

<b>Seguridad informática</b>			
<b>Teoría</b>	<b>RA</b>	<b>CE</b>	
	30,00 %		<b>1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.</b>
X		12,00 %	a) Se ha valorado la importancia de mantener la información segura.
X		12,00 %	b) Se han descrito las diferencias entre seguridad física y lógica.
X		12,00 %	c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
X		12,00 %	d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
		10,00 %	e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
		10,00 %	f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
X		12,00 %	g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
		10,00 %	h) Se ha valorado la importancia de establecer una política de contraseñas.
		10,00 %	i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
<b>Teoría</b>	<b>RA</b>	<b>CE</b>	
	10,00 %		<b>2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.</b>
		10,00 %	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
X		10,00 %	b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
X		10,00 %	c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
X		10,00 %	d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.
X		10,00 %	e) Se han seleccionado estrategias para la realización de copias de seguridad.
X		10,00 %	f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
		10,00 %	g) Se han realizado copias de seguridad con distintas estrategias.
X		10,00 %	h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
		10,00 %	i) Se han utilizado medios de almacenamiento remotos y extraíbles.
		10,00 %	j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.
<b>Teoría</b>	<b>RA</b>	<b>CE</b>	
	25,00 %		<b>3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.</b>
X		15,00 %	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
X		15,00 %	b) Se han clasificado los principales tipos de software malicioso.
X		15,00 %	c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
X		15,00 %	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
		20,00 %	e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.
		20,00 %	f) Se han aplicado técnicas de recuperación de datos.
<b>Teoría</b>	<b>RA</b>	<b>CE</b>	
	25,00 %		<b>4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.</b>
X		10,00 %	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.
X		20,00 %	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.

UNIDAD

1

1

2

2

5

2

3

3

2

8

8

8

8

8

8

8

8

8

8

7

6

6

5

6

7

9

4

## PropuestaSI

X		10,00 %	c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	3
		10,00 %	d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	9
X		10,00 %	e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	9
X		20,00 %	f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	4
		10,00 %	g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	5
		10,00 %	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	9
<b>Teoría</b>	<b>RA</b>	<b>CE</b>		
	10,00 %		<b>5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.</b>	
X		15,00 %	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	10
X		15,00 %	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	10
X		15,00 %	c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	10
		20,00 %	d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	10
X		15,00 %	e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	10
		20,00 %	f) Se han contrastado las normas sobre gestión de seguridad de la información.	10

100,00 %

PropuestaSI