TABLA 8: CE y Cb

Resultado de Aprendizaje	**RA 1.** Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	Aplicación de medidas de seguridad pasiva. Aplicación de mecanismos de seguridad activa.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha valorado la importancia de mantener la información segura.	Aplicación de medidas de seguridad pasiva. Principios de la seguridad informática. Políticas, planes y procedimientos de seguridad. Elementos de las políticas de seguridad.	Contenidos Básicos	Conocimiento de mantener la información segura.	Valoración de la importancia de las propiedades de seguridad en los sistemas informáticos
	b) Se han descrito las diferencias entre seguridad física y lógica.	Principios de la seguridad informática.		Diferenciación entre seguridad física y lógica.	Reconocimiento de los conceptos de seguridad física y lógica, diferencias entre ambas y ejemplos.
	c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.	Ubicación y protección física de los equipos y servidores.		Definición de las condiciones físicas óptimas para los equipos y servidores.	Adopción de pautas de ubicación física y condiciones ambientales en los equipos.

	d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	Ubicación y protección física de los equipos y servidores. Sistemas de alimentación ininterrumpida.		Valoración de la necesidad de protección física de los sistemas informáticos.	Reconocimiento de la seguridad física de los sistemas.
	e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	Sistemas de alimentación ininterrumpida.		Verificación del funcionamiento de sistemas de alimentación ininterrumpida.	Rigurosidad en la verificación del funcionamiento de los sistemas de alimentación ininterrumpida.
	f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	Sistemas de alimentación ininterrumpida.		Ubicación y aplicación de sistemas de alimentación ininterrumpida	Valoración de los puntos de aplicación de los sistemas de alimentación ininterrumpida.
	g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.	Listas de control de acceso.		Obtención de la política de seguridad de listas de control de acceso.	Rigurosidad en la implantación de una política de seguridad basada en listas de control de acceso.
	h) Se ha valorado la importancia de establecer una política de contraseñas.	Política de contraseñas.		Valoración de la importancia de las políticas de contraseñas	Rigurosidad en la implantación de política de contraseñas.

	i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	Ubicación y protección física de los equipos y servidores. Política de contraseñas.		Definición de las ventajas de utilización de sistemas biométricos.	Identificación de los usos actuales y futuros de los sistemas biométricos.

Resultado de Aprendizaje	**RA2.** Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	Gestión de dispositivos de almacenamiento.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	Medios de almacenamiento.	Contenidos Básicos	Interpretación de documentación técnica de políticas de almacenamiento.	Reconocimiento de la documentación técnica de políticas de almacenamiento.
	b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).	Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.		Valoración de los factores inherentes al almacenamiento de la información.	Consideración de rendimiento, disponibilidad y accesibilidad en los sistemas de almacenamiento de información
	c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.	Almacenamiento redundante y distribuido. Almacenamiento remoto y extraíble.		Conocimiento de los métodos de almacenamiento, así como las implementaciones locales y en red.	Clasificación de métodos de almacenamiento y los sistemas de almacenamiento en red.
	d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	Almacenamiento redundante y distribuido.		Descripción de las tecnologías del almacenamiento redundante y distribuido.	Identificación de almacenamiento redundante y distribuido.

	e) Se han seleccionado estrategias para la realización de copias de seguridad.	Copias de seguridad e imágenes de respaldo.		Selección de estrategias de las copias de seguridad.	Rigurosidad en la implementación de las estrategias para la realización de copias de seguridad.
	f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.	Copias de seguridad e imágenes de respaldo.		Selección de características (frecuencia y esquema de rotación) de las copias de seguridad.	Rigurosidad en la implementación de la frecuencia y esquema de rotación de las copias de seguridad.
	g) Se han realizado copias de seguridad con distintas estrategias.	Copias de seguridad e imágenes de respaldo.		Realización de copias de seguridad con distintas estrategias.	Adopción de pautas en la realización de copias de seguridad.
	h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.	Almacenamiento remoto y extraíble.		Conocimiento de las características almacenamiento remotos y extraíbles.	Clasificación de las características de medios de almacenamiento remotos y extraíbles.
	i) Se han utilizado medios de almacenamiento remotos y extraíbles.	Almacenamiento remoto y extraíble.		Uso de medios de almacenamiento remotos y extraíbles.	Rigurosidad en el uso de medios de almacenamiento remoto y extraíbles.
	j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	Copias de seguridad e imágenes de respaldo.		Creación y restauración de imágenes de respaldo de sistemas de funcionamiento.	Rigurosidad en la creación y restauración de imágenes de respaldo de sistemas.

Resultado de Aprendizaje	**RA3.** Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	Aplicación de mecanismos de seguridad activa.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.	Herramientas de protección y desinfección. Técnicas de recuperación de datos. Planes de contingencia.	Contenidos Básicos	Ejecución de planes de contingencia ante problemas de seguridad.	Adopción de pautas y planes de contingencia.
	b) Se han clasificado los principales tipos de software malicioso.	Software malicioso. Clasificación.		Conocimiento de los principales tipos de software malicioso.	Asimilación de las características de los principales tipos de software malicioso.
	c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.	Aplicación de mecanismos de seguridad activa.		Adopción de planes periódicos de actualización de los sistemas.	Asimilación de la importancia de las actualizaciones de los sistemas y aplicarla.
	d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.	Aplicación de mecanismos de seguridad activa.		Reconocimiento del origen y autenticidad del software que se instala en los sistemas.	Asimilación de la importancia de verificar el origen y autenticidad de las aplicaciones que se instalan y aplicarlo.

	e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	Herramientas de protección y desinfección.		Instalación y uso de aplicaciones que previenen y eliminan software malicioso.	Rigurosidad en la detección y eliminación de software malicioso.
	f) Se han aplicado técnicas de recuperación de datos.	Técnicas de recuperación de datos.		Aplicación de técnicas de recuperación de información.	Rigurosidad en la utilización de técnicas de recuperación de datos .

Resultado de Aprendizaje	**RA4.** Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico.	Aseguramiento de la privacidad. Vulnerabilidades de un sistema informático: Causas y tipos.	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.	Métodos para asegurar la privacidad de la información transmitida.	Contenidos Básicos	Control de servicios de red.	Reconocimiento de la necesidad de inventariar y controlar los servicios de red.
	b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.	Fraudes informáticos y robos de información.		Uso de herramientas preventivas ante fraudes informáticos.	Adopción de pautas para detectar técnicas de ingeniería social y fraudes.
	c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	Técnicas y herramientas para luchar contra el correo no deseado.		Uso de técnicas y herramientas contra el correo no deseado.	Interiorización de la importancia de minimizar publicidad y correo no deseado.
	d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	Control de la monitorización en redes cableadas.		Control de la monitorización de las redes cableadas.	Rigurosidad en el control de monitorización de redes cableadas.
	e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	Seguridad en los protocolos para comunicaciones inalámbricas.		Enumeración y descripción de los protocolos de comunicaciones inalámbricas.	Interiorización de la importancia de mantener la seguridad en

					comunicaciones inalámbricas
	f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	Sistemas de identificación: firma electrónica, certificados digitales y otros.		Descripción de los sistemas de identificación como firma electrónica, certificados digitales y otros.	Reconocimiento de los sistemas de identificación digitales
	g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	Sistemas de identificación: firma electrónica, certificados digitales y otros.		Uso los sistemas de identificación como firma electrónica, certificados digitales y otros.	Rigurosidad en la utilización de sistemas de identificación
	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	Cortafuegos en equipos y servidores.		Instalación y configuración de cortafuegos en equipo o servidor.	Conocimiento de la importancia de utilizar cortafuegos.

Resultado de Aprendizaje	**RA5.** Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	Cumplimiento de la legislación y de las 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.	Asimilación de la importancia de protección de datos.
	b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	Legislación sobre protección de datos.		Control de acceso a la información personal almacenada.	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.	Reconocimiento de las figuras legales para el tratamiento y mantenimiento de datos
	d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	Legislación sobre protección de datos.		Reconocimiento de poner los datos personales a disposición de sus titulares.	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	Cumplimiento de la legislación actual de los servicios de la sociedad de

				sociedad de la información y comercio electrónico.	la información y el 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.	Asimilación de la importancia de cumplir las normas de gestión de seguridad de la información