



1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019669	Armando Cotarelo Valledor	Vilagarcía de Arousa	2024/2025

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	2024/2025	6	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	MANUEL ÁNGEL REIJA LAMAS
Outro profesorado	

Estado: Pendente de supervisión equipo directivo



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

PERFIL PROFESIONAL DO TÍTULO

O perfil profesional do título de técnico superior en administración de sistemas informáticos en rede determínase pola súa competencia xeral, polas súas competencias profesionais, persoais e sociais, así como pola relación de cualificacións e, de ser o caso, unidades de competencia do Catálogo Nacional de Cualificacións Profesionais incluídas no título.

COMPETENCIA XERAL

A competencia xeral deste título consiste en configurar, administrar e manter sistemas informáticos, garantindo a funcionalidade e a integridade dos recursos e dos servizos do sistema, coa calidade exixida e conforme a regulamentación.

COMPETENCIAS PROFESIONAIS, PERSOAIS E SOCIAIS

- a) Administrar sistemas operativos de servidor, instalando e configurando o software en condicións de calidade, para asegurar o funcionamento do sistema.
- b) Administrar servizos de rede (web, mensaxaría electrónica, transferencia de ficheiros, etc.) instalando e configurando o software, en condicións de calidade.
- c) Administrar aplicacións instalando e configurando o software en condicións de calidade, para responder ás necesidades da organización.
- d) Implantar e xestionar bases de datos instalando e administrando o software de xestión en condicións de calidade, segundo as características da explotación.
- e) Mellorar o rendemento do sistema configurando os dispositivos de hardware consonte os requisitos de funcionamento.
- f) Avaliar o rendemento dos dispositivos de hardware identificando posibilidades de mellora segundo as necesidades de funcionamento.
- g) Determinar a infraestrutura de redes telemáticas, elaborando esquemas e seleccionando equipamentos e elementos.
- h) Integrar equipamentos de comunicacións en infraestruturas de redes telemáticas, determinando a configuración para asegurar a súa conectividade.
- i) Pór en práctica solucións de alta dispoñibilidade, analizando as opcións do mercado, para protexer e recuperar o sistema ante situacións imprevistas.
- j) Supervisar a seguridade física segundo especificacións de fábrica e o plan de seguridade, para evitar interrupcións na prestación de servizos do sistema.
- k) Asegurar o sistema e os datos segundo as necesidades de uso e as condicións de seguridade establecidas, para previr fallos e ataques externos.
- l) Administrar usuarios de acordo coas especificacións de explotación, para garantir os accesos e a dispoñibilidade dos recursos do sistema.
- m) Diagnosticar as disfuncións do sistema e adoptar as medidas correctivas para restablecer a súa funcionalidade.
- n) 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.
- ñ) Efectuar consultas á persoa adecuada e saber respectar a autonomía do persoal subordinado, informando cando sexa conveniente.



- o) Manter o espírito de innovación e actualización no ámbito de ou seu traballo para adaptarse aos cambios tecnolóxicos e organizativos de ou seu ámbito profesional.
- p) 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.
- q) Resolver problemas e tomar decisións individuais, seguindo as normas e os procedementos establecidos, definidos dentro do ámbito da súa competencia.
- r) Xestionar a propia carreira profesional, analizando as oportunidades de emprego, de autoemprego e de aprendizaxe.
- s) Participar de xeito activo na vida económica, social e cultural, con actitude crítica e responsable.
- t) Crear e xestionar unha pequena empresa, realizando un estudo de viabilidade de produtos, de planificación da produción e de comercialización.

OBXECTIVOS XERAIS DO CICLO

Os obxectivos xerais deste ciclo formativo son os seguintes:

- a) Analizar a estrutura do software de base, comparando as características e as prestacións de sistemas libres e propietarios, para administrar sistemas operativos de servidor.
- b) Instalar e configurar o software de base, seguindo documentación técnica e especificacións dadas, para administrar sistemas operativos de servidor.
- c) Instalar e configurar software de mensaxaría e transferencia de ficheiros, entre outros, tendo en conta a súa aplicación e seguindo documentación e especificacións dadas, para administrar servizos de rede.
- d) Instalar e configurar software de xestión, seguindo especificacións e analizando contornos de aplicación, para administrar aplicacións.
- e) Instalar e administrar software de xestión, tendo en conta a súa explotación, para implantar e xestionar bases de datos.
- f) Configurar dispositivos de hardware, analizando as súas características funcionais, para mellorar o rendemento do sistema.
- g) Configurar hardware de rede, analizando as súas características funcionais e tendo en conta o seu campo de aplicación, para integrar equipamentos de comunicacións.
- h) Analizar tecnoloxías de interconexión e describir as súas características e as súas posibilidades de aplicación, para configurar a estrutura da rede telemática e avaliar o seu rendemento.
- i) Elaborar esquemas de redes telemáticas utilizando software específico para configurar a estrutura das redes.
- j) Seleccionar sistemas de protección e recuperación, analizando as súas características funcionais, para pór en marcha solucións de alta dispoñibilidade.
- k) Identificar condicións de equipamentos e instalacións, interpretando plans de seguridade e especificacións de fábrica, para supervisar a seguridade física.
- l) Aplicar técnicas de protección contra ameazas externas, así como típicas e avalias, para asegurar o sistema.
- m) Aplicar técnicas de protección contra perdas de información, analizando plans de seguridade e necesidades de uso para asegurar os datos.
- n) Asignar os accesos e os recursos do sistema, aplicando as especificacións da explotación, para administrar usuarios.
- ñ) Aplicar técnicas de monitorización, interpretar os resultados e relacionalos coas medidas correctoras, para diagnosticar e corrixir as disfuncións.
- o) Establecer a planificación de tarefas, analizando actividades e cargas de traballo do sistema, para xestionar o mantemento.
- p) Identificar os cambios tecnolóxicos, organizativos, económicos e laborais na actividade propia, analizando as súas implicacións no ámbito de traballo, para resolver problemas e manter unha cultura de actualización e innovación.
- q) Identificar formas de intervención en situacións colectivas, analizando o proceso de toma de decisións e efectuando consultas para lideralas.

- r) Identificar e valorar as oportunidades de aprendizaxe e a súa relación co mundo laboral, analizando as ofertas e as demandas do mercado, para xestionar a propia carreira profesional.
- s) Recoñecer as oportunidades de negocio, identificando e analizando demandas do mercado, para crear e xestionar unha pequena empresa.
- t) Recoñecer os dereitos e os deberes como axente activo na sociedade, analizando o marco legal que regula as condicións sociais e laborais, para participar na cidadanía democrática.
- u) Analizar e valorar a participación, o respecto, a tolerancia e a igualdade de oportunidades, para facer efectivo o principio de igualdade entre homes e mulleres.

OBXETIVOS XERAIS DO MÓDULO

A formación do módulo contribúe a alcanzar os obxectivos xerais j), k), l), m), o) e p) do ciclo formativo, e as competencias profesionais, persoais e sociais e), f), i), j), k), m), n), o), r) e s).

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	Introdución a seguridade informática	Panorámica da problemática da seguridade nas tecnoloxías da información e das comunicaciónsPanorámica da seguridade informática	11	10
2	Lexislación e normas		5	5
3	Seguridade física e ambiental		20	15
4	Alta dispoñibilidade		20	15
5	Seguridade lóxica		20	15
6	Seguridade da rede		20	15
7	Firewalls		15	15
8	Proxy		15	10

4. Por cada unidade didáctica
4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución a seguridade informática	11



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 reconece 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

4.1.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.
CA1.2 Descríbóronse as diferenzas entre seguridade física e lóxica.
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.
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
CA2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
CA2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.

4.1.e) Contidos

Contidos
Fiabilidade, confidencialidade, integridade e dispoñibilidade.
Elementos vulnerables no sistema informático: hardware, software e datos.



Contidos
Análise das principais vulnerabilidades dun sistema informático.
Pautas e prácticas seguras.
Tipos de ameazas: físicas e lóxicas.
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento.
Cifraxa simétrico
Cifraxa asimétrico
Funcións hash criptográficas
Códigos de autenticación de mensaxes
Firma dixital
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.
Ataques e contramedidas en sistemas informáticos.
Clasificación dos ataques.
Realización de auditorías de seguridade.
Recuperación de datos.
Actualización de sistemas e aplicacións.
Seguridade na conexión con redes públicas.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Lexislación e normas	5



4.2.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

4.2.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 Identifícaronse 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.

4.2.e) Contidos

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

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Seguridade física e ambiental	20



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
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	NO

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

Criterios de avaliación
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
0CA2.10 Describíronse os tipos e as características dos sistemas de prevención de intrusións
CA2.11 Describíronse os tipos e as características dos sistemas de xestión de eventos de seguridade
CA2.12 Implantáronse sistemas de detección de intrusións
CA2.13 Implantáronse sistemas de prevención de intrusións
CA2.14 Implantáronse sistemas de xestión de eventos de seguridade
CA6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.
CA6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.
CA6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
CA6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.



4.3.e) Contidos

Contidos
Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida. Sistemas de prevención de intrusionés Sistemas de xestión de eventos de seguridade Ferramentas preventivas e paliativas: instalación e configuración. Copias de seguridade e imaxes de respaldo.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Alta dispoñibilidade	20

4.4.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.	NO

4.4.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.
CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
CA6.5 Implantouse un balanceador de carga á entrada da rede interna.
CA6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
CA6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.



4.4.e) Contidos

Contidos
Definición e obxectivos.
Análise de configuracións de alta dispoñibilidade. Funcionamento ininterrompido. Integridade de datos e recuperación de servizo. Servidores redundantes. Sistemas de clústers. Balanceadores de carga.
Instalación e configuración de solucións de alta dispoñibilidade.
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
Virtualización en contornos de produción.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Seguridade lóxica	20

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
CA1.5 Adoptáronse políticas de contrasinais.
CA2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.
CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.



Criterios de avaliación
CA2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.
CA2.6 Utilizáronse técnicas de cifraxa, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.
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.

4.5.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. Cifraxa simétrico Cifraxa asimétrico Funcións hash criptográficas Códigos de autenticación de mensaxes Firma dixital Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias. Ferramentas empregadas na análise forense. Realización de auditorías de seguridade.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Seguridade da rede	20



4.6.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
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	SI

4.6.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.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
CA2.6 Utilizáronse técnicas de cifraxa, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.
CA2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
CA3.1 Descríbóronse 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.
CA3.3 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.
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.



4.6.e) Contidos

Contidos
OTécnicas de cifrado da información: clave pública e clave privada; certificados dixitais; sinaturas. 0 Xestión de claves públicas 0 Firma electrónica 0 Protocolo TLS 0 Implantación dunha PKI 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. Anatomía de ataques e análise de software malicioso. Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes privadas virtuais. Perímetros de rede. Zonas desmilitarizadas. Arquitectura débil e forte de subrede protexida. 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	Firewalls	15

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

Resultado de aprendizaxe do currículo	Completo
RA4 - Instala tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.	SI

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

Criterios de avaliación
CA4.1 Descríbense as características, os tipos e as funcións dos tornalumes.
CA4.2 Clasifícanse os niveis en que se realiza a filtraxe de tráfico.
CA4.3 Configúranse filtros nun tornalume 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.

4.7.e) Contidos

Contidos
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.



Contidos
Regras de filtraxe de toralumes. Probas de funcionamento: sondaxe. Rexistros de sucesos nos toralumes.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Proxy	15

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	SI

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

Criterios de avaliación
CA5.1 Identifícanse os tipos de proxy, as súas características e as súas funcións principais.
CA5.2 Instalouse e configurouse un servidor proxy cache.
CA5.3 Configúranse os métodos de autenticación no proxy.
CA5.4 Configúrase un proxy en modo transparente.
CA5.5 Utilízase o servidor proxy para establecer restricións de acceso web.
CA5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.
CA5.7 Realízanse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.
CA5.8 Configúrase un servidor proxy en modo inverso.



Criterios de avaliación

CA5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.

4.8.e) Contidos

Contidos

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.

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

5.1. MÍNIMOS EXIXIBLES

Os mínimos exixibles son detallados no apartado 4.c xunto cos criterios de avaliación e instrumentos de avaliación asociados polo que non serán detallados de novo. Para aprobar é preciso acadar cada un deses mínimos exixibles.

5.2. CRITERIOS DE CUALIFICACIÓN

Existen tres sesións de avaliación onde se emitirá unha nota (con cifras enteiras do 1 ao 10) .



Para o cálculo da nota terase en conta:

PARTE A. Proba de avaliación.

A proba de avaliación que poderá ser escrita e/ou práctica co ordenador: probas individuais acerca dos contidos estudados nunha ou varias unidades didácticas. Poden conter preguntas teóricas de tipo test, respostas curtas ou desenvolvemento, así como esixi-la resolución de exercicios e supostos prácticos, podendo estes ser realizados en papel ou no ordenador.

NOTA: As respostas de tipo test incorrectas restarán 2 mal por 1 ben

As preguntas tipo test poderán ter mais dunha resposta correcta, de maneira que pra cunha pregunta sexa correcta haberá que marcar todas as respostas (de non ser así considerarase como mal contestada e restará)

As preguntas en branco non puntuarán. As preguntas tipo test incorrectas restarán, dúas preguntas tipo test incorrectas restará unha pregunta correcta. Poderá haber algunhas preguntas (que serán marcadas debidamente como mínimos esixibles) que deberán ser contestadas correctamente pra seguir corrixiendo o exame; e dicir, de habelas, terán que ser contestadas todas elas correctamente para aproba-lo exame, se algunha destas preguntas non fose correcta, automaticamente o exame estaría suspenso.

Os instrumentos necesarios pra realización da proba serán papel e bolígrafo de cor negra ou azul. Non será corrixiendo ningún exercicio que se realice empregando ferramentas diferentes ás indicadas, ou que non se cubra segundo as indicacións establecidas no enunciado do exame. Non se corrixiendo ningún exercicio feito con lápiz ou con algún tipo de tinta correctora.

Excluíranse as persoas aspirantes que leven a cabo calquera actuación de tipo fraudulento ou incumpran as normas indicadas. Neste caso, o profesor ou a profesora do módulo profesional cualificará esa parte da proba do módulo cun cero.

O aspirante deberá identificar claramente a súa proba, en caso contrario non se corrixiendo.

Queda totalmente prohibido o emprego de teléfonos móbiles ou calquera outro dispositivo similar ou electrónico (reloxo dixital, etc ...), deberán estar totalmente apagados e nunca visibles.

As probas serán presenciais ou telemáticas según indique a dirección do centro en función da situación sanitaria que se dea por mor da pandemia ou doutra emerxencia similar. No caso de que a proba fora telemática o alumno poderá ser requerido durante a proba a conectar micro, cámara web ou seguir outras instrucións que se precisen para autenticar a súa identidade. Despois do exame o profesor poderá entrevistarse co alumno



pra verifica-la autoría do exame por parte do alumno.

PARTE B. Entrega das tarefas propostas na aula virtual.

Tódalas tarefas propostas deberán ser entregadas en tempo e forma (establecerase un primeiro prazo na aula virtual, que é o que marcará a entrega en tempo e forma), así coma te-lo calificativo de APTAS pra poder ser avaliadas e formar parte da nota final, é dicir non ten que faltar nengunha tarefa proposta e co calificativo de APTA para cas tarefas poidan ser consideradas na nota final da avaliación.

Se as tarefas entregáranse fora do primeiro prazo enton como máximo poderán valer a metade da nota máxima de haberse entregado en tempo e forma,

Traballos, tarefas ou prácticas:

-A nota dos traballos será individual, poida co alumnado teña que defendelos ante o docente respondendo unha serie de cuestións referentes as partes do mesmo.

A nota dependerá das respostas dadas e, de non ser respondidas correctamente, dita parte pode ser considerada como non superada.

-Os traballos poderán ser expostos de forma individual ante o resto de alumnado, se así o considera o mestre. Neste caso, unha parte da nota dependerá do control do tema, o desenvolvemento durante a presentación, os recursos utilizados e as respostas as preguntas efectuadas polo docente e o resto do alumnado.

Autoría de actividades,tarefas, probas ou traballos:

-poderá ser verificada a autoría de calesqueira das probas/traballos/tarefas/actividades a realizar polos alumnos/as, ben sexan teóricas ou prácticas, actividades en clase ou na casa, etc. por parte do profesor en calqueira momento da celebración ou realización da proba/traballo/tarefa/actividade ou ben con posterioridade a ésta.

Se o resultado é copia ou falsificación ou calqueira outro método de suplantación da autoría (uso de ferramentas de intelixencia artificial non autorizadas, ferramentas de internet non autorizadas, etc) a nota global da proba/traballo/tarefa/actividade será a nota mínima da mesma.

NOTA FINAL

A nota final da avaliación farase ca seguinte fórmula $A*0.90+B*0.10$

Pra aplicación desta fórmula terase que aprobar cada parte (cada parte evaluarase de 1 a 10, o aprobado estará no 5 en cada parte)

De non se-lo caso, a nota resultante será a da proba escrita (ponderada por 0.9).De non aprobarse unha das partes, dita parte na fórmula pasará a valer 0

A nota resultante en cada unha das avaliacións será a do redondeo matemático a un numero enteiro (do 1 ao 10) tras aplica-la fórmula antes indicada.

O redondeo que se empregará será o seguinte:



nota x.00 a x.50 redondearase a x
nota x.51 a x.99 redondearase a x+1

Pra supera-lo módulo en cada avaliación é preciso obter unha nota resultante igual ou superior a 5.

Os alumnos que non superen o módulo durante a avaliación ordinaria, terán que superar unha proba final, cualificada entre 1 e 10, na que deberán obter unha nota igual ou superior a 5 pra cada unha das avaliacións para poder aproba-la asignatura, nese caso a nota final será a media aritmética das partes avaliadas

A nota final será calculada a partir da media aritmética das tres avaliacións sempre e cando estas fosen superiores a 5. En caso de ter unha ou mais avaliacións con nota inferior a 5, o alumno/a terá que facer unha proba final pra cada avaliación non superada cos contidos correspondentes a esa avaliación.

O resultado de cada unha desas probas substitúe ás notas das avaliacións ordinarias suspensas no cálculo da nota final.

Se a situación ocasionada polo COVID non permite a realización de probas presenciais, estas adaptaránse a probas telemáticas.

En calquera dos escenarios e con motivo das posibles restriccións pola pandemia e necesidade de distanciamento social, pode requirirse pra preparación e organización das probas que o alumnado CONFIRME a intención de realizar éstas con polo menos con anterioridade de 48h á súa realización. De requirirse, e de non confirmarse por parte do alumno a súa participación nestas probas de avaliación, podería ter unha condición de NON APTO na proba de avaliación

De detectarse calquer comportamento incorrecto como copiar traballos, actividades ou probas, dito traballo, actividade ou proba contará como non superada.

O docente pode esixir a defensa total ou parcial de calquera actividade, traballo ou proba mediante unha serie de preguntas individuais. De non ser respondidas correctamente, a actividade, traballo ou proba pode ser considerada como non superada.

De non superar o alumno una proba de exame, está terá que recuperala no exame final

RESUMO CUALIFICACIÓN POR AVALIACION:

-- Proba escrita y/o práctica da avaliación (ponderada por 0.9)

-- Actividades Prácticas realizadas ata ese momento dende o principio de curso (ponderada por 0.10)

-- A avaliación considerase aprobada cando a NOTA MEDIA PONDERADA (proba escrita e actividades prácticas) sexa igual ou superior a 5 sobre 10.
(pra face-la media ponderada na proba de avaliación deberá aprobarse cada unha das partes)



NOTAL FINAL NA AVALIACIÓN CONTINUA

- Se se aproban tódalas avaliacións a nota final da última avaliación será a media das notas de cada avaliación (conseguidas pra cada avaliación segundo a fórmula arriba indicada)
- Se se suspende alguha avaliación a nota final na avaliación continua será a de suspenso e haberá que ir a proba extraordinaria de xuño

NOTA FINAL ACADADA NA PROBA EXTRAORDINARIA DE XUÑO

- Estarán exentos da realización desta proba os alumnos que xa teñan a condición de apto na avaliación continua.
- Realizarán esta proba os alumnos que non acadaron a condición de APTO na avaliación continua ou que perderan o seu dereito de avaliación continuada por calqueira razón.
- As actividades prácticas realizadas durante o curso non serán obxecto de avaliación nin serán consideradas na nota final desta convocatoria.
- Será unha proba teórico-práctica. A nota final será exclusivamente referida a esta proba nunha escala de 1 a 10. Dita proba poderá estar dividida por avaliacións e pra aprobar haberá que aprobar cada avaliación, sendo a nota final, unha vez aprobadas tódalas probas das avaliacións, a media das mesmas

NOTA: O momento temporal no que se da unha unidade didáctica pode variar, é dicir, pódese cambiar a orde de desordenrolo dos temas. Pero en calqueira caso, antes da proba dunha avaliación dirase que unidades entran nesa avaliación, mediante a aula virtual

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Como cada unidade é avaliada de forma independente unidade a unidade solo se recuperarán as partes suspensas no período extraordinario (Xuño) onde se manterán os pesos dos instrumentos e o tipo de tarefas.

En marzo, só no caso de que o alumnado non supere 3 UD pendentes como máximo, ofreceráselle unha posibilidade extraordinaria de recuperación das UD pendentes, nos mesmos termos que a final de xuño, có obxectivo de que poda acceder á FCT no período de abril-xuño.

Este exame final consistirá en:

- * Unha proba escrita teórico/práctica que abarcará os contidos e os procedementos expostos durante o curso.
- * Unha proba práctica que abarcará os procedementos expostos durante o curso.

Poderá esixirse unha revisión oral de calquera das probas realizadas.

Cada alumno só se enfrontará aos contidos e procedementos das unidades didácticas que ten suspensas.



A nota da avaliación final ordinaria será a da última avaliación, modificada, de ser o caso, pola recuperación realizada durante a mesma.
O alumno deberá obter unha nota mínima dun 5 nas probas escritas/prácticas de recuperación para ter superado as unidades nela avaliadas.

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

O alumnado que perdeu o dereito á avaliación continua pode presentarse a unha proba final que se desenvolverá durante a avaliación final ordinaria en Xuño.
A proba final consistirá nun exame teórico (35%) e un exame práctico (65%) sobre os contidos e procedementos do módulo.
Poderase esixir que o alumnado obteña unha puntuación mínima de 4 en cada unha das notas para facer o cálculo anterior. De non ser así a nota final será a nota suspensa máis próxima á media.
Poderá esixirse unha revisión oral de calquera das probas realizadas.

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

Contéplanse tres niveis de seguimento da programación e de avaliación da propia práctica docente:

Nivel individual:
O profesorado que imparta o módulo fará un seguimento continuo da programación e unha avaliación continua da propia práctica docente.

Nivel de curso:
As reunións de avaliación servirán tamén para facer seguimento da programación, avaliar a práctica docente e coordinar a práctica docente entre os módulos dun mesmo curso.

Nivel de departamento:
Farase o seguimento das programacións de tódolos módulos coa frecuencia mínima estipulada pola Administración Educativa e ademais durante o último trimestre do curso haberá como mínimo un profesor por ciclo adicado á revisión das programacións e á avaliación da práctica docente. Este grupo de profesores propondrá ao departamento ao final do curso, modificacións nas mesmas baseándose na súa revisión particular, na experiencia docente dos profesores que impartiron cada módulo e na práctica docente dos mesmos. As propostas anteriores que sexan aprobadas polo departamento, serán levadas a cabo ao principio do curso seguinte polos profesores de cada módulo.



8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Realizarase unha enquisa ao alumnado para coñecer a experiencia laboral, académica e persoal con relación aos contidos do módulo naqueles aspectos non tratados na enquisa xeral que levará a cabo o titor do curso. Os resultados da enquisa e os que se derivan da comunicación directa entre profesor e alumnado serán compartidos co resto do profesorado docente durante a sesión de avaliación inicial que se celebrará na data determinada por Xefatura de estudos.

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 para os criterios de avaliación avaliados cunha proba escrita consistirán no repaso dos conceptos por parte do alumno e coa axuda do profesor.

As medidas de reforzo para os criterios de avaliación avaliados cunha lista de cotexo consistirán na resolución de supostos cunha metodoloxía distinta e máis detallada. Estes supostos serán resolto polo alumno sempre coa axuda do profesor.

As medidas de reforzo para os criterios de avaliación avaliados cunha táboa de observación consistirán na proposta do profesor de cambio na actitude do alumno e o cambio de actitude por parte do alumno verificada polo profesor.

9. Aspectos transversais

9.a) Programación da educación en valores

En todas as unidades didácticas inculcaranse os seguintes valores, actitudes e normas e valorarase a súa consecución.

Valores, actitudes e normas de aspecto persoal:

- Respecto ós demais, tolerancia e comportamento correcto.
- Atención prestada en clase.
- Participación diaria na clase.
- Comunicación e diálogo.



- Puntualidade e asistencia.
- 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.

Valores, actitudes e normas de aspecto técnico:

- Respecto ás normas e ao material que se use.
- Predisposición pola adopción sistemática de medidas de seguridade dos sistemas e da información.
- Costume de documentar os resultados presentados.
- Preocupación pola busca de eficiencia nas solucións presentadas.
- Preocupación pola optimización do resultado final, refugando solucións correctas pero non óptimas.
- Preocupación polo estilo empregado tanto na documentación e escritura como na presentación de resultados.

9.b) Actividades complementarias e extraescolares

As que estableza o departamento á principios de curso.