



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Ciclo Formativo: Administración de Sistemas Informáticos en Red
Módulo Profesional: Seguridad y Alta Disponibilidad

RA1	Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.		20%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
15	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	Tarea individual	100
5	b) Se han descrito las diferencias entre seguridad física y lógica.	Tarea individual	100
5	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	Tarea individual	100
5	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	Tarea individual	100
5	e) Se han adoptado políticas de contraseñas.	Tarea individual	100
5	f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	Tarea individual	100
5	g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	Tarea individual	100
5	h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.	Tarea práctica individual	50
		FEM	50
5	i) Se han identificado las fases del análisis forense ante ataques a un sistema.	Tarea individual	100
5	j) -se han analizado evidencias forenses para obtener información relevante.	Tarea individual	100
5	k) Se han descrito los tipos de criptosistemas y reconocido los algoritmos crittográficos seguros.	Tarea individual	100
10	l) Se han identificado los tipos de sistemas de alimentación ininterrumpida.	Prueba individual	100



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Ciclo Formativo: Administración de Sistemas Informáticos en Red
Módulo Profesional: Seguridad y Alta Disponibilidad

RA1	Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.		20%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
15	m) Se ha calculado la potencia necesaria del sistema de alimentación ininterrumpida en función de la carga	Prueba individual	100
5	n) Se han analizado estrategias de copias de seguridad.	Trabajo de investigación	100
5	ñ) Se han realizado copias de seguridad	Trabajo de investigación	100

RA2	Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.		20%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
5	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	Tarea práctica	100
10	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.	Tarea práctica	100
10	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	Tarea práctica	50
		FEM	50
20	d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	Tarea práctica	100
20	e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	Tarea práctica	100
10	f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un	Tarea práctica	100



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Administración de Sistemas Informáticos en Red
 Módulo Profesional: Seguridad y Alta Disponibilidad

RA2	Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.		20%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
	entorno de trabajo basado en el uso de redes públicas.		
5	g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	Tarea práctica	100
10	h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	Tarea práctica	100
10	i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.	Tarea práctica	50
		FEM	50

RA3	Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
10	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	Trabajo investigación	100
10	b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	Trabajo investigación	50
		FEM	50
10	c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.	Tarea práctica	100
17	d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.	Tarea práctica	100
18	e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	Tarea práctica	100



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Ciclo Formativo: Administración de Sistemas Informáticos en Red
Módulo Profesional: Seguridad y Alta Disponibilidad

RA3	Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
15	f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.	Tarea práctica	100
20	g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	Tarea práctica	100

RA4	Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
10	a) Se han descrito las características, tipos y funciones de los cortafuegos.	Tarea de investigación	100
10	b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	Tarea de investigación	100
15	c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	Tarea práctica	100
17	d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	Tarea práctica	100
12	e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	Tarea práctica	50
		FEM	50
12	f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	Tarea práctica	100
12	g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	Tarea práctica	100
12		Tarea práctica	50



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Administración de Sistemas Informáticos en Red
 Módulo Profesional: Seguridad y Alta Disponibilidad

RA4	Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
	h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	FEM	50

RA5	Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
10	a) Se han identificado los tipos de «proxy», sus características y funciones principales.	Tarea de investigación	100
15	b) Se ha instalado y configurado un servidor «proxy-cache».	Tarea práctica	100
10	c) Se han configurado los métodos de autenticación en el «proxy».	Tarea práctica	100
10	d) Se ha configurado un «proxy» en modo transparente.	Tarea práctica	100
10	e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.	Tarea práctica	100
10	f) Se han solucionado problemas de acceso desde los clientes al «proxy».	Tarea práctica	100
15	g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.	Tarea práctica	100
10	h) Se ha configurado un servidor «proxy» en modo inverso.	Tarea práctica	100
10	i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».	Tarea práctica	50
		FEM	50



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Administración de Sistemas Informáticos en Red
 Módulo Profesional: Seguridad y Alta Disponibilidad

RA6	Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.		15%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
10	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	Reto	50
		FEM	50
10	b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	Reto	100
10	c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	Reto	100
15	d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	Reto	100
15	e) Se ha implantado un balanceador de carga y “proxy” inverso a la entrada de la red interna, gestionando certificados y repartiendo las conexiones de uno o varios clústeres de servicios.	Reto	100
15	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	Tarea práctica	100
10	g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.	Tarea práctica	100
10	h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	Reto	100
5	i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	Tarea práctica	50
		FEM	50



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Ciclo Formativo: Administración de Sistemas Informáticos en Red
Módulo Profesional: Seguridad y Alta Disponibilidad

RA7	Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.		5%
%CE	Criterios de evaluación	Instrumentos de evaluación	%IE
20	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	Prueba teórica	100
10	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	Trabajo investigación	100
20	c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	Trabajo investigación	100
10	d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	Trabajo investigación	100
20	e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	Trabajo investigación	100
10	f) Se han contrastado las normas sobre gestión de seguridad de la información.	Trabajo investigación	100
10	g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	Trabajo investigación	50
		FEM	50