TABLA 11: Unidades de Aprendizaje

Unidad de Aprendizaje Nº 1. Seguridad informática en el entorno físico		
Temporalización: 1er trimestre	**Duración**: 30 horas	**Ponderación**: 21%

Objetivos Generales	Competencias
a,c,d,e,g,k,l	a,c,i,j,l,n,o,p,t

Resultados de Aprendizaje
RA1

Aspectos del Saber Hacer	Aspectos del Saber
• Conocimiento de mantener la información segura. • Diferenciación entre seguridad física y lógica. • Definición de las condiciones físicas óptimas para los equipos y servidores. • Valoración de la necesidad de protección física de los sistemas informáticos. • Verificación del funcionamiento de sistemas de alimentación ininterrumpida. • Ubicación y aplicación de sistemas de alimentación ininterrumpida • Obtención de la política de seguridad de listas de control de acceso. • Valoración de la importancia de las políticas de contraseñas • Definición de las ventajas de utilización de sistemas biométricos.	• Aplicación de medidas de seguridad pasiva. • Principios de la seguridad informática. • Políticas, planes y procedimientos de seguridad. Elementos de las políticas de seguridad. • Principios de la seguridad informática. • Ubicación y protección física de los equipos y servidores. • Ubicación y protección física de los equipos y servidores. • Sistemas de alimentación ininterrumpida.
Aspectos del Saber Estar	
• Valoración de la importancia de las propiedades de seguridad en los sistemas informáticos • Reconocimiento de los conceptos de seguridad física y lógica, diferencias entre ambas y ejemplos.	

• Adopción de pautas de ubicación física y condiciones ambientales en los equipos. • Reconocimiento de la seguridad física de los sistemas. • Rigurosidad en la verificación del funcionamiento de los sistemas de alimentación ininterrumpida. • Valoración de los puntos de aplicación de los sistemas de alimentación ininterrumpida. • Rigurosidad en la implantación de una política de seguridad basada en listas de control de acceso. • Rigurosidad en la implantación de política de contraseñas. • Identificación de los usos actuales y futuros de los sistemas biométricos.	• Listas de control de acceso. • Política de contraseñas. • Ubicación y protección física de los equipos y servidores.

Tareas y Actividades

- Se realizarán varias actividades prácticas y teóricas en clase, cuyas soluciones pondremos en común para que los alumnos/as puedan revisar y ampliar sus propias soluciones previas.
- Realizará una tarea teórica de forma individual en la que tendrán que explicar una serie de conceptos vistos en clase, así como elegir entre varias opciones de equipos de seguridad, siempre justificando sus respuestas.
- En grupos de 3 alumnos realizarán una propuesta para a provisionar un CPD expuesto por el profesor de todos los sistemas de seguridad que ellos consideren necesarios. Tendrán que elaborar la propuesta técnica y económica en su solución.

Criterios de Evaluación	%	IE	%IE
a) Se ha valorado la importancia de mantener la información segura.	10	Tarea teórica individual	100%
b) Se han descrito las diferencias entre seguridad física y lógica.	10	Tarea teórica individual	100%
c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.	15		100%

d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	10	Actividad grupal de investigación	100%
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	10	Actividad grupal de investigación	30%
		Tarea teórica individual	70%
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	10	Actividad grupal de investigación	30%
		Tarea teórica individual	70%
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.	10	Actividad grupal de investigación	30%
		Tarea teórica individual	70%
h) Se ha valorado la importancia de establecer una política de contraseñas.	15	Actividad grupal de investigación	30%
		Tarea teórica individual	70%
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	10	Actividad grupal de investigación	30%
		Tarea teórica individual	70%

		Actividad grupal de investigación	

Recursos
• Apuntes teóricos proporcionados por el profesor. • Aula de ordenadores.

Observaciones

Unidad de Aprendizaje Nº 2. Políticas de almacenamiento y resguardo de la información.		
Temporalización: 1er trimestre	**Duración**: 21 horas	**Ponderación**: 20%

Objetivos Generales	Competencias
a,c,d,e,g,k,l	a,c,i,j,l,n,o,p,t

Resultados de Aprendizaje

RA2

Aspectos del Saber Hacer	Aspectos del Saber
• Interpretación de documentación técnica de políticas de almacenamiento. • Valoración de los factores inherentes al almacenamiento de la información. • Conocimiento de los métodos de almacenamiento, así como las implementaciones locales y en red. • Descripción de las tecnologías del almacenamiento redundante y distribuido. • Selección de estrategias de las copias de seguridad. • Selección de características (frecuencia y esquema de rotación) de las copias de seguridad. • Realización de copias de seguridad con distintas estrategias. • Conocimiento de las características almacenamiento remotos y extraíbles. • Uso de medios de almacenamiento remotos y extraíbles. • Creación y restauración de imágenes de respaldo de sistemas de funcionamiento.	• Medios de almacenamiento. • Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad. • Almacenamiento redundante y distribuido. • Almacenamiento remoto y extraíble. • Copias de seguridad e imágenes de respaldo.
Aspectos del Saber Estar	
• Reconocimiento de la documentación técnica de políticas de almacenamiento.	

• Consideración de rendimiento, disponibilidad y accesibilidad en los sistemas de almacenamiento de información • Clasificación de métodos de almacenamiento y los sistemas de almacenamiento en red. • Identificación de almacenamiento redundante y distribuido. • Rigurosidad en la implementación de las estrategias para la realización de copias de seguridad. • Rigurosidad en la implementación de la frecuencia y esquema de rotación de las copias de seguridad. • Adopción de pautas en la realización de copias de seguridad. • Clasificación de las características de medios de almacenamiento remotos y extraíbles. • Rigurosidad en el uso de medios de almacenamiento remoto y extraíbles. • Rigurosidad en la creación y restauración de imágenes de respaldo de sistemas.	

Tareas y Actividades

- Se realizarán varias actividades prácticas y teóricas en clase, cuyas soluciones pondremos en común para que los alumnos/as puedan revisar y ampliar sus propias soluciones previas.
- Realizará una actividad individual de investigación en la que tendrán que explicar una serie de conceptos vistos en clase, así como elegir entre varias opciones de equipos de almacenamiento, siempre justificando sus respuestas.
- Realizarán una tarea práctica individual en la que deberán manejar varios de los sistemas vistos en clase para la gestión del almacenamiento de la información.
- Tendrán una prueba teórica en la que deberán demostrar que han adquirido los conocimientos inherentes de esta unidad.

Criterios de Evaluación	%	IE	%IE

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	10	Actividad individual de investigación	100%
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).	10	Actividad individual de investigación Prueba teórica	40% 60%
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.	10	Actividad individual de investigación Prueba teórica	40% 60%
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	10	Actividad individual de investigación Prueba teórica Tarea práctica individual	40% 60%
e) Se han seleccionado estrategias para la realización de copias de seguridad.	10	Actividad individual de investigación Prueba teórica	100% 40%
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.	10	Tarea práctica individual	60%
	10	Actividad individual de investigación	100%

g) Se han realizado copias de seguridad con distintas estrategias. h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles. i) Se han utilizado medios de almacenamiento remotos y extraíbles. j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	10 10	Prueba teórica Tarea práctica individual Tarea práctica individual	40% 60% 100% 100%

Recursos

- Apuntes teóricos proporcionados por el profesor.
- Aula de ordenadores.

Observaciones

Unidad de Aprendizaje Nº 3. Seguridad del software		
Temporalización: 2º trimestre	**Duración**: 30 horas	**Ponderación**: 21%

Objetivos Generales	Competencias
a,c,d,e,g,k,l	a,c,i,j,l,n,o,p,t

Resultados de Aprendizaje

RA3

Aspectos del Saber Hacer	Aspectos del Saber
• Ejecución de planes de contingencia ante problemas de seguridad. • Conocimiento de los principales tipos de software malicioso. • Adopción de planes periódicos de actualización de los sistemas. • Reconocimiento del origen y autenticidad del software que se instala en los sistemas. • Instalación y uso de aplicaciones que previenen y eliminan software malicioso. • Aplicación de técnicas de recuperación de información.	• Herramientas de protección y desinfección. • Técnicas de recuperación de datos. • Planes de contingencia. • Software malicioso. Clasificación. • Aplicación de mecanismos de seguridad activa. • Herramientas de protección y desinfección. • Técnicas de recuperación de datos.
• Aspectos del Saber Estar	
• Adopción de pautas y planes de contingencia. • Asimilación de las características de los principales tipos de software malicioso. • Asimilación de la importancia de las actualizaciones de los sistemas y aplicarla.	

• Asimilación de la importancia de verificar el origen y autenticidad de las aplicaciones que se instalan y aplicarlo. • Rigurosidad en la detección y eliminación de software malicioso. • Rigurosidad en la utilización de técnicas de recuperación de datos.	

Tareas y Actividades

- Se realizarán varias actividades prácticas y teóricas en clase, cuyas soluciones pondremos en común para que los alumnos/as puedan revisar y ampliar sus propias soluciones previas.
- Realizará una actividad individual de investigación en la que tendrán que explicar una serie de conceptos vistos en clase, así como elegir entre varias opciones de equipos de almacenamiento, siempre justificando sus respuestas.
- Realizarán una tarea práctica individual en la que deberán manejar varios de los sistemas vistos en clase para la gestión del almacenamiento de la información.

Criterios de Evaluación	%	IE	%IE
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.	15	Tarea práctica individual	100%
b) Se han clasificado los principales tipos de software malicioso.	15	Actividad individual de investigación	100%
c) Se han identificado las principales causas de vulnerabilidad de los sistemas informáticos.	10	Actividad individual de investigación	100%
d) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.	20	Tarea práctica individual	100%

e) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.	15	Actividad individual de investigación	100%
f) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	15	Tarea práctica individual	100%
g) Se han aplicado técnicas de recuperación de datos.	10	Tarea práctica individual	100%

Recursos

- Apuntes teóricos proporcionados por el profesor.
- Aula de ordenadores.

Observaciones

Unidad de Aprendizaje Nº 4. Redes Seguras		
Temporalización: 2º trimestre	**Duración**: 27 horas	**Ponderación**: 24%

Objetivos Generales	Competencias
a,c,g,k,l	a,c,i,l,n,o,p,t

Resultados de Aprendizaje

RA4

Aspectos del Saber Hacer

- Control de servicios de red.
- Uso de herramientas preventivas ante fraudes informáticos.
- Uso de técnicas y herramientas contra el correo no deseado.
- Control de la monitorización de las redes cableadas.
- Enumeración y descripción de los protocolos de comunicaciones inalámbricas.
- Descripción de los sistemas de identificación como firma electrónica, certificados digitales y otros.
- Uso los sistemas de identificación como firma electrónica, certificados digitales y otros.
- Instalación y configuración de cortafuegos en equipo o servidor.

Aspectos del Saber Estar

- Reconocimiento de la necesidad de inventariar y controlar los servicios de red.
- Adopción de pautas para detectar técnicas de ingeniería social y fraudes.
- Interiorización de la importancia de minimizar publicidad y correo no deseado.

Aspectos del Saber

- Métodos para asegurar la privacidad de la información transmitida
- Fraudes informáticos y robos de información.
- Técnicas y herramientas para luchar contra el correo no deseado.
- Control de la monitorización en redes cableadas.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos en equipos y servidores.

• Rigurosidad en el control de monitorización de redes cableadas. • Interiorización de la importancia de mantener la seguridad en comunicaciones inalámbricas • Reconocimiento de los sistemas de identificación digitales • Rigurosidad en la utilización de sistemas de identificación • Conocimiento de la importancia de utilizar cortafuegos.	

Tareas y Actividades

- Se realizarán varias actividades prácticas y teóricas en clase, cuyas soluciones pondremos en común para que los alumnos/as puedan revisar y ampliar sus propias soluciones previas.
- Realizará una actividad individual de investigación en la que tendrán que explicar una serie de conceptos vistos en clase, así como elegir entre varias opciones de equipos de almacenamiento, siempre justificando sus respuestas.
- Realizarán una tarea práctica individual en la que deberán manejar varios de los sistemas vistos en clase para la gestión del almacenamiento de la información.
- Tendrán una prueba teórica en la que deberán demostrar que han adquirido los conocimientos inherentes de esta unidad.

Criterios de Evaluación	%	IE	%IE
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.	10	Actividad individual de investigación	100%
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.	10	Actividad individual de investigación Prueba teórica	40% 60%
c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	10	Actividad individual de investigación	40%

		Prueba teórica	60%
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	10	Tarea práctica individual	100%
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	15	Actividad individual de investigación Prueba teórica	40% 60%
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	15	Prueba teórica	100%
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	15	Tarea práctica individual	100%
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	15	Tarea práctica individual	100%

Recursos

- Apuntes teóricos proporcionados por el profesor.
- Aula de ordenadores.

Observaciones

Unidad de Aprendizaje Nº 5. Legislación sobre seguridad informática y protección de datos.		
Temporalización: 2º trimestre	**Duración**: 12 horas	**Ponderación**: 14%

Objetivos Generales	Competencias
k	i,l,o,p

Resultados de Aprendizaje
RA5

Aspectos del Saber Hacer	Aspectos del Saber
• Descripción de la legislación sobre protección de datos • Control de acceso a la información personal almacenada. • Identificación de las figuras que intervienen en la protección de datos. • Reconocimiento de poner los datos personales a disposición de sus titulares. • 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	
• Asimilación de la importancia de protección de datos. • Interiorización de la necesidad de controlar el acceso a la información personal almacenada. • Reconocimiento de las figuras legales para el tratamiento y mantenimiento de datos • Asimilación de la obligación de poner a disposición de las personas los datos personales. • Cumplimiento de la legislación actual de los servicios de la sociedad de la información y el comercio electrónico.	

• Asimilación de la importancia de cumplir las normas de gestión de seguridad de la información	

Tareas y Actividades

- Se realizarán varias actividades prácticas y teóricas en clase, cuyas soluciones pondremos en común para que los alumnos/as puedan revisar y ampliar sus propias soluciones previas.
- Realizará una actividad grupal de investigación en la que tendrán que explicar una serie de conceptos vistos en clase, así como elegir entre varias opciones de equipos de almacenamiento, siempre justificando sus respuestas.
- Tendrán una prueba teórica en la que deberán demostrar que han adquirido los conocimientos inherentes de esta unidad.

Criterios de Evaluación	%	IE	%IE
a) Se ha descrito la legislación sobre protección de datos de carácter personal.	20	Actividad grupal de investigación	100%
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	20	Actividad grupal de investigación Prueba teórica	30% 70%
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	20	Actividad grupal de investigación Prueba teórica	30% 70%
d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	15	Actividad grupal de investigación Prueba teórica	30% 70%
	15		100%

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.	10	Actividad grupal de investigación Actividad grupal de investigación Prueba teórica	30% 70%
Recursos			
• Apuntes teóricos proporcionados por el profesor. • Aula de ordenadores.			
Observaciones			