CICLO FORMATIVO DE GRADO SUPERIOR "ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED"

"SEGURIDAD y ALTA DISPONIBILIDAD"

CURSO 2019-2020

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 200/2010, de 03/08/2010, por el que se establece el currículo del Ciclo Formativo de Grado Superior correspondiente al título de Técnico o Técnica Superior en Administración de Sistemas Informáticos en Red, en la Comunidad Autónoma de Castilla-La Mancha (Diario oficial del 6 de agosto). A continuación se establecen los indicadores que permitirán evaluar los diferentes resultados de aprendizaje así como su calificación:

U. T. 1. La seguridad informática		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO 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	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han descrito las diferencias entre seguridad física y lógica.	Pruebas escritas Notas de clase
	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	Pruebas escritas Notas de clase
	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han identificado las fases del análisis forense ante ataques a un sistema.	Pruebas escritas Pruebas prácticas Notas de clase

	j) Se han identificado las herramientas hardware y software para realizar un análisis forense.	Pruebas prácticas Notas de clase
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	Pruebas escritas Notas de clase
	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.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	Pruebas escritas Pruebas prácticas Notas de clase

U. T. 2. Medidas de seguridad pasiva

Resultados de aprendizaje	Criterios de evaluación	INSTRUMENTO 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	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han descrito las diferencias entre seguridad física y lógica.	Pruebas escritas Notas de clase
	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	Pruebas escritas Notas de clase
	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	Pruebas escritas Notas de clase
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	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.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	Pruebas escritas Pruebas prácticas Notas de clase

	f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	Pruebas escritas Pruebas prácticas Notas de clase
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase

U. T. 3. Dispositivos de almacenamiento y copias de seguridad		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO 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	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	Pruebas escritas Notas de clase
	g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	Pruebas escritas Pruebas prácticas Notas de clase
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	Pruebas escritas Notas de clase

ante amenazas o ataques al sistema.	f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	Pruebas escritas Pruebas prácticas Notas de clase
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	Pruebas escritas Pruebas prácticas 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 el deber de poner a disposición de las personas los datos personales que les conciernen.	Pruebas escritas Pruebas prácticas Notas de clase

	f) Se han contrastado las normas sobre gestión de seguridad de la información	Pruebas escritas Pruebas prácticas Notas de clase

U. T. 4. Aseguramiento de la privacidad		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO 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	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han descrito las diferencias entre seguridad física y lógica.	Pruebas escritas Notas de clase
	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	Pruebas escritas Notas de clase
	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	e) Se han adoptado políticas de contraseñas.	Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	Pruebas escritas Pruebas prácticas Notas de clase
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	Pruebas escritas Notas de clase

contramedidas ante amenazas o ataques al sistema.	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.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	Pruebas escritas Pruebas prácticas Notas de clase
	g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	Pruebas escritas Pruebas prácticas Notas de clase

U.T. 5. Medidas de seguridad activa		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO 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.	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	Pruebas escritas Pruebas prácticas Notas de clase
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante	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.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	Pruebas escritas Pruebas prácticas Notas de clase

amenazas o ataques al sistema.	d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	Pruebas escritas Pruebas prácticas Notas de clase
	e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	Pruebas escritas Pruebas prácticas Notas de clase
	h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.	Pruebas escritas Pruebas prácticas Notas de clase
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad	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.	

U. T. 6. Cortafuegos en equipos y servidores

Resultados de aprendizaje	Criterios de evaluación	INSTRUMENTO DE EVALUACIÓN
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	a) Se han descrito las características, tipos y funciones de los cortafuegos.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	Pruebas prácticas Notas de clase
	d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	Pruebas prácticas Notas de clase

	e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	Pruebas escritas Pruebas prácticas Notas de clase
	f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	Pruebas prácticas Notas de clase
	g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	Pruebas prácticas Notas de clase
	h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos	Pruebas escritas Pruebas prácticas Notas de clase

U. T. 7. Despliegue de servidores proxy		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO DE EVALUACIÓN**
5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio	a) Se han identificado los tipos de «proxy», sus características y funciones principales.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se ha instalado y configurado un servidor «proxy-cache».	Pruebas prácticas Notas de clase
	c) Se han configurado los métodos de autenticación en el «proxy».	Pruebas prácticas Notas de clase
	d) Se ha configurado un «proxy» en modo transparente.	Pruebas prácticas Notas de clase
	e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.	Pruebas prácticas Notas de clase
	f) Se han solucionado problemas de acceso desde los clientes al «proxy».	Pruebas prácticas Notas de clase
	g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.	Pruebas prácticas Notas de clase
	h) Se ha configurado un servidor «proxy» en modo inverso	Pruebas prácticas Notas de clase

	i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».	Pruebas escritas Pruebas prácticas Notas de clase

U. T. 8. ALTA DISPONIBILIDAD		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO DE EVALUACIÓN**
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase
	b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	Pruebas escritas Pruebas prácticas Notas de clase
	c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase
	d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	Pruebas prácticas Notas de clase
	e) Se ha implantado un balanceador de carga a la entrada de la red interna.	Pruebas prácticas Notas de clase
	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	Pruebas prácticas Notas de clase
	g) Se ha evaluado la utilidad de los sistemas de «clúster» para aumentar la fiabilidad y productividad del sistema.	Pruebas escritas Pruebas prácticas Notas de clase
	h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	Pruebas escritas Pruebas prácticas Notas de clase
	i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	Pruebas escritas Pruebas prácticas Notas de clase

U.T. 9. Cumplimiento de la legislación y de las normas sobre seguridad		
Resultados de aprendizaje	**Criterios de evaluación**	**INSTRUMENTO DE EVALUACIÓN**

7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	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 Notas de clase
	d) Se ha contrastado el deber 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 Notas de clase
	f) Se han contrastado las normas sobre gestión de seguridad de la información.	Pruebas escritas Notas de clase
	g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	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. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo	**25 %**	**UT 1, UT 2, UT3**
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema	**25%**	**UT 1, UT3, UT4, UT5**
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad	**10 %**	**UT 5**
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus	**10 %**	**UT 6**

prestaciones y controlando el tráfico hacia la red interna		
5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio	**5 %**	**UT 7**
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	**10 %**	**UT 8**
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	**15 %**	**UT 9**

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.

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.

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