TABLA 11: Unidades de Aprendizaje

(Una por cada Unidad)

Unidad de Aprendizaje Nº 1: Adopción de pautas de seguridad informática		
Temporalización: Semana 1 a 3	**Duración**: 12 horas	**Ponderación**: 20%

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**
Conocimiento de seguridad física y lógica y sus formas de implementación para determinar las diferencias entre ambas. Enumeración y descripción de las vulnerabilidades de un sistema informático según su tipología y origen. Aplicación de políticas de contraseñas. Aplicación de criptografía en el almacenamiento y transmisión de la información. Enumeración y descripción de las fases de análisis forense ante ataques a un sistema.	– Dimensiones de la seguridad de la información: confidencialidad, integridad y disponibilidad. – Elementos vulnerables en el sistema informático: *hardware, software* y datos. – Análisis de las principales vulnerabilidades de un sistema informático. – Ingeniería social y fraude electrónico: • Características de la ingeniería social. • Características del fraude electrónico y tipos. • Buenas prácticas. • Denunciar una estafa electrónica. – Amenazas. Tipos: • Amenazas físicas. • Amenazas lógicas. – Seguridad física y ambiental:
Aspectos del Saber Estar	

Valoración de la importancia de las propiedades de seguridad en los sistemas informáticos 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.	• Ubicación y protección física de los equipos y servidores. • Sistemas de alimentación ininterrumpida. – Seguridad lógica: • Criptografía. Tipos de criptosistemas y algoritmos. • Cifrado de ficheros y unidades. • Codificación. • Listas de control de acceso. • Establecimiento de políticas de contraseñas seguras. • Gestores de contraseñas. • Políticas de almacenamiento. • Copias de seguridad e imágenes de respaldo. – Análisis forense en sistemas informáticos: • Objetivos del análisis forense. • Fases del análisis forense. • Recolección, análisis y presentación de las evidencias.

Tareas y Actividades

Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad.
Desarrollo: realización de prácticas individuales para ayudar a comprender los contenidos.
Evaluación: prácticas individuales y realización de tutoriales y guías de instalación.

Criterios de Evaluación	%	IE
a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	15	Tarea individual
b) Se han descrito las diferencias entre seguridad física y lógica.	5	Tarea individual
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	5	Tarea individual
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	5	Tarea individual
e) Se han adoptado políticas de contraseñas.	5	Tarea individual

f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	5	Tarea individual
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	5	Tarea individual
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.	5	Tarea individual + FEM
i) Se han identificado las fases del análisis forense ante ataques a un sistema. i) Se han identificado las fases del análisis forense ante ataques a un sistema.	5	Tarea individual
j) -se han analizado evidencias forenses para obtener información relevante.	5	Tarea individual
k) Se han descrito los tipos de criptosistemas y reconocido los algoritmos crittográficos seguros.	5	Tarea individual
l) Se han identificado los tipos de sistemas de alimentación ininterrupida.	10	Prueba individual
m) Se ha calculado la potencia necesaria del sistema de alimentación ininterrumpida en función de la carga	15	Prueba individual
n) Se han analizado estrategias de copias de seguridad.	5	Trabajo de investigación
ñ) Se han realizado copias de seguridad	5	Trabajo de investigación

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 Nº 2: Implantación de mecanismos de seguridad activa		
Temporalización: Semana 4 a 6	**Duración**: 12 horas	**Ponderación**: 20%

Objetivos Generales	Competencias
k, l, m, o, p	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	Aspectos del Saber
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. Evaluación de las medidas de seguridad de los protocolos en redes inalámbricas. Enumeración y descripción de las características de los sistemas de detección de intrusos.	− 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. • Riesgos potenciales de los servicios de red. • Monitorización del tráfico en redes.
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

Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad.
Desarrollo: realización de prácticas individuales para ayudar a comprender los contenidos.
Evaluación: se realiza una prueba final y una prueba intermedia para determinar la adquisición de los conceptos y habilidades.
Además, se realiza una actividad de investigación para afianzar los contenidos necesarios.

Criterios de Evaluación	%	IE
a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	5	Tarea práctica
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.	10	Tarea práctica
c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	10	Tarea práctica + FEM
d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	20	Tarea práctica
e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	20	Tarea práctica
f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	10	Tarea práctica
g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	5	Tarea práctica
h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.	10	Tarea práctica
i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.	10	Tarea práctica + FEM

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 Nº 3: Implantación de técnicas de acceso remoto. Seguridad perimetral		
Temporalización: Semana 7 a 9	**Duración**: 12 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. Descripción y uso de protocolos seguros de comunicación. Aplicación de soluciones de seguridad perimetral. Configuración de VPN mediante protocolos a distintos niveles. Instalación de servidor como pasarela de acceso a la red interna desde ubicaciones remotas. Aplicar diferentes configuraciones de autenticación en el acceso de	− 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. − Técnicas de cifrado. Clave pública y clave privada: • VPN a nivel de red. SSL, IPSec. • VPN a nivel de aplicación. SSH. − Servidores de acceso remoto: • Protocolos de autenticación. • Configuración de parámetros de acceso. • Servidores de autenticación.

usuarios remotos a través de la pasarela. Instalación y configuración en la pasarela de un servidor remoto de autenticación.	
Aspectos del Saber Estar	
Reconocer la importancia de la seguridad de redes internas y aplicar las pautas de diseño para fortificarlas. Valorar las distintas situaciones y establecer las soluciones necesarias de seguridad perimetral	

Tareas y Actividades

Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad.
Evaluación: se realiza una prueba final y una prueba intermedia para determinar la adquisición de los conceptos y habilidades.
Evaluación: se realiza un cuestionario final para determinar la adquisición de los conceptos.

Criterios de Evaluación	%	IE
a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	10	Trabajo investigación
b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	10	Trabajo investigación + FEM
c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.	10	Tarea práctica
d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.	17	Tarea práctica
e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	18	Tarea práctica
f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.	15	Tarea práctica
g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	20	Tarea práctica

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 Nº 4: Implantación de soluciones de alta disponibilidad		
Temporalización: Semana 10 a 16	**Duración**: 22 horas	**Ponderación**: 15%

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
Análisis de sistemas con necesidad de alta disponibilidad. Conocimiento de soluciones hardware para alta disponibilidad. Conocimiento de virtualización para alta disponibilidad. Implantación de servidor redundante. Implantación de balanceador de carga. 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.	− Definición y objetivos. − Análisis de configuraciones de alta disponibilidad. • Funcionamiento ininterrumpido. • Integridad de datos y recuperación de servicio. • Servidores redundantes. • Sistemas de «clusters». • Balanceadores de carga. − 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.
Aspectos del Saber Estar	
Asimilación de necesidad de alta disponibilidad y su implementación en los sistemas.	

Tareas y Actividades

Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad.

Evaluación: reto, FEM y prácticas individuales.

Evaluación: se realiza un cuestionario final para determinar la adquisición de los conceptos.

Criterios de Evaluación	%	IE
a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	10	Reto + FEM
b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	10	Reto
c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	10	Reto
d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	15	Reto
e) Se ha implantado un balanceador de carga y "proxy" inverso a la entrada de la red interna, gestionando certificados y repartiendo las conexiones de uno o varios clústeres de servicios.	15	Reto
f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	15	Tarea práctica
g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.	10	Tarea práctica
h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	10	Reto
i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	5	Tarea práctica + FEM

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 Nº :5 Instalación y configuración de cortafuegos		
Temporalización: Semana 17 a 20	**Duración**: 10 horas	**Ponderación**: 15%

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.	− 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		
Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad. Desarrollo: realización de prácticas individuales para ayudar a comprender los contenidos. Evaluación: se realiza una prueba final y una prueba intermedia para determinar la adquisición de los conceptos y habilidades.		
Criterios de Evaluación	**%**	**IE**
a) Se han descrito las características, tipos y funciones de los cortafuegos.	10	Tarea de investigación
b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	10	Tarea de investigación
c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	15	Tarea práctica
d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	17	Tarea práctica
e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	12	Tarea práctica + FEM
f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	12	Tarea práctica
g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	12	Tarea práctica
h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	12	Tarea práctica + FEM
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 Nº 6: Instalación y configuración de servidores <<proxy>>		
Temporalización: Semana 20 a 23	**Duración**: 10 horas	**Ponderación**: 15%

Objetivos Generales	Competencias
k, l, p	e, f, i, j, o, r, s

Resultados de Aprendizaje

RA5. Implanta 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. 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.	− 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 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		
Iniciales: cuestionario inicial de ideas previas para introducir los conceptos más relevantes de la unidad. Desarrollo: realización de prácticas individuales para ayudar a comprender los contenidos. Evaluación: se realiza una prueba final y una prueba intermedia para determinar la adquisición de los conceptos y habilidades.		
Criterios de Evaluación	**%**	**IE**
a) Se han identificado los tipos de «proxy», sus características y funciones principales.	10	Tarea de investigación
b) Se ha instalado y configurado un servidor «proxy-cache».	15	Tarea práctica
c) Se han configurado los métodos de autenticación en el «proxy».	10	Tarea práctica
d) Se ha configurado un «proxy» en modo transparente.	10	Tarea práctica
e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.	10	Tarea práctica
f) Se han solucionado problemas de acceso desde los clientes al «proxy».	10	Tarea práctica
g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.	15	Tarea práctica
h) Se ha configurado un servidor «proxy» en modo inverso.	10	Tarea práctica
i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».	10	Tarea práctica + FEM
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 Nº 7: Legislación y normas sobre seguridad		
Temporalización: Semanas 23 a 25	**Duración**: 4 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
Descripción de la legislación sobre protección de datos. Identificación de las figuras que intervienen en la protección de datos. Descripción de la legislación actual de los servicios de la sociedad de la información y comercio electrónico. Revisión de las normas de gestión de la seguridad de la información.	− Legislación sobre protección de datos. − Legislación sobre los servicios de la sociedad de la información y correo electrónico.
Aspectos del Saber Estar	
Interiorización de la necesidad de controlar el acceso a la información personal almacenada. Asimilación de la obligación de poner a disposición de las personas los datos personales. Asimilación de la necesidad y conveniencia de conocer y respetar la normativa legal aplicable	

Tareas y Actividades

En esta unidad, al tener un aspecto mayormente teórico, se irán realizando actividades de investigación referentes a cada criterio de evaluación para la correcta adquisición de los contenidos.

Criterios de Evaluación	%	IE
a) Se ha descrito la legislación sobre protección de datos de carácter personal.	20	Prueba teórica
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	10	Trabajo investigación
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	20	Trabajo investigación
d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	10	Trabajo investigación
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	20	Trabajo investigación
f) Se han contrastado las normas sobre gestión de seguridad de la información.	10	Trabajo investigación
g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	10	Trabajo investigación + FEM

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