

IES JUAN DE MAIRENA (Mairena del Aljarafe)

**PROGRAMACIÓN DIDÁCTICA
DEPARTAMENTO DE INFORMÁTICA**

**Seguridad Informática
2º C.F.G.M. Sistemas Microinformáticos y Redes**

Curso 2018-2019

2. Programación de seguridad informática	4
2.1. Objetivos	4
2.2 Competencias profesionales, personales y sociales que contribuye a alcanzar este módulo.	5
2.3 Orientaciones Metodológicas	5
2.4 Contenidos, criterios de evaluación y estándares de aprendizaje asociados a las competencias claves a adquirir, señalando secuenciación y temporalización.	7
3. Evaluación	16
3.1 Instrumentos de evaluación	16
3.2. Criterios de calificación generales especificando porcentajes	16
3.3 Medidas de atención a la diversidad	19

2. PROGRAMACIÓN DE SEGURIDAD INFORMÁTICA

2.1. Objetivos

Los objetivos generales de este ciclo formativo a los que contribuye a alcanzar este módulo son los siguientes:

- a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
- b) Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.
- c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
- e) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
- h) Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- i) Interpretar y seleccionar información para elaborar documentación técnica y administrativa.
- j) Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.
- k) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
- l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
- m) Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.
- n) Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.

2.2 Competencias profesionales, personales y sociales que contribuye a alcanzar este módulo.

- Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos, interpretando la documentación técnica asociada y organizando los recursos necesarios.
- Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.
- Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información.
- Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.
- Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste.
- Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.
- Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.
- Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.
- Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y aprendizaje.

2.3 Orientaciones Metodológicas

Las clases serán fundamentalmente prácticas.

En cada bloque temático se realizará una exposición teórica de los contenidos del mismo y se realizarán exposiciones prácticas para explicar los procedimientos necesarios para llevar a cabo las capacidades profesionales en estudio.

El profesor resolverá las dudas que puedan tener los alumnos del ciclo, tanto teóricas como prácticas, incluso si él lo considerase necesario se realizarán ejercicios específicos que aclaren los conceptos que más cueste comprender a los alumnos.

El profesor propondrá un conjunto de ejercicios, de contenido similar a los que ya se han resuelto en clase, que deberán ser resueltos por los alumnos, bien en horas de clase o bien en casa.

El profesor propondrá también la resolución de ejercicios que conlleven un proceso de investigación y búsqueda de información. Finalmente el profesor corregirá y resolverá junto a los alumnos dichos ejercicios.

Además se propondrá algún trabajo que englobe conocimientos de varios bloques temáticos para comprobar que los conocimientos mínimos exigidos en cada uno de ellos han sido satisfactoriamente asimilados por los alumnos del Ciclo Formativo.

Las prácticas se resolverán de forma individual o en grupo, en función del tipo de práctica que se esté realizando.

También se propondrá resolver casos prácticos reales relacionados con la materia que se esté impartiendo (por ejemplo: instalación de la red del aula, añadir conexiones nuevas en el edificio, configurar las propiedades de red de equipos que estén prestando servicio en el centro, etc.) para que los alumnos vayan habituándose a resolver situaciones análogas a las que se enfrentarán en el futuro en el mundo laboral.

Todos los materiales, actividades y ejercicios se facilitarán a través de la plataforma Moodle y también a través del Servidor FTP del Ciclo Formativo.

Dentro del uso de nuevas tecnologías acorde con la participación del centro en el PRODIG, los alumnos y alumnas podrán utilizar sus dispositivos móviles para actividades de distinto tipo (individuales y/o grupales), siempre con finalidad pedagógica, tras el permiso de sus profesores/as y bajo su supervisión. Tal uso podrá hacerse en las actividades lectivas, complementarias y extraescolares en las condiciones anteriormente especificadas.

Proyecto Lector

La finalidad del Proyecto Lector es el tratamiento global de la competencia lectora desde todas las áreas, y que los alumnos sean lectores competentes.

De acuerdo con el compromiso adquirido por el Departamento de Informática respecto a dicho proyecto, que estipula un tiempo mínimo que se debe dedicar a la lectura, en este este módulo se trabajará la lectura concretándola en las siguientes actuaciones:

Textos utilizados

Por la naturaleza de la materia que se trata en este módulo, los textos estarán en su mayoría en soporte digital. Unas veces serán apuntes, prácticas, tutoriales o manuales elaborados por el profesor, y otras serán contenidos diversos descargados de la Web.

En cuanto a su tipología, los tipos de textos que usaremos son:

Textos teóricos sobre las unidades temáticas programadas.

Textos que contienen prácticas a realizar por los alumnos, cuya finalidad es reforzar y ampliar los conocimientos teóricos.

Textos divulgativos sobre temas relacionados con las unidades temáticas.

Textos técnicos y científicos sobre los temas impartidos

Manuales y tutoriales de instalación, montaje, herramientas informáticas etc..

Videos y presentaciones audiovisuales de carácter técnico.

Lectura.

Por cada unidad temática tratada en este módulo se realizarán las siguientes actividades que persiguen los objetivos del Proyecto Lector:

- Lectura conjunta de los contenidos teóricos de la unidad, prestando especial atención a la comprensión de las ideas fundamentales del tema, y a la adquisición del vocabulario técnico específico.
- En las prácticas propuestas sobre cada unidad habrá un apartado destinado al trabajo de investigación, para lo que se utilizará como principal fuente Internet, que tendrá como finalidad la búsqueda selectiva de textos, objetivo primordial de las búsquedas en Internet, y la elaboración de

conclusiones.

Proyecto Escritor

La finalidad del Proyecto Escritor es el tratamiento global de la competencia escritora desde todas las áreas, y que los alumnos sean escritores competentes.

De acuerdo con el compromiso adquirido por el Departamento de Informática respecto a dicho proyecto, que estipula un tiempo mínimo que se debe dedicar a la escritura, en este este módulo se trabajará la escritura concretándola en las siguientes actuaciones:

- En los distintos trabajos o prácticas que han de entregar los alumnos/as, se les pedirá que expliquen claramente los pasos que van dando para resolver dichos trabajos o prácticas.

2.4 Contenidos, criterios de evaluación y estándares de aprendizaje asociados a las competencias claves a adquirir, señalando secuenciación y temporalización.

2.4.1. CONTENIDOS BÁSICOS

Los contenidos básicos que se le exigirán al alumno para la superación del módulo, vienen recogidos en el RD 1691/2007:

Aplicación de medidas de seguridad pasiva:

- Seguridad informática. Clasificación, técnicas y prácticas de tratamiento seguro de la información.
- Ubicación y protección física de los equipos y servidores.
- Sistemas de alimentación ininterrumpida.

Gestión de dispositivos de almacenamiento:

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.
- Almacenamiento remoto y extraíble.
- Criptografía.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Política de almacenamiento.
- Recuperación de datos.

Aplicación de mecanismos de seguridad activa:

- Identificación digital.

- Sistemas biométricos de identificación.
- Firma electrónica y certificado digital.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Utilización de cortafuegos en un sistema o servidor.
- Listas de control de acceso.
- Política de contraseñas.
- Recuperación de datos.
- Software malicioso .Clasificación, protección y desinfección.
- Auditorias de seguridad.
- Actualización de sistemas y aplicaciones.

Aseguramiento de la privacidad:

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

Cumplimiento de la legislación y de las normas sobre seguridad:

- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

2.4.2. RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

Criterios de evaluación:

1. Se ha valorado la importancia de mantener la información segura.
2. Se han descrito las diferencias entre seguridad física y lógica.
3. Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
4. Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
5. Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
6. Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
7. Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
8. Se ha valorado la importancia de establecer una política de contraseñas.
9. Se han valorado las ventajas que supone la utilización de sistemas biométricos.

RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

Criterios de evaluación:

- 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.

RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

Criterios de evaluación:

- Se han seguido planes de contingencia para actuar ante fallos de seguridad.
- Se han clasificado los principales tipos de software malicioso.
- Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
 - a) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
 - b) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

- c) Se han aplicado técnicas de recuperación de datos.

RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

Criterios de evaluación:

- 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 sistemas de identificación como la firma electrónica, certificado digital, entre otros.
- g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
- h) Se ha instalado y configurado un cortafuego en un equipo o servidor.

RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

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 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.

2.4.3. UNIDADES DIDÁCTICAS

RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

Los contenidos, agrupados por unidades y contenidos específicos, que se impartirán son los siguientes:

Unidad 1. Conceptos básicos de seguridad informática

(RA5)

1.1 Seguridad informática. Introducción. Objetivos.

1.2 Clasificación de seguridad

 Seguridad física y lógica

 Seguridad activa y pasiva

1.3 Tipos de amenazas y fraudes en los sistemas de la información

1.4 Vulnerabilidades

Unidad 2. Seguridad pasiva. Recuperación de datos.

(RA1 RA2 y RA3)

2.1 Copias de seguridad.

- Tipos de copias de seguridad. Política de copias.
- Creación de copias de seguridad de los datos
- *Recuperación de datos.*
- *Recuperación del arranque en Sistemas operativos*
- Otras copias de seguridad
 - Imágenes de respaldo
 - Copia de seguridad del registro
 - *Puntos de restauración del sistema operativo.*

- Copias de seguridad de los datos de correo electrónico

Unidad 3. Seguridad pasiva. Hardware y almacenamiento (RA1, RA2 y RA3)

3.1 Ubicación y protección física de los equipos y servidores.

3.2 Condiciones ambientales de los equipos

3.3 Sistemas de alimentación ininterrumpida (SAI)

8. Tipos de SAI

9. Modo de funcionamiento

3.4 Gestión de dispositivos de almacenamiento.

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Métodos de almacenamiento
 - Almacenamiento redundante y distribuido.
 - RAIDs
 - Clusters
 - Almacenamiento remoto y extraíble.

Unidad 4. Sistemas de identificación. Criptografía.

(RA2 y RA3)

4.1 Criptografía. Principios básicos.

4.2 Criptografía simétrica y asimétrica.

4.3 Firma digital

4.4 Certificados digitales

Unidad 5. Seguridad activa en el sistema

(RA2 y RA3)

5.1 Sistemas de identificación. Autenticación de usuarios

5.1.1 Política de contraseñas.

5.1.2 Identificación digital.

5.1.3 Sistemas biométricos de identificación.

5.1.4 Firma electrónica y certificado digital.

5.1.5 Listas de control de acceso. Permisos de archivos y directorios.

5.2 Seguridad en el acceso al ordenador

5.2.1 Protección de la BIOS

5.2.2 Protección del gestor de arranque

5.2.3 Cifrado de particiones

5.2.4 Cuotas de disco

5.3 Software malicioso.

5.3.1 Clasificación. Tipos de ataques.

5.3.2 Protección, *detección y eliminación de software malicioso*.

5.3.3 Actualización de sistemas y aplicaciones.

Unidad 6. Seguridad activa en redes

(RA3 y RA4)

6.1 Métodos para asegurar la privacidad de la información transmitida.

6.2 Seguridad en redes

Servicios de red

Arranque y parada de los servicios

Vulnerabilidades

Monitorización de redes. Escaneo de puertos.

Detección de intrusos

Protocolos seguros (https, ssh)

Permisos de recursos compartidos en red

Seguridad en los navegadores

Seguridad en las redes sociales

6.3. Seguridad en redes inalámbricas

Tecnologías Wi-Fi

Seguridad Wi-Fi.

Monitorización de redes Wi-Fi

Detección de intrusos.

6.4 Seguridad en el correo electrónico

Publicidad y correo no deseado.

6.5 Sistemas cortafuegos en equipos y servidores.

1. Tipos de Cortafuegos
2. Instalación y configuración de proxys.
3. Control Parental
4. Instalación y configuración de cortafuegos.
5. Registros de actividad del cortafuegos

2.4.4 TEMPORALIZACIÓN DE LOS CONTENIDOS

UNIDAD	HORAS	TRIMESTRE	FECHAS APROX.
UD 1. Conceptos básicos de seguridad informática	10	1	Del 15 de septiembre al 30 de septiembre
UD 2. Seguridad pasiva. Recuperación de datos	25	1	Del 2 de octubre al 31 de octubre
UD 3. Seguridad pasiva. Hardware y almacenamiento	20	1	Del 4 de noviembre al 28 de noviembre
UD 4. Sistemas de identificación. Criptografía.	10	1	Del 2 de diciembre al 16 de diciembre
UD 5. Seguridad activa en el sistema	25	2	Del 8 de enero al 6 de febrero
UD 6. Seguridad activa en redes	15	2	Del 10 de febrero al 27 de febrero
TOTAL	105		

3. EVALUACIÓN

3.1 Instrumentos de evaluación

Los instrumentos de evaluación se pueden agrupar en dos modalidades:

1. **Instrumentos de evaluación continua**, mediante los que se valoran especialmente los procedimientos que se están adquiriendo y las actitudes del alumnado: revisión de los cuadernos del alumnado, contestación a preguntas y valoración de las intervenciones en clase, puntuaciones correspondientes a trabajos presentados individualmente o en grupos, y prácticas realizadas en clase.

2. **Instrumentos de evaluación programada**, mediante los que se valoran especialmente los conceptos y los procedimientos adquiridos por el alumnado: cuestionarios, exámenes escritos y orales, exámenes prácticos, ejercicios y pruebas objetivas, trabajos y proyectos.

3.2. Criterios de calificación generales especificando porcentajes

PROCEDIMIENTO DE EVALUACIÓN

El **peso** que, en la evaluación del alumnado, tendrán los distintos tipos de instrumentos de evaluación será el siguiente:

Instrumentos de evaluación continua: (30%)

- Actitud: 10%
- Prácticas, trabajos y ejercicios 20%

Instrumentos de evaluación programada: (70%)

- Se realizarán varios exámenes o pruebas específicas en cada evaluación. Cada prueba tendrá un peso en función de la importancia que determine el profesor. La suma de los pesos de las distintas pruebas deberá coincidir con lo especificado en “instrumentos de evaluación programada”

En cada examen el alumno deberá contestar preguntas teóricas y realizar uno o varios ejercicios prácticos. **Se procurará en la medida de lo posible la realización de ejercicios prácticos en los ordenadores y que conlleven el uso de las herramientas del taller.**

CRITERIOS DE CORRECCIÓN

Los **criterios de corrección** de las pruebas escritas o sobre el ordenador se basarán en:

- **Funcionamiento**
- Cumplimiento de los requisitos expuestos en el examen.
- Seguimiento de las normas de actuación desarrolladas en el aula.
- Ausencia total de errores sintácticos y semánticos.

(En los casos donde las pruebas incumplan alguno de los requisitos anteriores, perderá parte de su valor o la totalidad de este **primando el funcionamiento y adecuación a los requisitos del problema** sobre el resto de criterios).

Para evaluar la **actitud** se tendrá en cuenta lo siguiente:

- Participación activa en las prácticas realizadas.
- Trabajo en equipo.
- Responsabilidad con el material de trabajo.
- Orden y limpieza.
- Iniciativa propia.
- Interés por la materia tratada.
- Predisposición a tomar apuntes y buscar información complementaria.
- Participación activa en las exposiciones y debates.

PROCESO DE EVALUACIÓN

El proceso de evaluación constará de **tres evaluaciones**, una por cada trimestre. Para obtener la calificación de cada trimestre, se obtendrá la media de los distintos instrumentos de evaluación aplicando los porcentajes anteriormente detallados.

En el caso de tener algunos **periodos de evaluación no superados**, podrán proponerse pruebas específicas, ejercicios y trabajos para la recuperación de los mismos.

La **calificación final** del alumnado se calculará mediante la media de las calificaciones obtenidas en los sucesivos periodos de evaluación que se realicen durante el curso, incluyendo las calificaciones correspondientes, en su caso, a los ejercicios de recuperación.

El alumnado que no obtenga calificación positiva en la materia, realizará una **prueba extraordinaria** en la **Evaluación Final** sobre los contenidos no superados, realizándose la media entre las calificaciones positivas alcanzadas durante el curso y la calificación alcanzada en esta prueba extraordinaria.

Cada evaluación se evalúa por separado con una calificación de entre 0 y 10.

Para calcular la nota final de cada evaluación, **es necesario tener al menos un 5** en cada uno de los apartados descritos en el apartado “**PROCEDIMIENTO DE EVALUACIÓN**”

La **evaluación** se considera **superada** si la nota **media es igual o superior a 5**.

La nota final del módulo es la media de las evaluaciones, siempre que todas ellas estén aprobadas.

ASISTENCIA A CLASE

Por un lado, tenemos un proceso de evaluación continuo en el que se requiere la asistencia a clase por parte del alumno/a, de forma que no podrá acceder a la evaluación continua si el número de faltas de asistencias es mayor al establecido en el Reglamento Interior del Centro. En caso de que las faltas sean por enfermedad, accidente, asuntos familiares u otros especiales, serán estudiadas por el equipo educativo del curso que se encargará de aplicar las reglas adecuadas respetando la legalidad.

ALUMNOS CON EL MÓDULO PENDIENTE

El departamento de informática aplicando la legislación vigente adaptará el horario para facilitar que el alumnado con módulos pendientes de 1º curso pueda asistir a las clases de dichos módulos, al menos a la mayoría de ellos, pudiendo compatibilizar con la asistencia a las clases de los módulos de 2º curso, que esté cursando.

3.3 Medidas de atención a la diversidad

En términos generales podemos encontrar los siguientes tipos de alumnos/as:

- **Alumnos con dificultades de aprendizaje**

Son aquellos alumnos/as que tienen más dificultades que sus compañeros para acceder al aprendizaje determinado en los currículos que corresponden a su edad. Se proponen:

- Medidas de refuerzo educativo
- Aportar **ejercicios resueltos, ejemplos adicionales**, etc. (todos a través de la plataforma).
- Integrar a los alumnos/as con más carencias en **grupos de trabajo mixtos**.
- Adaptar la programación delimitando aquellos aspectos que sean considerados como mínimo exigible según el currículo.

- **Alumnos con mayor capacidad intelectual**

En general son aquellos alumnos cuya capacidad intelectual es superior a la media, presentan un alto nivel de creatividad y un alto grado de dedicación a las tareas.

Se plantea un seguimiento individualizado del alumno/a que consistirá fundamentalmente en la **realización de actividades de ampliación** en cada unidad didáctica y cuyo resultado sea un enriquecimiento del alumno y una mayor motivación. Estas actividades estarán enfocadas a configuraciones más complejas y funcionalidades adicionales de algunas de las prácticas de cada unidad, para ello se le darán al alumno algunas directrices para la realización de trabajos de investigación que después, con apoyo del profesor, deberán poner aplicar a la actividad encomendada.

- **Alumnos con discapacidades**

Aquí englobamos a todos aquellos alumnos con dificultades físicas o de comunicación tales como invidentes, sordos, alumnos en silla de ruedas etc. Antes de tomar cualquier medida, siempre solicitaremos la colaboración y asesoramiento del departamento de orientación.