“SEGURIDAD INFORMÁTICA” 2º SMR
CURSO 2019/2020

1. Evaluación FORMACIÓN PRESENCIAL

Criterios de calificación

Para la superación de este módulo formativo el alumno debe alcanzar todos los resultados de aprendizaje establecidos en el decreto 107/2009, de 04/08/2009, por el que se establece el currículo del ciclo formativo de grado medio correspondiente al Título de Técnico o Técnica en Sistemas Microinformáticos y Redes, en la comunidad autónoma de Castilla-La Mancha.

A continuación se establecen los indicadores que permitirán evaluar los diferentes resultados de aprendizaje así como su calificación:

1. Introducción a la seguridad informática			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Notas de clase
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico	b) Se ha identificado la necesidad de inventariar y controlar los servicios de red.		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.		Pruebas escritas Pruebas prácticas Notas de clase
5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento	d) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada		Pruebas escritas Pruebas prácticas Notas de clase

2. Seguridad física			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas prácticas Notas de clase
	b) Se han descrito las diferencias entre seguridad física y lógica.		Pruebas escritas Pruebas prácticas Notas de clase

	c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores		Pruebas escritas Pruebas prácticas Notas de clase
	d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.		Pruebas escritas Pruebas prácticas Notas de clase
	e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.		Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida		Pruebas escritas Pruebas prácticas Notas de clase

3. Seguridad lógica			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han descrito las diferencias entre seguridad física y lógica.		Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.		Pruebas escritas Pruebas prácticas Notas de clase
	h) Se ha valorado la importancia de establecer una política de contraseñas.		Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.		Pruebas escritas Notas de clase

4. Criptografía			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes y robos de información.		Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital entre otros.		Pruebas escritas Pruebas prácticas Notas de clase

5. Aplicaciones de la criptografía			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.		Pruebas escritas Pruebas prácticas Notas de clase
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes y robos de información.		Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital entre otros		Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros		Pruebas escritas Pruebas prácticas Notas de clase

6. Software malicioso			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	b) Se han clasificado los principales tipos de software malicioso.		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.		Pruebas escritas Pruebas prácticas Notas de clase
	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.		Pruebas escritas Pruebas prácticas Notas de clase
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.		Pruebas prácticas Notas de clase
	c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado		Pruebas prácticas Notas de clase

7. Medidas de protección contra el malware			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.		Pruebas prácticas Notas de clase
	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.		Pruebas prácticas Notas de clase
	e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.		Pruebas escritas Pruebas prácticas Notas de clase
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.		Pruebas escritas Pruebas prácticas Notas de clase
	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.		Pruebas prácticas Notas de clase

8. Gestión del almacenamiento			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
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.		Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red		Pruebas escritas Pruebas prácticas Notas de clase

	d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.		Pruebas escritas Pruebas prácticas Notas de clase
	e) Se han seleccionado estrategias para la realización de copias de seguridad.		Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han tenido en cuenta la frecuencia y el esquema de rotación.		Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han realizado copias de seguridad con distintas estrategias.		Pruebas escritas Pruebas prácticas Notas de clase
	h) Se han identificado las características de los medios de almacenamiento remoto y extraíble.		Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han utilizado medios de almacenamiento remotos y extraíbles.		Pruebas escritas Pruebas prácticas Notas de clase
	j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.		Pruebas prácticas Notas de clase

9. Seguridad en redes (9 horas)			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Pruebas prácticas Notas de clase
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.		Pruebas escritas Pruebas prácticas Notas de clase
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.		Pruebas escritas Pruebas prácticas Notas de clase
	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.		Pruebas escritas Pruebas prácticas Notas de clase
	d) Se han aplicado medidas para evitar la monitorización de redes cableadas.		Pruebas escritas Pruebas prácticas Notas de clase
	e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.		Pruebas escritas Pruebas prácticas Notas de clase

	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor		Pruebas prácticas Notas de clase

10. Normativa sobre seguridad y protección de datos (6 horas)			
Resultados de aprendizaje	**Criterios de evaluación**	**CRITERIOS DE CALIFICACIÓN**	**INSTRUMENTO DE EVALUACIÓN**
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.		Pruebas escritas Notas de clase
	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.		Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.		Pruebas escritas Pruebas prácticas Notas de clase
	d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.		Pruebas escritas Pruebas prácticas Notas de clase
	e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.		Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han contrastado las normas sobre gestión de la seguridad de la información.		Pruebas escritas Pruebas prácticas Notas de clase

Cada uno de los resultados de aprendizaje tendrá una calificación proporcional según:

RESULTADOS DE APRENDIZAJE	CRITERIOS DE CALIFICACIÓN	EVALUADO EN LAS UNIDADES DE TRABAJO
1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades	**30 %**	**UT 1, UT 2, UT 3, UT 5, UT 6. UT 7, UT 9**
2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	**15 %**	**UT 8, UT 3**
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático	**20 %**	**UT 3, UT 5, UT 6, UT 7, UT 9**

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico	**25 %**	**UT 1, UT 4, UT 5, UT 6, UT 7, UT 9**
5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	**10 %**	**UT 10**

Al considerar que cada resultado de aprendizaje tiene la proporción asignada en la nota final del curso, todas las pruebas escritas, pruebas prácticas y notas de clase notas obtenidas nos llevaran a obtener una nota según cada uno de los resultados de aprendizaje y su proporción. Sólo se hará media si para cada resultado de aprendizaje se obtuvo una nota superior o igual a 5. Las calificaciones serán un número entero entre 1 y 10, lo cual implica, que una vez realizada la media aritmética para obtener una nota, sólo se tomará la parte entera de la misma, despreciando los decimales sin aplicar ningún tipo de redondeo.

Si alguna práctica se suspende o no se entrega a tiempo, implica que un resultados de aprendizaje no se supera, por tanto deberá ser corregida o entregada antes de realizar la preceptiva Evaluación trimestral o final. No hacerlo así lleva consigo no tener superado sus resultados de aprendizaje, por tanto no ser calificado positivamente.

La nota de las evaluaciones parciales se obtendrá valorando los criterios de evaluación y su ponderación en los resultados de aprendizaje impartidos en cada evaluación.

Si el número de faltas superara el 20% del módulo el alumno perderá el derecho a evaluación continua y deberá presentarse a una prueba final de todos los indicadores incluidos en el módulo.

Criterios de recuperación

En la 2ª evaluación (antes de acceder a la FCT) y en junio, habrá una prueba escrita para dar al alumno la posibilidad de recuperar los resultados de aprendizaje no superados.

Para aquellos alumnos y alumnas que hayan perdido el derecho a la evaluación continua se realizará, en las mismas fechas, una prueba final que incluirá los indicadores de todo el módulo.

Para acceder a dicha prueba, cualquier alumno, es necesario haber presentado con anterioridad todas las prácticas y ejercicios pedidos a los alumnos durante el desarrollo del curso.

La calificación máxima obtenida en una prueba de recuperación siempre será de 5, ya que la prueba siempre versara sobre los indicadores mínimos exigibles del módulo.

2. Evaluación FORMACIÓN SEMIPRESENCIAL,

Entendemos que la Formación semipresencial no trae consigo variaciones con respecto a la Evaluación considerada en la Formación presencial, excepto en situaciones individualizadas, si un alumno ha mostrado dejadez en el seguimiento diario no es lo mismo a que un alumno por

enfermedad o confinamiento no haya podido lleva a cabo un completo seguimiento del proceso de enseñanza, por tanto, la evaluación debe tener en cuenta cada situación.

3. Evaluación FORMACIÓN NO PRESENCIAL.

En esta situación los exámenes serán online, no podemos precisar en estos momentos si orales o escritos. Para que estos exámenes ejerzan menos presión sobre los alumnos, durante el tiempo de confinamiento se ampliaran los ejercicios y prácticas que los alumnos deben entregar y así tener en cuenta su calificación para el momento de obtener las notas finales.

Para la superación de este módulo formativo el alumno debe alcanzar los resultados de aprendizaje establecidos en la programación de acuerdo con lo establecido en el decreto del currículo de este ciclo, y para los criterios de recuperación se toma como base lo expresado en su epígrafe