Programación Didáctica

Módulo: **Seguridad y Alta Disponibilidad**

IES “Aldebarán” Fuensalida (Toledo)

2º C.F.G.S: **Seguridad y Alta Disponibilidad**
Curso: **2023/24**

INDICE

1.- Introducción

La Formación Profesional está orientada tanto al desarrollo y satisfacción personal del alumno como a la obtención de unos conocimientos de tipo técnico y/o humanístico que han de ser preparatorios para el mundo laboral o la Universidad.

La reforma educativa promulgada por la L.O.G.S.E. (Ley Orgánica de Ordenación General del Sistema Educativo) supuso un cambio radical en el sistema educativo existente hasta entonces. La Formación Profesional tradicional pasó a denominarse Ciclos Formativos, quedando estructurada en familias y niveles. Así, los Ciclos Formativos de Grado Medio permiten obtener el título de Técnico, mientras que los Ciclos Formativos de Grado Superior permiten obtener el título de Técnico Superior.

Posteriormente, la L.O.E. (Ley Orgánica de la Educación) estableció una nueva ordenación de los ciclos formativos, estableciendo el nuevo catálogo de la formación profesional, las unidades de competencia y los módulos formativos asociados del Catálogo Modular de Formación Profesional. Este nuevo marco formativo no hace sino acercar la Formación Profesional a las necesidades actuales de la sociedad del conocimiento, donde la movilidad laboral, las nuevas tecnologías, la cohesión e inserción laboral exigen un nuevo planteamiento del mercado laboral. Así pues, se pretende proporcionar a las personas la formación requerida por el sistema productivo y de acercar los títulos de formación profesional a la realidad del mercado laboral. Los Ciclos Formativos ofertados por la LOE están separados por familias, siendo una de ellas Informática.

Dado el extraordinario auge de la informática, y su gran implantación en la gran mayoría de trabajos actualmente, no es de extrañar que este ciclo formativo sea considerado por los alumnos como una buena alternativa profesional para su futuro.

Para la inserción de los alumnos en el mundo laboral de modo rápido y eficaz, el alumno debe aprender las técnicas y métodos más adecuados que garanticen la adquisición de los conocimientos y destrezas para desenvolverse en el sector informático.

Esta programación está referida al módulo de **Seguridad y Alta disponibilidad** del ciclo formativo de grado superior **Administración de Sistemas Informáticos en Red** en el centro **I.E.S. Aldebarán** de **Fuensalida (Toledo)**.

El módulo "Seguridad y Alta Disponibilidad" tiene asignada una duración de 100 horas lectivas distribuidas en 5 horas semanales durante 25 semanas aproximadamente.

1.1. Análisis del contexto

Para desarrollar una programación didáctica correcta y útil para una adecuada formación de los alumnos/as, no se puede trabajar de espaldas a la realidad social y económica en la que éstos viven. Por tanto, en este punto se comentarán las principales características del entorno en el que se encuentra el centro educativo, indicando cómo afectan estas al proyecto curricular.

Como ya se ha indicado al principio de la misma, esta programación didáctica de "Seguridad y alta disponibilidad" está desarrollada para impartirse en 2º del C.F.G.S. de Administración de Sistemas Informáticos en Red en el IES Aldebarán de Fuensalida (Toledo).

Para poder realizar una correcta programación es necesario analizar el entorno que nos rodea:

- La principal fuente de riqueza de la zona son polígonos industriales situados en la misma localidad y de las poblaciones próximas, donde se ubican múltiples empresas que abarcan diversas actividades industriales.
- Otra de las fuentes de empleo es Toledo, con multitud de empresas dedicadas principalmente a los servicios o la administración pública.
- Este es el único centro educativo público de la localidad en el que se imparte la educación secundaria obligatoria y los estudios de Bachillerato, siendo también el único en el que se imparten los ciclos formativos de la familia de Informática y Comunicaciones (“Administración de Sistemas Informáticos en Red” y “Sistemas Microinformáticos y Redes”), Programas de Formación Profesional Básica (“Electricidad y electrónica” y “Servicios comerciales”) y el ciclo de grado medio la familia profesional de Comercio (“Actividades Comerciales”).
- El centro tiene la siguiente lista de municipios de influencia (todos ellos de Toledo): Arcícollar, Camarena, Camarenilla, Fuensalida, Huecas, Portillo de Toledo, Santa Cruz de Retamar y Villamiel de Toledo.

Vistas las consideraciones anteriores, se puede añadir que, por regla general, los alumnos/as dispondrán de un ambiente familiar adecuado para el estudio, aunque muchas de las familias tienen un nivel económico bajo-medio, pero que permite la disponibilidad de medios didácticos en el hogar, como ordenador propio con acceso a internet.

En esta programación, se asumirá que la situación socioeconómica es la que se acaba de citar, no obstante, se tomarán medidas para asegurar que todos los alumnos/as tengan las mismas oportunidades, en el caso de que sus familias se desenvuelvan en situaciones desfavorables (económicamente o por otros motivos).

1.2. Características del módulo profesional

El módulo profesional de “Seguridad y Alta Disponibilidad” se imparte en el segundo curso del ciclo formativo de grado superior de “Administración de Sistemas Informáticos en Red”, y, junto con el resto de los módulos que componen el ciclo, contiene la formación necesaria para que el alumno pueda insertarse laboralmente y desarrollar su carrera profesional en el sector de los sistemas informáticos y redes.

Este módulo profesional abarca la formación necesaria para seleccionar y utilizar técnicas y herramientas específicas de seguridad informática en el ámbito de la administración de sistemas. Además, servirá para conocer arquitecturas de alta disponibilidad y utilizar herramientas de virtualización en la implantación de servicios de alta disponibilidad.

Las funciones de la administración segura de sistemas incluyen aspectos como:

- El conocimiento y correcta manipulación de todos los elementos que forman el componente físico y lógico de los equipos.
- La adopción de prácticas seguras de acuerdo al plan de seguridad física del sistema.
- La adopción de prácticas seguras de acuerdo al plan de seguridad lógica del sistema.

- El conocimiento y uso de técnicas seguras de acceso remoto a un sistema, tanto en modo usuario como en modo administrativo.
- La selección y aplicación de técnicas y herramientas de seguridad activa que actúen como medidas preventivas y/o paliativas ante ataques a al sistema.
- La instalación y configuración de herramientas de protección perimetral, cortafuegos y servidores «proxy».
- La instalación y configuración de servicios de alta disponibilidad que garanticen la continuidad de servicios y la disponibilidad de datos.
- El conocimiento y aplicación de la legislación vigente en el ámbito del tratamiento digital de la información.

Las actividades profesionales asociadas a estas funciones se aplican en:

- Mantenimiento de equipos. Hardware y software.
- Administración de sistemas en pequeñas y medianas empresas.
- Personal técnico de administración de sistemas en centros de proceso de datos.
- Personal técnico de apoyo en empresas especializadas en seguridad informática.

La formación del módulo contribuye a alcanzar los objetivos generales j), k), l), m), o), y p) del ciclo formativo.

También las competencias profesionales, personales y sociales e), f), i), j), k), m), n), o), r) y s) del título:

e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.
o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
r) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.
s) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- El conocimiento de las prácticas y pautas adecuadas, relativas a la seguridad física y lógica en un sistema informático.

- El conocimiento y análisis de técnicas y herramientas de seguridad activa, que actúen como medidas preventivas y/o paliativas ante ataques al sistema.
- El análisis y aplicación de técnicas y herramientas de seguridad activa.
- El análisis y aplicación de técnicas seguras de acceso remoto a un sistema.
- El análisis de herramientas y técnicas de protección perimetral para un sistema.
- La instalación, configuración y prueba de cortafuegos y servidores “proxy” como herramientas básicas de protección perimetral.
- El análisis de los servicios de alta disponibilidad más comunes, que garanticen la continuidad de servicios y aseguren la disponibilidad de datos.
- El conocimiento y análisis de la legislación vigente en el ámbito del tratamiento digital de la información.

1.3. Características del alumnado

Por regla general, el perfil más común del alumnado en el ciclo formativo que nos ocupa es el de un sujeto de 18 años o más, que ha finalizado los estudios de Bachillerato, ciclo formativo de grado medio de Informática o accede al ciclo habiendo superado la prueba de acceso, y busca obtener una rápida cualificación para acceder a una actividad profesional. Pero también hay casos de alumnos y alumnas que se matriculan por oferta modular, ya que pueden no haber superado la prueba de acceso correspondiente.

En este curso hay matriculados 23 alumnos. Es una enseñanza postobligatoria y específica, encaminada a la incorporación al mundo laboral, por lo tanto, se puede decir que es un alumnado motivado, que conoce el área profesional de la informática y que está deseoso de realizar una Formación en Centros de Trabajo en un puesto relacionado con la informática.

2.- Objetivos

El decreto que establece el currículo para Castilla La Mancha, establece los siguientes resultados de aprendizaje:

- Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
- Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
- Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
- Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
- Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
- Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
- Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

3.- Contenidos

Los contenidos se han estructurado de manera que quedan englobados en 8 Unidades de Trabajo:La siguiente tabla resume los períodos lectivos dedicados a cada unidad.

En cada uno se combinará una parte teórica con otra práctica. Duración: 104 horas.

Unidad	Temporalización
Unidad 1.Conceptos básicos de la seguridad informática	8
Unidad 2. Criptografía	32
Unidad 3. Hardware y almacenamiento	15
Unidad 4. Pentesting	14
Unidad 5. Cortafuegos	12
Unidad 6. Proxies	12
Unidad 7. Alta Disponibilidad	12

3.1.- Secuenciación de las Unidades de trabajo

Este módulo se impartirá en la misma aula donde hay un equipo informático para cada alumno.

El curso se divide en dos evaluaciones a lo largo de las cuales se irán distribuyendo las unidades didácticas de la siguiente forma:

Evaluación	Unidad
Primera (52 periodos lectivos)	Unidad 1.Conceptos básicos de la seguridad informática
	Unidad 2. Sistemas de identificación. Criptografía
	Unidad 3. Hardware y almacenamiento
Segunda	Unidad 4. Pentesting
	Unidad 5.Cortafuegos

	(52 periodos lectivos)	Unidad 6. Proxies
		Unidad 7. Alta Disponibiidad

Esta es una secuenciación ideal que, previsiblemente, se verá afectada por el ritmo de aprendizaje del alumnado.

4.- Metodología

a. Tipos de actividades de E/A

Los contenidos y prácticas a realizar por los alumnos, se transmitirán por los siguientes medios:

- Papás.
- Aula virtual de Educamos CLM.
- Blogs personales del profesor:

  https://seguridadfuensalida.blogspot.com/

- Google:
  - Classroom.

La materia se divide en clases teóricas y clases prácticas en el aula se distribuirán, siempre que se pueda, un alumno por ordenador.

No se debe interpretar la exposición oral como una metodología marcadamente expositiva sino como una forma de colaboración o de engranaje en la que, en algunos puntos, será el propio alumno el que individualmente o en grupos tenga que preparar e indagar sobre algún

contenido propuesto y exponerlo al resto o realizar puestas en común con sus compañeros.

El nivel de profundización estará en función del grado inicial de formación de los alumnos en esta materia, incluyendo tanto teoría como práctica.

b. Agrupamiento del alumnado

1 alumno por ordenador

c. Organización de espacios y tiempos

Las clases se dan en periodos lectivos de 55 minutos.

d. Fuentes bibliográficas, documentales y de información

e. Recursos materiales

Los contenidos y prácticas a realizar por los alumnos, se transmitirán por los siguientes medios:

- Papás.
- Classroom de Google.

Las prácticas tendrán una fecha de entrega máxima y se podrá utilizar algún procedimiento telemático de evaluación si fuera necesario.

Recursos informáticos del aula.

Para los puestos de los alumnos:

16 Ordenadores clientes de prestaciones actuales. Estos equipos deberán estar interconectados en red con Windows 10.

Para el puesto del profesor:

- 1 Ordenador cliente de prestaciones actuales, conectado a la red, con Windows 10. (semejante al de los alumnos).
- Proyector de pantallas conectado al ordenador del profesor.

Sistemas operativos.

Sistema Servidor tipo Microsoft Windows 2003,2008,2016 Server. Sistema Operativo Microsoft Windows 10 y Ubuntu en cada uno de los puestos.

Sistema de protección Antivirus.

Antivirus Nod32 u otro.

Recursos bibliográficos.

No

5.- Evaluación

Criterios de evaluación

Se definen para cada uno de los resultados de aprendizaje.

1. **Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades:**

b) Se ha valorado la importancia de mantener la información segura.

c) Se han descrito las diferencias entre seguridad física y lógica.

d) Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.

e) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.

f) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.

g) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.

h) Se han indicado las características de una política de seguridad basada en listas de control de acceso.

i) Se ha valorado la importancia de establecer una política de contraseñas.

j) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información:

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.

b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad entre otros).

c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.

d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.

e) Se han seleccionado estrategias para la realización de copias de seguridad.

f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.

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.

3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático:

a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.

b) Se han clasificado los principales tipos de software malicioso.

c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.

d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.

e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

f) Se han aplicado técnicas de recuperación de datos.

4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico:

a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.

b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.

c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.

d) Se han aplicado medidas para evitar la monitorización de redes cableadas.

e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.

f) Se han descrito y utilizado sistemas de identificación como la firma electrónica o certificado digital, entre otros.

g) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.

b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.

c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.

d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.

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.

Procedimientos de evaluación

Se realizarán exámenes escritos de teoría, prácticas, trabajos y ejercicios durante todo el curso. Las prácticas podrán ser individuales o en grupo dependiendo lo que demanden las mismas.

Habrá un examen final al finalizar las clases para todos aquellos alumnos que tengan suspendida la asignatura.

Criterios de calificación

Los criterios de calificación se establecen en la siguiente tabla:

<table>
<tr><th colspan="3">1ª Ordinaria</th></tr>
<tr><td>Primera Evaluación</td><td>● Prácticas 20%
● Examen 80%</td><td rowspan="2">Calificación final:

Se calcula realizando la media aritmética de las dos evaluaciones. En el caso de alumnos suspensos o con pérdida de evaluación continua, esta calificación será la correspondiente a la media obtenida entre la calificación del examen final</td></tr>
<tr><td>Segunda Evaluación</td><td>● Prácticas 20%
● Examen 80%</td></tr>
</table>

		y la calificación obtenida en las prácticas entregadas
Para aplicar los porcentajes en cada una de las evaluaciones, la calificación obtenida en cada una de las partes ha de ser MAYOR O IGUAL A 4; por debajo de esta calificación no se realizará el cálculo de porcentajes considerándose la evaluación como NO SUPERADA		
Para considerar una evaluación como SUPERADA, la calificación obtenida en la misma debe ser MAYOR O IGUAL QUE 5, en caso contrario, la evaluación se considerará NO SUPERADA.		
2ª Ordinaria: examen teórico y práctico		

Medidas de recuperación y profundización

Durante el primer y segundo periodo evaluativo.

El alumno que no vaya adquiriendo los elementos de capacidad en este periodo será objeto de un seguimiento y refuerzo especial por parte del profesor. Si aún así no se consigue una nota positiva al final del periodo evaluativo queda a criterio del profesor la realización de pruebas de recuperación y evaluación en posteriores periodos evaluativos.

Durante el último periodo evaluativo.

El alumno que no vaya adquiriendo los elementos de capacidad en este periodo podrá, a criterio del profesor y atendiendo a los Proyectos curriculares del centro y del ciclo, realizar pruebas evaluativas para demostrar que ha adquirido las competencias básicas del módulo con el peso de calificación señalado en la programación.

Así mismo, los alumnos también tendrán que presentar aquellos trabajos que no hubieran presentado o que fueran desechados en el plazo solicitado.

Las pruebas de recuperación final de la primera evaluación ordinaria y la segunda evaluación ordinaria serán de aquellas que el

alumno no haya superado y será una prueba escrita y en base a los mínimos exigibles de la evaluación.

Evaluación del proceso de enseñanza/aprendizaje

Al final del curso, se pasará una encuesta al alumnado para valorar el proceso.

Planificación de las actividades de recuperación de los módulos no superados

Dado que se utiliza la plataforma EducamosCLM a lo largo del módulo, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de la segunda convocatoria ordinaria.

Pérdida de la evaluación continúa

En el caso de que un alumno no asista a clase, puede perder el derecho a ser evaluado de forma continua. En concreto aquellos alumnos que tengan un 20% de faltas de asistencia injustificadas POR MÓDULO perderán el derecho a la evaluación continua de ese módulo, por lo que deberán presentarse a una prueba objetiva al finalizar el módulo.

En este módulo, el máximo número de faltas injustificadas que puede tener un alumno antes de perder el derecho a la evaluación continua es 20.

La pérdida de la evaluación continua se realiza únicamente para el módulo en el que se hayan detectado las faltas de asistencia injustificadas, y no para todo el ciclo formativo.

La justificación válida para los alumnos se realizará mediante un justificante médico expedido por autoridades médicas o por causas de fuerza mayor que el alumno pueda alegar y sean aceptadas por el profesor. Este justificante deberá presentarse en el plazo de quince días desde la falta de asistencia.

Adicionalmente, para fomentar el cuidado y corresponsabilidad del material de clase y prepararles para el trabajo en empresa de forma responsable, los alumnos que causen daño intencionado o por negligencia no cuiden el mismo deberán reparar el daño causado al amparo de la Ley de Autoridad del Profesorado. En el caso de que no reparen el daño causado **perderán el derecho a la evaluación continua**. Los alumnos volverán a ser evaluados de forma continuada cuando reparen el daño causado.

6.- Atención al alumnado con necesidades específicas de atención educativa

Se contemplan diferentes tipos de actuaciones:

- Adaptar las actividades, si fuera posible, a sus circunstancias. En todo caso, siempre deberían cubrir las necesidades para la adquisición de la competencia profesional.
- Trabajar en coordinación con el departamento de orientación en la orientación efectiva de estos alumnos, si su desarrollo profesional dentro del perfil definido en el ciclo resultase imposible.
- Favorecer la integración de este alumno en el grupo-aula a través de actividades donde desarrolle un papel reconocido por el grupo y mejore su nivel de autoestima.

Esta situación propiciará que se diseñen los siguientes tipos de actividades:

- Actividades generales de cada unidad de trabajo.
- Actividades de refuerzo para aquellos alumnos que se considere necesario.
- Actividades de ampliación para aquellos alumnos que avancen a un ritmo mayor que otros alumnos del aula.

Además, en los casos en que sea imposible la realización o asimilación de determinados contenidos, se valorará la posibilidad de sustituir dichos contenidos por ampliación o profundización en otros, en la medida de lo posible, de manera que la carencia de una determinada capacidad sea sustituida por la especialización en otra.

7.- Actividades Complementarias.

Para el presente curso escolar no se contempla ninguna actividad complementaria relacionada con el módulo de Seguridad Informática.

8.- Relación entre los criterios de evaluación e indicadores.

CRITERIOS DE EVALUACIÓN	INDICADORES
UT1. Conceptos sobre Seguridad Informática. ● Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. ● Se han descrito las diferencias entre seguridad física y lógica. ● Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. ● Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. ● Se han identificado las fases del análisis forense ante ataques a un sistema. ● Se han identificado las herramientas hardware y software para realizar un análisis forense. ● Se ha identificado el lugar más idóneo en el que situar un CPD. ● Se ha regulado adecuadamente los Sistemas de alimentación ininterrumpida (SAI)	Analiza la problemática general de la seguridad informática. Conoce los principios sobre los que se sustenta. Conoce el significado de alta disponibilidad. Identifica las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas. Diferencia la seguridad física y lógica, y la pasiva de la activa. Conoce las diferentes medidad de seguridad física. Conoce los diferentes tipso de SAIs-
UT2. Seguridad Lógica. ● Se han establecido planes de actuación incluyendo copias de seguridad. ● Se ha valorado la importancia de mantener actualizadas las copias de seguridad. ● Se han adoptado políticas de contraseñas. ● Se han valorado las ventajas que supone la utilización de sistemas biométricos.	Profundizar en aspectos de seguridad lógica. Valorar la importancia del uso de contraseñas seguras. Restringir el acceso autorizado en el arranque, sistemas operativos, ficheros, carpetas y aplicaciones. Garantizar el acceso restringido de los usuarios a datos y aplicaciones, mediante políticas de seguridad.

● Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. ● Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.	Valora la importancia de realizar periódicamente copias de seguridad de la información sensible de nuestros sistemas. Aprende las diferencias, ventajas e inconvenientes entre los sistemas de almacenamiento redundante (RAID) y conoce sus opciones de configuración y prueba
UT3. Criptografía. ● Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. ● Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	Profundiza en aspectos de criptografía asociada a la confidencialidad de la información y de las comunicaciones. Garantiza la confidencialidad de la información. Garantiza la privacidad de las comunicaciones. Diferencia ventajas e inconvenientes de la criptografía simétrica y asimétrica. Analiza nuevos procesos de identificación digital seguros mediante firma digital, certificado digital y DNI electrónico.
UT4. Seguridad Activa. ● Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. ● Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. ● Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	Profundiza en aspectos de seguridad activa. Analizar las ventajas de disponer el sistema y aplicaciones actualizadas. Conocer los diferentes tipos de malware. Valorar la utilidad del software de seguridad. Valorar la utilidad del software antispam. Analiza las ventajas de disponer de sistema y aplicaciones actualizadas. Entender el concepto de Hardening. Analizar la seguridad en las redes corporativas.
UT5. Seguridad Perimetral. ● Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. ● Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna. ● Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. ● Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	Valora los peligros externos a las redes corporativas y conoce las medidas de seguridad perimetrales para hacerles frente. Valora los nuevos peligros derivados de la conexión a redes. Adopta medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas. Analiza las principales vulnerabilidades de las redes inalámbricas. Comprende la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros.

● Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. ● Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. ● Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. ● Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	Conoce y emplea protocolos y aplicaciones seguras en comunicaciones.
UT6. El cortafuegos ● Se han descrito las características, tipos y funciones de los cortafuegos. ● Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. ● Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. ● Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. ● Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. ● Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	Comprende la importancia de los puertos de comunicaciones y su filtrado mediante cortafuegos o firewall. Aprende el significado de las listas de control de acceso (ACL) en routers y cortafuegos. Comprender el comando iptables. Añadir reglas a iptables. Entender el registro de sucesos.

UT7. El proxy ● Se han identificado los tipos de «proxy», sus características y funciones principales. ● Se ha instalado y configurado un servidor «proxy-cache». ● Se han configurado los métodos de autenticación en el «proxy». ● Se ha configurado un «proxy» en modo transparente. ● Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web. ● Se han solucionado problemas de acceso desde los clientes al «proxy». ● Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas. ● Se ha configurado un servidor «proxy» en modo inverso. ● Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».	Comprende la importancia y aprende a configurar servidores proxy. Aprender a configurar el cliente proxy. Entender los proxies inversos.
UT8. Configuraciones de alta disponibilidad. ● Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. ● Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. ● Se han evaluado las posibilidades de la vitalización de sistemas para implementar soluciones de alta disponibilidad. ● Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal. ● Se ha implantado un balanceador de carga a la entrada de la red interna. ● Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. ● Se ha evaluado la utilidad de los sistemas de «clúster» para aumentar la fiabilidad y productividad del sistema.	Analiza las distintas configuraciones de alta disponibilidad. Valora la importancia de realizar un buen análisis de riesgos potenciales en sistemas críticos y adopta medidas para paliar sus posibles consecuencias. Conoce las opciones de configuración y administración de balanceo de carga entre distintas conexiones de red. Realiza configuraciones de alta disponibilidad de servidores mediante virtualización de sistemas operativos.

● Se han analizado soluciones de futuro para un sistema con demanda creciente. ● Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.	
UT9. Normativa legal en materia de seguridad informática. ● Se ha descrito la legislación sobre protección de datos de carácter personal. ● Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. ● Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. ● Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen. ● Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. ● Se han contrastado las normas sobre gestión de seguridad de la información. ● Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	Conoce la normativa española en materia de seguridad informática. Analiza la normativa y aplicaciones del RGPD, en materia de seguridad de los datos. Analiza la legislación sobre certificado digital y forma electrónica. Analiza la normativa y aplicaciones de la LSSICE, en materia de comercio electrónico y actividades empresariales vía Internet. Valora la importancia de la normativa como reguladora de derechos y obligaciones a ciudadanos y empresas. Conoce el Código Penal en lo referente a los delitos informáticos.

Anexo I.- Plan de lectura

El nivel de los estudios y los contenidos del módulo implican actualización permanente y búsqueda constante de soluciones para los múltiples escenarios de aprendizaje que

se presentarán. Además, la continua aparición de nuevos ataques, así como de las herramientas utilizadas para su detección y prevención, obliga a consultas frecuentes de los manuales correspondientes.

En cada una de las unidades en el Aula virtual de EcucamosCLM se recomienda al alumno la lectura de artículos, libros, así como de TFG entra otros textos para ampliar y complementar los contenidos de cada unidad.

Es por ello que se recomendará al alumnado la búsqueda y comparación de recursos en línea entre la amplia variedad de blogs tecnológicos y sitios web especializados.