TABLA 8: CE y Cb

Resultado de Aprendizaje	**RA 1.** Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	Adopción de pautas de seguridad informática.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	− Fiabilidad, confidencialidad, integridad y disponibilidad.	Contenidos Básicos		Valoración de la importancia de las propiedades de seguridad en los sistemas informáticos
	b) Se han descrito las diferencias entre seguridad física y lógica.	− Seguridad física y ambiental: • Ubicación y protección física de los equipos y servidores. • Sistemas de alimentación ininterrumpida. − Seguridad lógica: • Criptografía. • Listas de control de acceso. • Establecimiento de políticas de contraseñas.		Conocimiento de seguridad física y lógica y sus formas de implementación para determinar las diferencias entre ambas.	

		• Políticas de almacenamiento. • Copias de seguridad e imágenes de respaldo. • Medios de almacenamiento.			
	c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	− Análisis de las principales vulnerabilidades de un sistema informático.		Enumeración y descripción de las vulnerabilidades de un sistema informático según su tipología y origen.	
	d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	• Amenazas lógicas.			Adopción de pautas para detectar técnicas de ingeniería social y fraudes.
	e) Se han adoptado políticas de contraseñas.	• Establecimiento de políticas de contraseñas.		Aplicación de políticas de contraseñas.	
	f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.				Identificación de los usos actuales y futuros de los sistemas biométricos.
	g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	• Criptografía.		Aplicación de criptografía en el almacenamiento y transmisión de la información.	
	h) Se ha reconocido la necesidad de establecer un plan integral de protección	− Elementos básicos de la seguridad perimetral.			Asimilar la conveniencia de planes integrales de protección perimetral en

	perimetral, especialmente en sistemas conectados a redes públicas.	− Perímetros de red. Zonas desmilitarizadas.			sistemas conectados a redes públicas.
	i) Se han identificado las fases del análisis forense ante ataques a un sistema.	− Análisis forense en sistemas informáticos.		Enumeración y descripción de las fases de análisis forense ante ataques a un sistema.	

Resultado de Aprendizaje	**RA2.** Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	Adopción de pautas de seguridad informática.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	− Amenazas. Tipos: • Amenazas físicas. • Amenazas lógicas.	Contenidos Básicos	Enumeración y descripción de amenazas lógicas.	
	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.	• Actualización de sistemas y aplicaciones.			Asimilación de la importancia de verificar el origen, autenticidad y actualización del S.O. y de las aplicaciones que se instalan.
	c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	• Anatomía de ataques y análisis de software malicioso. • Herramientas preventivas. Instalación y configuración. • Herramientas paliativas. Instalación y configuración.		Enumeración y descripción de ataques más habituales, así como medidas preventivas y paliativas.	

	d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	− Ataques y contramedidas en sistemas personales: • Clasificación de los ataques.		Análisis de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	
	e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	• Herramientas preventivas. Instalación y configuración. • Herramientas paliativas. Instalación y configuración.		Instalación de aplicaciones para la detección y eliminación de software malicioso.	
	f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	• Seguridad en la conexión con redes públicas. • Pautas y prácticas seguras.		Uso de técnicas de cifrado, firmas y certificado digitales en en redes públicas.	
	g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	• Seguridad en los protocolos para comunicaciones inalámbricas.		Evaluación de las medidas de seguridad de los protocolos en redes inalámbricas.	
	h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	• Riesgos potenciales de los servicios de red.			Reconocimiento de la necesidad de inventariar y controlar los servicios de red para evaluar los riesgos.
	i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.	• Monitorización del tráfico en redes.		Enumeración y descripción de las características de los	

				sistemas de detección de intrusos.	

Resultado de Aprendizaje	**RA3.** Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	Implantación de técnicas de acceso remoto. Seguridad perimetral.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	− Elementos básicos de la seguridad perimetral.	Contenidos Básicos	Descripción de sistemas con conexión a redes públicas que aplican seguridad en la red interna.	Reconocer la importancia de la seguridad de redes internas y aplicar las pautas de diseño para fortificarlas.
	b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	− Arquitectura débil de subred protegida. − Arquitectura fuerte de subred protegida.		Aplicación de criterios de seguridad perimetral para clasificar zonas de riesgo.	
	c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.	− Redes privadas virtuales. VPN. − Beneficios y desventajas con respecto a las líneas dedicadas.		Descripción y uso de protocolos seguros de comunicación.	
	d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.	− Técnicas de cifrado. Clave pública y clave privada: • VPN a nivel de red. SSL, IPSec. • VPN a nivel de aplicación. SSH.		Configuración de VPN mediante protocolos a distintos niveles.	

	e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	− Servidores de acceso remoto: • Protocolos de autenticación. • Configuración de parámetros de acceso. • Servidores de autenticación.		Instalación de servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	
	f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.	• Protocolos de autenticación.		Aplicar diferentes configuraciones de autenticación en el acceso de usuarios remotos a través de la pasarela.	
	g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	− Servidores de acceso remoto: • Protocolos de autenticación. • Configuración de parámetros de acceso. • Servidores de autenticación.		Instalación y configuración en la pasarela de un servidor remoto de autenticación.	

Resultado de Aprendizaje	**RA4.** Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	Instalación y configuración de cortafuegos.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han descrito las características, tipos y funciones de los cortafuegos.	− Tipos de cortafuegos. Características. Funciones principales.	Contenidos Básicos	Enumeración y descripción de cortafuegos.	Inclusión de los cortafuegos como elemento básico en el diseño de red.
	b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	− Filtrado de paquetes de datos.		Descripción de los niveles del filtrado de tráfico.	Aplicación del tipo de cortafuego adecuado.
	c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	− Instalación de cortafuegos. Ubicación. Arquitecturas de red con cortafuegos. – Integración de los cortafuegos en la arquitectura de red perimetral.		Inclusión de cortafuegos en los diseños de redes.	
	d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	− Reglas de filtrado de cortafuegos.		Configuración de filtros de cortafuegos a partir de especificaciones.	
	e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	− Registros de sucesos de un cortafuegos.		Revisión del tráfico que pasa por el cortafuegos.	

	f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	− Utilización de cortafuegos. – Productos software para configurar cortafuegos.		Instalación de cortafuegos software y hardware.	
	g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	− Pruebas de funcionamiento. Sondeo.		Diagnóstico de problemas en el tráfico que pasa por el cortafuegos.	
	h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	− Utilización de cortafuegos. − Instalación de cortafuegos. Ubicación.		Realización de documentación relativa al cortafugos.	

Resultado de Aprendizaje	**RA5.** Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	Instalación y configuración de servidores «proxy».	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado los tipos de «proxy», sus características y funciones principales.	− Tipos de «proxy». Características y funciones.	Contenidos Básicos	Enumeración y descripción de proxies.	Inclusión de los proxies como elemento básico en el diseño de red. Aplicación del tipo de proxy adecuado.
	b) Se ha instalado y configurado un servidor «proxy-cache».	− Instalación de servidores «proxy». – Configuración del almacenamiento en la caché de un «proxy».		Instalación y configuración de proxy cache.	
	c) Se han configurado los métodos de autenticación en el «proxy».	− Métodos de autenticación en un «proxy».		Configuración de métodos de autenticación en el proxy.	
	d) Se ha configurado un «proxy» en modo transparente.	− Instalación de servidores «proxy». − Instalación y configuración de clientes «proxy».		Configuración de proxy transparente.	
	e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.	− Configuración de filtros. Reglas de control de acceso y seguridad.		Configuración del proxy para restringir webs.	

	f) Se han solucionado problemas de acceso desde los clientes al «proxy».	− Instalación de servidores «proxy». − Instalación y configuración de clientes «proxy». − Configuración de filtros.		Diagnóstico de problemas en el tráfico que pasa por el proxy.	
	g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.	− Instalación de servidores «proxy». − Instalación y configuración de clientes «proxy».		Revisión del tráfico que pasa por el proxy.	
	h) Se ha configurado un servidor «proxy» en modo inverso.	− Instalación de servidores «proxy».		Configuración de proxy en modo inverso.	
	i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».	− Instalación de servidores «proxy». − Instalación y configuración de clientes «proxy».		Realización de documentación relativa al proxy.	

Resultado de Aprendizaje	**RA6.** Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	Implantación de soluciones de alta disponibilidad.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	− Definición y objetivos. − Análisis de configuraciones de alta disponibilidad.	Contenidos Básicos	Análisis de sistemas con necesidad de alta disponibilidad.	Asimilación de necesidad de alta disponibilidad y su implementación en los sistemas.
	b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	• Funcionamiento ininterrumpido. • Integridad de datos y recuperación de servicio. • Servidores redundantes. • Sistemas de «clusters». • Balanceadores de carga.		Conocimiento de soluciones hardware para alta disponibilidad.	
	c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	− Virtualización de sistemas. − Posibilidades de la virtualización de sistemas. • Entornos personales. • Entornos empresariales. − Herramientas para la virtualización.		Conocimiento de virtualización para alta disponibilidad.	

		− Configuración y utilización de máquinas virtuales. − Alta disponibilidad y virtualización. − Simulación de servicios con virtualización.			
	d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	• Servidores redundantes.		Implantación de servidor redundante.	
	e) Se ha implantado un balanceador de carga a la entrada de la red interna.	• Balanceadores de carga.		Implantación de balanceador de carga.	
	f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	• Servidores redundantes.		Implantación de sistema de almacenamiento redundante.	
	g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.	• Sistemas de «clusters».		Análisis de clusters para alta disponibilidad.	
	h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	− Análisis de configuraciones de alta disponibilidad.		Análisis de soluciones en sistemas con demanda creciente.	
	i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	− Análisis de configuraciones de alta disponibilidad.		Documentación de soluciones para alta disponibilidad.	

Resultado de Aprendizaje	**RA7.** Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	Legislación y normas sobre seguridad.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	− Legislación sobre protección de datos.	Contenidos Básicos	Descripción de la legislación sobre protección de datos.	
	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	− Legislación sobre protección de datos.			Interiorización de 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.	− Legislación sobre protección de datos.		Identificación de las figuras que intervienen en la protección de datos.	
	d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	− Legislación sobre protección de datos.			Asimilación de la obligación de poner a disposición de las personas los datos personales.
	e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	− Legislación sobre los servicios de la sociedad de la información y correo electrónico.		Descripción de la legislación actual de los servicios de la	

				sociedad de la información y comercio electrónico.	
	f) Se han contrastado las normas sobre gestión de seguridad de la información.	− Legislación sobre protección de datos. − Legislación sobre los servicios de la sociedad de la información y correo electrónico.		Revisión de las normas de gestión de la seguridad de la información.	
	g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	− Legislación sobre protección de datos. − Legislación sobre los servicios de la sociedad de la información y correo electrónico.			Asimilación de la necesidad y conveniencia de conocer y respetar la normativa legal aplicable