



TABLA 11: Unidades de Aprendizaje

(Una por cada Unidad)

Unidad de Aprendizaje N° 1: Legislación y normas sobre seguridad		
Temporalización: Semana 1º	Duración: 5 horas	Ponderación: 5%

Objetivos Generales	Competencias
p	o, r, s
Resultados de Aprendizaje	
RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	
Aspectos del Saber Hacer	Aspectos del Saber
<p>Descripción de la legislación sobre protección de datos.</p> <p>Identificación de las figuras que intervienen en la protección de datos.</p> <p>Descripción de la legislación actual de los servicios de la sociedad de la información y comercio electrónico.</p> <p>Revisión de las normas de gestión de la seguridad de la información.</p>	<p>– Legislación sobre protección de datos.</p> <p>– Legislación sobre los servicios de la sociedad de la información y correo electrónico.</p>
Aspectos del Saber Estar	
<p>Interiorización de la necesidad de controlar el acceso a la información personal almacenada.</p> <p>Asimilación de la obligación de poner a disposición de las personas los datos personales.</p>	



Asimilación de la necesidad y conveniencia de conocer y respetar la normativa legal aplicable		
Tareas y Actividades		
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.		
Criterios de Evaluación	%	IE
a) Se ha descrito la legislación sobre protección de datos de carácter personal.	20	Tarea
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	7,5	Autoevaluación
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	70	Prueba
d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	2,5	Foro
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.		
f) Se han contrastado las normas sobre gestión de seguridad de la información.		
g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable. (5% FEM)		
Recursos		
<ul style="list-style-type: none">Aula-taller con ordenadores para cada uno de los alumnos de la clase.Los equipos deben disponer del software necesario para la realización de las prácticas.Una pantalla o proyector.		
Observaciones		



Unidad de Aprendizaje Nº 2: Adopción de pautas de seguridad informática		
Temporalización: Semana 2ª-4ª	Duración: 15 horas	Ponderación: 15%

Objetivos Generales	Competencias
k, l, m, o, p	e, f, i, j, k, n, o, r, s
Resultados de Aprendizaje	
RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	
Aspectos del Saber Hacer	Aspectos del Saber
<p>Conocimiento de seguridad física y lógica y sus formas de implementación para determinar las diferencias entre ambas.</p> <p>Enumeración y descripción de las vulnerabilidades de un sistema informático según su tipología y origen.</p> <p>Aplicación de políticas de contraseñas.</p> <p>Aplicación de criptografía en el almacenamiento y transmisión de la información.</p> <p>Enumeración y descripción de las fases de análisis forense ante ataques a un sistema.</p>	<p>– Fiabilidad, confidencialidad, integridad y disponibilidad.</p> <p>– Elementos vulnerables en el sistema informático: hardware, software y datos</p> <p>– Análisis de las principales vulnerabilidades de un sistema informático.</p> <p>– Amenazas. Tipos:</p> <p>– Seguridad física y ambiental:</p> <ul style="list-style-type: none"> • Ubicación y protección física de los equipos y servidores. • Sistemas de alimentación ininterrumpida. <p>– Seguridad lógica:</p> <ul style="list-style-type: none"> • Criptografía. • Listas de control de acceso. • Establecimiento de políticas de contraseñas. • Políticas de almacenamiento. • Copias de seguridad e imágenes de respaldo. • Medios de almacenamiento.
Aspectos del Saber Estar	
<p>Valoración de la importancia de las propiedades de seguridad en los sistemas informáticos</p>	<ul style="list-style-type: none"> • Amenazas lógicas. • Establecimiento de políticas de contraseñas. • Criptografía. <p>– Elementos básicos de la seguridad perimetral.</p>



Adopción de pautas para detectar técnicas de ingeniería social y fraudes. Identificación de los usos actuales y futuros de los sistemas biométricos. Asimilar la conveniencia de planes integrales de protección perimetral en sistemas conectados a redes públicas.	– Perímetros de red. Zonas desmilitarizadas.		
Tareas y Actividades			
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.			
Criterios de Evaluación	%	IE	
a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han clasificado las principales 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. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. (FEM) i) Se han identificado las fases del análisis forense ante ataques a un sistema.	20 7,5 70 2,5	Tarea Autoevaluación Prueba Foro	
Recursos			
• Aula-taller con ordenadores para cada uno de los alumnos de la clase.			



- Los equipos deben disponer del software necesario para la realización de las prácticas.
- Una pantalla o proyector.

Observaciones

Unidad de Aprendizaje N° 3: Implantación de mecanismos de seguridad activa

Temporalización:

Semana 5ª - 7ª

Duración: 15 horas

Ponderación: 20%

Objetivos Generales

k, l, m, o, p

Competencias

e, f, i, j, k, n, o, r, s

Resultados de Aprendizaje

RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

Aspectos del Saber Hacer

Enumeración y descripción de amenazas lógicas.
Enumeración y descripción de ataques más habituales, así como medidas preventivas y paliativas.
Análisis de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
Instalación de aplicaciones para la detección y eliminación de software malicioso.
Uso de técnicas de cifrado, firmas y certificado digitales en en redes públicas.

Aspectos del Saber

– Amenazas. Tipos:

- Amenazas físicas.
- Amenazas lógicas.
- Actualización de sistemas y aplicaciones.
- Anatomía de ataques y análisis de software malicioso.
- Herramientas preventivas. Instalación y configuración.
- Herramientas paliativas. Instalación y configuración.

– Ataques y contramedidas en sistemas personales:

- Clasificación de los ataques.
- Seguridad en la conexión con redes públicas.
- Pautas y prácticas seguras.
- Seguridad en los protocolos para comunicaciones inalámbricas.



Evaluación de las medidas de seguridad de los protocolos en redes inalámbricas.	<ul style="list-style-type: none">• Riesgos potenciales de los servicios de red.• Monitorización del tráfico en redes.		
Enumeración y descripción de las características de los sistemas de detección de intrusos.			
Aspectos del Saber Estar			
Asimilación de la importancia de verificar el origen, autenticidad y actualización del S.O. y de las aplicaciones que se instalan. Reconocimiento de la necesidad de inventariar y controlar los servicios de red para evaluar los riesgos.			
Tareas y Actividades			
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.			
Criterios de Evaluación	%	IE	
a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. 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. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. (FEM) d) Se han analizado diversos tipos 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. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	20 7,5 70 2,5	Tarea Autoevaluación Prueba Foro	



i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.		
Recursos		
<ul style="list-style-type: none"> • Aula-taller con ordenadores para cada uno de los alumnos de la clase. • Los equipos deben disponer del software necesario para la realización de las prácticas. • Una pantalla o proyector. 		
Observaciones		

Unidad de Aprendizaje Nº 4: Implantación de técnicas de acceso remoto. Seguridad perimetral		
Temporalización: Semana 8ª - 10ª	Duración: 15 horas	Ponderación: 15%

Objetivos Generales	Competencias
k, l, p	e, f, i, j, o, r, s
Resultados de Aprendizaje	
RA 3: Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	
Aspectos del Saber Hacer	Aspectos del Saber
Descripción de sistemas con conexión a redes públicas que aplican seguridad en la red interna. Aplicación de criterios de seguridad perimetral para clasificar zonas de riesgo.	<ul style="list-style-type: none">– Elementos básicos de la seguridad perimetral.– Arquitectura débil de subred protegida.– Arquitectura fuerte de subred protegida.– Redes privadas virtuales. VPN.– Beneficios y desventajas con respecto a las líneas dedicadas.



<p>Descripción y uso de protocolos seguros de comunicación.</p> <p>Aplicación de soluciones de seguridad perimetral.</p> <p>Configuración de VPN mediante protocolos a distintos niveles.</p> <p>Instalación de servidor como pasarela de acceso a la red interna desde ubicaciones remotas.</p> <p>Aplicar diferentes configuraciones de autenticación en el acceso de usuarios remotos a través de la pasarela.</p> <p>Instalación y configuración en la pasarela de un servidor remoto de autenticación.</p>	<p>– Técnicas de cifrado. Clave pública y clave privada:</p> <ul style="list-style-type: none">• VPN a nivel de red. SSL, IPSec.• VPN a nivel de aplicación. SSH. <p>– Servidores de acceso remoto:</p> <ul style="list-style-type: none">• Protocolos de autenticación.• Configuración de parámetros de acceso.• Servidores de autenticación.	
<p>Aspectos del Saber Estar</p>		
<p>Reconocer la importancia de la seguridad de redes internas y aplicar las pautas de diseño para fortificarlas.</p> <p>Valorar las distintas situaciones y establecer las soluciones necesarias de seguridad perimetral</p>		
<p>Tareas y Actividades</p>		
<p>En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.</p>		
<p>Criterios de Evaluación</p>	<p>%</p>	<p>IE</p>
<p>a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.</p> <p>b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. (FEM)</p> <p>c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.</p>	<p>20 7,5 70 2,5</p>	<p>Tarea Autoevaluación Prueba Foro</p>



<p>d) Se han valorado y establecido soluciones de seguridad perimetral a situaciones concretas.</p> <p>e) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. (FEM)</p> <p>f) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.</p> <p>g) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.</p> <p>h) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.</p>		
Recursos		
<ul style="list-style-type: none"> • Aula-taller con ordenadores para cada uno de los alumnos de la clase. • Los equipos deben disponer del software necesario para la realización de las prácticas. • Una pantalla o proyector. 		
Observaciones		

Unidad de Aprendizaje Nº 5: Instalación y configuración de cortafuegos		
Temporalización:	Duración: 15 horas	Ponderación: 15%
Semana 11ª - 13ª		

Objetivos Generales	Competencias
k, l, p	e, f, i, j, o, r, s
Resultados de Aprendizaje	
RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	
Aspectos del Saber Hacer	Aspectos del Saber



Enumeración y descripción de cortafuegos. Descripción de los niveles del filtrado de tráfico. Inclusión de cortafuegos en los diseños de redes. Configuración de filtros de cortafuegos a partir de especificaciones. Revisión del tráfico que pasa por el cortafuegos. Instalación de cortafuegos software y hardware. Diagnóstico de problemas en el tráfico que pasa por el cortafuegos. Realización de documentación relativa al cortafuegos.	<ul style="list-style-type: none">– Tipos de cortafuegos. Características. Funciones principales.– Filtrado de paquetes de datos.– Instalación de cortafuegos. Ubicación. Arquitecturas de red con cortafuegos.– Integración de los cortafuegos en la arquitectura de red perimetral.– Reglas de filtrado de cortafuegos.– Registros de sucesos de un cortafuegos.– Utilización de cortafuegos.– Productos software para configurar cortafuegos.– Pruebas de funcionamiento. Sondeo.		
Aspectos del Saber Estar			
Inclusión de los cortafuegos como elemento básico en el diseño de red. Aplicación del tipo de cortafuego adecuado.			
Tareas y Actividades			
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.			
Criterios de Evaluación	%	IE	
a) Se han descrito las características, tipos y funciones de los cortafuegos.	20	Tarea	
b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	7,5	Autoevaluación	
c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	70	Prueba	
d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	2,5	Foro	



<p>e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. (FEM)</p> <p>f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.</p> <p>h) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.</p> <p>i) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos. (FEM)</p>		
Recursos		
<ul style="list-style-type: none"> • Aula-taller con ordenadores para cada uno de los alumnos de la clase. • Los equipos deben disponer del software necesario para la realización de las prácticas. • Una pantalla o proyector. 		
Observaciones		

Unidad de Aprendizaje Nº 5: Instalación y configuración de servidores <<proxy>>		
Temporalización: Semana 14ª - 16ª	Duración: 15 horas	Ponderación: 15%

Objetivos Generales	Competencias
k, l, p	e, f, i, j, o, r, s
Resultados de Aprendizaje	
RA5. Instala servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	
Aspectos del Saber Hacer	Aspectos del Saber
Enumeración y descripción de proxies. Instalación y configuración de proxy cache. Configuración de métodos de autenticación en el proxy.	– Tipos de «proxy». Características y funciones. – Instalación de servidores «proxy». – Configuración del almacenamiento en la caché de un «proxy». – Métodos de autenticación en un «proxy». – Instalación y configuración de clientes «proxy».



Configuración de proxy transparente. Configuración del proxy para restringir webs. Diagnóstico de problemas en el tráfico que pasa por el proxy. Revisión del tráfico que pasa por el proxy. Configuración de proxy en modo inverso. Realización de documentación relativa al proxy.	– Configuración de filtros. Reglas de control de acceso y seguridad.	
Aspectos del Saber Estar		
Inclusión de los proxies como elemento básico en el diseño de red. Aplicación del tipo de proxy adecuado.		
Tareas y Actividades		
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.		
Criterios de Evaluación	%	IE
a) Se han identificado los tipos de «proxy», sus características y funciones principales.	20	Tarea
b) Se ha instalado y configurado un servidor «proxy-cache».	7,5	Autoevaluación
c) Se han configurado los métodos de autenticación en el «proxy».	70	Prueba
d) Se ha configurado un «proxy» en modo transparente.	2,5	Foro
e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.		
f) Se han solucionado problemas de acceso desde los clientes al «proxy».		
g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.		



h) Se ha configurado un servidor «proxy» en modo inverso.		
i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy». (FEM)		
Recursos		
<ul style="list-style-type: none"> • Aula-taller con ordenadores para cada uno de los alumnos de la clase. • Los equipos deben disponer del software necesario para la realización de las prácticas. • Una pantalla o proyector. 		
Observaciones		

Unidad de Aprendizaje Nº 6: Implantación de soluciones de alta disponibilidad		
Temporalización:	Duración: 15 horas	Ponderación: 15%
Semana 17ª - 19ª		

Objetivos Generales	Competencias
k, l, p	e, f, i, j, o, r, s
Resultados de Aprendizaje	
RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	
Aspectos del Saber Hacer	Aspectos del Saber
<p>Análisis de sistemas con necesidad de alta disponibilidad.</p> <p>Conocimiento de soluciones hardware para alta disponibilidad.</p> <p>Conocimiento de virtualización para alta disponibilidad.</p> <p>Implantación de servidor redundante.</p>	<p>– Definición y objetivos.</p> <p>– Análisis de configuraciones de alta disponibilidad.</p> <ul style="list-style-type: none"> • Funcionamiento ininterrumpido. • Integridad de datos y recuperación de servicio. • Servidores redundantes. • Sistemas de «clusters». • Balanceadores de carga.



Implantación de balanceador de carga.	<ul style="list-style-type: none">– Instalación y configuración de soluciones de alta disponibilidad– Virtualización de sistemas.– Posibilidades de la virtualización de sistemas.• Entornos personales.• Entornos empresariales.– Herramientas para la virtualización.– Configuración y utilización de máquinas virtuales.– Alta disponibilidad y virtualización.– Simulación de servicios con virtualización.	
Implantación de sistema de almacenamiento redundante.		
Análisis de clusters para alta disponibilidad.		
Análisis de soluciones en sistemas con demanda creciente.		
Documentación de soluciones para alta disponibilidad.		
Aspectos del Saber Estar		
Asimilación de necesidad de alta disponibilidad y su implementación en los sistemas.		
Tareas y Actividades		
En esta unidad, se harán actividades de desarrollo, autoevaluación, prueba presencial y foro.		
Criterios de Evaluación	%	IE
a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. (FEM)	20	Tarea
	7,5	Autoevaluación
	70	Prueba
	2,5	Foro
b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.		
c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.		
d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.		
e) Se ha implantado un balanceador de carga a la entrada de la red interna.		
f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.		
g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.		



<p>h) Se han analizado soluciones de futuro para un sistema con demanda creciente.</p> <p>i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad. (FEM)</p>		
Recursos		
<ul style="list-style-type: none">• Aula-taller con ordenadores para cada uno de los alumnos de la clase.• Los equipos deben disponer del software necesario para la realización de las prácticas.• Una pantalla o proyector.		
Observaciones		