TABLA 8: CE y Cb

Resultado de Aprendizaje	**RA 1.** Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.	1. Diseño de planes de securización:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.	- Análisis de riesgos. - Principios de la Economía Circular en la Industria 4.0.	Contenidos Básicos	identificar los activos, las amenazas y vulnerabilidades de la organización.	
	b) Se ha evaluado las medidas de seguridad actuales.	- Plan de medidas técnicas de seguridad. - Políticas de securización más habituales. - Guías de buenas prácticas para la securización de sistemas y redes.		Valorar las medidas de seguridad actuales.	Es riguroso en la recopilación de la información
	c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización	- Estándares de securización de sistemas y redes.		Elaborar un análisis de riesgo de la situación actual en ciberseguridad de la organización	Es meticuloso en la redacción de los documentos afectados.
	d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los	- Caracterización de procedimientos, instrucciones y recomendaciones.		Priorizar las medidas técnicas de seguridad a implantar en la organización teniendo también	

	principios de la Economía Circular.			en cuenta los principios de la Economía Circular.	
	e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.	- Niveles, escalados y protocolos de atención a incidencias.		Diseñar y elaborar un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.	Interioriza la importancia de las medidas que se adoptan y las repercusiones que habrá si se toma una mala decisión
	f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización	- Niveles, escalados y protocolos de atención a incidencias.		Identificar las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización	

Resultado de Aprendizaje	**RA2.** Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.	2. Configuración de sistemas de control de acceso y autenticación de personas:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	- Mecanismos de autenticación. - Tipos de factores.	Contenidos Básicos	Definir los mecanismos de autenticación en base a distintos/múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	Asimila la importancia de implantar medidas que fortalezcan la seguridad contra intrusiones.
	b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.	- Autenticación basada en distintas técnicas: - Contraseñas, frases de paso.		Definir protocolos y políticas de autenticación basados en contraseñas y frases de paso, tomando como base las principales vulnerabilidades y tipos de ataques.	Es riguroso en la definición de los protocolos y políticas
	c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.	- Protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes.		Definir protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.	

	d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.	- Protocolos y políticas de autenticación basados en tokens, OTPs.		Definir protocolos y políticas de autenticación basados en tokens, OTPs, etc., tomando como base las principales vulnerabilidades y tipos de ataques.	
	e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.	- Protocolos y políticas de autenticación basados en características biométricas.		Definir protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.	

Resultado de Aprendizaje	**RA3**. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.	3. Administración de credenciales de acceso a sistemas informáticos:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado los tipos de credenciales más utilizados.	− Gestión de credenciales.	Contenidos Básicos	Identificar los tipos de credenciales más utilizados.	Asimila la importancia de fortalecer las medidas de acceso como prevención ante intrusiones.
	b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.	− Infraestucturas de Clave Pública (PKI).		Generar y utilizar diferentes certificados digitales como medio de acceso a un servidor remoto.	Interioriza la necesidad de los certificados digitales para asegurar la información
	c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.	− Acceso por medio de Firma electrónica.		Comprobar la validez y la autenticidad de un certificado digital de un servicio web.	
	d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.	− Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red). − Gestión de cuentas privilegiadas.		Comparar certificados digitales válidos e inválidos por diferentes motivos.	

	e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)	− Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.		Instalar y configurar un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)	

Resultado de Aprendizaje	**RA4.** Diseña redes de computadores contemplando los requisitos de seguridad.	4. Diseño de redes de computadores seguras:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	− Segmentación de redes. − Subnetting.	Contenidos Básicos	Incrementar el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	Adopta medidas eficientes en el diseño de las redes.
	b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).	− Redes virtuales (VLANs).		Optimizar una red local plana utilizando técnicas de segmentación lógica (VLANs).	
	c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.	− Zona desmilitarizada (DMZ).		Adaptar un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.	
	d) Se han configurado las medidas de seguridad adecuadas en los dispositivos	− Seguridad en redes inalámbricas (WPA2, WPA3, etc.).		Configurar las medidas de seguridad adecuadas en los dispositivos que dan acceso a	Interioriza el peligro de las redes inalámbricas con equipos BYOC

	que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).			una red inalámbrica (routers, puntos de acceso, etc.).	
	e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.	− Protocolos de red seguros (IPSec, etc.).		Establecer un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.	

Resultado de Aprendizaje			Bloque de contenidos		
	RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.	5. Configuración de dispositivos y sistemas informáticos:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	− Seguridad perimetral. Firewalls de Próxima Generación.	Contenidos Básicos	Configurar dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	Es riguroso en la configuración de las barreras de protección de acceso a los equipos.
	b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.	− Seguridad de portales y aplicativos webs. Soluciones WAF (Web Aplication Firewall). − Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware. − Seguridad de entornos cloud. Soluciones CASB. − Seguridad del correo electrónico − Soluciones DLP (Data Loss Prevention) − Herramientas de almacenamiento de logs.		Detectar errores de configuración de dispositivos de red mediante el análisis de tráfico.	Es meticuloso en la rutina de seguimiento de los puntos sensibles ante posibles ataques.

		− Protección ante ataques de denegación de servicio distribuido (DDoS). − Configuración segura de cortafuegos, enrutadores y proxies. − Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).			
	c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.	− Monitorización de sistemas y dispositivos. − Herramientas de monitorización (IDS, IPS).		Identificar comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.	
	d) Se han implementado contramedidas frente a comportamientos no deseados en una red.	− SIEMs (Gestores de Eventos e Información de Seguridad).		Implementar contramedidas frente a comportamientos no deseados en una red.	
	e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.	− Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.		Instalar y configurar diferentes herramientas de monitorización.	

Resultado de Aprendizaje	**RA6.** Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.	6. Configuración de dispositivos para la instalación de sistemas informáticos:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.	− Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.	Contenidos Básicos	Configurar la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.	Interioriza la necesidad de proteger los dispositivos de acceso y almacenamiento de datos.
	b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.	− Seguridad en el arranque del sistema informático,		Preparar un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.	
	c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.	− configuración del arranque seguro.		Configurar un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.	
	d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del	− Seguridad de los sistemas de ficheros, cifrado,		Instalar un sistema informático utilizando sus capacidades de	

	sistema de ficheros para evitar la extracción física de datos.			cifrado del sistema de ficheros para evitar la extracción física de datos.	
	e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.	− particionado, entre otros.		Particionar el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.	

Resultado de Aprendizaje	**RA7.** Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.	1. Configuración de los sistemas informáticos:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	− Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros. − Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.). −	Contenidos Básicos	Enumerar y/o eliminar los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	Es riguroso en la enumeración de todos los servicios no necesarios en los distintos sistemas.
	b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.	− Eliminación de protocolos de red innecesarios (ICMP, entre otros).		Configurar las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.	
	c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.	− Securización de los sistemas de administración remota.		Incrementar la seguridad del sistema de administración remoto SSH y otros.	Interioriza la necesidad de fortalecer los servicios a través de la configuración de los mismos.

	d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.	− Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).		Instalar y configurar un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.	
	e) Se han instalado y configurado sistemas de copias de seguridad.	− Configuración de actualizaciones y parches automáticos. − Sistemas de copias de seguridad. − Shadow IT y políticas de seguridad en entornos SaaS.		Instalar y configurar sistemas de copias de seguridad.	