TABLA 11: Unidades de Aprendizaje

(Una por cada Unidad)

Unidad de Aprendizaje Nº 1 DISEÑO DE PLANES DE SECURIZACIÓN		
Temporalización: Semana 1 - 3	**Duración**: 18 horas	**Ponderación**: 10 %

Objetivos Generales	**Competencias**
e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad. f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido. g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.	c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes. d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos cumpliendo los requisitos de seguridad Y minimizando las posibilidades de exposición a ataques. e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con Creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
Resultados de Aprendizaje	
RA1: Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.	
Aspectos del Saber Hacer	**Aspectos del Saber**

identificar los activos, las amenazas y vulnerabilidades de la organización.	Recopilar información de la organización sensible en cuanto a su seguridad y elaborar un plan de securización teniendo en cuenta qué elementos se necesitan y de cuáles se disponen.
Valorar las medidas de seguridad actuales.	
Elaborar un análisis de riesgo de la situación actual en ciberseguridad de la organización	
Priorizar las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.	
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.	
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	
Aspectos del Saber Estar	
Es riguroso en la recopilación de la información	
Es meticuloso en la redacción de los documentos afectados.	
Interioriza la importancia de las medidas que se adoptan y las repercusiones que habrá si se toma una mala decisión	
Tareas y Actividades	
✓ Desarrollar una infraestructura tenga, como mínimo: dos redes, un router, dos servidores en una red y varios clientes en la otra. ✓ Establecer los roles comunes de los equipos.	

- ✓ Evaluar los riesgos de: la infraestructura, servidores y clientes.
- ✓ Escanear y buscar vulnerabilidades. Realizar informe de la situación.
- ✓ Indicar qué medidas preventivas deben realizarse para minimizar el riesgo.

Criterios de Evaluación	%	IE
a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.	15	Actividad individual de investigación.
b) Se ha evaluado las medidas de seguridad actuales.	15	Actividad individual de investigación.
c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización	15	Actividad individual de investigación.
d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.	20	Actividad individual de investigación.
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.	20	Actividad individual de investigación.
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.	15	Mapa conceptual individual.

Recursos
Software de virtualización. Archivos ISO de los distintos sistemas operativos.

Observaciones

Unidad de Aprendizaje Nº 2 CONFIGURACIÓN DE SISTEMAS DE CONTROL DE ACCESO Y AUTENTICACIÓN DE PERSONAS		
Temporalización: Semana 4 - 5	**Duración**: 27 horas	**Ponderación**: 15%

Objetivos Generales	**Competencias**
h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.	d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
Resultados de Aprendizaje	
RA2: Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Definir los mecanismos de autenticación en base a distintos/múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	Establecer las medidas de seguridad de autenticación para todos los usuarios.
Definir protocolos y políticas de autenticación basados en contraseñas y frases de paso, tomando como base las principales vulnerabilidades y tipos de ataques.	
Definir protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.	
Definir protocolos y políticas de autenticación basados en tokens, OTPs,	

etc., tomando como base las principales vulnerabilidades y tipos de ataques.	
Definir protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.	
Aspectos del Saber Estar	
Asimila la importancia de implantar medidas que fortalezcan la seguridad contra intrusiones.	
Es riguroso en la definición de los protocolos y políticas	

Tareas y Actividades

- ✓ Investigar los sistemas más comunes y los más seguros de autenticación existentes en la actualidad.
- ✓ Establecer, en el servicio SSH, políticas de autenticación mediante “frase de paso”.
- ✓ Establecer, como requisito de acceso, segundo factor de autenticación.

Criterios de Evaluación	%	IE
a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	15	Actividad individual de investigación.
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.	20	Actividad individual práctica
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.	25	Actividad individual práctica
d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.	25	Actividad individual práctica

e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.	15	Actividad individual de investigación.

Recursos
Software de virtualización. Archivos ISO de los distintos sistemas operativos.
Observaciones

Unidad de Aprendizaje Nº 3 ADMINISTRACIÓN DE CREDENCIALES DE ACCESO A SISTEMAS INFORMÁTICOS.		
Temporalización: Semana 5-10	**Duración**: 39 horas	**Ponderación**: 20%

Objetivos Generales	**Competencias**
j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.	d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
Resultados de Aprendizaje	
RA3: Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Identificar los tipos de credenciales más utilizados.	Definir los métodos seguros de acceso mediante certificados digitales u otros sistemas robustos en cuanto a seguridad.
Generar y utilizar diferentes certificados digitales como medio de acceso a un servidor remoto.	
Comprobar la validez y la autenticidad de un certificado digital de un servicio web.	
Comparar certificados digitales válidos e inválidos por diferentes motivos.	
Instalar y configurar un servidor seguro para la administración de credenciales (tipo RADIUS – Remote Access Dial In User Service)	
Aspectos del Saber Estar	

Asimila la importancia de fortalecer las medidas de acceso como prevención ante intrusiones.	
Interioriza la necesidad de los certificados digitales para asegurar la información	

Tareas y Actividades

- ✓ Investigar los sistemas de credenciales más utilizados.
- ✓ Crear una autoridad digital y una subordinada en la infraestructura.
- ✓ Generar certificados digitales y utilizarlos en distintos servicios.
- ✓ Configurar accesos mediante credenciales de acceso a redes utilizando servicios tipo Radius.

Criterios de Evaluación	%	IE
a) Se han identificado los tipos de credenciales más utilizados.	15	Actividad individual de investigación.
b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.	25	Actividad individual práctica
c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.	15	Actividad individual práctica
d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.	20	Actividad individual práctica
e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS – Remote Access Dial In User Service)	25	Actividad individual práctica

Recursos

Software de virtualización.
Archivos ISO de los distintos sistemas operativos.

Observaciones

Unidad de Aprendizaje Nº 4 DISEÑO DE REDES DE COMPUTADORES SEGURAS.		
Temporalización: Semana 11-16	**Duración**: 39 horas	**Ponderación**: 20%

Objetivos Generales	Competencias
i) Configurar dispositivos de red para cumplir con los requisitos de seguridad. j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado. s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.	d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización. l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
Resultados de Aprendizaje	
RA4: Diseña redes de computadores contemplando los requisitos de seguridad.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Incrementar el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	Elaborar un plan de separación de redes mediante técnicas de subnetting, vlans y enrutamientos.

Optimizar una red local plana utilizando técnicas de segmentación lógica (VLANs).	
Adaptar un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.	
Configurar las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).	
Establecer un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.	
Aspectos del Saber Estar	
Adopta medidas eficientes en el diseño de las redes.	
Interioriza el peligro de las redes inalámbricas con equipos BYOC	

Tareas y Actividades

- ✓ Investigar cómo generar seguridad en redes sin segmentar utilizando la infraestructura creada como base de trabajo.
- ✓ Utilizando simuladores de redes, crear una infraestructura (a partir de la propia), aumentar dispositivos interconectarlos, separar las redes mediante VLANS y, mediante ACLs, permitir acceso y denegaciones a servicios desde distintas ubicaciones.
- ✓ Crear túneles seguros mediante simuladores e integrar redes mediante IPSEC.

Criterios de Evaluación	%	IE
a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	15	Actividad individual de investigación.

b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).	20	Actividad individual práctica
c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.	15	Actividad individual práctica
d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).	20	Actividad individual de investigación.
e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.	30	Actividad individual práctica
Recursos		
Software de virtualización. Archivos ISO de los distintos sistemas operativos.		
Observaciones		

Unidad de Aprendizaje Nº 5 CONFIGURACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS		
Temporalización: Semana 17 - 21	**Duración**: 39 horas	**Ponderación**: 20%

Objetivos Generales	**Competencias**
q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.	k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos. l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

Resultados de Aprendizaje	
RA5: Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Configurar dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	Establecer herramientas de monitorización e instalarlas. Comprobar su comportamiento detectando accesos no deseados y establecer niveles de alerta.
Detectar errores de configuración de dispositivos de red mediante el análisis de tráfico.	
Identificar comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.	

Implementar contramedidas frente a comportamientos no deseados en una red.	
Instalar y configurar diferentes herramientas de monitorización.	
Aspectos del Saber Estar	
Es riguroso en la configuración de las barreras de protección de acceso a los equipos.	
Es meticuloso en la rutina de seguimiento de los puntos sensibles ante posibles ataques.	

Tareas y Actividades

- ✓ Crear un esquema de seguridad perimetral tanto físico como lógico.
- ✓ Estableces sistemas informáticos de control de acceso a dispositivos conectados en red.
- ✓ Se han detectado intentos de acceso no autorizados y bloqueados estos.
- ✓ Instalar y evaluar distintas herramientas de detección de intrusos.

Criterios de Evaluación	%	IE
l) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	20	Mapa conceptual individual.
b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.	20	Actividad individual práctica
c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.	20	Actividad individual práctica
d) Se han implementado contramedidas frente a comportamientos no deseados en una red.	20	Actividad individual práctica

e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.	20	Actividad individual de investigación.
Recursos		
Software de virtualización. Archivos ISO de los distintos sistemas operativos.		
Observaciones		

Unidad de Aprendizaje Nº 6 CONFIGURACIÓN DE DISPOSITIVOS PARA LA INSTALACIÓN DE SISTEMAS INFORMÁTICOS		
Temporalización: Semana 21 - 22	**Duración**: 12 horas	**Ponderación**: 5%

Objetivos Generales	Competencias
r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas». v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.	l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Resultados de Aprendizaje	
RA6: Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Configurar la BIOS para incrementar la seguridad del dispositivo y su contenido	

<table>
<tr><td>minimizando las probabilidades de exposición a ataques.</td><td rowspan="6">Establecer las medidas de seguridad de cualquier equipo. Comprobar con qué dispositivos puede arrancarse los equipos informáticos.

Establecer medidas adicionales para evitar ataques “in situ”.</td></tr>
<tr><td>Preparar un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.</td></tr>
<tr><td>Configurar un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.</td></tr>
<tr><td>Instalar un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.</td></tr>
<tr><td>Particionar el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.</td></tr>
<tr><td>Aspectos del Saber Estar</td></tr>
<tr><td>Interioriza la necesidad de proteger los dispositivos de acceso y almacenamiento de datos.</td><td></td></tr>
<tr><td colspan="2">Tareas y Actividades</td></tr>
<tr><td colspan="2">✓ Estudiar las medidas de protección de las BIOS y UEFI.
✓ Establecer medidas de protección ante intrusiones directas contra los dispositivos. Evitar cambiar la secuencia de arranque.
✓ Organizar los dispositivos de almacenamiento interno para evitar el robo de información. Tipos de encriptado.
✓ Estudiar la conveniencia o no del encriptado de particiones.</td></tr>
</table>

Criterios de Evaluación	%	IE
a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.	15	Actividad individual de investigación.

b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.	15	Mapa conceptual individual.
c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.	30	Actividad individual de investigación.
d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.	20	Actividad individual práctica
e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.	20	Actividad individual práctica
Recursos		
Software de virtualización. Archivos ISO de los distintos sistemas operativos.		
Observaciones		

Unidad de Aprendizaje Nº 7 CONFIGURACIÓN DE LOS SISTEMAS INFORMÁTICOS		
Temporalización: Semana 23-25	**Duración**: 26 horas	**Ponderación**: 10%

Objetivos Generales	**Competencias**
t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».	l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

Resultados de Aprendizaje	
RA7: Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Enumerar y/o eliminar los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	Fortalecimiento de los sistemas informáticos mediante técnicas de ahorro de servicios no imprescindibles, revisión de sus configuraciones y detección de intrusos.
Configurar las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.	

Incrementar la seguridad del sistema de administración remoto SSH y otros.	
Instalar y configurar un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.	
Instalar y configurar sistemas de copias de seguridad.	
Aspectos del Saber Estar	
Es riguroso en la enumeración de todos los servicios no necesarios en los distintos sistemas.	
Interioriza la necesidad de fortalecer los servicios a través de la configuración de los mismos.	

Tareas y Actividades

- ✓ En la infraestructura creada: qué servicios se utilizan y cuales no. Medidas que se deben adoptar para proteger el sistema.
- ✓ Fortalecer la configuración del servidor SSH y “enjaular” a los usuarios.
- ✓ Instalación y configuración de un sistema HIDS (detección de intrusos).
- ✓ Crear estrategias de copia de seguridad y restauración.

Criterios de Evaluación	%	IE
a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	15	Actividad individual de investigación.
b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.	15	Actividad individual de investigación.
c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.	30	Actividad individual práctica

d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.	20	Actividad individual práctica
e) Se han instalado y configurado sistemas de copias de seguridad.	20	Actividad individual práctica
Recursos		
Software de virtualización. Archivos ISO de los distintos sistemas operativos.		
Observaciones		