

# Seguridad y Alta Disponibilidad

## 2º ASIR (tardes)

Programación didáctica

Curso: 2018/2019

Departamento de Informática

*Álvaro Pérez*

## Índice de contenidos

<b>1. Introducción</b>	3
<b>1.1. Contextualización</b>	3
<b>2. Objetivos</b>	4
<b>2.1. Resultados de aprendizaje</b>	4
<b>2.2. Competencias profesionales, personales y sociales</b>	4
<b>3. Contenidos</b>	6
<b>3.1. Secuenciación y temporización</b>	8
<b>4. Metodología didáctica</b>	9
<b>5. Evaluación</b>	10
<b>5.1. Criterios de evaluación</b>	10
<b>5.2. Criterios de calificación</b>	13
<b>5.3. Actividades de refuerzo y ampliación</b>	14
<b>5.4. Evaluación del proceso de enseñanza y aprendizaje</b>	14
<b>6. Criterios de recuperación</b>	16
<b>6.1. Alumnos pendientes</b>	16
<b>7. Medidas de atención a la diversidad y alumnos con N.E.E.</b>	17
<b>8. Fomento de la lectura</b>	19
<b>9. Recursos didácticos</b>	20
<b>10. Bibliografía de referencia</b>	21
<b>11. Actividades complementarias y extraescolares</b>	22

# 1. Introducción

El módulo de Seguridad y Alta Disponibilidad se encuadra en el segundo curso del Ciclo Formativo de Grado Superior correspondiente a la titulación Técnico Superior de Administración de Sistemas Informáticos en Red. Dicho módulo posee una duración de 100 horas lectivas (5 horas semanales).

## 1.1. Contextualización

Esta programación está orientada teniendo en cuenta las características del centro en el que se imparte. Estas características son:

- Centro Público, ubicado en un núcleo urbano con una población que ronda los 55.000 habitantes, donde acuden numerosos alumnos de zonas cercanas con menor población en régimen diurno y vespertino.
- El municipio dispone de gran cantidad de empresas del sector servicios que satisfacen las necesidades de todo el sector industrial de la zona. Ante esta situación, existe una creciente demanda de profesionales que sean capaces de desarrollar aplicaciones informáticas, y que son demandados tanto por las industrias como por las empresas de servicios.
- Las asignaturas y los módulos de informática llevan impartándose en este centro diversos años, por lo que está dotado de todos los recursos necesarios para llevar a cabo los contenidos.
- Es un centro ubicado en un municipio muy cercano a una gran ciudad por lo que cuenta con amplias redes de transporte, que facilitarán las posibilidades de desplazamiento para el caso de actividades extraescolares y complementarias, con una amplia oferta cultural.
- En cuanto a la climatología será apacible, propia de la Comunidad Valenciana, que evitará en parte el absentismo escolar.

## 2. Objetivos

El módulo de Seguridad y Alta Disponibilidad se encuadra en el segundo curso del Ciclo Formativo de Grado Superior correspondiente a la titulación Técnico Superior de Administración de Sistemas Informáticos en Red. Dicho módulo posee una duración de 100 horas lectivas (5 horas semanales).

### 2.1. Resultados de aprendizaje

Los resultados de aprendizaje que se pretenden alcanzar con este módulo son:

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

### 2.2. Competencias profesionales, personales y sociales

La formación impartida en este módulo tiene como fin contribuir a alcanzar las siguientes competencias profesionales, personales y sociales:

1. e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
2. f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
3. i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
4. j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
5. k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

6. m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
7. 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
8. o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
9. r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
10. s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

Este módulo profesional contiene 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. La definición de estas funciones incluye 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
- La adopción de prácticas seguras de acuerdo al plan de seguridad lógica del
- 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, cortafuego 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.

## 3. Contenidos

### UT1: PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD

1. Introducción a la seguridad informática
2. Confidencialidad. Integridad. Disponibilidad.
3. Elementos vulnerables. Hardware, Software y datos.
4. Amenazas
5. Protección. Auditorias de Seguridad. Medidas de seguridad

### UT2: SEGURIDAD PASIVA. HARDWARE Y ALMACENAMIENTO

1. Ubicación y protección física
2. Sistemas de alimentación ininterrumpida (SAI)
3. Almacenamiento de la información
4. Alta disponibilidad de almacenamiento (RAID)
5. Almacenamiento externo
6. Network Attached Storage. FreeNAS
7. Storage Area Network

### UT3: SEGURIDAD PASIVA. RECUPERACIÓN DE DATOS

1. Introducción
2. Tipos de copias de seguridad
3. Copias de seguridad de los datos en Windows y Linux
4. Modos de recuperación frente a pérdidas en el sistema operativo
5. Creación de imágenes del sistema
6. Copia de seguridad del registro
7. Políticas de copias de seguridad

### UT4: CRIPTOGRAFÍA

1. ¿Cómo aseguramos la privacidad de la información?
2. Un poco de historia de la criptografía
3. Criptografía simétrica y asimétrica
4. Algoritmos
5. Función Resumen
6. Firma digital
7. Certificados digitales
8. PKI

### UT5: ALTA DISPONIBILIDAD

1. Alta disponibilidad

2. Redundancia y tolerancia a fallos
3. Sistemas de clusters
4. Clasificación de los clusters
5. Balanceadores de carga
6. Redundancia en enrutadores

## **UT6: AUDITORÍA DE SEGURIDAD**

1. Estándares / Modelos / Listas de seguridad
2. Auditoria / Test de intrusión
3. Tipos de auditoria
4. Test de intrusión
5. Footprint
6. Fingerprint
7. Fingerprinting desde Metasploit

## **UT7: SOFTWARE ANTIMALWARE**

1. Software malicioso.
2. Clasificación del malware. Métodos de infección.
3. Protección y desinfección.

## **UT8: SEGURIDAD EN REDES CORPORATIVAS**

1. Seguridad en la conexión a redes no fiables
2. Protocolos seguros (HTTPS y SSH)
3. Seguridad en redes cableadas.
- 4.
5. Sistemas de Detección de intrusos (IDS)
6. Seguridad en redes inalámbricas

## **UT9: SEGURIDAD PERIMETRAL. CORTAFUEGOS**

1. Seguridad de alto nivel
2. Cortafuegos: qué son y para qué sirven
3. Tipos de cortafuegos
4. Filtrado de paquetes
5. Uso de cortafuegos
6. Arquitecturas de red con cortafuegos
7. Monitorización y logs

## **UT10: SEGURIDAD PERIMETRAL. PROXY**

1. Introducción
2. Características del proxy

3. Funcionamiento del proxy
4. WinGate
5. Squid

## **UT11: LEGISLACIÓN Y NORMAS SOBRE SEGURIDAD**

1. Ley Orgánica de Protección de Datos (LOPD).
2. Reglamento General de Protección de Datos (RGPD)
3. Ley de Servicios de la sociedad de la información y de comercio electrónico (LSSICE)

### **3.1. Secuenciación y temporización**

#### **Primera evaluación**

**UT1: PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD**

**UT2: SEGURIDAD PASIVA. HARDWARE Y ALMACENAMIENTO**

**UT3: SEGURIDAD PASIVA. RECUPERACIÓN DE DATOS**

**UT4: CRIPTOGRAFÍA**

**UT5: ALTA DISPONIBILIDAD**

**UT6: AUDITORÍA DE SEGURIDAD**

#### **Segunda evaluación**

**UT7: SOFTWARE ANTIMALWARE**

**UT8: SEGURIDAD EN REDES CORPORATIVAS**

**UT9: SEGURIDAD PERIMETRAL. CORTAFUEGOS**

**UT10: SEGURIDAD PERIMETRAL. PROXY**

**UT11: LEGISLACIÓN Y NORMAS SOBRE SEGURIDAD**

## **4. Metodología didáctica**

El método que se seguirá para el desarrollo de las clases será el siguiente:

1. Exposición de conceptos teóricos en clase a partir del libro de texto y los materiales complementarios que el profesor estime convenientes para una mejor comprensión de los contenidos.
2. Planteamiento de ejercicios y actividades en el aula de aquellos temas que lo permitan, resolviéndose aquellos que se estime oportuno.
3. Presentación en clase de las diversas prácticas a realizar y desarrollo en la misma de todas aquellas que el equipamiento permita.
4. Realización de trabajos y exposiciones por parte del alumnado, de aquellos temas que se brinden a ello o que se propongan directamente por el profesor, con lo que se conseguirá una activa participación y un mayor acercamiento a los conceptos y contenidos del módulo.

En una etapa inicial del curso, se seguirá el método tradicional de exposición por parte del profesor, con el fin de explicar los conceptos básicos que éste módulo necesita para poder arrancar.

Tan pronto como sea posible, la metodología pasará a ser fundamentalmente procedimental, con la realización de prácticas, invitando al alumno, bien individualmente o bien en grupo, a que exponga su planteamiento ante sus compañeros, para efectuar los pertinentes comentarios, intercambio de pareceres y discusión de las soluciones propuestas.

En la medida de lo posible se tendrá una atención individualizada por parte de los profesores a cada alumno o grupo de alumnos. Se fomentará que cada uno plantee sus dudas o problemas sobre el ejercicio. Finalmente se comentarán las posibles soluciones, así como los fallos y errores que suelen cometerse de forma más habitual.

## 5. Evaluación

El proceso de evaluación trata dos vertientes igual de importantes. Estas son, la evaluación del proceso de aprendizaje del alumno y la evaluación del proceso de enseñanza empleado por el profesor.

El proceso de evaluación, ha de ser además, continuo durante todo el proceso educativo, abarcando tanto una evaluación formativa para obtener información constante de carencias y progresos educacionales, como una evaluación sumativa con el fin de analizar el grado de consecución de los objetivos propuestos.

### 5.1. Criterios de evaluación

Los criterios de evaluación para cada resultado de aprendizaje son los siguientes:

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

#### **Criterios de evaluación:**

- 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.
- i) Se han identificado las fases del análisis forense ante ataques a un sistema.

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

#### **Criterios de evaluación:**

- 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.
- 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.
- i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

**Criterios de evaluación:**

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

4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

**Criterios de evaluación:**

- a) Se han descrito las características, tipos y funciones de los cortafuegos.
- b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
- c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
- d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
- e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las

reglas se aplican correctamente.

- f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
- g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
- h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

**Criterios de evaluación:**

- a) Se han identificado los tipos de «proxy», sus características y funciones principales.
- b) Se ha instalado y configurado un servidor «proxy-cache».
- c) Se han configurado los métodos de autenticación en el «proxy».
- d) Se ha configurado un «proxy» en modo transparente.
- 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».

6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

**Criterios de evaluación:**

- a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
- 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.
- h) Se han analizado soluciones de futuro para un sistema con demanda creciente.
- i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

7. Reconoce la legislación y normativa sobre seguridad y protección de datos

valorando su importancia.

**Criterios de evaluación:**

- 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 el deber 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.
- g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

## 5.2. Criterios de calificación

Para la evaluación del módulo se utilizará el siguiente baremo al final de cada una de las evaluaciones:

- Un 60% de la nota lo determinará la entrega de prácticas (parte práctica del módulo).
- El 40% los exámenes (parte teórica del módulo).

La nota mínima para aprobar es de 5, siendo necesario tener como mínimo un 5 en la parte práctica y teórica para poder hacer media.

Los trabajos prácticos tendrán una fecha tope de entrega, una vez superada dicha fecha, el alumno podrá entregar las prácticas, pero como máximo su nota será un 5 en dicha práctica.

Es obligatorio tener más de un 4 todas las prácticas para aprobar el módulo. Si un alumno tiene en una práctica menos de un 4, suspende el módulo, indistintamente como tenga el resto de tareas.

A su vez, según el plan de mejora elaborado por el centro se tendrán en cuenta las faltas de ortografía en todos los trabajos y exámenes en esta forma:

- sanción de -0,20 puntos por error gráfico (cuatro tildes= 1 falta) hasta un máximo de penalización de 2,5 puntos.

Por otra parte, actitudes como utilizar el ordenador para jugar, instalar software no autorizado, cambiar la configuración de los equipos, actitudes que impidan el funcionamiento de clase con interrupciones continuas, no traer material, será tenido en cuenta y penalizado, independientemente de las sanciones que pudiera dictar el consejo escolar.

## **Calificación final**

La nota final del módulo será la media aritmética de las 2 evaluaciones.

## **Recuperación final**

Habrà una recuperación final, la recuperación de los bloques temáticos suspendidos se realizará en un examen final de toda la materia del módulo, sin que existan exámenes de recuperación parciales.

No habrá recuperación de prácticas final. No obtener por lo menos un 5 en prácticas se suspende el módulo.

## **5.3. Actividades de refuerzo y ampliación**

Se dispone de diversidad de actividades de refuerzo y ampliación por unidad didáctica. Con este tipo de actividades pretendemos dar respuesta a los diferentes ritmos de aprendizaje que presentan los alumnos. Las actividades de refuerzo permitirán que alumnos con un ritmo de aprendizaje menor lleguen a alcanzar las capacidades de la unidad, mientras que las actividades de ampliación permitirán que alumnos con un ritmo de aprendizaje mayor puedan profundizar en los contenidos de la unidad una vez alcanzadas las capacidades.

## **5.4. Evaluación del proceso de enseñanza y aprendizaje**

La evaluación del proceso de aprendizaje está dirigida a conocer el nivel de competencia alcanzado en el desarrollo de las capacidades, a adaptar la enseñanza a sus necesidades.

Para la evaluación del proceso de aprendizaje, entre otros, los siguientes aspectos:

La evaluación se realizará tomando como referencia las capacidades y criterios de evaluación establecidos.

Para la evaluación del proceso de enseñanza, entre otros, los siguientes aspectos:

### **¿Qué evaluar?**

Por tanto se debe evaluar la programación, la intervención del profesor, los recursos, los espacios y tiempos previstos, la participación de alumnos, los criterios e instrumentos de evaluación aplicados, etc. Pero además, se debe evaluar la coordinación docente, la adecuación de las decisiones del Proyecto curricular de etapa y la coherencia entre los Proyectos curriculares de cada etapa así como con el Proyecto educativo de centro.

### **¿Cómo evaluar?**

En relación a los procedimientos e instrumentos para la evaluación de la enseñanza, utilizaremos los siguientes:

El contraste de experiencias con otros compañeros del equipo docente o de otros centros.

La reflexión a partir del análisis comparativo entre resultados esperados y los obtenidos.

Los cuestionarios contestados por los propios profesores y por los alumnos sobre asuntos que afecten a la marcha general del centro y del módulo.

### **¿Cuándo evaluar?**

La intervención educativa debe ser continua y conviene tomar datos a lo largo del proceso para hacer los cambios pertinentes en el momento adecuado. No obstante, dadas las características de los diferentes elementos del proceso y de los documentos en que se plasman, hay momentos especialmente indicados para recoger la información que sirve de base para la evaluación.

La evaluación inicial al comienzo de curso para situar tanto el punto de partida del grupo aula como la del equipo docente, así como los recursos materiales y humanos de que dispone el centro.

Tras la finalización de cada unidad didáctica para tomar decisiones sobre posibles cambios en la propia unidad o siguientes.

Al final del módulo, los datos tomados permitirán evaluar y tomar decisiones de modificación de las programaciones.

## **6. Criterios de recuperación**

Habr  una recuperaci3n final en la evaluaci3n ordinaria, esta recuperaci3n consistir  en un examen final de toda la materia del m3dulo, sin que existan ex menes de recuperaci3n parciales. No habr  recuperaci3n de pr cticas final. No obtener por lo menos un 5 en pr cticas se suspende el m3dulo, y el alumno tendr  que ir a la convocatoria extraordinaria.

Si al finalizar la convocatoria ordinaria de marzo, el alumno no consigue superar los objetivos m nimos del m3dulo, el equipo educativo decidir  si repite el m3dulo de forma presencial el curso siguiente o si acceder  a la convocatoria extraordinaria, seg n especifica el D.O.G.V. 3.531 Resoluci3n del 24 de junio de 1999.

Para la convocatoria extraordinaria se va con toda la parte de teor a. Los alumnos con teor a suspendida y pr cticas aprobadas, se guarda la nota de pr cticas. Los alumnos con pr cticas suspendidas y teor a aprobada, NO se guarda la nota de teor a para la extraordinaria. Para recuperar pr cticas habr  que hacer uno o varios trabajos, que el profesor habr  propuesto en Marzo.

### **6.1. Alumnos pendientes**

Los alumnos con el m3dulo pendiente que no asistan habitualmente a clase, para la convocatoria ordinaria del m3dulo, ser n evaluados durante el mes de junio, de acuerdo con las directrices generales especificadas por el equipo directivo para la asignaci3n de fechas para la realizaci3n de dichas pruebas. Para la prueba de la convocatoria extraordinaria, regir n los mismos criterios que el resto de alumnos del m3dulo.

## 7. Medidas de atención a la diversidad y alumnos con N.E.E.

### Introducción y objetivos

Esta etapa educativa debe atender las necesidades educativas de los alumnos y alumnas, tanto de los que requieren un refuerzo porque presentan ciertas dificultades en el aprendizaje como de aquellos cuyo nivel esté por encima del habitual.

Escalonar el acceso al conocimiento y graduar los aprendizajes constituye un medio para lograr responder a la diversidad del alumnado, de manera que se puedan valorar progresos parciales. Representa también un factor importante el hecho de que los alumnos y alumnas sepan qué es lo que se espera de ellos.

De los objetivos generales del módulo, se tendrá en cuenta que, la adquisición de las capacidades presentará diversos grados, en función de esta diversidad del alumnado.

Por último será el profesor o profesora el que adopte la decisión de que objetivos, contenidos, metodología, actividades, instrumentos y criterios de evaluación adaptará según las características del alumnado de los grupos que imparta.

### Metodología

La atención a la diversidad es uno de los elementos fundamentales a la hora del ejercicio de la actividad educativa, pues se trata de personalizar el proceso de enseñanza-aprendizaje, adecuándolo a las necesidades y al ritmo de trabajo y desarrollo del alumnado.

Se pueden ofrecer vías para la atención a la particular evolución de los alumnos y alumnas, tanto proponiendo una variada escala de dificultad en sus planteamientos y actividades como manteniendo el ejercicio reforzado de las habilidades básicas. La atención a la diversidad se podrá contemplar de la siguiente forma:

- Desarrollando **cuestiones de diagnóstico previo**, al inicio de cada unidad didáctica, para detectar el nivel de conocimientos y de motivación del alumnado que permita valorar al profesor el punto de partida y las estrategias que se van a seguir. Conocer el nivel del que partimos nos permitirá saber qué alumnos y alumnas requieren unos conocimientos previos antes de comenzar la unidad, de modo que puedan abarcarla sin dificultades. Asimismo, sabremos qué alumnos y alumnas han trabajado antes ciertos aspectos del contenido para poder emplear adecuadamente los criterios y actividades de ampliación, de manera que el aprendizaje pueda seguir adelante.
- Incluyendo **actividades de diferente grado de dificultad**, bien sean de contenidos mínimos, de ampliación o de refuerzo o profundización, permitiendo que el profesor seleccione las más oportunas atendiendo a las capacidades y al interés de los alumnos

y alumnas.

- Ofreciendo **textos de refuerzo o de ampliación** que constituyan un complemento más en el proceso de enseñanza-aprendizaje.
- Programando **actividades de refuerzo** cuando sea considerado necesario para un seguimiento más personalizado.

## 8. Fomento de la lectura

A fin de que el alumno desarrolle su comprensión lectora, se aplicarán estrategias que le faciliten su consecución:

- Favorecer que los alumnos activen y desarrollen sus conocimientos previos.
- Permitir que el alumno busque por sí solo la información, jerarquice ideas y se oriente dentro de un texto.
- Activar sus conocimientos previos tanto acerca del contenido como de la forma del texto.
- Relacionar la información del texto con sus propias vivencias, con sus conocimientos, con otros textos, etc.
- Jerarquizar la información e integrarla con la de otros textos.
- Reordenar la información en función de su propósito.
- Ayudar a que los alumnos elaboren hipótesis sobre el tema del texto que se va a leer con apoyo de los gráficos o imágenes que aparecen junto a él.
- Realizar preguntas específicas sobre lo leído.
- Formular preguntas abiertas, que no puedan contestarse con un sí o un no.
- Coordinar una discusión acerca de lo leído.

Para la enseñanza y el aprendizaje de la lectura vamos a trabajar con:

- Lectura de textos cortos relacionados con el tema y preguntas relacionadas con ellas.
- Lectura de materiales que se habilitarán en la plataforma moodle del centro educativo.
- Lectura en voz alta motivadora de materiales de clase con su explicación correspondiente.
- Lectura silenciosa que antecede a la comprensión, estudio y memorización.
- Lectura de periódicos y comentarios en clase de informaciones relacionadas con la materia.

En cada sesión se dedicarán entre 10-15 minutos a la lectura de textos relacionados con los contenidos de la unidad que se esté tratando, tanto aquellos provistos por los libros y materiales, como los elaborados por los propios alumnos (ejercicios realizados como deberes para casa, actividades de investigación, etc.). Se incrementará el tiempo en función del nivel de progresión de los grupos.

Diseño y aplicación de las estrategias de comprensión lectora:

- Se realizarán actividades en cada unidad didáctica leyendo individualmente para ejercitar la comprensión.

## **9. Recursos didácticos**

Los materiales y recursos que se utilizarán para el desarrollo del módulo serán los siguientes:

- El aula virtual con Moodle donde estarán todo el material necesario para el módulo.
- Un ordenador dedicado para el uso del profesor.
- Sistemas Operativos: Windows y Linux
- Ordenador para cada alumnos
- Varios Puntos de acceso Wifi para realizar pruebas
- Tarjetas de red inalámbricas

## **10. Bibliografía de referencia**

La bibliografía empleada para el desarrollo del módulo será la siguiente:

**Libro: Seguridad y Alta Disponibilidad.**

**Editorial: Ra - Ma**

**Autor: Jesús Costas Santos**

## **11. Actividades complementarias y extraescolares**

Se fomentará entre el alumnado la labor de investigación personal sobre los diferentes temas tratados a lo largo del curso y la realización de actividades complementarias que permitan conocer casos reales de implantación de los diversos aspectos abordados en el módulo.

Además, se propondrán visitas a exposiciones, organismos o empresas del entorno en los que los alumnos puedan observar en la práctica los aspectos teóricos vistos. En todo caso, estas visitas dependerán de las posibilidades que se vayan descubriendo en el entorno y de cómo se vaya desarrollando el módulo a lo largo del curso.

También se asistirá a diversas charlas y exposiciones realizadas por expertos en el propio centro.