escritos, prácticas y trabajos	UC959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas microinformáticos. UC_958_2 Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de clientes. UC_957_2 Mantener y regular el subsistema físico en sistemas informáticos