## 1. Identificación da programación

### Centro educativo

| Código | Centro | Concello | Ano académico |
|---|---|---|---|
| 15027307 | Isidro Parga Pondal | Carballo | 2019/2020 |

### Ciclo formativo

| Código da familia profesional | Familia profesional | Código do ciclo formativo | Ciclo formativo | Grao | Réxime |
|---|---|---|---|---|---|
| IFC | Informática e comunicacións | CSIFC01 | Administración de sistemas informáticos en rede | Ciclos formativos de grao superior | Réxime xeral-ordinario |

### Módulo profesional e unidades formativas de menor duración (*)

| Código MP/UF | Nome | Curso | Sesións semanais | Horas anuais | Sesións anuais |
|---|---|---|---|---|---|
| MP0378 | Seguridade e alta dispoñibilidade | 2019/2020 | 6 | 105 | 126 |

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

### Profesorado responsable

| | |
|---|---|
| **Profesorado asignado ao módulo** | JUAN FRANCISCO PUENTES CALVO |
| **Outro profesorado** | |

Estado: Pendente de supervisión departamento

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

Os sistemas informáticos son unha das pezas clave dentro de todo sistema social e é produtivo xa que do seu correcto funcionamento depende a integridade, seguridade e dispoñibilidade da información dentro da empresa.
É por iso que a súa seguridade e dispoñibilidade son fundamentais para a explotación do sistema no contorno produtivo:

+ Administrar sistemas operativos de servidor, instalando e configurando o software en condicións de calidade, para asegurar o funcionamento do sistema.
+ Administrar servizos de rede (web, mensaxería electrónica, transferencia de ficheiros, etc.) instalando e configurando o software, en condicións de calidade.
+ Administrar aplicacións instalando e configurando o software en condicións de calidade, para responder ás necesidades da organización.
+ Implantar e xestionar bases de datos instalando e administrando o software de xestión en condicións de calidade, segundo as características da explotación.
+ Mellorar o rendemento do sistema configurando os dispositivos de hardware consonte os requisitos de funcionamento.
+ Avaliar o rendemento dos dispositivos de hardware identificando posibilidades de melloras segundo as necesidades de funcionamento.
+ Determinar a infraestrutura de redes telemáticas, elaborando esquemas e seleccionando equipamentos e elementos.
+ Integrar equipamentos de comunicacións en infraestruturas de redes telemáticas, determinando a configuración para asegurar a súa conectividade.
+ Pór en práctica solucións de alta dispoñibilidade, analizando as opcións do mercado, para protexer e recuperar o sistema ante situacións imprevistas.
+ Supervisar a seguridade física segundo especificacións de fábrica e o plan de seguridade, para evitar interrupcións na prestación de servizos do sistema.
+ Asegurar o sistema e os datos segundo as necesidades de uso e as condicións de seguridade establecidas, para previr fallos e ataques externos.
+ Administrar usuarios de acordo coas especificacións de explotación, para garantir os accesos e a dispoñibilidade dos recursos do sistema.
+ Diagnosticar as disfuncións do sistema e adoptar as medidas correctivas para restablecer a súa funcionalidade.
+ Xestionar e/ou realizar o mantemento dos recursos da súa área (programando e verificando ou seu cumprimento), en función das cargas de traballo e o plan de mantemento.
+ Efectuar consultas, dirixíndose á persoa adecuada e saber respectar a autonomía dos subordinados, informando cando sexa conveniente.
+ Manter o espírito de innovación e actualización no ámbito de ou seu traballo para adaptarse aos cambios tecnolóxicos e organizativos de ou seu entorno profesional.
+ Liderar situacións colectivas que se poidan producir, mediando en conflitos persoais e laborais, contribuíndo ao establecemento dun ambiente de traballo agradable e actuando en todo momento de forma sincera, respectuosa e tolerante.
+ Resolver problemas e tomar decisións individuais, seguindo as normas e procedementos establecidos, definidos dentro do ámbito da súa competencia.
+ Xestionar a propia carreira profesional, analizando as oportunidades de emprego, de autoemprego e de aprendizaxe.
+ Participar de xeito activo na vida económica, social e cultural, con actitude crítica e responsable.
+ Crear e xestionar unha pequena empresa, realizando un estudo de viabilidade de produtos, de planificación da produción e de comercialización.

**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 | Principios de seguridade e alta dispoñibilidade. | Principios de seguridade e alta dispoñibilidade. | 6 | 4 |
| 2 | Seguridade pasiva. | Seguridade pasiva. | 18 | 4 |
| 3 | Seguridade lóxica. | Seguridade lóxica. | 18 | 4 |
| 4 | Software antimalware. | Software antimalware. | 12 | 4 |
| 5 | Criptografía. | Criptografía. | 18 | 24 |
| 6 | Seguridade en redes corporativas. | Seguridade en redes corporativas. | 12 | 20 |
| 7 | Seguridade perimetral | Seguridade perimetral | 12 | 20 |
| 8 | Configuracións de alta dispoñibilidade. | Configuracións de alta dispoñibilidade. | 18 | 15 |
| 9 | Normativa legal en materia de seguridade informática. | Normativa legal en materia de seguridade informática. | 12 | 5 |

## 4. Por cada unidade didáctica

### 4.1.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 1 | Principios de seguridade e alta dispoñibilidade. | 6 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar. | 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 asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos. |
| CA1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe. |
| CA1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas. |
| CA1.5 Adoptáronse políticas de contrasinais. |

### 4.1.e) Contidos

| Contidos |
|---|
| Fiabilidade, confidencialidade, integridade e dispoñibilidade.<br><br>Elementos vulnerables no sistema informático: hardware, software e datos.<br><br>Análise das principais vulnerabilidades dun sistema informático.<br><br>Pautas e prácticas seguras. |

### 4.2.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 2 | Seguridade pasiva. | 18 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar. | NO |

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

| Criterios de avaliación |
|---|
| CA1.2 Describíronse as diferenzas entre seguridade física e lóxica. |
| CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos. |

### 4.2.e) Contidos

| Contidos |
|---|
| Tipos de ameazas: físicas e lóxicas.<br><br>Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida. |

### 4.3.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 3 | Seguridade lóxica. | 18 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar. | NO |
| RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema. | NO |

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

| Criterios de avaliación |
|---|
| CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema. |
| CA2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático. |
| CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles. |

### 4.3.e) Contidos

| Contidos |
|---|
| Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. |
| Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias. |
| Ferramentas empregadas na análise forense. |
| Realización de auditorías de seguridade. |
| Ferramentas preventivas e paliativas: instalación e configuración. |
| Copias de seguridade e imaxes de respaldo. |
| Recuperación de datos. |
| Actualización de sistemas e aplicacións. |

### 4.4.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 4 | Software antimalware. | 12 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema. | NO |

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

| Criterios de avaliación |
|---|
| CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo. |
| CA2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados. |
| CA2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso. |

### 4.4.e) Contidos

| Contidos |
|---|
| Anatomía de ataques e análise de software malicioso. |

### 4.5.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 5 | Criptografía. | 18 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar. | NO |
| RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema. | NO |

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

| Criterios de avaliación |
|---|
| CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información. |
| CA2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas. |

### 4.5.e) Contidos

| Contidos |
|---|
| 0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas. |

### 4.6.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 6 | Seguridade en redes corporativas. | 12 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema. | NO |
| RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade. | NO |

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

| Criterios de avaliación |
|---|
| CA2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación. |
| CA2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema. |
| CA2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións. |
| CA3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso. |
| CA3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis. |
| CA3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas. |

### 4.6.e) Contidos

| Contidos |
|---|
| Ataques e contramedidas en sistemas informáticos. |
| Monitorización do tráfico en redes: captura e análise; aplicacións. |
| Seguridade nos protocolos para comunicacións sen fíos. |
| Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades. |
| Intentos de penetración: tipoloxía. |
| Sistemas de detección de intrusións. |
| Clasificación dos ataques. |
| Redes privadas virtuais. VPN. Beneficios e desvantaxes con respecto ás liñas dedicadas. VPN a nivel de enlace. VPN a nivel de rede. SSL e IPSec. VPN a nivel de aplicación. SSH. |
| Servidores de acceso remoto: Protocolos de autenticación. Configuración de parámetros de acceso. Servidores de autenticación. |

### 4.7.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 7 | Seguridade perimetral | 12 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar. | NO |
| RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade. | NO |
| RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna. | SI |
| RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo. | SI |

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

| Criterios de avaliación |
|---|
| CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas. |
| CA3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna. |
| CA3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral. |
| CA3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela. |
| CA3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación. |
| CA4.1 Describíronse as características, os tipos e as funcións dos tornalumes. |
| CA4.2 Clasificáronse os niveis en que se realiza a filtraxe de tráfico. |
| CA4.3 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe. |
| CA4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente. |
| CA4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria. |
| CA4.6 Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware. |
| CA4.7 Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes. |
| CA4.8 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede. |
| CA4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes. |
| CA5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais. |
| CA5.2 Instalouse e configurouse un servidor proxy cache. |
| CA5.3 Configuráronse os métodos de autenticación no proxy. |
| CA5.4 Configurouse un proxy en modo transparente. |

| Criterios de avaliación |
|---|
| CA5.5 Utilizouse o servidor proxy para establecer restricións de acceso web. |
| CA5.6 Arranxáronse problemas de acceso desde os clientes ao proxy. |
| CA5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas. |
| CA5.8 Configurouse un servidor proxy en modo inverso. |
| CA5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy. |

### 4.7.e) Contidos

| Contidos |
|---|
| Seguridade na conexión con redes públicas. |
| Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes privadas virtuais. |
| Perímetros de rede. Zonas desmilitarizadas. |
| Arquitectura débil e forte de subrede protexida. |
| Utilización de tornalumes. |
| Filtraxe de paquetes de datos. |
| Tipos de tornalumes: características e funcións principais: Uso das características de tornalumes incorporadas no sistema operativo. Implantación de tornalumes en sistemas libres e propietarios. Instalación e configuración. Tornalumes hardware. |
| Regras de filtraxe de tornalumes. |
| Probas de funcionamento: sondaxe. |
| Rexistros de sucesos nos tornalumes. |
| Tipos de proxy: características e funcións. |
| Instalación de servidores proxy. |
| Instalación e configuración de clientes proxy. |
| Configuración do almacenamento na cache dun proxy. |
| Configuración de filtros. |
| Métodos de autenticación nun proxy. |
| Proxy inverso. |
| Encadeamento e xerarquías. |
| Probas de funcionamento. |

### 4.8.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 8 | Configuracións de alta dispoñibilidade. | 18 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba. | SI |

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

| Criterios de avaliación |
|---|
| CA6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade. |
| CA6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema. |
| CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade. |
| CA6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal. |
| CA6.5 Implantouse un balanceador de carga á entrada da rede interna. |
| CA6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos. |
| CA6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema. |
| CA6.8 Analizáronse solucións de futuro para un sistema con demanda crecente. |
| CA6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade. |

### 4.8.e) Contidos

| Contidos |
|---|
| Definición e obxectivos.<br><br>Análise de configuracións de alta dispoñibilidade. Funcionamento ininterrompido. Integridade de datos e recuperación de servizo. Servidores redundantes. Sistemas de clústers. Balanceadores de carga.<br>Instalación e configuración de solucións de alta dispoñibilidade.<br><br>Virtualización de sistemas. Posibilidades da virtualización de sistemas. Ferramentas para a virtualización. Configuración e uso de máquinas virtuais. Alta dispoñibilidade e virtualización. Simulación de servizos con virtualización. Análise e optimización<br>Virtualización en contornos de produción. |

### 4.9.a) Identificación da unidade didáctica

| N.º | Título da UD | Duración |
|---|---|---|
| 9 | Normativa legal en materia de seguridade informática. | 12 |

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

| Resultado de aprendizaxe do currículo | Completo |
|---|---|
| RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia. | SI |

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

| Criterios de avaliación |
|---|
| CA7.1 Describiuse a lexislación sobre protección de datos de carácter persoal. |
| CA7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada. |
| CA7.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos. |
| CA7.4 Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen. |
| CA7.5 Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico. |
| CA7.6 Contrastáronse as normas sobre xestión de seguridade da información. |
| CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable. |

### 4.9.e) Contidos

| Contidos |
|---|
| Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico. |

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

O principal criterio a ter en conta para acadar unha avaliación positiva é o do seguimento diario do traballo realizado na aula, polo que a asistencia a clase considérase imprescindible.
Participación efectiva en clase realizando os traballos programados para cada unidade polo profesor ou profesora.
Resolución dos supostos prácticos que permitan desenvolver os contidos deseñados en cada unha das unidades didácticas.
A comprensión dos elementos conceptuais básicos tratados nas diferentes unidades didácticas.
Os criterios anteriores son un referente básico para a obtención dunha cualificación positiva do alumno, xa que o comportamento do alumno na aula e o grao de participación poderán modificar a nota final do alumno/a.
Poderanse realizar probas escritas periódicas para controlar o grao de aprendizaxe dos distintos contidos.
Consideraranse tamén as actividades persoais relacionadas con este módulo que realicen os alumnos como consecuencia da súa propia iniciativa.
Os alumnos que non acaden cualificación positiva considerando os aspectos anteriores poderán ser sometidos a probas de recuperación, ben escritas ou no ordenador dependendo da natureza da proba e das dispoñibilidades.
Para que un alumno aprobe o módulo deberá ter unha nota mínima de 5.

CRITERIOS DE CUALIFICACIÓN

En función dos distintos contidos do módulo, teranse en conta os seguintes criterios de cualificación:

Contidos teóricos:
+ Probas escritas ou tipo test (3 por 1), valorando a claridade e corrección das respostas.
+ Traballos de investigación e ampliación: valorando que o material sexa completo e tamén as conclusións obtidas polo alumnado.

Contidos procedimentais:
+ Actividades prácticas có material da clase: valorando a soltura e eficacia no seu manexo.
+ Actividades de instalación e configuración de software.

Contidos actitudinais:
+ Asistencia e puntualidade.
+ Iniciativa na resolución dos problemas e á hora de ampliar os contidos por conta propia.
+ Atención, comunicación e corrección na clase.

De forma xeral os contidos teóricos conformarán o 50% da nota final, os procedimentais o 40 % e os actitudinais o 10%.

### 6. Procedemento para a recuperación das partes non superadas

### 6.a) Procedemento para definir as actividades de recuperación

Os alumnos que non acaden cualificación positiva ó remate das actividades programadas para o módulo, deberán recuperalo a través de:

+ Realización de traballos relativos á materia pendente, conforme ao realizado no curso polos alumnos de avaliación continua segundo a programación especificada anteriormente.
+ Asistencia ás actividades que programadas para ese módulo, se realicen na propia aula durante o horario que a tal fin se determine.

A recuperación realizarase a través de:

+ Valoración dos traballos realizados durante esta fase.

Poderá ser realizada unha proba escrita ou tipo test (3 por 1).

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

Os alumnos e alumnas que perdan o dereito á avaliación continúa, perden tamén o dereito de asistir ás clases e non serán avaliados ata a avaliación final extraordinaria do módulo no mes de Xuño.

Esta avaliación poderá consistir en probas teóricas ou prácticas, en papel ou co ordenador, que abarquen todo os contidos do módulo e poderase esixir ao alumno ou alumna a entrega e defensa oral dun traballo práctico.

As causas polas que un alumno pode perder o dereito á avaliación continua son, entre outras:

+ Acumular un número de faltas de asistencia que supere ó 10% do número total de sesións de que consta o módulo.
+ Acumular mais de 25 faltas nun período de 30 días, entre tódolos módulos do curso, e sen xustificar por causa grave.
+ Ser descuberto copiando dun compañeiro ou deixándose copiar por outro, durante algunha proba de avaliación do módulo.
+ Cometer algunha falta de comportamento grave como pode ser calquera tipo de sabotaxe.

Realizaranse probas teórico prácticas que inclúan, polo menos, todos os contidos mínimos esixibles.

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

O departamento, nas reunións ordinarias, incluirá na orde do día o seguimento das programacións.

**8. Medidas de atención á diversidade**

**8.a) Procedemento para a realización da avaliación inicial**

O instrumento para levar a cabo a avaliación inicial consistirá nun formulario que alumnado deberá cubrir nas primeiras semanas do curso. Neste formulario o alumnado deberá detallar:

+ Datos persoais.
+ Estudios e formación anterior á súa matriculación no ciclo.
+ Coñecementos relacionados cos temarios dos módulos do Ciclo Superior ASI.
+ Material e recursos informáticos dispoñibles no fogar: ordenador, Internet, etc.

E calquera outro dato que poida ser de interese.

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

Coa denominación de necesidades educativas específicas, a lexislación presta especial atención aos alumnos estranxeiros, aos alumnos superdotados intelectualmente e aos alumnos con necesidades educativas especiais, ben pola presenza dunha ou varias discapacidades ou por

outros factores de análogos efectos, establecendo un marco xeral que permita ás Administracións educativas garantir, en todos os casos, unha axeitada resposta educativa ás circunstancias e necesidades que nestes alumnos concorren.

Có fin de asegurar o dereito individual a unha educación de calidade, os poderes públicos levarán a cabo as accións necesarias e aportarán os recursos e os apoios precisos que permitan compensar os efectos de situacións de desvantaxe social para o logro dos obxectivos de educación e de formación previstos.

En primeiro lugar, as Administracións educativas deben adoptar procedementos singulares naqueles centros escolares nos cales, resulte necesaria unha intervención educativa diferenciada, aportando os recursos materiais e de profesorado necesarios e proporcionarase o apoio técnico e humano preciso para o logro da compensación educativa.

En segundo lugar, o departamento de Orientación detectará, identificará e valorará as necesidades educativas especiais, e deseñará e coordinará os plans de apoio para atender á diversidade do alumnado do centro. Para isto contará con un equipo de profesionais cualificados e estará en contacto cós profesores titores e cós pais. Por último, cada profesor terá en conta as necesidades educativas específicas no seu grupo elaborando unha programación flexible e aberta que favoreza os cambios que o profesor debe introducir para dar resposta ás diferenzas individuais en estilos de aprendizaxe, motivacións, intereses ou dificultades de aprendizaxe.

Como medidas de atención á diversidade adoptaranse as seguintes:

1. fomento do traballo práctico.
2. creación dun ambiente de traballo que favoreza a autonomía e o traballo en grupo. Se se obtén este clima, o profesor dispón de máis tempo para identificar os alumnos que precisan axuda e proporcionar a mellor axuda en cada caso.
3. Fomentar a axuda mutua entre compañeiros e compañeiras de diferentes niveis.
4. agrupamentos flexibles e ritmos distintos.
5. metodoloxías diversas nas formas de enfocar as exposicións e as actividades.
6. actividades diferenciadas e adaptadas ás motivacións e necesidades dos alumnos.
7. actividades de reforzo en grupos pequenos.

Como medidas individuais, para os alumnos estranxeiros que descoñezan a lingua e cultura española, ou que presenten graves carencias en coñecementos básicos, fomentarase a lectura de libros e catálogos de carácter técnico e empregaranse diccionarios e tradutores para favorecer o uso e entendemento de distintas linguas.

Cós alumnos superdotados intelectualmente, para que as actividades non resulten desmotivadoras, será maior o grao de esixencia nos aspectos científicos e de deseño dos contidos. Ademais unha vez satisfeitos os obxectivos básicos, proporánse actividades complementarias que estimulen a súa creatividade e autonomía.

Os alumnos con necesidades educativas especiais que requiran, nun período da súa escolarización ou ó longo de toda ela, e en particular no que se refire á avaliación, determinados apoios e atencións educativas, específicas por padecer discapacidades físicas, psíquicas, sensoriais, ou por manifestar graves trastornos da personalidade ou de conducta, terán unha atención especializada, con acordo ós principios de non discriminación e normalización educativa.

## 9. Aspectos transversais

### 9.a) Programación da educación en valores

En primeiro lugar, en cada actividade inclúense precaucións e recomendacións para tomar as medidas de seguridade e hixiene que sexan necesarias. O manexo do ordenador entraña riscos, principalmente para a vista e para o lombo, sen esquecer os riscos psicolóxicos derivados do seu
abuso. Ademais ao alumno váiselle valorar a organización do seu posto de traballo e das actividades que realiza.

Outro tema que se trata é o idioma técnico. Moitos dos manuais técnicos están dispoñibles exclusivamente en inglés polo que é preciso que o alumno posúa uns coñecementos básicos deste idioma, polo menos a nivel de tradución. Dada a importancia que este idioma ten nos procesos de selección de técnicos cualificados no mundo laboral potenciarase o seu coñecemento e a súa práctica. Neste sentido fomentarase tamén o uso de tradutores automáticos para acceder a certos contidos escritos noutras linguas.

Dada a escasa vida útil dos equipos informáticos, valorarase os esforzos dalgunhas empresas por fabricar os seus equipos con materiais reciclables e a recollida por parte dos alumnos do material antigo para a súa reutilización.

### 9.b) Actividades complementarias e extraescolares

Este módulo non ten programado actividades extraescolares.

### 10.Outros apartados

### 10.1) 3. Recursos dispoñibles na aula

Ao igual que noutros módulos, este módulo do ciclo ten por recursos da aula:

+ Un ordenador por alumno con o S.O. Ubuntu Desktop instalado.
+ Unha conta de usuario por alumno no dominio pargapondal.inf.
+ A wiki do departamento.
+ A infraestrutura de aula dixital (moodle).
+ A súa carpeta de usuario compartida no servidor do dominio mediante NFS v4.
+ O aplicativo VirtualBox para Linux.
+ Sistemas operativos en formato ISO coa correspondente licenza listos para ser instalados en máquinas virtuais.

Ao iniciar o módulo invitarase au alumno a crear tantas máquinas virtuais coma esixan as prácticas e traballar nelas usando una rede privada local as máquinas virtuais.

Ter conta no dominio da acceso aos alumnos ao blog, a wiki e a o moodle do departamento segundo os permisos establecidos no dominio; todo elo accesible dende Internet.