1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
27015311	A Pinguela	Monforte de Lemos	2023/2024

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CMIFC01	Sistemas microinformáticos e redes	Ciclos formativos de grao medio	Réxime xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP0226	Seguridade informática	2023/2024	8	140	168

(*) No caso de que o módulo profesional estea organizado en unidades formativas de menor duración

Profesorado responsable

Profesorado asignado ao módulo	JAVIER RODRÍGUEZ LORENZO
Outro profesorado	

Estado: Pendente de supervisión equipo directivo

2. Concreción do currículo en relación coa súa adecuación ás características do ámbito produtivo

O ámbito produtivo da comarca desenvólvese en diversos aspectos dentro das empresas de novas tecnoloxías. De acordo con estes ámbitos de traballo faise unha exposición de contidos do módulo pensando na súa aplicación e aproveitamento nas mesmas, ben na fase da formación en centros de traballo (FCT en adiante), ou ben en fases xa de incorporación ó mundo laboral dentro da comarca do alumno. Sen menoscabo de coincidencia na empresa nas dúas fases comentadas, FCT e contrato laboral posterior.

Observáronse tamén empresas de outros ámbitos e comprobouse o seu traballo na utilización masiva de novas tecnoloxías no caso das oportunidades que hoxe en día nos produce.

Tendo en conta todo isto e seguindo as directrices do currículo, os contidos do módulo están orientados a acadar os seguintes resultados de aprendizaxe:

- RA1. Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.
- RA2. Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.
- RA3. Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.
- RA4. Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.
- RA5. Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.
- RA6. Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.

Este módulo profesional contén a formación necesaria para desempeñar a función de implantació de medidas de seguridade en sistemas informáticos.

A definición desta función abrangue aspectos como:

- Instalación de equipamentos e servidores en contornos seguros.
- Incorporación de procedementos de seguridade no tratamento da información.
- Actualización dos sistemas operativos e do software de aplicación instalado.
- Protección fronte a software malicioso.
- Aplicación da lexislación e da normativa sobre seguridade e protección da información.

As actividades profesionais asociadas a esta función aplícanse en:

- Instalación de equipamentos informáticos.
- Tratamento, transmisión e almacenaxe da información.
- Mantemento dos sistemas informáticos.

As liñas de actuación no proceso de ensino e aprendizaxe que permiten alcanzar os obxectivos do módulo han versar sobre:

- Protección de equipamentos e redes informáticas.
- Protección da información transmitida e almacenada.
- Lexislación e normativa en materia de seguridade.

A formación do módulo contribúe a desenvolver as competencias básicas das áreas prioritarias de idiomas e tecnoloxías da información e da comunicación, e a afondar nestas competencias

3. Relación de unidades didácticas que a integran, que contribuirán ao desenvolvemento do módulo profesional, xunto coa secuencia e o tempo asignado para o desenvolvemento de cada unha

U.D.	Título	Descrición	Duración (sesións)	Peso (%)
1	Introducción a seguridade informática	Esta UD trata o relativo á seguridade informática e a súa clasificación . Nela aprenderase a identificar as ameazas, ataques e vulnerabilidades dos sistemas.	10	11
2	Medidas de seguridade física e ambiental	Mecanismos de seguridade pasiva, os SAIs.	21	11
3	Mecanismos de seguridade lóxica	Políticas de control de acceso, de usuarios e grupos.	21	11
4	Software antimalware	Protección e desinfección con software antimalware	21	11
5	Criptografía	Cifrado e firma electrónica de información	21	11
6	Medidas de seguridade en redes.	Identificación e rectificación de vulnerabilidades en redes locais.	21	11
7	Seguridade perimetral	Seguridade con cortafogos e proxys	21	11
8	Configuracións de alta dispoñibilidade	Alta dispoñibilidade con RAID	21	11
9	Cumprimento da lexislación e das normas sobre seguridade.	Estudio da normativa legal aplicable á seguridade informática	11	12

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introducción a seguridade informática	10

4.1.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO

4.1.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.1 Valorouse a importancia de manter a información segura.
CA1.2 Clasificouse a información no ámbito da seguridade.
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.7 Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.
CA1.8 Establecéronse as normas básicas para incluír nun manual de seguridade informática.
CA1.9 Presentación do Módulo. Metodoloxía de avaliación.

4.1.e) Contidos

Contidos
Presentación do Módulo. Metodoloxía de avaliación. Seguridade física e lóxica. Políticas de seguridade.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Medidas de seguridade física e ambiental	21

4.2.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	NO
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	NO
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

4.2.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.
CA2.1 Definíronse as características do emprazamento e as condicións ambientais dos equipamentos e dos servidores.
CA2.2 Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
CA2.3 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
CA2.7 Valoráronse as vantaxes do uso de sistemas biométricos.
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.
CA3.5 Seleccionáronse estratexias para a realización de copias de seguridade.
CA3.6 Tívose en conta a frecuencia e o esquema de rotación.
CA3.7 Realizáronse copias de seguridade seguindo diversas estratexias.
CA3.10 Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.
CA4.7 Aplicáronse técnicas de recuperación de datos.

4.2.e) Contidos

Contidos
Seguridade física e lóxica. Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida.

Contidos
Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade.
Copias de seguridade e imaxes de respaldo.
Medios de almacenaxe.
Sistemas biométricos de identificación.
Recuperación de datos.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Mecanismos de seguridade lóxica	21

4.3.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	NO
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

4.3.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.
CA2.5 Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.

4.3.e) Contidos

Contidos
Seguridade física e lóxica. Localización e protección física dos equipamentos e dos servidores. Listas de control de acceso. Política de contrasinais.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Software antimalware	21

4.4.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

4.4.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.
CA4.2 Clasificáronse os principais tipos de software malicioso.
CA4.3 Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.
CA4.4 Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.
CA4.5 Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.
CA4.6 Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.

4.4.e) Contidos

Contidos
Monitorización de sistemas. Auditorías de seguridade. Software malicioso: clasificación. Ferramentas de protección e desinfección. Actualización de sistemas e aplicacións. Manual de seguridade e plans de continxencia.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Criptografía	21

4.5.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

4.5.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.4 Identificáronse as principais técnicas criptográficas.
CA1.5 Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.
CA1.6 Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).
CA5.7 Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.

4.5.e) Contidos

Contidos
Criptografía. Métodos para asegurar a privacidade da información transmitida. Identificación dixital: sinatura electrónica e certificado dixital.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Medidas de seguridade en redes.	21

4.6.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

4.6.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA5.1 Identificouse a necesidade de inventariar e controlar os servizos de rede.
CA5.2 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.
CA5.3 Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.
CA5.4 Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.5 Identificáronse as ameazas na navegación por internet.
CA5.6 Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.

4.6.e) Contidos

Contidos
Métodos para asegurar a privacidade da información transmitida.
Monitorización do tráfico en redes con cables.
Seguridade en redes sen fíos.
Riscos potenciais dos servizos de rede.
Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc.
Publicidade e correo non desexados.
Fraudes informáticas e roubos de información.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Seguridade perimetral	21

4.7.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

4.7.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA5.5 Identificáronse as ameazas na navegación por internet.
CA5.8 Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.

4.7.e) Contidos

Contidos
0Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade. Utilización de devasas (firewalls) en equipamentos e en servidores.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Configuracións de alta dispoñibilidade	21

4.8.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	NO

4.8.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.
CA3.2 Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).
CA3.3 Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
CA3.4 Describíronse as tecnoloxías de almacenaxe redundante e distribuída.
CA3.8 Identificáronse as características dos medios de almacenaxe remotos e extraíbles.
CA3.9 Utilizáronse medios de almacenaxe remotos e extraíbles.

4.8.e) Contidos

Contidos
Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade. Almacenaxe redundante e distribuída. Almacenaxe remota e extraíble. Medios de almacenaxe.

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Cumprimento da lexislación e das normas sobre seguridade.	11

4.9.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	SI

4.9.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA6.1 Describiuse a lexislación sobre protección de datos de carácter persoal.
CA6.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA6.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.
CA6.5 Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.
CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.
CA6.7 Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

4.9.e) Contidos

Contidos
Lexislación sobre protección de datos. Lexislación sobre os servizos da sociedade da información e o correo electrónico. Normas ISO sobre xestión de seguridade da información.

5. Mínimos exixibles para alcanzar a avaliación positiva e os criterios de cualificación

Os mínimos esixibles serán os seguintes:
CA1.1 - Valorouse a importancia de manter a información segura.
CA1.2 - Clasificouse a información no ámbito da seguridade.
CA1.3 - Describíronse as diferenzas entre seguridade física e lóxica.
CA1.4 - Identificáronse as principais técnicas criptográficas.
CA1.5 - Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.
CA1.6 - Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).
CA2.2 - Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
CA2.3 - Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.6 - Valorouse a importancia de establecer unha política de contrasinais.
CA3.2 - Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).
CA3.3 - Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
CA3.4 - Describíronse as tecnoloxías de almacenaxe redundante e distribuída.
CA3.5 - Seleccionáronse estratexias para a realización de copias de seguridade.
CA3.7 - Realizáronse copias de seguridade seguindo diversas estratexias.
CA3.10 - Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.
CA4.1 - Seguíronse plans de continxencia para actuar ante fallos de seguridade.
CA4.2 - Clasificáronse os principais tipos de software malicioso.
CA4.3 - Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.
CA4.5 - Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.
CA4.6 - Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.
CA4.7 - Aplicáronse técnicas de recuperación de datos.
CA5.1 - Identificouse a necesidade de inventariar e controlar os servizos de rede.
CA5.2 - Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.
CA5.4 - Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.5 - Identificáronse as ameazas na navegación por internet.
CA5.7 - Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA5.8 - Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.
CA6.1 - Describiuse a lexislación sobre protección de datos de carácter persoal.
CA6.3 - Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA6.4 - Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.
CA6.5 - Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.
CA6.7 - Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

Criterios de cualificación:
En cada unha das tres sesións de avaliación emitirase unha nota (con cifras de 0 a 10) do módulo segundo os criterios de avaliación expresados en cada unidade didáctica e utilizando os instrumentos e o sistema de avaliación que se citan de contado.

Sistema de avaliación:
A nota de cada unidade didáctica calcúlase da seguinte maneira:

Os exercicios entregables de cada unidade didáctica valerán un 30% da nota da unidade, tendo cada exercicio o mesmo peso nesa porcentaxe final.

A proba escrita e a proba práctica representan o 70% da nota da unidade. No caso de que existan as dúas probas a porcentaxe correspondente será de 30% para a proba escrita e 70% para a parte práctica (dentro dese 70%). Se non existe proba escrita, a proba práctica acumulará o porcentaxe da práctica e viceversa. Cómpre aprobar tanto a parte teórica como a parte práctica para ter unha calificación positiva no global de cada Unidade Didáctica.

No caso de que non existan na unidade exercicios entregables, a súa porcentaxe acumularase na da proba escrita e práctica, que pasaría a valer o 100% da nota final da unidade.

..

As notas de avaliación calcúlanse como a media aritmética das notas das unidades avaliadas ata a data da avaliación sempre que tódalas unidades superen o 4. No caso da última unidade que ten un peso de 12% (diferente ao resto) terase en conta esa diferencia na hora de calcular as medias asignado un maior peso específico.
A avaliación superase cunha nota superior a 5 se tódalas unidades superan o 4. Se algunha unidade tivese unha nota inferior a 4 a avaliación será suspensa. Existirán probas ao remate de cada avaliación para recuperar as unidades suspensas.

A nota final da avaliación ordinaria do módulo será a que corresponda a terceira avaliación. Para aprobar o módulo será necesario ter unha nota maior ou igual a 5.

Tendo en conta a ORDE do 12 de maio de 2011 pola que se regulan as seccións bilingües en centros sostidos con fondos públicos de ensino non universitario, esta materia ten autorizada unha Sección Bilingüe para este curso polo cal parte do curso será impartido en parte na lingua inglesa segundo as pautas establecidas na antedita orde.

En caso de ensinanza non presencial os criterios de cualificación serán os mesmos. Empregarase a plataforma de conferencia web BigBlueButton integrada na aula virtual do curso para resolver dúbidas e valorar o avance do alumnado.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Para facer a recuperación das unidades pendentes establecerase un calendario coas datas de entrega dos traballos, e das probas, escritas e prácticas, que se deben realizar. Os instrumentos de avaliación serán os descritos no apartado de avaliación ordinaria.

Existirá unha proba ao remata de cada avaliación para a recuperación das unidades suspensas.

O profesor fará un seguimento do traballo e a evolución dos/as alumnos/as co obxecto de avaliar a actitude dos/as alumnos/as.

Para calcular a nota do módulo na avaliación final extraordinaria aplicaranse os mesmos criterios que na avaliación final ordinaria.

6.b) Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito a avaliación continua

Este alumnado será avaliado ó final do módulo.

Para superar o módulo deberá superar as seguinte probas:

Unha proba escrita na que se incluirán contidos conceptuais das unidades didácticas, que representará un 30% da cualificación final.

Unha proba práctica no ordenador na que se avaliará o manexo na materia de acordo cos contidos das unidades didácticas, que representará un 70%.

O maior peso da parte práctica débese a que terá unha importancia maior tanto no módulo como na proba de avaliación.

7. Procedemento sobre o seguimento da programación e a avaliación da propia práctica docente

Para levar a cabo o seguimento da programación usarase a propia aplicación de programacións, documento mediante o cal poderase determinar se a asignación horaria de cada unidade é a idónea. Hai que ter en conta que o ritmo de traballo virá determinado pola asimilación dos conceptos por parte do alumnado.
A práctica docente avaliarase seguindo o procedemento establecido polo control do sistema de calidade establecido no centro. Dito control realízase principalmente cumprimentando os seguintes documentos:
- Enquisa para a avaliación do profesor: avaliación feita polos alumnos da materia sobre as actividades docentes realizadas polo profesor. Mediante a enquisa de avaliación docente, obteranse resultados a valorar ao remate das avaliacións.
- Recollida de datos para a xunta de avaliación: recolle as conformidades/non conformidades e as actuacións derivadas das non conformida-des referentes ao alumnado (suspensos, faltas de asistencia) e cumprimento da programación.
- Memoria fin de curso: na que, entre outros temas, trátase a porcentaxe da programación impartida, a realización de modificacións na mesma e as propostas de mellora para o seguinte curso académico.
Ademais, en reunión de departamento, ao longo do curso, realizarase o seguimento e control da programación, tomando as medidas oportunas se é o caso.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Para a realización da avaliación inicial e co obxecto de determinar a formación previa do alumnado na materia, farase un cuestionario escrito con preguntas breves para coñecer o punto de partida do alumnado e polo tanto das explicacións.

8.b) Medidas de reforzo educativo para o alumnado que non responda globalmente aos obxectivos programados

As medidas de reforzo teñen como obxectivo intentar axudar a superar algunha unidade didáctica a aqueles alumnos que non acadaron os obxectivos mínimos esixibles.

As medidas de reforzo da parte práctica da unidade didáctica consistirán na resolución de supostos con unha metodoloxía distinta e máis detallada. Estes supostos serán resoltos polo alumno sempre coa axuda do profesor.

As medidas de reforzo da parte conceptual da unidade didáctica consistirán no repaso dos conceptos por parte do alumno e coa axuda do profesor que fará propostas de cuestionarios sobre a materia, que o alumno debe cumprimentar.

As medidas de reforzo da parte actitudinal da unidade didáctica consistirán na proposta de cambio por parte do alumno e a supervisión do profesor.

Para alumnado que acadade os obxectivos nun espazo de tempo inferior ao establecido na programación facilitaráselles documentación complementaria e actividades de ampliación para que poidan profundizar nos contidos do módulo.

9. Aspectos transversais

9.a) Programación da educación en valores

Respecto ós demais, tolerancia e comportamento correcto.
Atención prestada .
Participación diaria na clase. Comunicación e diálogo.
Puntualidade e asistencia.
Respecto ás normas e o material que se use.
Colaboración nas tarefas de investigación que poidan xurdir, de forma que as responsabilidades estean equitativamente repartidas dentro do grupo.
Cooperación na superación de dificultades que se presenten ó grupo, cunha actitude tolerante cara as ideas e as actitudes do resto dos compañeiros.

9.b) Actividades complementarias e extraescolares

Participación nas que figuran na programación conxunta do departamento e no resto de actividades dos ciclos formativos da familia de informática do centro, así como naquelas organizadas polo centro e que se consideren de interese xeral.

10.Outros apartados

10.1) Constancia de información ao alumnado

A presentación do módulo con información relativa á programación didáctica (obxectivos, contidos, criterios de avaliación, cualificación e procedementos e mínimos esixibles) está colgada na Web do Instituto a disposición de toda a comunidade educativa. Deste feito son informados os alumnos e pais nas respectivas guías.

10.2) Metodoloxía en caso de ensino a distancia

Presencial
Empregarase a aula virtual e un aula de informática do centro educativo.

Non presencial

No caso de que algún alumno tivese debidamente xustificado o poder recibir clases de xeito non presencial, a plataforma a utilizar será a de videoconferencia da propia aula virtual ou outras como Cisco Webex.